Modicon

Commutateur MCSESM, MCSESM-E, MCSESP avec fonctionnalité d'administration Manuel d'utilisation Configuration

QGH59080.02

www.schneider-electric.com

Schneider Electric

Le présent document comprend des descriptions générales et/ou des caractéristiques techniques des produits mentionnés. Il ne peut pas être utilisé pour définir ou déterminer l'adéquation ou la fiabilité de ces produits pour des applications utilisateur spécifiques. Il incombe à chaque utilisateur ou intégrateur de réaliser l'analyse de risques complète et appropriée, l'évaluation et le test des produits pour ce qui est de l'application à utiliser et de l'exécution de cette application. Ni la société Schneider Electric ni aucune de ses sociétés affiliées ou filiales ne peuvent être tenues pour responsables de la mauvaise utilisation des informations contenues dans le présent document. Si vous avez des suggestions, des améliorations ou des corrections à apporter à cette publication, veuillez nous en informer.

Toutes les réglementations locales, régionales et nationales pertinentes doivent être respectées lors de l'installation et de l'utilisation de ce produit. Pour des raisons de sécurité et afin de garantir la conformité aux données système documentées, seul le fabricant est habilité à effectuer des réparations sur les composants.

Lorsque des équipements sont utilisés pour des applications présentant des exigences techniques de sécurité, suivez les instructions appropriées.

La non-utilisation du logiciel Schneider Electric ou d'un logiciel approuvé avec nos produits matériels peut entraîner des blessures, des dommages ou un fonctionnement incorrect.

Le non-respect de cette consigne peut entraîner des lésions corporelles ou des dommages matériels.

En tant que membre d'un groupe d'entreprises responsables et inclusives, nous actualisons nos communications qui contiennent une terminologie non inclusive. Cependant, tant que nous n'aurons pas terminé ce processus, notre contenu pourra toujours contenir des termes standardisés du secteur qui pourraient être jugés inappropriés par nos clients.

Sommaire

Consignes de sécurité

Remarque importante : Veuillez lire attentivement ces instructions et vous familiariser avec l'équipement avant de l'installer, de le mettre en service ou d'effectuer sa maintenance. Les consignes suivantes peuvent figurer à différents endroits du présent document ou directement sur l'équipement. Ces consignes vous mettent en garde contre d'éventuels dangers ou vous fournissent des informations qui expliquent ou simplifient certaines opérations.

La présence de ce symbole sur une étiquette "Danger" ou "Avertissement" signale un risque d'électrocution qui provoquera des blessures physiques en cas de non-respect des consignes de sécurité.

Ce symbole est un symbole d'avertissement général. Il attire votre attention sur le risque de blessures. Respectez les consignes accompagnant ce symbole afin d'éviter toute blessure ou accident mortel.

⚠ DANGER

DANGER indique une situation immédiatement dangereuse qui, si elle n'est pas évitée, **entraînera** la mort ou des blessures graves.

⚠ AVERTISSEMENT

L'indication **AVERTISSEMENT** signale une situation potentiellement dangereuse et susceptible **d'entraîner** la mort ou des blessures graves.

⚠ ATTENTION

L'indication **ATTENTION** signale une situation potentiellement dangereuse et susceptible **d'entraîner** des blessures d'ampleur mineure à modérée.

AVIS

AVIS indique des pratiques n’entraînant pas de risques corporels.

Remarque importante : L'installation, l'utilisation, la réparation et la maintenance des équipements électriques doivent être assurées par du personnel qualifié uniquement. Schneider Electric décline toute responsabilité quant aux conséquences de l'utilisation de ce matériel.

Une personne qualifiée est une personne disposant de compétences et de connaissances dans le domaine de la construction, du fonctionnement et de l'installation des équipements électriques, et ayant suivi une formation en sécurité leur permettant d'identifier et d'éviter les risques encourus.

A propos de ce manuel

Champ d'application

Les données et illustrations fournies dans cette documentation ne sont pas contractuelles. Nous nous réservons le droit de modifier nos produits conformément à notre politique de développement permanent. Les informations présentes dans ce document peuvent faire l'objet de modifications sans préavis et ne doivent pas être interprétées comme un engagement de la part de Schneider Electric.

Commentaires utilisateur

Vos commentaires et remarques sont toujours les bienvenus. Pour cela, il suffit de nous envoyer un e-mail à l'adresse suivante : techpub@schneider-electric.com

Document consulter

Le manuel d'utilisation « Configuration » contient toutes les informations dont vous avez besoin pour la mise en service de l'équipement. Il vous guide pas à pas de la première mise en service jusqu'aux réglages fondamentaux pour un fonctionnement approprié de votre environnement.

Le manuel d'utilisation « Installation » contient une description de l'équipement, des instructions de sécurité, une description de l'affichage, et les autres informations dont vous avez besoin pour installer l'équipement.

Le manuel de référence « Interface utilisateur graphique » contient des informations détaillées relatives à l'interface utilisateur graphique vous permettant d'utiliser les fonctions individuelles de l'équipement.

Le manuel de référence « Interface de ligne de commande » contient des informations détaillées relatives à l'interface de ligne de commande vous permettant d'utiliser les fonctions individuelles de l'équipement.

Le logiciel d'administration de réseau ConneXium Network Manager offre des options supplémentaires permettant une configuration et une supervision aisées :
- Auto-apprentissage de la topologie réseau
- Interface de navigateur
- Structure client/serveur
- Traitement des événements
- Journal des événements
- Configuration simultanée de plusieurs équipements
- Interface utilisateur graphique avec plan du réseau
- Passerelle SNMP/OPC

Key

Le tableau ci-dessous décrit les conventions utilisées dans ce manuel :

▶	Énumération
☐	Étape de travail
Lien	Lien hypertexte
Commentaire :	Une remarque souligne une information importante ou attire votre attention sur une dépendance.
`Courier`	Représentation d'une commande de la CLI ou de contenus de champs dans l'interface utilisateur graphique

Exécution dans l'interface utilisateur graphique

Exécution dans l'interface de ligne de commande

Remplacer un équipement

L'équipement offre les solutions plug-and-play suivantes de remplacement d'un équipement par un équipement du même type, par exemple, si une défaillance a été détectée ou pour une maintenance préventive :

- Le nouvel équipement charge le profil de configuration de l'équipement remplacé depuis la mémoire externe.
  Voir « Chargement du profil de configuration depuis la mémoire externe » à la page 108.
- Le nouvel équipement reçoit son adresse IP à l'aide de DHCP *Option 82*.
  Voir « Relais DHCP L2 » à la page 324.
  Voir « Configuration d'un serveur DHCP avec l'option 82 » à la page 369.

Avec chaque solution, lors d'un redémarrage, le nouvel équipement reçoit les mêmes réglages IP que l'équipement remplacé.

- Pour accéder à l'administration de l'équipement à l'aide de HTTPS, l'équipement utilise un certificat numérique. Vous avez la possibilité d'importer votre propre certificat sur l'équipement.
  Voir « Gestion des certificats HTTPS » à la page 375.
- Pour accéder à l'administration de l'équipement à l'aide de SSH, l'équipement utilise une clé d'hôte RSA. Vous avez la possibilité d'importer votre propre clé d'hôte sur l'équipement au format PEM.
  Voir « Chargement de votre propre clé sur l'équipement » à la page 372.

1 Interfaces utilisateur

L'équipement vous permet de spécifier les réglages de l'équipement à l'aide des interfaces utilisateur suivantes.

Tableau 1 : Interfaces utilisateur pour accéder à l'administration de l'équipement

Interface utilisateur	Accessible via…	Prérequis
Interface utilisateur graphique	Ethernet (in-band)	Navigateur Web
Interface de ligne de commande	Ethernet (in-band) Interface série (out-of-band)	Logiciel d'émulation de terminal
Moniteur du système	Interface série (out-of-band)	Logiciel d'émulation de terminal

1.1 Interface utilisateur graphique

Configuration système requise

Pour ouvrir l'interface utilisateur graphique, vous avez besoin d'un navigateur Web (version d'ordinateur de bureau) prenant en charge HTML5.

Commentaire : Les logiciels tiers tels que les navigateurs Web valident des certificats basés sur des critères tels que la date d'expiration et les recommandations de paramètres cryptographiques actuelles. Les certificats périmés peuvent causer des problèmes dus à des informations non valides ou obsolètes. Exemple : un certificat expiré ou des recommandations cryptographiques changées. Pour résoudre les conflits de validation avec des logiciels tiers, transférez votre propre certificat mis à jour sur votre équipement ou regénérez le certificat avec le dernier firmware.

Démarrage de l'interface utilisateur graphique

Pour démarrer l'interface utilisateur graphique, il convient que les paramètres IP soient préalablement configurés dans l'équipement. Voir « Spécification des paramètres IP » à la page 45.

Exécutez les étapes suivantes :

- ☐ Lancez votre navigateur Web.
- ☐ Saisissez l'adresse IP de l'équipement dans le champ d'adresse du navigateur Web.
  Utilisez la forme suivante : `https://xxx.xxx.xxx.xxx`
  Le navigateur Web établit la connexion à l'équipement et affiche la boîte de dialogue de connexion.
- ☐ Lorsque vous souhaitez modifier la langue de l'interface utilisateur graphique, cliquez sur le lien approprié dans le coin supérieur droit de la boîte de dialogue de connexion.
- ☐ Saisissez le nom d'utilisateur.
- ☐ Saisissez le mot de passe.
- ☐ Cliquez sur le bouton *Login*.
  Le navigateur Web affiche l'interface utilisateur graphique.

1.2 Interface de ligne de commande

L'interface de ligne de commande vous permet d'utiliser les fonctions de l'équipement à l'aide d'une connexion locale ou à distance.

Les spécialistes IT trouvent dans l'interface de ligne de commande l'environnement de configuration habituel des équipements IT. En tant qu'utilisateur expérimenté ou administrateur, vous disposez de connaissances de base et maîtrisez l'utilisation des équipements Schneider Electric.

1.2.1 Préparation de la liaison de données

Les informations d'assemblage et de démarrage de votre équipement sont disponibles dans le manuel d'utilisation « Installation ».

- ☐ Connectez l'équipement avec le réseau. Pour établir une liaison de données avec succès, il convient préalablement de régler les paramètres de réseau de manière appropriée.

Vous pouvez accéder à l'interface utilisateur de l'interface de ligne de commande à l'aide du logiciel gratuit *PuTTY*, par exemple.

- ☐ Installez le programme *PuTTY* sur votre ordinateur.

1.2.2 Accès à l'interface de ligne de commande à l'aide de Telnet

Connexion Telnet avec Windows

Telnet n'est installé par défaut que dans les versions Windows antérieures à Windows Vista.

Exécutez les étapes suivantes :

- ☐ Démarrez le programme *Command Prompt* sur votre ordinateur.
- ☐ Saisissez la commande `telnet <IP_address>`.

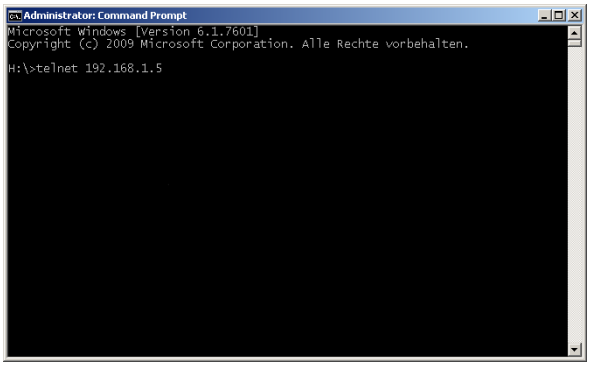


Figure 1 : Command Prompt : établissement de la connexion Telnet à l'équipement

Connexion Telnet avec PuTTY

Exécutez les étapes suivantes :

- ☐ Démarrez le programme *PuTTY* sur votre ordinateur.

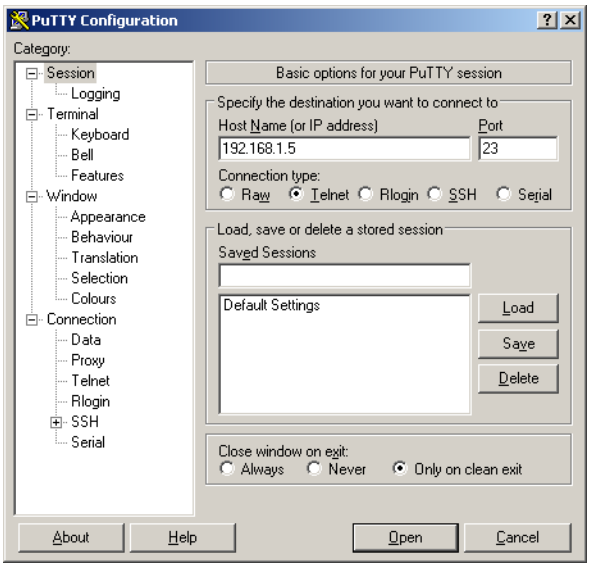


Figure 2 : Écran de saisie PuTTY

- ☐ Spécifiez l'adresse IP de votre équipement dans le champ *Host Name (or IP address)*. L'adresse IP se compose de 4 nombres décimaux présentant des valeurs allant de `0` à `255`. Les 4 nombres décimaux sont séparés par des points.
- ☐ Pour sélectionner le type de connexion, sélectionnez le bouton radio *Telnet* dans la liste d'options *Connection type*.
- ☐ Cliquez sur le bouton *Open* pour établir la liaison de données avec votre équipement. L'interface de ligne de commande apparaît à l'écran avec une fenêtre permettant de saisir le nom de l'utilisateur. L'équipement permet à un maximum de 5 utilisateurs d'avoir simultanément accès à l'interface de ligne de commande.

Commentaire : Cet équipement est un produit assurant la sécurité. Modifiez le mot de passe dès la première mise en service.

Exécutez les étapes suivantes :

- ☐ Saisissez le nom d'utilisateur.
  Le nom d'utilisateur par défaut est `admin`.
- ☐ Appuyez sur la touche <Entrée>.

- ☐ Saisissez le mot de passe.
  Le mot de passe par défaut est `private`.
- ☐ Appuyez sur la touche <Entrée>.

```
                    Copyright (c) 2011-2022 Schneider Electric

                                All rights reserved

                            MCSESM-E Release 08.7.00

                           (Build date 2022-07-11 16:29)


                  System Name    :  MCSESM-646038d5e846
                  Management IP  :  192.168.1.5
                  Subnet Mask    :  255.255.255.0
                  Base MAC       :  64:60:38:01:02:03
                  USB IP         :  91.0.0.100
                  USB Mask       :  255.255.255.0
                  System Time    :  2022-07-13 19:41:01


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESM-E>
```

Figure 3 : Démarrez l'écran de l'interface de ligne de commande

1.2.3 Accès à l'interface de ligne de commande à l'aide de SSH

Dans l'exemple suivant, nous utilisons le programme *PuTTY*. Vous pouvez également utiliser OpenSSH Suite pour accéder à votre équipement à l'aide du protocole SSH.

Exécutez les étapes suivantes :

- ☐ Démarrez le programme *PuTTY* sur votre ordinateur.

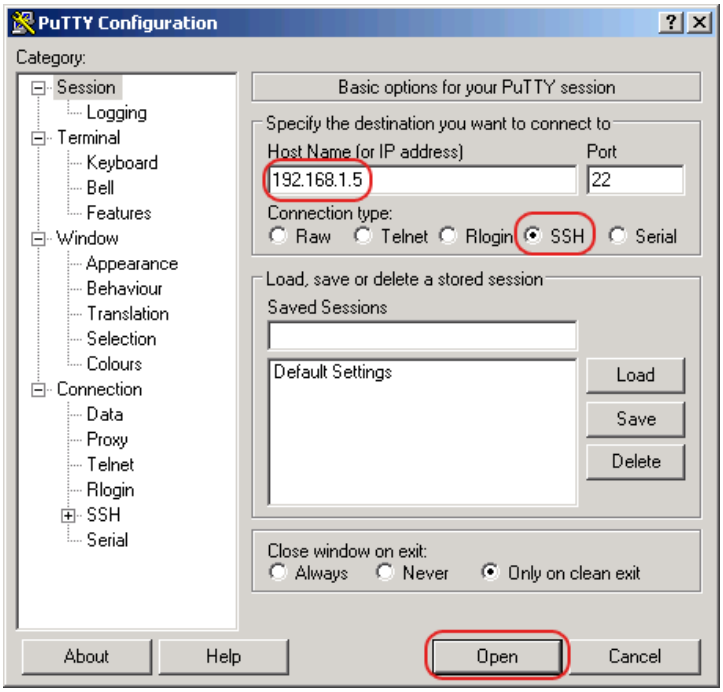


Figure 4 : Écran de saisie PuTTY

- ☐ Spécifiez l'adresse IP de votre équipement dans le champ *Host Name (or IP address)*.
  L'adresse IP se compose de 4 nombres décimaux présentant des valeurs allant de 0 à 255. Les 4 nombres décimaux sont séparés par des points.
- ☐ Pour sélectionner le type de connexion, sélectionnez le bouton radio *SSH* dans la liste d'options *Connection type*.
  Après la sélection et le réglage des paramètres requis, l'équipement vous permet d'établir la liaison de données à l'aide de SSH.

- Cliquez sur le bouton *Open* pour établir la liaison de données avec votre équipement.
  Selon l'équipement et le moment auquel SSH a été configuré, l'établissement de la liaison peut prendre jusqu'à une minute.
  Lorsque vous vous connectez pour la première fois, vers la fin de l'établissement de la liaison, le programme *PuTTY* affiche un message d'alerte de sécurité et vous permet de vérifier l'empreinte de la clé.

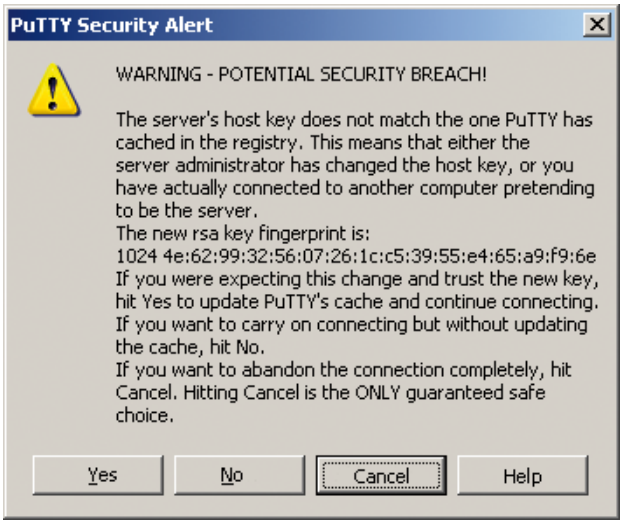


Figure 5 : Question de sécurité relative à l'empreinte

- Vérifiez l'empreinte.
  Vous contribuez ainsi à vous protéger contre les intrus.
- Lorsque l'empreinte correspond à celle de la clé de l'équipement, cliquez sur le bouton *Yes*.
  L'équipement vous permet d'afficher les empreintes des clés de l'équipement à l'aide de la commande `show ssh` ou dans l'onglet *SSH* de la boîte de dialogue *Device Security > Management Access > Server*.
  L'interface de ligne de commande apparaît à l'écran avec une fenêtre permettant de saisir le nom de l'utilisateur. L'équipement permet à un maximum de 5 utilisateurs d'avoir simultanément accès à l'interface de ligne de commande.
- Saisissez le nom d'utilisateur.
  Le nom d'utilisateur par défaut est `admin`.
- Appuyez sur la touche <Entrée>.
- Saisissez le mot de passe.
  Le mot de passe par défaut est `private`.
- Appuyez sur la touche <Entrée>.

Commentaire : Cet équipement est un produit assurant la sécurité. Modifiez le mot de passe dès la première mise en service.

```
login as: admin
admin@192.168.1.5's password:


                        Copyright (c) 2011-2022 Schneider Electric

                                  All rights reserved

                               MCSESM-E Release 08.7.00

                              (Build date 2022-07-11 16:29)


                     System Name    :  MCSESM-646038d5e846
                     Management IP  :  192.168.1.5
                     Subnet Mask    :  255.255.255.0
                     Base MAC       :  64:60:38:01:02:03
                     USB IP         :  91.0.0.100
                     USB Mask       :  255.255.255.0
                     System Time    :  2022-07-13 19:41:01


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESM-E>
```

Figure 6 : Démarrez l'écran de l'interface de ligne de commande

1.2.4 Accès à l'interface de ligne de commande à l'aide Interface série

L'interface série est utilisée pour connecter localement une station d'administration réseau externe (terminal VT100 ou PC avec émulation de terminal). L'interface vous permet d'établir une liaison de données avec l'interface de ligne de commande et avec le moniteur du système.

Exécutez les étapes suivantes :

- ☐ Connectez l'équipement à un équipement terminal à l'aide de l'interface série. Vous pouvez également connecter l'équipement à un port COM de votre PC doté d'une émulation de terminal VT100 et appuyer sur une touche quelconque.
- ☐ Vous pouvez également établir la liaison de données avec l'équipement via l'interface série à l'aide du programme *PuTTY*. Appuyez sur la touche <Entrée>.

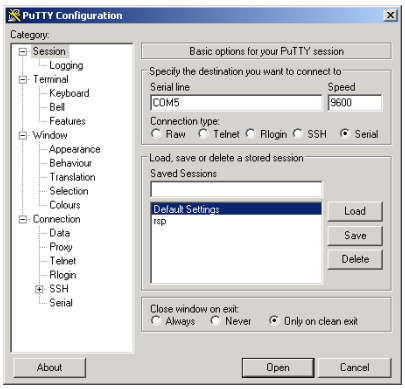


Figure 7 : Liaison de données série via l'interface série à l'aide du programme PuTTY

- ☐ Appuyez plusieurs fois sur une touche quelconque du clavier de votre équipement terminal jusqu'à ce que l'écran de connexion indique le mode CLI.
- ☐ Saisissez le nom d'utilisateur.
  Le nom d'utilisateur par défaut est `admin`.
- ☐ Appuyez sur la touche <Entrée>.
- ☐ Saisissez le mot de passe.
  Le mot de passe par défaut est `private`.
- ☐ Appuyez sur la touche <Entrée>.

Commentaire : Cet équipement est un produit assurant la sécurité. Modifiez le mot de passe dès la première mise en service.

```
                    Copyright (c) 2011-2022 Schneider Electric

                                All rights reserved

                             MCSESM-E Release 08.7.00

                            (Build date 2022-07-11 16:29)


                  System Name   :  MCSESM-646038d5e846
                  Management IP :  192.168.1.5
                  Subnet Mask   :  255.255.255.0
                  Base MAC      :  64:60:38:01:02:03
                  USB IP        :  91.0.0.100
                  USB Mask      :  255.255.255.0
                  System Time   :  2022-07-13 19:41:01


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESM-E>
```

Figure 8 : Démarrez l'écran de l'interface de ligne de commande

1.2.5 Hiérarchie des commandes par mode

Dans l'interface de ligne de commande, les commandes sont regroupées en différents modes selon le type de commande. Chaque mode de commande prend en charge des commandes spécifiques du logiciel Schneider Electric.

Les commandes auxquelles vous avez accès en tant qu'utilisateur dépendent de votre niveau de droits (administrateur, opérateur, invité, vérificateur). Elles dépendent également du mode que vous utilisez actuellement. Lorsque vous passez d'un mode spécifique à un autre, vous avez accès aux commandes du mode correspondant.

Les commandes du mode User Exec constituent une exception. L'interface de ligne de commande vous permet d'exécuter ces commandes en mode Privileged Exec.

La figure suivante présente les différents modes de l'interface de ligne de commande.

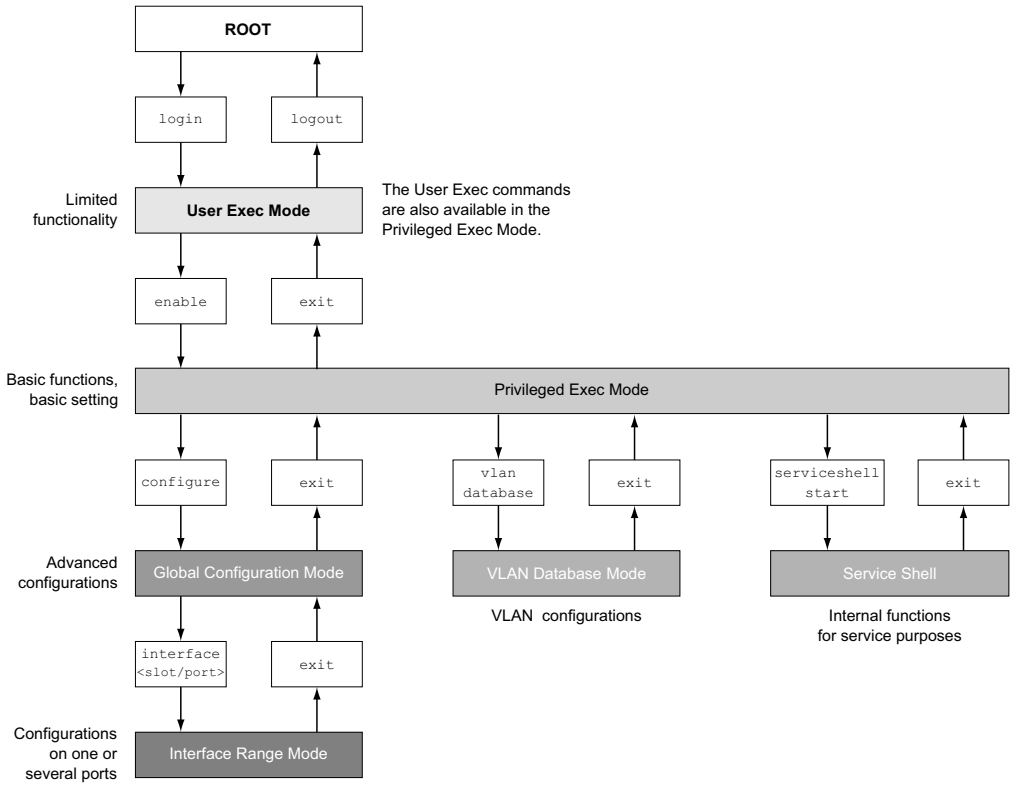


Figure 9 : Structure de l'interface de ligne de commande

En fonction du niveau de droits de l'utilisateur, l'interface de ligne de commande prend en charge les modes suivants :

- Mode User Exec
  Lorsque vous vous connectez à l'interface de ligne de commande, vous utilisez le mode User Exec. Le mode User Exec contient un nombre limité de commandes.
  Invite de commande : `(MCSESM-E) >`
- Mode Privileged Exec
  Pour accéder à l'ensemble des commandes, utilisez le mode Privileged Exec. Lorsque vous vous connectez en tant qu'utilisateur privilégié, vous pouvez utiliser le mode Privileged Exec. En mode Privileged Exec, vous pouvez également exécuter les commandes du mode User Exec.
  Invite de commande : `(MCSESM-E) #`
- Mode VLAN
  Le mode VLAN contient les commandes relatives au VLAN.
  Invite de commande : `(MCSESM-E) (VLAN)#`
- Service Shell
  Le Service Shell est uniquement utilisé à des fins d'assistance.
  Invite de commande : `/mnt/fastpath #`

- Mode Global Config
  Le mode Global Config vous permet d'apporter des modifications à la configuration actuelle. Ce mode regroupe les commandes de configuration générale.
  Invite de commande : `(MCSESM-E) (config)#`
- Mode Interface Range
  Les commandes du mode Interface Range affectent un port spécifique, un groupe de ports sélectionnés ou tous les ports de l'équipement. Ces commandes permettent de modifier une valeur ou d'activer ou de désactiver une fonction sur un ou plusieurs ports spécifiques.
  - Tous les ports physiques de l'équipement
    Invite de commande : `(MCSESM-E) ((interface) all)#`
    Exemple : lorsque vous passez du mode Global Config au mode Interface Range, l'invite de commande est modifiée de la manière suivante :
    ```
    (MCSESM-E) (config)#interface all
    (MCSESM-E) ((Interface)all)#
    ```
  - Un port individuel sur une interface
    Invite de commande : `(MCSESM-E) (interface <slot/port>)#`
    Exemple : lorsque vous passez du mode Global Config au mode Interface Range, l'invite de commande est modifiée de la manière suivante :
    ```
    (MCSESM-E) (config)#interface 2/1
    (MCSESM-E) (interface 2/1)#
    ```
  - Une plage de ports sur une interface
    Invite de commande : `(MCSESM-E) (interface <interface range> )#`
    Exemple : lorsque vous passez du mode Global Config au mode Interface Range, l'invite de commande est modifiée de la manière suivante :
    ```
    (MCSESM-E) (config)#interface 1/2-1/4
    (MCSESM-E) ((Interface)1/2-1/4)#
    ```
  - Une liste de ports individuels
    Invite de commande : `(MCSESM-E) (interface <interface list>)#`
    Exemple : lorsque vous passez du mode Global Config au mode Interface Range, l'invite de commande est modifiée de la manière suivante :
    ```
    (MCSESM-E) (config)#interface 1/2,1/4,1/5
    (MCSESM-E) ((Interface)1/2,1/4,1/5)#
    ```
  - Une liste de plages de ports et de ports individuels
    Invite de commande : `(MCSESM-E) (interface <complex range>)#`
    Exemple : lorsque vous passez du mode Global Config au mode Interface Range, l'invite de commande est modifiée de la manière suivante :
    ```
    (MCSESM-E) (config)#interface 1/2-1/4,1/6-1/9
    (MCSESM-E) ((Interface)1/2-1/4,1/6-1/9)
    ```

Le tableau suivant présente les modes de commandes, les invites de commande (caractères de requête de saisie) visibles dans le mode correspondant et l'option vous permettant de quitter ce mode.

Tableau 2 : Modes de commandes

Mode de commandes	Méthode d'accès	Quittez ou démarrez le prochain mode

Mode User Exec	Premier niveau d'accès. Effectuez des tâches de base et répertoriez les informations du système.	Pour quitter, saisissez `logout` :
		`(MCSESM-E) >logout`
		`Are you sure (Y/N) ?y`

Mode Privileged Exec	Depuis le mode User Exec, saisissez la commande `enable` :
	`(MCSESM-E) >enable`
	`(MCSESM-E) #`
		Pour quitter le mode Privileged Exec et revenir au mode User Exec, saisissez `exit` :
		`(MCSESM-E) #exit`
		`(MCSESM-E) >`

Mode VLAN	Depuis le mode Privileged Exec, saisissez la commande `vlan database` :
	`(MCSESM-E) #vlan database`
	`(MCSESM-E) (Vlan)#`
		Pour quitter le mode VLAN et revenir au mode Privileged Exec, saisissez `exit` ou appuyez sur Ctrl Z.
		`(MCSESM-E) (Vlan)#exit`
		`(MCSESM-E) #`

Mode Global Config	Depuis le mode Privileged Exec, saisissez la commande `configure` :
	`(MCSESM-E) #configure`
	`(MCSESM-E) (config)#`
	Depuis le mode User Exec, saisissez la commande `enable`, puis en mode Privileged Exec, saisissez la commande `Configure` :
	`(MCSESM-E) >enable`
	`(MCSESM-E) #configure`
	`(MCSESM-E) (config)#`
		Pour quitter le mode Global Config et revenir au mode Privileged Exec, saisissez `exit` :
		`(MCSESM-E) (config)#exit`
		`(MCSESM-E) #`
		Pour quitter ensuite le mode Privileged Exec et revenir au mode User Exec, saisissez à nouveau `exit` :
		`(MCSESM-E) #exit`
		`(MCSESM-E) >`

Mode Interface Range	Depuis le mode Global Config, saisissez la commande `interface {all|<slot/port>|<interface range>|<interface list>|<complex range>}`.
	`(MCSESM-E) (config)#interface <slot/port>`
	`(MCSESM-E) (interface slot/port)#`
		Pour quitter le mode Interface Range et revenir au mode Global Config, saisissez `exit`. Pour revenir au mode Privileged Exec, appuyez sur Ctrl Z.
		`(MCSESM-E) (interface slot/port)#exit`
		`(MCSESM-E) #`

Lorsque vous saisissez un point d'interrogation (?) après l'invite, l'interface de ligne de commande affiche une liste des commandes disponibles et une brève description des commandes.

```
(MCSESM-E)>
  cli              Set the CLI preferences.
  enable           Turn on privileged commands.
  help             Display help for various special keys.
  history          Show a list of previously run commands.
  logout           Exit this session.
  ping             Send ICMP echo packets to a specified IP address.
  show             Display device options and settings.
  telnet           Establish a telnet connection to a remote host.

(MCSESM-E)>
```

Figure 10 : Commandes du mode User Exec

1.2.6 Exécution des commandes

Analyse de syntaxe

Lorsque vous vous connectez à l'interface de ligne de commande, vous utilisez le mode User Exec. L'interface de ligne de commande affiche l'invite `(MCSESM-E)>` à l'écran.

Lorsque vous saisissez la commande et appuyez sur la touche <Entrée>, l'interface de ligne de commande commence l'analyse de syntaxe. L'interface de ligne de commande recherche la commande souhaitée dans l'arborescence des commandes.

Lorsque l'interface de ligne de commande ne fait pas partie du groupe de commandes de l'interface de ligne de commande, un message vous informe de l'erreur détectée.

Exemple :

Vous souhaitez exécuter la commande `show system info`, mais vous saisissez `info` sans `f` et appuyez sur la touche <Entrée>.

L'interface de ligne de commande affiche alors un message :

```
(MCSESM-E)>show system ino

Error: Invalid command 'ino'
```

Arborescence des commandes

Les commandes de l'interface de ligne de commande sont organisées selon une structure d'arborescence. Les commandes et, le cas échéant, les paramètres associés, se déploient en branches jusqu'à ce que la commande soit entièrement définie et donc exécutable. L'interface de ligne de commande vérifie la saisie. Lorsque vous avez saisi correctement et entièrement la commande et les paramètres, exécutez la commande avec la touche <Entrée>.

Une fois que vous avez saisi la commande et les paramètres requis, les autres paramètres saisis sont traités comme des paramètres optionnels. Lorsqu'un des paramètres est inconnu, l'interface de ligne de commande affiche un message de syntaxe.

L'arborescence des commandes déploie ses branches de paramètres jusqu'à ce que les paramètres requis aient atteints la dernière branche de la structure.

Avec les paramètres optionnels, l'arborescence des commandes déploie ses branches de paramètres jusqu'à ce que les paramètres requis et les paramètres optionnels aient atteints la dernière branche de la structure.

1.2.7 Structure d'une commande

Cette section décrit la syntaxe, les conventions et la terminologie, et les illustre au moyen d'exemples.

Format des commandes

La plupart des commandes incluent des paramètres.

Lorsqu'un paramètre de commande est manquant, l'interface de ligne de commande vous informe de la détection d'une syntaxe de commande incorrecte.

Ce manuel affiche les commandes et les paramètres dans la police `Courier`.

Paramètres

Il convient de respecter l'ordre des paramètres pour que la syntaxe d'une commande soit correcte.

Les paramètres peuvent être des valeurs requises, des valeurs optionnelles, des sélections ou une combinaison de tous ces éléments. La manière dont ils sont représentés indique le type des paramètres.

Tableau 3 : Syntaxe des paramètres et des commandes

`<command>`	Les commandes placées entre chevrons (<>) sont obligatoires.
`[command]`	Les commandes placées entre crochets ([]) sont optionnelles.
`<parameter>`	Les paramètres placées entre chevrons (<>) sont obligatoires.
`[parameter]`	Les paramètres placées entre crochets ([]) sont optionnelles.
`...`	Des points de suspension (3 points successifs sans espace) placés après un élément indiquent que vous pouvez répéter cet élément.

Tableau 3 : Syntaxe des paramètres et des commandes

`[Choice1 | Choice2]`	Une ligne verticale placée entre parenthèses indique une option de sélection. Sélectionnez une valeur. Les éléments séparés par une ligne verticale et placés entre crochets indiquent une sélection optionnelle (Option1 ou Option2 ou pas de sélection).
`{list}`	Des accolades (`{}`) indiquent qu'un paramètre doit être sélectionné dans une liste d'options.
`{Choice1 | Choice2}`	Les éléments séparés par une ligne verticale et placés entre accolades (`{}`) indiquent une option de sélection obligatoire (Option1 ou Option2).
`[param1 {Choice1 | Choice2}]`	Affiche un paramètre optionnel qui contient une sélection obligatoire.
`<a.b.c.d>`	Les lettres minuscules sont des caractères génériques. Vous pouvez saisir des paramètres à l'aide de la notation a.b.c.d avec des points décimaux (par exemple, des adresses IP)
`<cr>`	Pour créer un saut à la ligne (retour charriot), appuyez sur <Entrée>.

La liste suivante affiche les valeurs de paramètre possibles dans l'interface de ligne de commande :

Tableau 4 : Valeurs de paramètre dans l'interface de ligne de commande

Valeur	Désignation
Adresse IP	Ce paramètre représente une adresse IPv4 valide. Cette adresse se compose de 4 nombres décimaux présentant des valeurs allant de 0 à 255. Les 4 nombres décimaux sont séparés par un point. L'adresse IP `0.0.0.0` est une entrée valide.
Adresse MAC	Ce paramètre représente une adresse MAC valide. L'adresse se compose de 6 nombres hexadécimaux présentant une valeur allant de 0 à FF. Les nombres sont séparés par un double point, par exemple, `00:F6:29:B2:81:40`.
chaîne	Texte défini par l'utilisateur présentant une longueur comprise dans la plage spécifiée, par exemple un maximum de 32 caractères.
chaîne de caractères	Utilisez des guillemets doubles pour indiquer une chaîne de caractères, par exemple `"System name with space character"`.
nombre	Nombre entier compris dans la plage spécifiée, par exemple `0..999999`.
date	Date au format `YYYY-MM-DD`.
heure	Heure au format `HH:MM:SS`.

Adresses réseau

Les adresses réseau sont nécessaires à l'établissement d'une liaison de données avec poste de travail distant, un serveur ou un autre réseau. Il convient de faire la distinction entre les adresses IP et les adresses MAC.

L'adresse IP est une adresse attribuée par l'administrateur du réseau. L'adresse IP est unique dans une plage réseau.

Les adresses MAC sont attribuées par le fabricant de matériel. Les adresses MAC sont uniques au monde.

Le tableau suivant présente la représentation et la portée des types d'adresse :

Tableau 5 : Format et portée des adresses réseau

Type d'adresse	Format	Portée	Exemple
Adresse IP	nnn.nnn.nnn.nnn	nnn : 0 à 255 (nombre décimal)	192.168.11.110
Adresse MAC	mm:mm:mm:mm:mm:mm	mm : 00 à ff (paires de nombres hexadécimaux)	A7:C9:89:DD:A9:B3

Chaînes de caractères

Une chaîne de caractères est indiquée par des guillemets doubles. Par exemple, `"System name with space character"`. Les espaces ne constituent pas des chaînes de caractères définies par l'utilisateur valides. Ainsi, pour saisir un espace dans un paramètre, il convient de le placer entre guillemets.

Exemple :

```
*(MCSESM-E)#cli prompt Device name
Error: Invalid command 'name'

*(MCSESM-E)#cli prompt 'Device name'

*(Device name)#
```

1.2.8 Exemples de commandes

Exemple 1 : clear arp-table-switch

Commande permettant d'effacer le tableau ARP de l'agent d'administration (cache).

`clear arp-table-switch` est le nom de la commande. La commande peut être exécutée sans saisir aucun autre paramètre en appuyant sur la touche <Entrée>.

Exemple 2 : radius server timeout

Commande permettant de configurer la valeur du délai d'attente du serveur RADIUS.

```
(MCSESM-E) (config)#radius server timeout
 <1..30>              Timeout in seconds (default: 5).
```

`radius server timeout` est le nom de la commande.

Le paramètre est requis. La plage de valeurs est de `1..30`.

Exemple 3 : radius server auth modify <1..8>

Commande permettant de régler les paramètres du serveur d'authentification RADIUS 1.

```
(MCSESM-E) (config)#radius server auth modify 1
```

```
[name]              RADIUS authentication server name.
[port]              RADIUS authentication server port.
                    (default: 1812).
[msgauth]           Enable or disable the message authenticator
                    attribute for this server.
[primary]           Configure the primary RADIUS server.
[status]            Enable or disable a RADIUS authentication
                    server entry.
[secret]            Configure the shared secret for the RADIUS
                    authentication server.
[encrypted]         Configure the encrypted shared secret.
 <cr>               Press Enter to execute the command.
```

`radius server auth modify` est le nom de la commande.

Le paramètre `<1..8>` (index du serveur RADIUS) est requis. La plage de valeurs est de `1..8` (nombre entier).

Les paramètres `[name]`, `[port]`, `[msgauth]`, `[primary]`, `[status]`, `[secret]` et `[encrypted]` sont optionnels.

1.2.9 Invite de saisie

Mode de commandes

Avec l'invite de saisie, l'interface de ligne de commande indique le mode que vous utilisez actuellement, parmi les trois modes existants :

- `(MCSESM-E) >`
  Mode User Exec
- `(MCSESM-E) #`
  Mode Privileged Exec
- `(MCSESM-E) (config)#`
  Mode Global Config
- `(MCSESM-E) (Vlan)#`
  VLAN Database mode
- `(MCSESM-E) ((Interface)all)#`
  Mode Interface Range / Tous les ports de l'équipement
- `(MCSESM-E) ((Interface)2/1)#`
  Mode Interface Range / Un port individuel sur une seule interface
- `(MCSESM-E) ((Interface)1/2-1/4)#`
  Mode Interface Range / Une plage de ports individuel sur une seule interface
- `(MCSESM-E) ((Interface)1/2,1/4,1/5)#`
  Mode Interface Range / Une liste de ports individuels
- `(MCSESM-E) ((Interface)1/1-1/2,1/4-1/6)#`
  Mode Interface Range / Une liste de plages de ports et de ports individuels

Astérisque, dièse et point d'exclamation

- Astérisque `*`
  Un astérisque `*` placé en première ou en seconde position de l'invite de saisie vous indique que les réglages stockés dans la mémoire volatile diffèrent de ceux stockés dans la mémoire non volatile. Dans votre configuration, l'équipement a détecté des modifications qui n'ont pas été sauvegardées.
  `*(MCSESM-E)>`
- Dièse `#`
  Un dièse `#` placé en début d'invite de saisie vous indique que les paramètres de démarrage diffèrent des paramètres observés pendant la phase de démarrage.
  `*#(MCSESM-E)>`
- Point d'exclamation `!`
  Un point d'exclamation `!` placé en début d'invite de saisie indique que le mot de passe du compte d'utilisateur `user` ou `admin` correspond au réglage par défaut.
  `!(MCSESM-E)>`

Caractères génériques

L'équipement vous permet de modifier la ligne de commande.

L'interface de ligne de commande prend en charge les caractères génériques suivants :

Tableau 6 : Utilisation des caractères génériques dans l'invite de saisie de l'interface de ligne de commande

Caractère générique	Désignation
`%d`	Date système
`%t`	Heure système
`%i`	Adresse IP de l'équipement
`%m`	Adresse MAC de l'équipement
`%p`	Nom de produit de l'équipement

```
!(MCSESM-E)>enable

!(MCSESM-E)#cli prompt %i

!192.168.1.5#cli prompt (MCSESM-E)%d

!*(MCSESM-E)2022-07-13#cli prompt (MCSESM-E)%d%t

!*(MCSESM-E)2022-07-13 19:41:01#cli prompt %m

!*AA:BB:CC:DD:EE:FF#
```

1.2.10 Combinaisons de touches

Les combinaisons de touches suivantes permettent de faciliter l'utilisation de l'interface de ligne de commande :

Tableau 7 : Combinaisons de touches dans l'interface de ligne de commande

Combinaison de touches	Désignation
<CTRL> + <H>, <touche retour arrière>	Supprimer le caractère précédent
<CTRL> + <A>	Se rendre en début de ligne
<CTRL> + <E>	Se rendre en fin de ligne
<CTRL> + <F>	Avancer d'un caractère
<CTRL> + <B>	Reculer d'un caractère
<CTRL> + <D>	Supprimer le caractère actuel
<CTRL> + <U>, <X>	Supprimer jusqu'au début de la ligne
<CTRL> + <K>	Supprimer jusqu'à la fin de la ligne
<CTRL> + <W>	Supprimer le mot précédent
<CTRL> + <P>	Se rendre à la ligne précédente dans la mémoire tampon d'historique
<CTRL> + <R>	Réécrire ou coller la ligne
<CTRL> + <N>	Se rendre à la ligne suivante dans la mémoire tampon d'historique
<CTRL> + <Z>	Revenir à l'invite de commande racine
<CTRL> + <G>	Annule la session tcpdump en cours
<Tabulation>, <ESPACE>	Complétion de ligne de commande
`Exit`	Se rendre à l'invite de commande inférieure
<?>	Liste d'options

La commande Help (Aide) affiche à l'écran les combinaisons de touches possibles dans l'interface de ligne de commande :

```
(MCSESM-E) #help

HELP:
Special keys:

  Ctrl-H, BkSp delete previous character
  Ctrl-A  .... go to beginning of line
  Ctrl-E  .... go to end of line
  Ctrl-F  .... go forward one character
  Ctrl-B  .... go backward one character
  Ctrl-D  .... delete current character
  Ctrl-U, X .. delete to beginning of line
  Ctrl-K  .... delete to end of line
  Ctrl-W  .... delete previous word
  Ctrl-P  .... go to previous line in history buffer
  Ctrl-R  .... rewrites or pastes the line
  Ctrl-N  .... go to next line in history buffer
  Ctrl-Z  .... return to root command prompt
  Ctrl-G  .... aborts running tcpdump session
  Tab, <SPACE> command-line completion
  Exit    .... go to next lower command prompt
  ?       .... list choices

(MCSESM-E) #
```

Figure 11 : Affichage de la liste des combinaisons de touches à l'aide de la commande Help

1.2.11 Éléments de saisie de données

Complétion de commande

Pour simplifier la saisie des commandes, l'interface de ligne de commande vous permet d'utiliser la complétion de commande (complétion par tabulation). Vous êtes ainsi en mesure d'abréger la saisie des mots-clés.

- Tapez le début d'un mot-clé. Lorsque les caractères saisis permettent d'identifier un mot-clé, l'interface de ligne de commande complète le mot-clé lorsque vous appuyez sur la touche de tabulation ou la touche espace. En présence de plusieurs options de complétion, saisissez la ou les lettres permettant d'identifier le mot-clé de manière univoque. Appuyez à nouveau sur la touche de tabulation ou la touche espace. Le système complète alors la commande ou le paramètre.
- Lorsque vous effectuez une saisie non unique et que vous appuyez deux fois sur les touches <Tab> ou <Espace>, l'interface de ligne de commande affiche une liste d'options.
- En cas de saisie non unique et lorsque vous appuyez sur les touches <Tab> ou <Espace>, l'interface de ligne de commande complète la commande jusqu'à la fin de l'unicité. Lorsque plusieurs commandes existent et que vous appuyez à nouveau sur la touche <Tab> ou <Espace>, l'interface de ligne de commande affiche une liste d'options.
  Exemple :
  ```
  (MCSESM-E) (Config)#lo
  (MCSESM-E) (Config)#log
  logging logout
  ```
  Lorsque vous saisissez `lo` et que vous appuyez sur la touche <Tab> ou <Espace>, l'interface de ligne de commande complète la commande jusqu'à la fin de l'unicité, de manière à obtenir `log`.
  Lorsque vous appuyez à nouveau sur la touche <Tab> ou <Espace>, l'interface de ligne de commande affiche une liste d'options (`logging logout`).

Commandes/paramètres possibles

Vous pouvez obtenir une liste des commandes ou les paramètres possibles en saisissant `help` ou `?`, par exemple en saisissant `(MCSESM-E) >show ?`

Lorsque vous saisissez la commande affichée, vous obtenez une liste des paramètres disponibles pour la commande `show`.

Lorsque vous saisissez la commande sans ajouter d'espace devant le point d'interrogation, l'équipement affiche le texte d'aide pour la commande elle-même :

```
!*#(MCSESM-E)(Config)#show?

   show          Display device options and settings.
```

1.2.12 Cas d'application

Sauvegarde de la configuration

Sauvegardez la configuration pour vous assurer que les réglages de mot de passe et autres modifications de configuration sont conservés après une réinitialisation de l'équipement ou après une coupure de l'alimentation en tension. Pour ce faire, exécutez les étapes suivantes :

- ☐ Saisissez `enable` pour passer au mode Privileged Exec.
- ☐ Saisissez la commande suivante :
  `save [profile]`
- ☐ Exécutez la commande en appuyant sur la touche <Entrée>.

Syntaxe de la commande « radius server auth add »

Utilisez cette commande pour ajouter un serveur d'authentification RADIUS.

- Mode : mode `Global Config`
- Niveau de droits : Administrator
- Format : `radius server auth add <1..8> ip <a.b.c.d> [name <string>] [port <1..65535>]`
  - `[name]` : nom du serveur d'authentification RADIUS.
  - `[port]` : port du serveur d'authentification RADIUS (par défaut : `1813`).

Paramètre	Signification	Valeurs possibles
`<1..8>`	Index de serveur RADIUS.	`1..8`
`<a.b.c.d>`	Adresse IP du serveur de traçabilité RADIUS.	Adresse IP
`<string>`	Saisissez un texte défini par l'utilisateur d'une longueur maximale de 32 caractères.	
`<1..65535>`	Saisissez un numéro de port compris entre 1 et 65535.	`1..65535`

Mode et niveau de droits :

- Pour pouvoir exécuter la commande, il convient d'être préalablement en mode Global Config. Voir « Hiérarchie des commandes par mode » à la page 25.
- Pour pouvoir exécuter la commande, il convient de disposer préalablement du rôle d'accès Administrator.

Syntaxe des commandes et des paramètres : Voir « Structure d'une commande » à la page 30.

Exemples de commandes exécutables :

- `radius server auth add 1 ip 192.168.30.40`
- `radius server auth add 2 ip 192.168.40.50 name radiusserver2`
- `radius server auth add 3 ip 192.168.50.60 port 1813`
- `radius server auth add 4 ip 192.168.60.70 name radiusserver4 port 1814`

1.2.13 Service Shell

Le Service Shell est uniquement utilisé à des fins d'assistance.

La fonction Service Shell permet aux utilisateurs d'accéder aux fonctions internes de l'équipement. Lorsque vous avez besoin d'assistance pour utiliser votre équipement, le personnel d'assistance utilise le Service Shell pour surveiller les conditions internes, par exemple, les registres de commutateur ou de processeur.

ATTENTION
RISQUE QUE L'ÉQUIPEMENT NE FONCTIONNE PAS N'exécutez pas de fonctions internes telles que la suppression du contenu de la mémoire non volatile (*NVM*) sans disposer d'instructions d'un technicien d'assistance. **Le non-respect de ces instructions peut entraîner le non-fonctionnement de l'équipement.**

Démarrage du Service Shell

Il convient pour cela d'activer préalablement le mode User Exec : `(MCSESM-E) >`

Exécutez les étapes suivantes :

- ☐ Saisissez `enable` et appuyez sur la touche <Entrée>.
  Pour faciliter la saisie :
  - saisissez `e` et appuyez sur la touche <Entrée>.
- ☐ Saisissez `serviceshell start` et appuyez sur la touche <Entrée>.
  Pour faciliter la saisie :
  - saisissez `ser` et appuyez sur la touche <Entrée>.
  - saisissez `s` et appuyez sur la touche <Entrée>.

```
!MCSESM-E >enable

!*MCSESM-E #serviceshell start
 WARNING! The service shell offers advanced diagnostics and functions.
 Proceed only when instructed by a service technician.

 You can return to the previous mode using the 'exit' command.

 BusyBox v1.31.0 (2022-07-13 19:41:01 UTC) built-in shell (ash)
 Enter 'help' for a list of built-in commands.

!/mnt/fastpath #
```

Utilisation de Service Shell

Lorsque Service Shell est activé, le délai d'expiration de l'interface de l'interface de ligne de commande est désactivé. Pour contribuer à éviter les incohérences de configuration, arrêtez le Service Shell avant que tout autre utilisateur ne commence à transférer une nouvelle configuration à l'équipement.

Afficher les commandes Service Shell

La condition préalable est que le Service Shell ait déjà été démarré.

Exécutez les étapes suivantes :
☐ Saisissez `help` et appuyez sur la touche <Entrée>.

```
/mnt/fastpath # help
Built-in commands:
------------------
        . : [ [[ alias bg break cd chdir command continue echo eval exec
        exit export false fg getopts hash help history jobs kill let
        local pwd read readonly return set shift source test times trap
        true type ulimit umask unalias unset wait
/mnt/fastpath #
```

Arrêter le Service Shell

Exécutez les étapes suivantes :
☐ Saisissez `exit` et appuyez sur la touche <Entrée>.

Désactiver le Service Shell de manière permanente dans l'équipement

Lorsque vous désactivez le Service Shell, vous avez toujours la possibilité de configurer l'équipement. Cependant, vous limitez les capacités de diagnostic du système par le personnel d'assistance. Le technicien d'assistance ne pourra plus accéder aux fonctions internes de votre équipement.

La désactivation est irréversible. Le Service Shell restera désactivé de manière permanente. **Pour réactiver le Service Shell, l'équipement devra être démonté par le fabricant.**

Les conditions préalables requises pour cela sont les suivantes :
- Le Service Shell n'a pas été démarré.
- Vous êtes en mode User Exec : `(MCSESM-E) >`

Exécutez les étapes suivantes :
☐ Saisissez `enable` et appuyez sur la touche <Entrée>.
Pour faciliter la saisie :
– saisissez `e` et appuyez sur la touche <Entrée>.

- ☐ Saisissez `serviceshell deactivate` et appuyez sur la touche <Entrée>.
  Pour faciliter la saisie :
  - saisissez `ser` et appuyez sur la touche <Entrée>.
  - saisissez `dea` et appuyez sur la touche <Entrée>.
- ☐ **Ce processus est irréversible !**
  Appuyez sur la touche <Y>.

```
!MCSESM-E >enable

!*MCSESM-E #serviceshell deactivate
Notice: If you continue, then the Service Shell is permanently deactivated.
This step is irreversible!
For details, refer to the Configuration Manual.
Are you sure (Y/N) ?
```

1.3 Moniteur du système

Le moniteur du système vous permet de régler les paramètres d'exploitation de base avant le démarrage du système d'exploitation.

1.3.1 Étendue fonctionnelle

Dans le moniteur du système, vous pouvez exécuter les tâches suivantes, par exemple :
- Gestion du système d'exploitation et vérification de l'image logicielle
- Mise à jour du système d'exploitation
- Démarrage du système d'exploitation
- Suppression des profils de configuration, restauration des paramètres par défaut de l'équipement
- Vérification des informations de code de démarrage

1.3.2 Démarrage du moniteur du système

Vous établissez une connexion série avec l'équipement à l'aide de l'interface USB-C. Durant le processus de démarrage, l'interface série de l'équipement n'est pas disponible. Pour cette raison, le démarrage du moniteur du système fonctionne différemment des autres équipements Schneider Electric. Pour démarrer le moniteur du système, vous devez mettre l'équipement en mode de récupération.

Mettre l'équipement en mode de récupération

Accessoires nécessaires :
- Mémoire externe (recommandée : ACA22-USB-C)
- Adaptateur USB-C vers USB-A (uniquement si vous utilisez une mémoire externe différente de celle recommandée)
- Câble USB pour connecter le port USB-C de l'équipement à l'ordinateur
- Ordinateur avec émulation de terminal VT100 (par exemple PuTTY) ou un terminal série

Exécutez les étapes suivantes :
- ☐ Branchez la mémoire externe sur votre ordinateur.
- ☐ Dans le répertoire racine de la mémoire externe, créez un fichier vide nommé `recovery.txt`.
- ☐ Branchez la mémoire externe sur l'équipement.
- ☐ Redémarrez l'équipement.
- ☐ Observez les LED pendant que l'équipement démarre. Lorsque la LED *Status* clignote alternativement en rouge et en vert, l'équipement a démarré avec succès en mode de récupération.

Commentaire : Vous trouverez la description des éléments d'affichage dans le manuel d'utilisation « Installation ».

Accès au moniteur du système

Exécutez les étapes suivantes :
- ☐ Retirez la mémoire externe de l'équipement.
- ☐ Connectez votre ordinateur à l'équipement à l'aide du câble USB.

- Ouvrez l'émulation de terminal VT100 sur l'ordinateur pour afficher le moniteur du système.
- Sélectionnez le port COM approprié.

Lorsque l'ordinateur et l'équipement sont correctement connectés, un écran noir s'affiche.

Exécutez les étapes suivantes :
- Appuyez sur la touche <Entrée> pour afficher le moniteur du système.
  La vue suivante s'affiche sur votre ordinateur :

```
System Monitor 1
(Selected OS: ...-8.7 (2022-07-11 16:29))

1  Manage operating system
3  Start selected operating system
4  Manage configurations
5  Show boot code information
q  End (reset and reboot)




sysMon1>
```

Figure 12 : Vue System Monitor

- Pour sélectionner une option de menu, saisissez le numéro correspondant.
- Pour quitter un sous-menu et retourner au menu principal, appuyez sur la touche <Échap>.

Commentaire : Pour démarrer l'équipement normalement la prochaine fois, ajoutez uniquement la mémoire externe sans le fichier `recovery.txt`.

2 Spécification des paramètres IP

Lorsque vous installez l'équipement pour la première fois, saisissez les paramètres IP.

L'équipement offre les options suivantes de saisie des paramètres IP durant la première installation :

- Saisie à l'aide de l'interface de ligne de commande.
  Lorsque vous préconfigurez votre équipement en dehors de son environnement d'exploitation ou que vous restaurez l'accès du réseau (« in-band ») à l'équipement, choisissez cette méthode « out-of-band ».
- Saisie à l'aide du protocole Ethernet Switch Configurator.
  Si vous avez un équipement réseau préalablement installé ou une autre connexion Ethernet entre votre PC et l'équipement, choisissez cette méthode « in-band ».
- Configuration à l'aide de la mémoire externe.
  Si vous remplacez un équipement par un équipement du même type et que vous avez déjà sauvegardé la configuration dans la mémoire externe, choisissez cette méthode.
- À l'aide de BOOTP.
  Pour configurer l'équipement installé à l'aide de BOOTP, choisissez cette méthode « in-band ». Il vous faut pour cela un serveur BOOTP. Le serveur BOOTP affecte les données de configuration à l'équipement à l'aide de son adresse MAC. Le mode DHCP est le mode par défaut pour la référence des données de configuration.
- Configuration à l'aide de DHCP.
  Pour configurer l'équipement installé à l'aide de DHCP, choisissez cette méthode « In-Band ». Vous avez besoin d'un serveur DHCP pour cette méthode. Le serveur DHCP affecte les données de configuration à l'équipement à l'aide de son adresse MAC ou de son nom système.
- Configuration à l'aide de l'interface utilisateur graphique.
  Lorsque l'équipement a déjà une adresse IP et est accessible via le réseau, l'interface utilisateur graphique constitue une alternative pour la configuration des paramètres IP.

2.1 Notions de base sur les paramètres IP

2.1.1 IPv4

Adresse IP

L'adresse IP se compose de 4 octets. Ces 4 octets sont notés au format décimal, séparés par un point décimal.

La norme technique RFC 1340 de 1992 définit 5 classes d'adresses IP.

Tableau 8 : Classes d'adresses IP

Classe	Adresse de réseau	Adresse d'hôte	Plage d'adresses
A	1 Byte	3 Bytes	0.0.0.0 à 127.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 à 191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0 à 223.255.255.255
D			224.0.0.0 à 239.255.255.255
E			240.0.0.0 à 255.255.255.255

Le premier octet d'une adresse IP est l'adresse du réseau. L'organisme de réglementation international en charge de l'affectation des adresses de réseau est l'IANA (« Internet Assigned Numbers Authority »). Si vous avez besoin d'un bloc d'adresses IP, contactez votre Internet Service Provider (ISP). Votre ISP contactera son organisme supérieur local pour réserver un bloc d'adresses IP :

- APNIC (Asia Pacific Network Information Center)
  Région Asie/Pacifique
- ARIN (American Registry for Internet Numbers)
  Amériques et Afrique sub-saharienne
- LACNIC (Regional Latin-American and Caribbean IP Address Registry)
  Amérique latine et certaines îles caribbéennes
- RIPE NCC (Réseaux IP Européens)
  Europe et régions voisines

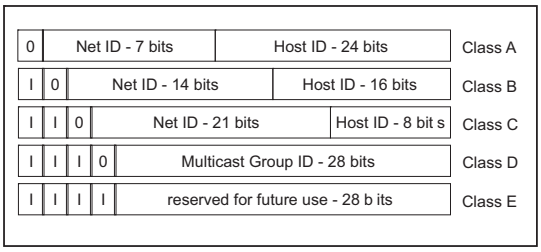


Figure 13 : Représentation en bits de l'adresse IP

Lorsque le premier bit d'une adresse IP est un zéro, elle appartient à la classe A ; par exemple, le premier octet est inférieur à 128.

Lorsque le premier bit d'une adresse IP est un un et que le deuxième bit est un zéro, elle appartient à la classe B ; par exemple, le premier octet est compris entre 128 et 191.

Lorsque les 2 premiers bits d'une adresse IP sont un un, elle appartient à la classe C ; par exemple, le premier octet est supérieur à 191.

L'affectation de l'adresse de l'hôte (host ID) est de la responsabilité de l'opérateur du réseau. L'opérateur du réseau est le seul responsable de l'unicité des adresses IP affectées.

Masque réseau

Les routeurs et Gateways subdivisent les grands réseaux en sous-réseaux. Le masque réseau affecte les adresses IP des équipements individuels à un sous-réseau spécifique.

Vous procédez à une division du sous-réseau à l'aide du masque réseau de manière très similaire à la division des adresses de réseau (net id) en classes A à C.

Définissez sur un les bits de l'adresse d'hôte (host id) qui représentent le masque. Définissez sur zéro les bits de l'adresse d'hôte restants (voir les exemples suivants).

Exemple d'un masque de sous-réseau :

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000

Subnetwork mask bits
Class B

Exemple d'application du masque de sous-réseau aux adresses IP pour l'affectation de sous-réseaux :

Decimal notation
129.218.65.17
└──── 128 < 129 191 › Class B

Binary notation
10000001.11011010.01000001.00010001
Subnetwork 1
Network address

Decimal notation
129.218.129.17
└──── 128 < 129 191 › Class B

Binary notation
10000001.11011010.10000001.00010001
Subnetwork 2
Network address

Exemple d'utilisation du masque réseau

Dans un grand réseau, il est possible que les Gateways et routeurs séparent l'agent d'administration de sa station d'administration réseau. Comment fonctionne l'adressage dans ce cas ?

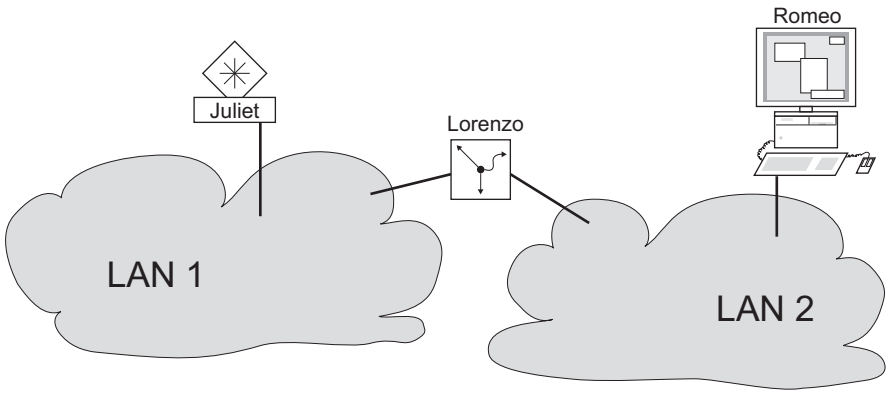


Figure 14 : L'agent d'administration est séparé de sa station d'administration réseau par un routeur.

La station d'administration réseau « Romeo » souhaite envoyer des données à l'agent d'administration « Juliet ». Romeo connaît l'adresse IP de Juliet et sait aussi que le routeur « Lorenzo » connaît le chemin d'accès à Juliet.

Aussi, Romeo met son message dans une enveloppe et écrit l'adresse IP de Juliet comme adresse cible ; pour l'adresse source, il écrit sa propre adresse IP sur l'enveloppe.

Roméo place ensuite cette enveloppe dans une autre enveloppe portant l'adresse MAC de Lorenzo comme adresse cible et sa propre adresse MAC comme adresse source. Ce processus est comparable au passage de la couche 3 à la couche 2 du modèle de référence de base ISO/OSI.

Enfin, Romeo met le paquet de données entier dans la boîte aux lettres, ce qui équivaut à passer de la couche 2 à la couche 1, c'est-à-dire à envoyer le paquet de données via Ethernet.

Lorenzo reçoit la lettre, retire l'enveloppe extérieure et reconnaît, d'après l'enveloppe intérieure, que la lettre est destinée à Juliet. Il place l'enveloppe intérieure dans une nouvelle enveloppe extérieure et cherche, dans sa liste d'adresses (le tableau ARP), l'adresse MAC de Juliet ; il écrit l'adresse MAC de cette dernière sur l'enveloppe extérieure comme adresse cible et sa propre adresse MAC comme adresse source. Il place ensuite le paquet de données entier dans la boîte aux lettres.

Juliet reçoit la lettre et retire l'enveloppe extérieure. Elle trouve l'enveloppe intérieure avec l'adresse IP de Romeo. L'ouverture de l'enveloppe intérieure et la lecture de son contenu correspondent au transfert du message aux couches de protocole supérieures du modèle de couches ISO/OSI.

Juliet souhaite à présent envoyer une réponse à Romeo. Elle met sa réponse dans une enveloppe avec l'adresse IP de Romeo comme adresse cible et sa propre adresse IP comme adresse source. Mais où doit-elle envoyer sa réponse ? En effet elle n'a pas reçu l'adresse MAC de Romeo. Celle-ci a été perdue puisque Lorenzo a remplacé l'enveloppe extérieure.

Dans la MIB, Juliet trouve Lorenzo répertorié sous la variable `NetGatewayIPAddr` comme moyen de communiquer avec Romeo. Aussi, elle met son enveloppe portant les adresses IP dans une autre enveloppe avec l'adresse MAC de Lorenzo comme adresse cible.

La lettre refait alors le trajet jusqu'à Romeo via Lorenzo, de la même manière que la première lettre envoyée par Romeo était parvenue à Juliet.

Classless Inter-Domain Routing

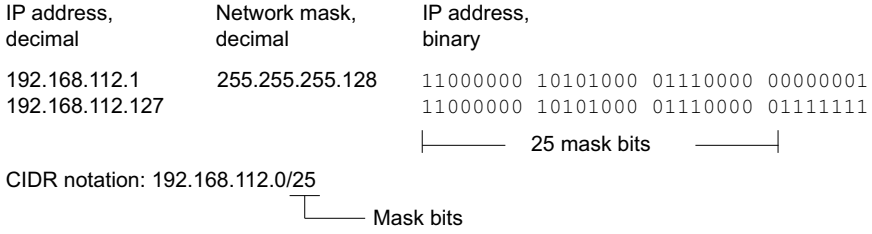
La classe C avec un maximum de 254 adresses était trop petite et la classe B avec un maximum de 65 534 adresses était trop grande pour la plupart des utilisateurs. Ce qui se traduisait par une utilisation inefficace des adresses de la classe B disponibles.

La classe D contient des adresses Multicast réservées. La classe E est dédiée à des fins expérimentales. Une Gateway non participante ignore les datagrammes expérimentaux avec ces adresses cibles.

Depuis 1993, RFC 1519 utilise Classless Inter-Domain Routing (CIDR) pour offrir une solution. CIDR ignore les classes établies et prend en charge les plages d'adresses sans classe.

Avec CIDR, vous saisissez le nombre de bits désignant la plage d'adresses IP. Vous représentez la plage d'adresses IP au format binaire et vous comptez les bits de masque désignant le masque réseau. Les bits de masque équivalent au nombre de bits utilisés pour le sous-réseau dans une plage d'adresses IP donnée.

Exemple :



Le terme de « sur-réseau » se réfère à la combinaison de plusieurs plages d'adresses de classe C. Cette technique vous permet de subdiviser des plages d'adresses de classe B à un degré plus fin.

2.1.2 IPv6

Notions de base sur les paramètres IP

Le protocole Internet version 6 (IPv6) est la nouvelle version du protocole Internet version 4 (IPv4). La mise en œuvre du protocole IPv6 a été rendue nécessaire par le fait que les adresses IPv4 ne suffisent plus face au développement actuel de l'Internet. Le protocole IPv6 est décrit dans RFC 8200.

Parmi les différences entre IPv6 et IPv4, citons les suivantes :
- Représentation et longueur des adresses
- Absence du type d'adresse broadcast
- Structure simplifiée de l'en-tête
- Fragmentation effectuée uniquement par l'hôte source
- Ajout de fonctionnalités pour l'identification des flux de paquets dans le réseau

Les deux protocoles IPv4 et IPv6 peuvent fonctionner simultanément sur l'équipement. Cela est possible grâce à l'utilisation de la technique Dual IP Layer, également appelée Dual Stack.

Commentaire : Si vous souhaitez que l'équipement fonctionne uniquement avec la fonction IPv4, désactivez la fonction IPv6 dans l'équipement.

Dans l'équipement, le protocole IPv6 présente les restrictions suivantes :
- Vous pouvez spécifier un nombre maximum de 8 adresses unicast IPv6 comme suit :
  - 4 adresses IPv6 à l'aide de la configuration manuelle
  - 2 adresses IPv6 lorsque le bouton radio *Auto* est sélectionné
  - 1 adresse IPv6 à l'aide du serveur DHCPv6
  - 1 adresse de lien local
- La fonction IPv6 peut être activée uniquement sur l'interface d'administration. Le nombre total d'adresses IPv6 configurables peut être utilisé simultanément sur l'interface.
- Les adresses IPv6 peuvent être utilisées pour définir l'adresse IP d'administration de l'équipement. D'autres services pour lesquels les adresses IPv6 peuvent être utilisées comprennent, entre autres, SNTP, SYSLOG, DNS et LDAP.

Représentation des adresses

L'adresse IPv6 se compose de 128 bits. Elle est représentée par 8 groupes de 4 chiffres hexadécimaux, chaque groupe représentant 16 bits, appelés hextet. Les hextets sont séparés par un double point (:). Les adresses IPv6 ne sont pas sensibles à la casse et peuvent donc être écrites en minuscules ou en majuscules.

Conformément à la RFC 4291, le format préféré pour une adresse IPv6 est x:x:x:x:x:x:x:x. Chaque « x » se compose de 4 valeurs hexadécimales et représente un hextet. Un exemple de format préféré d'une adresse IPv6 est présenté dans la figure ci-dessous.

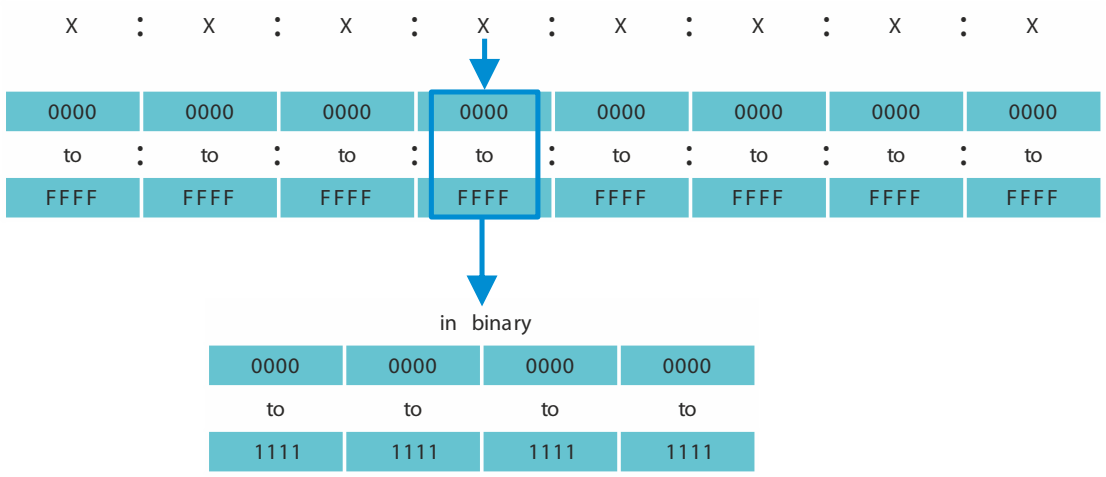


Figure 15 : Représentation d'une adresse IPv6

Comme le montre la figure ci-dessus, une adresse IPv6 contient généralement de nombreux zéros. Afin de raccourcir les adresses IPv6 contenant des bits définis sur 0, il est nécessaire de suivre 2 règles d'écriture :

- La première règle consiste à supprimer les zéros de tête dans chaque hextet. Cette règle s'applique uniquement aux zéros de tête et non aux zéros de queue d'un hextet. Si les zéros de queue sont également supprimés, l'adresse résultante est ambiguë.
- La deuxième règle utilise une syntaxe spéciale pour comprimer les zéros. Vous pouvez utiliser deux doubles points adjacents « :: » pour remplacer une chaîne d'hextets adjacents qui ne contiennent que des zéros. Le signe « :: » ne peut être utilisé qu'une seule fois dans une adresse. Sir le signe « :: » est utilisé plus d'une fois dans une représentation d'adresse, plusieurs adresses possibles peuvent être développées à partir de cette notation.

Lorsque ces deux règles sont appliquées, le résultat est communément désigné par le terme de format compressé.

Le tableau ci-dessous présente 2 exemples d'application de ces règles :

Tableau 9 : Compression d'adresse IPv6

Préféré	CC03:0000:0000:0000:0001:AB30:0400:FF02
Pas de zéros de tête	CC03: 0: 0: 0: 1:AB30: 400:FF02
Compressé	CC03::1:AB30:400:FF02

Tableau 9 : Compression d'adresse IPv6

Préféré	2008:00B7:0000:DEF0:DDDD:0000:E604:0001
Pas de zéros de tête	2008: B7: 0:DEF0:DDDD: 0:E604: 1
Compressé	2008:B7::DEF0:DDDD:0:E604:1

Longueur du préfixe

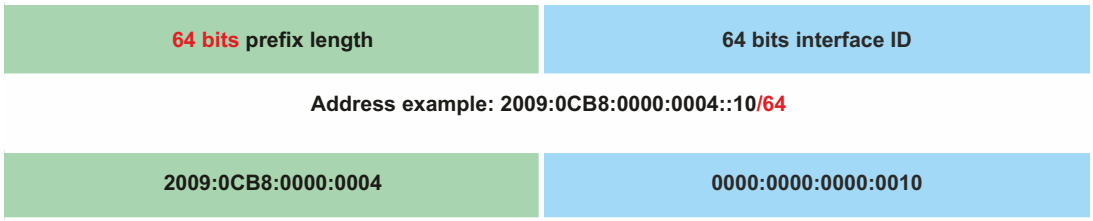
Contrairement à une adresse IPv4, une adresse IPv6 n'utilise pas de masque de sous-réseau pour identifier la partie réseau d'une adresse. Au lieu de cela, le protocole IPv6 utilise la longueur du préfixe.

La représentation textuelle des préfixes d'adresses IPv6 est similaire à la façon dont sont écrits les préfixes des adresses IPv4 dans Classless Inter-Domain Routing (CIDR) :

`<adresse-ipv6>/<longueur-du-préfixe>`

La longueur des préfixes est comprise entre `0..128`. La longueur typique des préfixes IPv6 pour les réseaux LAN et autres types de réseaux est /64. Cela signifie que la partie réseau de l'adresse a une longueur de 64 bits. Les 64 bits restants représentent l'ID d'interface, de manière similaire à la partie hôte de l'adresse IPv4.

La figure ci-dessous présente un exemple d'allocation de bits de longueur de préfixe.



Types d'adresses

Les types d'adresses IPv6 sont décrits dans RFC 4291.

Les types d'adresses IPv6 sont identifiés par les bits de poids fort de l'adresse, comme illustré dans le tableau ci-dessous :

Tableau 10 : Types d'adresses IPv6

Type d'adresse	Préfixe binaire	Notation IPv6
Non spécifié	00...0 (128 bits)	::/128
Bouclage	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Unicast lien local	1111111010	FE80::/10
Unicast globale	(everything else)	

L'adresse non spécifiée

L'adresse IPv6 dont tous les bits sont définis à 0 est appelée adresse non spécifiée, ce qui correspond à 0.0.0.0 dans IPv4. L'adresse non spécifiée sert uniquement à indiquer l'absence d'une adresse. Elle est généralement utilisée comme adresse source lorsqu'une adresse unique n'a pas encore été déterminée.

Commentaire : L'adresse non spécifiée ne peut pas être attribuée à une interface ou utilisée comme adresse cible.

L'adresse de bouclage

L'adresse unicast 0:0:0:0:0:0:0:1 est appelée adresse de bouclage. Elle peut être utilisée par un équipement pour s'envoyer un paquet IPv6 à lui-même. Elle ne peut pas être attribuée à une interface physique.

L'adresse multicast

Contrairement à IPv4, IPv6 n'a pas d'adresse broadcast. Mais il existe une adresse multicast IPv6 tous nœuds qui offre essentiellement le même résultat.

Une adresse multicast IPv6 est utilisée pour envoyer un paquet IPv6 à plusieurs destinations. Une adresse multicast est structurée comme suit : les 4 bits suivants identifient la portée de l'adresse multicast (jusqu'où le paquet est transmis) :

- Les 8 premiers bits sont définis sur `FF`.
- Les 4 bits suivants correspondent à la durée de vie de l'adresse : 0 est permanent et 1 est temporaire.
- Les 4 bits suivants identifient la portée de l'adresse multicast, c'est-à-dire la distance à laquelle les paquets sont transmis sur le réseau.

L'adresse de lien local

L'adresse de lien local est utilisée pour communiquer avec d'autres équipements sur le même lien. Le terme « lien » fait référence à un sous-réseau. Les routeurs ne transfèrent pas à d'autres liens les paquets dont l'adresse source ou cible est locale au lien.

Les adresses de lien local sont utilisées pour transmettre des paquets sur un seul lien à des fins telles que la configuration automatique des adresses et la découverte d'hôtes voisins ou lorsqu'aucun routeur n'est présent. Elles ont le format suivant :

Tableau 11 : Format d'adresse de lien local

10 bits	54 bits	64 bits
1111111010	0	ID d'interface

L'adresse de lien local est toujours configurée et ne peut être modifiée.

L'adresse unicast globale

Une adresse unicast globale est unique au monde et peut être acheminée sur Internet. Ce type d'adresses est équivalent aux adresses IPv4 publiques. Actuellement, seules les adresses unicast globales dont les trois premiers bits sont 001 ou 2000::/3 sont attribuées.

Une adresse unicast globale est composée de 3 parties :
- Préfixe de routage global
- ID de sous-réseau
- ID d'interface.

Le préfixe de routage global est la partie réseau de l'adresse.

L'ID de sous-réseau est utilisé par une organisation pour identifier ses sous-réseaux et sa longueur peut atteindre 16 bits. La longueur de l'ID de sous-réseau est déterminée par la longueur du préfixe de routage global.

L'ID d'interface identifie une interface d'un noeud particulier. Le terme ID d'interface est utilisé parce qu'un hôte peut avoir plusieurs interfaces, chacune ayant une ou plusieurs adresses IPv6.

Le format général des adresses unicast globales IPv6 est représenté dans la figure ci-dessous.

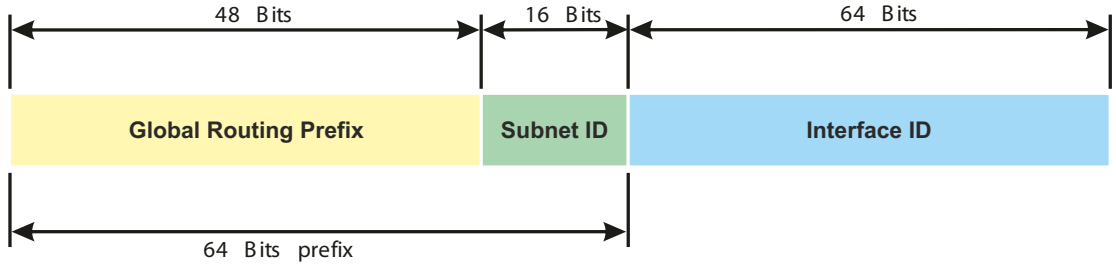


Figure 16 : Format général de l'adresse unicast globale IPv6

2.2 Spécification des paramètres IP à l'aide de l'interface de ligne de commande

2.2.1 IPv4

Il existe les méthodes suivantes pour entrer les paramètres IP :
- BOOTP/DHCP
- Protocole Ethernet Switch Configurator
- Mémoire externe
- Interface de ligne de commande à l'aide de la connexion série

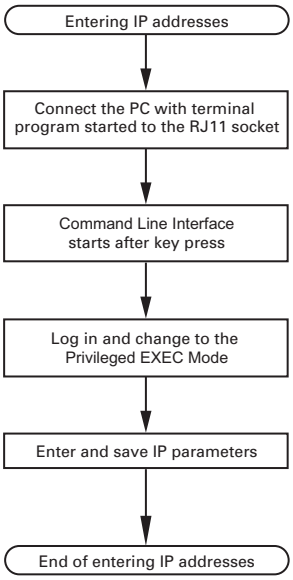


Figure 17 : Diagramme de déroulement de la saisie des adresses IP

Commentaire : Si aucun terminal ou PC avec émulation de terminal n'est disponible à proximité du lieu d'installation, vous pouvez configurer l'équipement sur votre propre poste de travail, puis le déplacer jusqu'à son lieu d'installation final.

Exécutez les étapes suivantes :
- ☐ Établissez une connexion avec l'équipement.
  La page d'accueil s'affiche.

- ☐ Désactivez DHCP.

☐ Saisissez les paramètres IP.
- ▶ Adresse IP locale
  Dans le réglage par défaut, l'adresse IP locale est `0.0.0.0`.
- ▶ Masque réseau
  Une fois votre réseau divisé en sous-réseaux et ces derniers identifiés avec un masque réseau, saisissez le masque réseau ici. Dans le réglage par défaut, le masque réseau local est `0.0.0.0`.
- ▶ Adresse IP de la Gateway.
  Cette entrée n'est requise que lorsque l'équipement et la station d'administration réseau ou le serveur TFTP se trouvent dans des sous-réseaux différents (voir page 47 « Exemple d'utilisation du masque réseau »).
  Spécifiez l'adresse IP de la Gateway entre le sous-réseau avec l'équipement et le chemin jusqu'à la station d'administration réseau.
  Dans le réglage par défaut, l'adresse IP est `0.0.0.0`.

☐ Sauvegardé la configuration spécifiée à l'aide de `copy config running-config nvm`.

`enable`	Basculez sur le mode Privileged EXEC.
`network protocol none`	Désactivation de DHCP.
`network parms 10.0.1.23 255.255.255.0`	Affectez à l'équipement l'adresse IP `10.0.1.23` et le masque réseau `255.255.255.0`. Vous avez la possibilité d'affecter aussi une adresse de Gateway.
`copy config running-config nvm`	Sauvegardez les réglages actuels dans la mémoire non volatile (`nvm`) dans le profil de configuration « Selected » (Sélectionné).

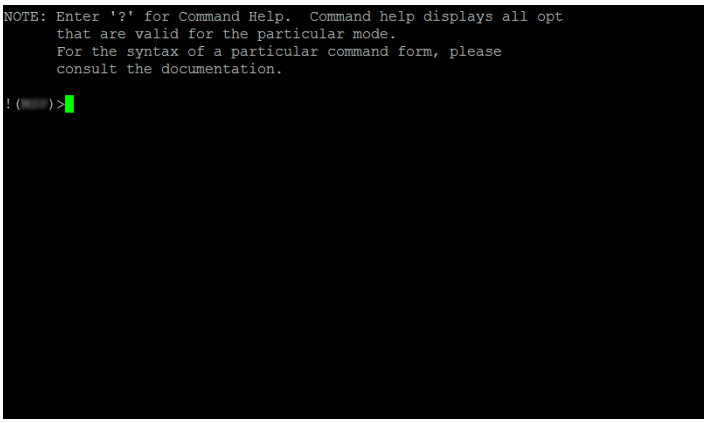
Après avoir saisi les paramètres IP, vous configurez facilement l'équipement à l'aide de l'interface utilisateur graphique.

2.2.2 IPv6

L'équipement vous permet de spécifier les paramètres IPv6 à l'aide de l'interface de ligne de commande via l'interface série. Vous pouvez également accéder à l'interface de ligne de commande à l'aide d'une connexion SSH en utilisant l'adresse d'administration IPv4.

Exécutez les étapes suivantes :

☐ Établissez une connexion avec l'équipement.
La page d'accueil s'affiche.



- ☐ Activez le protocole IPv6 si celui-ci est désactivé.
- ☐ Saisissez les paramètres IPv6.
  - ▶ Adresse IPv6
    Adresse IPv6 valide. L'adresse IPv6 est affichée dans un format compressé.
  - ▶ Longueur du préfixe
    Contrairement à une adresse IPv4, l'adresse IPv6 n'utilise pas de masque de sous-réseau pour identifier la partie réseau d'une adresse. Dans IPv6, ce rôle est assumé par la longueur du préfixe (voir page 51 « Longueur du préfixe »).
  - ▶ Fonction *EUI option*
    Vous pouvez utiliser la fonction *EUI option* pour configurer automatiquement l'ID d'interface de l'adresse IPv6. L'équipement utilise l'adresse MAC de son interface avec les valeurs `ff` et `fe` ajoutées entre l'octet 3 et l'octet 4 pour générer un ID d'interface de 64 bits.
    Vous ne pouvez sélectionner cette option que pour les adresses IPv6 dont la longueur du préfixe est égale à `64`.
  - ▶ Adresse de passerelle IPv6
    L'adresse de passerelle IPv6 est l'adresse d'un routeur par lequel l'équipement accède à d'autres équipements en dehors de son propre réseau.
    Vous pouvez spécifier n'importe quelle adresse IPv6, à l'exception des adresses de bouclage et *Multicast*.
    Dans le réglage par défaut, l'adresse de passerelle IPv6 est `::`.

`enable`	Basculez sur le mode Privileged EXEC.
`network ipv6 operation`	Activez le protocole IPv6 si celui-ci est désactivé. Dans le réglage par défaut, le protocole IPv6 est activé.
`network ipv6 address add 2001::1 64 eui-64`	Attribuez l'adresse IPv6`2001::1` et la longueur de préfixe `64`. Le paramètre `eui-64` est facultatif. Vous pouvez également attribuer une adresse de passerelle.
`copy config running-config nvm`	Sauvegardez les réglages actuels dans la mémoire non volatile (`nvm`) dans le profil de configuration « Selected » (Sélectionné).

Après avoir saisi les paramètres IPv6, vous configurez facilement l'équipement à l'aide de l'interface utilisateur graphique. Pour utiliser une adresse IPv6 dans une URL, utilisez la syntaxe URL suivante :`https://[<ipv6_address>]`.

2.3 Spécification des paramètres IP à l'aide de Ethernet Switch Configurator

Le protocole Ethernet Switch Configurator vous permet d'affecter des paramètres IP à l'équipement via Ethernet.

Vous configurez facilement d'autres paramètres à l'aide de l'interface utilisateur graphique.

Installez le logiciel Ethernet Switch Configurator sur votre PC.

Exécutez les étapes suivantes :
- ☐ Lancez le programme Ethernet Switch Configurator.

Lorsque Ethernet Switch Configurator est démarré, Ethernet Switch Configurator explore automatiquement le réseau à la recherche d'équipements compatibles avec le protocole Ethernet Switch Configurator.

Ethernet Switch Configurator utilise la première interface réseau trouvée sur le PC. Si votre ordinateur a plusieurs cartes réseau, vous pouvez sélectionner celle de votre choix dans la barre d'outils Ethernet Switch Configurator.

Ethernet Switch Configurator affiche une ligne pour chaque équipement qui répond à une requête du protocole Ethernet Switch Configurator.

Ethernet Switch Configurator permet l'identification des équipements affichés.
- ☐ Sélectionnez une ligne d'équipement.
- ☐ Pour que les LED clignotent pour l'équipement sélectionné, cliquez sur le bouton *Signal* dans la barre d'outils. Pour arrêter le clignotement, cliquez de nouveau sur le bouton *Signal*.
- ☐ En double-cliquant sur une ligne, vous ouvrez une fenêtre dans laquelle vous spécifiez le nom de l'équipement et les paramètres IP.

Commentaire : Désactivez la fonction Ethernet Switch Configurator dans l'équipement après avoir attribué les paramètres IP à l'équipement.

Commentaire : Sauvegardez les réglages, de manière à les conserver après un redémarrage.

2.4 Spécification des paramètres IP à l'aide de l'interface utilisateur graphique

2.4.1 IPv4

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Network > Global*.

Dans cette boîte de dialogue, vous spécifiez le VLAN dans lequel l'administration de l'équipement est accessible et vous configurez l'accès Ethernet Switch Configurator.

- ☐ Dans la colonne *VLAN ID*, vous spécifiez le VLAN dans lequel l'administration de l'équipement est accessible via le réseau.

Notez ici que vous ne pouvez accéder à l'administration de l'équipement qu'à l'aide des ports qui sont membres du VLAN concerné.

Le champ *MAC address* affiche l'adresse MAC de l'équipement avec laquelle vous accédez à l'équipement via le réseau.

- ☐ Dans le cadre *Ethernet Switch Configurator protocol v1/v2*, vous spécifiez les réglages pour accéder à l'équipement à l'aide du logiciel Ethernet Switch Configurator.
- ☐ Le protocole Ethernet Switch Configurator vous permet d'attribuer une adresse IP à l'équipement sur la base de son adresse MAC. Activez le protocole Ethernet Switch Configurator si vous souhaitez attribuer une adresse IP à l'équipement depuis votre PC avec le logiciel Ethernet Switch Configurator.
- ☐ Ouvrez la boîte de dialogue *Basic Settings > Network > IPv4*.

Dans cette boîte de dialogue, vous spécifiez la source de laquelle l'équipement reçoit ses paramètres IP après démarrage.

- ☐ Dans le cadre *Management interface*, vous spécifiez d'abord d'où l'équipement reçoit ses paramètres IP :

- ▶ En mode `BOOTP`, la configuration utilise un serveur BOOTP ou DHCP sur la base de l'adresse MAC de l'équipement.
- ▶ En mode `DHCP`, la configuration utilise un serveur DHCP sur la base de l'adresse MAC ou du nom de l'équipement.
- ▶ En mode `Local`, l'équipement utilise les paramètres réseau issus de la mémoire interne de l'équipement.

Commentaire : Lorsque vous changez le mode d'attribution de l'adresse IP, l'équipement active le nouveau mode dès que vous avez cliqué sur le bouton ✓.

- ☐ Si nécessaire, vous saisissez l'adresse IP, le masque réseau et la Gateway dans le cadre *IP parameter*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

2.4.2 IPv6

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Network > IPv6*.
- ☐ Le protocole IPv6 est activé par défaut. Vérifiez si le bouton radio `On` est sélectionné dans le cadre *Operation*.
- ☐ Dans le cadre *Configuration*, vous spécifiez d'où l'équipement reçoit ses paramètres IPv6 :
  - ▶ Si le bouton radio *None* est sélectionné, l'équipement reçoit ses paramètres IPv6 manuellement.
    Vous pouvez spécifier manuellement un nombre maximum de 4 adresses IPv6. Vous ne pouvez pas spécifier les adresses de bouclage, de lien local et *Multicast* comme adresses IPv6 statiques.
  - ▶ Si le bouton radio *Auto* est sélectionné, l'équipement reçoit ses paramètres IPv6 de manière dynamique, par exemple, à l'aide d'un Router Advertisement Daemon (radvd).
    L'équipement reçoit un maximum de 2 adresses IPv6.
  - ▶ Si le bouton radio *DHCPv6* est sélectionné, l'équipement reçoit ses paramètres IPv6 d'un serveur DHCPv6.
    L'équipement ne peut recevoir qu'une seule adresse IPv6 du serveur DHCPv6.
  - ▶ Si le bouton radio *All* est sélectionné, l'équipement reçoit ses paramètres IPv6 au moyen de toutes les possibilités d'affectation dynamique et manuelle.

  Commentaire : Lorsque vous changez le mode d'attribution de l'adresse IPv6, l'équipement active le nouveau mode dès que vous avez cliqué sur le bouton ✓.
- ☐ Si nécessaire, vous saisissez l'*Gateway address* dans le cadre *IP parameter*.

  Commentaire : Si le bouton radio *Auto* est sélectionné et que vous utilisez un Router Advertisement Daemon (radvd), l'équipement reçoit automatiquement une *Gateway address* de type lien local avec une métrique plus élevée que l'*Gateway address* définie manuellement.
- ☐ Dans le cadre *Duplicate Address Detection*, vous pouvez spécifier le nombre de messages *Neighbor Solicitation* consécutifs que l'équipement envoie pour la fonction *Duplicate Address Detection*(voir page 65 « Duplicate Address Detection »).

Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

Spécifiez manuellement une adresse IPv6. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Network > IPv6*.
- ☐ Cliquez sur le bouton ⊞.
  La boîte de dialogue affiche la fenêtre *Create*.
- ☐ Saisissez l'adresse IPv6 dans le champ *IP address*.
- ☐ Saisissez la longueur du préfixe de l'adresse IPv6 dans le champ *PrefixLength*.
- ☐ Cliquez sur le bouton *Ok*.
  L'équipement ajoute une nouvelle entrée de tableau.

2.5 Spécification des paramètres IP à l'aide de BOOTP

Avec la fonction *BOOTP* activée, l'équipement envoie un message de requête de démarrage au serveur BOOTP. Le message de requête de démarrage contient l'ID client configuré dans la boîte de dialogue *Basic Settings > Network > IPv4*. Le serveur BOOTP saisit l'ID client dans une base de données et affecte une adresse IP. Le serveur répond avec un message de réponse de démarrage. Le message de réponse de démarrage contient l'adresse IP affectée.

2.6 Spécification des paramètres IP à l'aide de DHCP

2.6.1 IPv4

Le protocole DHCP (Dynamic Host Configuration Protocol) est un développement de BOOTP, qu'il a remplacé. De plus, le DHCP permet la configuration d'un client DHCP à l'aide d'un nom au lieu d'utiliser l'adresse MAC.

Pour le DHCP, ce nom s'appelle le « Client Identifier » conformément à RFC 2131.

L'équipement utilise le nom saisi sous sysName dans le groupe système de la MIB II comme Client Identifier. Vous pouvez modifier le nom système à l'aide de l'interface utilisateur graphique (voir la boîte de dialogue *Basic Settings > System*), de l'interface de ligne de commande ou de SNMP.

L'équipement transmet son nom système au serveur DHCP. Le serveur DHCP utilise alors le nom système pour attribuer une adresse IP comme alternative à l'adresse MAC.

Outre l'adresse IP, le serveur DHCP envoie
- le masque réseau,
- la Gateway par défaut (si disponible),
- l'URL TFTP du fichier de configuration (si disponible).

L'équipement applique les données de configuration aux paramètres appropriés. Lorsque le serveur DHCP affecte l'adresse IP, l'équipement sauvegarde de manière permanente les données de configuration dans la mémoire non volatile.

Tableau 12 : Options DHCP requises par l'équipement

Options	Signification
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
42	NTP server
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

L'avantage d'utiliser DHCP au lieu de BOOTP est que le serveur DHCP peut restreindre la validité des paramètres de configuration (« Lease ») sur une durée donnée (attribution d'adresse dynamique). Avant l'échéance de cette période (« Lease Duration »), le client DHCP peut tenter de renouveler cette période de validité. Sinon, le client peut négocier une nouvelle période de validité. Le serveur DHCP attribue alors une adresse libre aléatoire.

Pour éviter cela, les serveurs DHCP offrent l'option de configuration explicite consistant à affecter à un client donné la même adresse IP sur la base d'un ID matériel unique (attribution d'adresse statique).

Dans les réglages par défaut, DHCP est désactivé. Tant que DHCP est activé, l'équipement tente d'obtenir une adresse IP. Si l'équipement ne trouve pas un serveur DHCP après redémarrage, il n'a pas d'adresse IP. La boîte de dialogue *Basic Settings > Network > IPv4* vous permet d'activer ou de désactiver DHCP.

Commentaire : Si vous utilisez l'administration du réseau ConneXium Network Manager, vérifiez que DHCP attribue l'adresse IP d'origine à chaque équipement.

L'annexe contient un exemple de configuration du serveur BOOTP/DHCP.

Exemple de fichier de configuration DHCP :

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Les lignes débutant avec le caractère `#` contiennent des commentaires.

Les lignes précédant les équipements individuels répertoriés se rapportent aux réglages applicables à l'équipement suivant.

La ligne d'adresse fixe affecte une adresse IP permanente à l'équipement.

Pour plus d'informations, consultez le manuel du serveur DHCP.

2.6.2 IPv6

Le protocole de configuration dynamique d'hôte version 6 (DHCPv6) est un protocole réseau permettant de spécifier dynamiquement des adresses IPv6. Ce protocole est l'équivalent IPv6 du protocole DHCP pour IPv4. Le protocole DHCPv6 est décrit dans RFC 8415.

L'équipement utilise un DHCP Unique Identifier (DUID) pour envoyer une requête au serveur DHCPv6. Dans l'équipement, le DUID représente l'*Client ID* que le serveur DHCPv6 utilise pour identifier l'équipement qui a demandé une adresse IPv6.

L'*Client ID* est affiché dans la boîte de dialogue *Basic Settings > Network > IPv6*, cadre *DHCP*.

L'équipement ne peut recevoir qu'une seule adresse IPv6 du serveur DHCPv6, avec une *PrefixLength* de `128`. Aucune information sur l'*Gateway address* n'est fournie. Si nécessaire, vous pouvez spécifier manuellement les informations relatives à l'*Gateway address*.

Dans le réglage par défaut, le protocole DHCPv6 est désactivé. Vous pouvez activer ou désactiver le protocole dans la boîte de dialogue *Basic Settings > Network > IPv6*. Vérifiez que le bouton radio *DHCPv6* est sélectionné dans le cadre *Configuration*.

Si vous souhaitez obtenir dynamiquement une adresse IPv6 avec une *PrefixLength* différente de `128`, sélectionnez le bouton radio *Auto*. L'utilisation de Router Advertisement Daemon (radvd) en est un exemple. Le radvd utilise les messages *Router Solicitation* et *Router Advertisement* pour configurer automatiquement une adresse IPv6.

Dans le réglage par défaut, le bouton radio *Auto* est sélectionné. Vous pouvez sélectionner ou désélectionner le bouton radio *Auto* dans le boîte de dialogue *Basic Settings > Network > IPv6*, cadre *Configuration*.

Si le bouton radio *All* est sélectionné, l'équipement reçoit ses paramètres IPv6 au moyen de toutes les possibilités d'affectation dynamique et manuelle.

2.7 Administration de la détection des conflits d'adresses

Vous affectez une adresse IP à l'équipement à l'aide de différentes méthodes. Cette fonction permet à l'équipement de détecter des conflits d'adresses IP sur un réseau après démarrage ; l'équipement effectue aussi des vérifications périodiques en cours de fonctionnement. Cette fonction est décrite dans RFC 5227.

Lorsqu'elle est activée, l'équipement envoie un trap SNMP vous informant de la détection d'un conflit d'adresses IP.

La liste suivante contient les réglages par défaut pour cette fonction :
- *Operation*: `On`
- *Detection mode*: `active and passive`
- *Send periodic ARP probes* : `coché`
- *Detection delay [ms]*: `200`
- *Release delay [s]*: `15`
- *Address protections*: `3`
- *Protection interval [ms]*: `200`
- *Send trap* : `coché`

2.7.1 Détection active et passive

La vérification active du réseau permet d'éviter que l'équipement ne se connecte au réseau avec une adresse IP dupliquée. Après connexion de l'équipement à un réseau ou après configuration de l'adresse IP, l'équipement vérifie immédiatement si son adresse IP existe dans le réseau. Pour rechercher des conflits d'adresses dans le réseau, l'équipement envoie 4 sondes ARP avec un délai de détection de 200 ms dans le réseau. Si l'adresse IP existe, l'équipement tente de revenir à la configuration précédente et effectue une nouvelle vérification une fois le délai configuré écoulé.

Si vous désactivée la détection active, l'équipement envoie 2 annonces APR gratuites à intervalles de 2 s. Grâce aux annonces ARP avec détection passive activée, l'équipement scrute le réseau pour déterminer la présence éventuelle d'un conflit d'adresses. Après avoir résolu un conflit d'adresses ou après expiration du délai, l'équipement se reconnecte au réseau. Après 10 conflits détectés, lorsque le délai configuré est inférieur à 60 s, l'équipement définit le délai sur 60 s.

Après exécution par l'équipement d'une détection active ou bien si vous désactivez la fonction de détection active et la détection passive étant activée, l'équipement scrute le réseau à la recherche d'autres équipements utilisant la même adresse IP. Lorsque l'équipement détecte une adresse IP dupliquée, il défend initialement son adresse en utilisant le mécanisme ACD en mode de détection passive, puis envoie des ARP gratuits. Le nombre de protections envoyées par l'équipement et l'intervalle de protection sont configurables. Pour résoudre les conflits, si l'équipement distant reste connecté au réseau, l'interface réseau de l'équipement local se déconnecte du réseau.

Lorsqu'un serveur DHCP affecte une adresse IP à l'équipement et qu'un conflit d'adresses survient, l'équipement retourne un message de rejet DHCP.

L'équipement utilise la méthode des sondes ARP. Les avantages sont les suivants :
- Les caches ARP sur d'autres équipements restent inchangés.
- La méthode est robuste grâce aux multiples transmissions de sondes ARP.

2.8 Duplicate Address Detection

La fonction *Duplicate Address Detection* détermine l'unicité d'une adresse unicast IPv6 sur une interface. La fonction est exécutée lorsqu'une adresse IPv6 est configurée à l'aide des méthodes manuelle, *DHCPv6* ou *Auto*. La fonction est également déclenchée par un changement d'état du lien, par exemple, de down à up.

La fonction *Duplicate Address Detection* utilise les messages *Neighbor Solicitation* et *Neighbor Advertisement*. Vous avez la possibilité de définir le nombre de messages consécutifs *Neighbor Solicitation* que l'équipement envoie. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Network > IPv6*.
- ☐ Dans le cadre *Duplicate Address Detection*, définissez la valeur nécessaire dans le champ *Number of neighbor solicitants*.
  Valeurs possibles :
  - `0`
    La fonction est désactivée.
  - `1..5` (réglage par défaut : `1`)
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`network ipv6 dad-transmits <0..5>`	Défnissez le nombre de messages *Neighbor Solicitation* que l'équipement envoie. La valeur `0` désactive la fonction.

Commentaire : Si la fonction *Duplicate Address Detection* détecte qu'une adresse IPv6 n'est pas unique sur un lien, l'équipement ne consigne pas cet événement dans le fichier log (log système).

3 Accès à l'équipement

3.1 Rôles d'accès

Les fonctions de l'équipement auxquelles vous avez accès en tant qu'utilisateur dépendent de votre rôle d'accès. Lorsque vous êtes connecté avec un rôle d'accès spécifique, vous avez accès aux fonctions correspondantes du rôle d'accès.

Les commandes auxquelles vous avez accès en tant qu'utilisateur dépendent également du mode de l'interface de ligne de commande actuellement utilisé. Voir « Hiérarchie des commandes par mode » à la page 25.

L'équipement offre les rôles d'accès suivants :

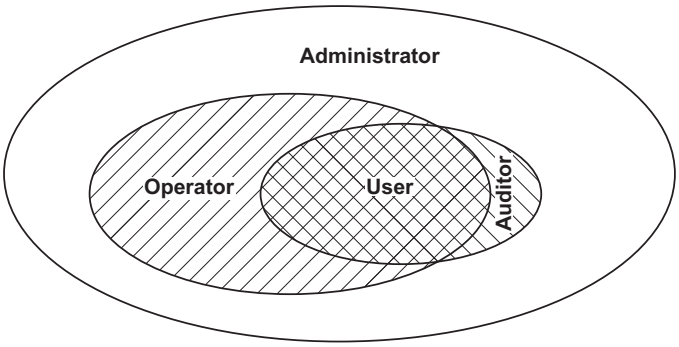


Tableau 13 : Rôles d'accès et portée des autorisations de l'utilisateur

Rôle d'accès	Autorisations de l'utilisateur
`User`	Les utilisateurs connectés avec le rôle d'accès `User` sont autorisés à surveiller l'équipement.
`Auditor`	Les utilisateurs connectés avec le rôle d'accès `Auditor` sont autorisés à surveiller l'équipement et à sauvegarder le fichier log dans la boîte de dialogue *Diagnostics > Report > Audit Trail*.
`Operator`	Les utilisateurs connectés avec le rôle d'accès `Operator` sont autorisés à surveiller l'équipement et à modifier les réglages – à l'exception des réglages de sécurité relatifs à l'accès à l'équipement.
`Administrator`	Les utilisateurs connectés avec le rôle d'accès `Administrator` sont autorisés à surveiller l'équipement et à modifier les réglages.
`Unauthorized`	Les utilisateurs non autorisés sont bloqués, et l'équipement rejette la connexion de l'utilisateur. Affectez cette valeur pour verrouiller temporairement le compte d'utilisateur. Lorsqu'une erreur est détectée à l'occasion d'un changement de rôle d'accès, l'équipement affecte ce rôle d'accès au compte d'utilisateur.

3.2 Première connexion (modification du mot de passe)

Pour contribuer à protéger l'équipement contre l'accès indésirable, il est impératif de modifier le mot de passe par défaut lors de la configuration initiale.

Exécutez les étapes suivantes :

- ☐ La première fois que vous vous connectez, ouvrez l'interface utilisateur graphique, l'application SE View ou l'interface de ligne de commande.
- ☐ Connectez-vous avec le mot de passe par défaut.
  L'équipement vous invite à saisir un nouveau mot de passe.
- ☐ Saisissez votre nouveau mot de passe.
  Pour contribuer à augmenter la sécurité, choisissez un mot de passe d'au moins 8 caractères contenant des lettres majuscules, des lettres minuscules, des caractères numériques et des caractères spéciaux.
- ☐ Lorsque vous vous connectez à l'équipement à l'aide de l'interface de ligne de commande, l'équipement vous invite à confirmer votre nouveau mot de passe.
- ☐ Connectez-vous à nouveau avec votre nouveau mot de passe.

Commentaire : Si vous avez perdu votre mot de passe, contactez votre équipe d'assistance locale.

3.3 Listes d'authentification

Lorsqu'un utilisateur accède à l'équipement à l'aide d'une connexion spécifique, l'équipement vérifie les identifiants de connexion de l'utilisateur dans une liste d'authentification qui contient les stratégies que l'équipement applique en matière d'authentification.

Pour qu'un utilisateur puisse accéder à l'administration de l'équipement, il convient qu'au moins une stratégie soit affectée à la liste d'authentification de l'application à l'aide de laquelle l'accès est effectué.

3.3.1 Applications

L'équipement fournit une application pour chaque type de connexion permettant à un utilisateur d'accéder à l'équipement :

- Accédez à l'interface de ligne de commande à l'aide d'une connexion série : `Console(V.24)`
- Accédez à l'interface de ligne de commande à l'aide de SSH : `SSH`
- Accédez à l'interface de ligne de commande à l'aide de Telnet : `Telnet`
- Accédez à l'interface utilisateur graphique : `WebInterface`

L'équipement fournit également une application pour contrôler l'accès au réseau à partir d'équipements terminaux connectés à l'aide d'un contrôle d'accès basé sur port : `8021x`

3.3.2 Stratégies

Lorsqu'un utilisateur se connecte avec des données de connexion valides, l'équipement permet à l'utilisateur d'accéder à l'administration de l'équipement. L'équipement authentifie les utilisateurs à l'aide des stratégies suivantes :

- Gestion des utilisateurs de l'équipement
- LDAP
- RADIUS

Lorsque l'équipement terminal se connecte à l'aide de données de connexion valides, l'équipement permet aux équipements terminaux connectés d'accéder au réseau à l'aide du contrôle d'accès basé sur port conformément à IEEE 802.1X. L'équipement authentifie les équipements terminaux à l'aide des stratégies suivantes :

- RADIUS
- IAS (Integrated Authentication Server)

L'équipement vous permet d'opter pour une solution de repli. À cette fin, spécifiez plus d'une stratégie dans la liste d'authentification. Lorsque l'authentification échoue à l'aide de la stratégie actuelle, l'équipement applique la stratégie spécifiée suivante.

3.3.3 Gestion des listes d'authentification

Vous pouvez gérer les listes d'authentification dans l'interface utilisateur graphique ou dans l'interface de ligne de commande. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Authentication List*.

La boîte de dialogue affiche les listes d'authentification configurées.

`show authlists`	Affiche les listes d'authentification configurées.

☐ Désactivez la liste d'authentification pour les applications au moyen desquelles aucun accès à l'équipement n'est effectué, par exemple `8021x` .

- ☐ Dans la colonne *Active* de la liste d'authentification `defaultDot1x8021AuthList`, décochez la case.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

`authlists disable defaultDot1x8021AuthList`	Désactive la liste d'authentification `default-Dot1x8021AuthList`.

3.3.4 Ajustement des réglages

Exemple : configurez une liste d'authentification séparée pour l'applicationn `WebInterface` qui est incluse par défaut dans la liste d'authentification `defaultLoginAuthList`.

L'équipement transmet les requêtes d'authentification à un serveur RADIUS intégré au réseau. Lorsqu'il utilise la solution de repli, l'équipement authentifie les utilisateurs à l'aide de la gestion locale des utilisateurs. Pour ce faire, exécutez les étapes suivantes :

☐ Créez une liste d'authentification `loginGUI`.

- ☐ Ouvrez la boîte de dialogue *Device Security > Authentication List*.
- ☐ Cliquez sur le bouton  .
  La boîte de dialogue affiche la fenêtre *Create*.
- ☐ Saisissez un nom évocateur dans le champ *Name*.
  Dans cet exemple, saisissez le nom `loginGUI`.
- ☐ Cliquez sur le bouton *Ok*.
  L'équipement ajoute une nouvelle entrée de tableau.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`authlists add loginGUI`	Crée une liste d'authentification `loginGUI`.

☐ Sélectionnez les stratégies pour la liste d'authentification `loginGUI`.

- ☐ Dans la colonne *Policy 1*, sélectionnez la valeur *`radius`*.
- ☐ Dans la colonne *Policy 2*, sélectionnez la valeur *`local`*.
- ☐ Dans les colonnes *Policy 3* à *Policy 5*, sélectionnez la valeur *`reject`* pour empêcher tout recours à une solution de repli supplémentaire.
- ☐ Dans la colonne *Active*, cochez la case.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`authlists set-policy loginGUI radius local reject reject reject`	Affecte les stratégies `radius`, `local` et `reject` à la liste d'authentification `loginGUI`.
`show authlists`	Affiche les listes d'authentification configurées.
`authlists enable loginGUI`	Active la liste d'authentification `loginGUI`.

☐ Affecte une application à la liste d'authentification `loginGUI`.

- ☐ Dans la boîte de dialogue *Device Security > Authentication List*, mettez en surbrillance la liste d'authentification `loginGUI`.
- ☐ Cliquez sur le bouton ☰ puis sur l'élément *Allocate applications*.
  La boîte de dialogue affiche la fenêtre *Allocate applications*.
- ☐ Dans la colonne de gauche, mettez en surbrillance l'application `WebInterface`.
- ☐ Cliquez sur le bouton ▸.
  La colonne de droite affiche désormais l'application `WebInterface`.
- ☐ Cliquez sur le bouton *Ok*.
  La boîte de dialogue affiche les réglages mis à jour :
  - La colonne *Dedicated applications* de la liste d'authentification `loginGUI` affiche l'application `WebInterface`.
  - La colonne *Dedicated applications* de la liste d'authentification `defaultLoginAuthList` n'affiche plus l'application `WebInterface`.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`show applists`	Affiche les applications les listes affectées.
`applists set-authlist WebInterface loginGUI`	Affecte l'application `loginGUI` à la liste d'authentification `WebInterface`.

3.4 Gestion des utilisateurs

Lorsqu'un utilisateur se connecte avec des données de connexion valides, l'équipement permet à l'utilisateur d'accéder à l'administration de l'équipement. L'équipement authentifie les utilisateurs soit à l'aide de la gestion locale des utilisateurs ou à l'aide d'un serveur RADIUS intégré au réseau. Pour que l'équipement utilise la gestion des utilisateurs, affectez la stratégie `local` à une liste d'authentification, voir la boîte de dialogue *Device Security > Authentication List*.

La gestion locale des utilisateurs vous permet de gérer les comptes d'utilisateur. Un compte d'utilisateur est habituellement affecté à chaque utilisateur.

3.4.1 Rôles d'accès

L'équipement vous permet d'utiliser un modèle d'autorisation basé sur le rôle pour contrôler spécifiquement l'accès à l'administration de l'équipement. Les utilisateurs auxquels un profil d'autorisation spécifique est affecté sont autorisés à utiliser les commandes et fonctions à l'aide du même profil d'autorisation ou d'un profil inférieur.

L'équipement utilise les profils d'autorisation sur chaque application permettant d'accéder à l'administration de l'équipement.

Chaque compte d'utilisateur est associé à un rôle d'accès qui gère l'accès aux fonctions individuelles de l'équipement. Affectez à l'utilisateur un rôle d'accès pré-défini en fonction de l'activité planifiée pour l'utilisateur respectif. L'équipement fait la distinction entre les rôles d'accès suivants.

Tableau 14 : Rôles d'accès pour les comptes d'utilisateur

Role	Désignation	Autorisé pour les activités suivantes
Administrator	L'utilisateur est autorisé à surveiller et à administrer l'équipement.	Toutes les activités bénéficiant d'un accès en lecture/écriture, y compris les activités suivantes réservées à un administrateur : ▶ Ajouter, modifier ou supprimer des comptes d'utilisateur ▶ Activer, désactiver ou déverrouiller des comptes d'utilisateur ▶ Modifier tous les mots de passe ▶ Configurer la gestion des mots de passe ▶ Régler ou modifier l'heure système ▶ Charger les fichiers sur l'équipement, par exemple, les configurations de l'équipement, les certificats ou les images logicielles ▶ Restaurer la configuration d'origine des réglages de l'équipement et des réglages de sécurité ▶ Configurer le serveur RADIUS et les listes d'authentification ▶ Appliquer les scripts à l'aide de l'interface de ligne de commande ▶ Activer/désactiver la consignation des commandes de la CLI et des requêtes SNMP ▶ Activer/désactiver la mémoire externe ▶ Activer/désactiver le moniteur du système ▶ Activer/désactiver les services permettant l'accès à l'administration de l'équipement (par exemple SNMP) ▶ Configurer les restriction de l'accès à l'interface utilisateur graphique ou à l'interface de ligne de commande en fonction des adresses IP
Operator	L'utilisateur est autorisé à surveiller et à configurer l'équipement - à l'exception des réglages de sécurité.	Toutes les activités bénéficiant d'un accès en lecture/écriture, à l'exception des activités précitées, qui sont réservées à un administrateur :

Tableau 14 : Rôles d'accès pour les comptes d'utilisateur (cont

Role	Désignation	Autorisé pour les activités suivantes
Auditor	L'utilisateur est autorisé à surveiller l'équipement et à sauvegarder le fichier log dans la boîte de dialogue *Diagnostics > Report > Audit Trail*.	Surveillance des activités bénéficiant d'un accès en lecture.
Guest	L'utilisateur est autorisé à surveiller l'équipement - à l'exception des réglages de sécurité.	Surveillance des activités bénéficiant d'un accès en lecture.
Unauthorized	Aucun accès à l'équipement n'est possible. ▶ En tant qu'administrateur, affectez ce rôle d'accès pour verrouiller temporairement un compte d'utilisateur. ▶ Lorsqu'un administrateur affecte un rôle d'accès différent au compte d'utilisateur et qu'une erreur est détectée, l'équipement affecte ce rôle d'accès au compte d'utilisateur.	Aucune activité n'est autorisée.

3.4.2 Gestion des comptes d'utilisateur

Vous pouvez gérer les comptes d'utilisateur dans l'interface utilisateur graphique ou dans l'interface de ligne de commande. Pour ce faire, exécutez les étapes suivantes :

☐ Ouvrez la boîte de dialogue *Device Security > User Management*.

La boîte de dialogue affiche les comptes d'utilisateur configurés.

`show users` Affiche les comptes d'utilisateur configurés.

3.4.3 Réglage par défaut

Dans la configuration d'origine, les comptes d'utilisateur `admin` et `user` sont configurés dans l'équipement.

Tableau 15 : Réglages par défaut pour la configuration d'origine des comptes d'utilisateur

Paramètre	Réglage par défaut	
User name	`admin`	`user`
Password	`private`	`public`
Role	`administrator`	`guest`
User locked	`case non cochée`	`case non cochée`
Policy check	`case non cochée`	`case non cochée`
SNMP auth type	`hmacmd5`	`hmacmd5`
SNMP encryption type	`des`	`des`

Modifiez le mot de passe du compte d'utilisateur `admin` avant de rendre l'équipement accessible sur le réseau.

3.4.4 Modification des mots de passe par défaut

Modifiez le mot de passe des comptes d'utilisateur par défaut pour contribuer à la protection contre l'accès indésirable. Pour ce faire, exécutez les étapes suivantes :

☐ Modifiez les mots de passe des comptes d'utilisateur `admin` et `user`.

☐ Ouvrez la boîte de dialogue *Device Security > User Management*.

La boîte de dialogue affiche les comptes d'utilisateur configurés.

☐ Pour créer un mot de passe présentant un haut niveau de complexité, cochez la case dans la colonne *Policy check*.
Avant de le sauvegarder, l'équipement vérifie le mot de passe à l'aide de la stratégie spécifiée dans le cadre *Password policy*.

Commentaire : La vérification du mot de passe peut provoquer l'affichage d'un message dans le cadre *Security status* de la boîte de dialogue *Basic Settings > System*. Spécifiez les réglages provoquant l'affichage de ce message dans la boîte de dialogue *Basic Settings > System*.

☐ Cliquez sur la ligne du compte d'utilisateur concerné dans le champ *Password*. Saisissez un mot de passe d'au moins 6 caractères.
Jusqu'à 64 caractères alphanumériques sont autorisés.
- ▶ L'équipement fait la distinction entre majuscules et minuscules.
- ▶ La longueur minimale du mot de passe est spécifiée dans le cadre *Configuration*. L'équipement vérifie constamment la longueur minimale du mot de passe.

☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`users password-policy-check <user> enable`	Active la vérification du mot de passe pour le compte d'utilisateur `<user>` en fonction de la stratégie spécifiée. Vous êtes ainsi en mesure d'appliquer un niveau de complexité plus élevé au mot de passe.

Commentaire : Lorsque vous affichez l'état de la sécurité, la vérification du mot de passe peut provoquer l'affichage d'un message (`show security-status all`). Spécifiez les réglages provoquant l'affichage de ce message à l'aide de la commande `security-status monitor pwd-policy-inactive`.

`users password <user> SECRET`	Spécifie le mot de passe `SECRET` pour le compte d'utilisateur `<user>`. Saisissez au moins 6 caractères.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

3.4.5 Configuration d'un nouveau compte d'utilisateur

Affectez un compte d'utilisateur séparé à chaque utilisateur qui accède à l'administration de l'équipement. Vous être ainsi en mesure de contrôler spécifiquement les autorisations d'accès.

Dans l'exemple suivant, nous configurerons le compte d'utilisateur d'un utilisateur `USER` doté du rôle `operator`. Les utilisateurs dotés du rôle `operator` sont autorisés à surveiller et à configurer l'équipement - à l'exception des réglages de sécurité. Pour ce faire, exécutez les étapes suivantes :

☐ Créez un nouveau compte d'utilisateur.

- ☐ Ouvrez la boîte de dialogue *Device Security > User Management*.
- ☐ Cliquez sur le bouton  .
  La boîte de dialogue affiche la fenêtre *Create*.
- ☐ Saisissez le nom dans le champ *User name*.
  Dans cet exemple, nous donnons au compte d'utilisateur le nom de `USER`.
- ☐ Cliquez sur le bouton *Ok*.
- ☐ Pour créer un mot de passe présentant un haut niveau de complexité, cochez la case dans la colonne *Policy check*.
  Avant de le sauvegarder, l'équipement vérifie le mot de passe à l'aide de la stratégie spécifiée dans le cadre *Password policy*.
- ☐ Dans le champ *Password*, saisissez un mot de passe d'au moins 6 caractères.
  Jusqu'à 64 caractères alphanumériques sont autorisés.
  - ▶ L'équipement fait la distinction entre majuscules et minuscules.
  - ▶ La longueur minimale du mot de passe est spécifiée dans le cadre *Configuration*. L'équipement vérifie constamment la longueur minimale du mot de passe.
- ☐ Dans la colonne *Role*, sélectionnez le rôle d'utilisateur.
  Dans cet exemple, nous sélectionnerons la valeur `operator`.
- ☐ Pour activer le compte d'utilisateur, cochez la case dans la colonne *Active*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .
  La boîte de dialogue affiche les comptes d'utilisateur configurés.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`users add USER`	Crée le compte d'utilisateur `USER`.
`users password-policy-check USER enable`	Active la vérification du mot de passe pour le compte d'utilisateur `USER` en fonction de la stratégie spécifiée. Vous êtes ainsi en mesure d'appliquer un niveau de complexité plus élevé au mot de passe.

`users password USER SECRET`	Spécifie le mot de passe `SECRET` pour le compte d'utilisateur `USER`. Saisissez au moins 6 caractères.
`users access-role USER  operator`	Affecter le rôle d'utilisateur `operator` au compte d'utilisateur `USER`.
`users enable USER`	Active le compte d'utilisateur `USER`.
`show users`	Affiche les comptes d'utilisateur configurés.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

Commentaire : Lorsque vous configurez un nouveau compte d'utilisateur dans l'interface de ligne de commande, n'oubliez pas d'affecter le mot de passe.

3.4.6 Désactivation du compte d'utilisateur

Une fois qu'un compte d'utilisateur est désactivé, l'équipement empêche l'accès de l'utilisateur à l'administration de l'équipement. Contrairement à sa suppression complète, la désactivation d'un compte d'utilisateur vous permet de conserver les réglages et de les réutiliser ultérieurement. Pour ce faire, exécutez les étapes suivantes :

☐ Pour conserver les réglages du compte d'utilisateur et les réutiliser ultérieurement, désactivez temporairement le compte d'utilisateur.

- ☐ Ouvrez la boîte de dialogue *Device Security > User Management*.
  La boîte de dialogue affiche les comptes d'utilisateur configurés.
- ☐ Dans la ligne du compte d'utilisateur concerné, décochez la case dans la colonne *Active*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`users disable <user>`	Pour désactiver le compte d'utilisateur.
`show users`	Affiche les comptes d'utilisateur configurés.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

☐ Pour désactiver les réglages du compte d'utilisateur de manière permanente, supprimez le compte d'utilisateur.

- ☐ Mettez en surbrillance la ligne du compte d'utilisateur concerné.
- ☐ Cliquez sur le bouton  .

`users delete <user>`	Supprime le compte d'utilisateur `<user>`.
`show users`	Affiche les comptes d'utilisateur configurés.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

3.4.7 Ajustement des stratégies de mots de passe

L'équipement vous permet de vérifier si les mots de passe des comptes d'utilisateur respectent la stratégie spécifiée. Lorsque les mots de passe respectent la stratégie, vous bénéficiez d'un niveau de complexité supérieur pour les mots de passe.

La gestion des utilisateurs de l'équipement vous permet d'activer ou de désactiver la vérification séparément pour chaque compte d'utilisateur. Lorsque vous cochez la case et que le nouveau mot de passe remplit les exigences de la stratégie, l'équipement accepte la modification du mot de passe.

Avec les réglages par défaut, les valeurs pratiques relatives à la stratégie sont configurées dans l'équipement. Vous avez la possibilité d'ajuster la stratégie de manière à ce qu'elle se conforme à vos exigences. Pour ce faire, exécutez les étapes suivantes :

☐ Ajustez la stratégie relative aux mots de passe de manière à ce qu'elle se conforme à vos exigences.

☐ Ouvrez la boîte de dialogue *Device Security > User Management*.

Dans le cadre *Configuration*, spécifiez le nombre autorisé de tentatives de connexion de l'utilisateur avant que l'équipement ne verrouille l'utilisateur. Vous pouvez également spécifier le nombre minimum de caractères contenus dans un mot de passe.

Commentaire : L'équipement permet uniquement aux utilisateurs dotés de l'autorisation `administrator` de supprimer le verrouillage.

Le nombre de tentatives de connexion ainsi que le verrouillage possible de l'utilisateur ne s'appliquent que lors de l'accès à l'administration de l'équipement par :

- l'interface utilisateur graphique
- le protocole SSH
- le protocole Telnet

Commentaire : Lors de l'accès à l'administration de l'équipement à l'aide de l'interface de ligne de commande via la connexion série, le nombre de tentatives de connexion est illimité.

☐ Spécifiez les valeurs correspondant à vos exigences.

- Dans le champ *Login attempts*, vous spécifiez le nombre de tentatives de connexion pouvant être effectuées par un utilisateur. Ce champ vous permet de définir une valeur comprise dans l'intervalle `0..5`.
  Dans l'exemple ci-dessus, la valeur `0` permet de désactiver la fonction.
- Le champ *Min. password length* vous permet de saisir des valeurs comprises dans l'intervalle `1..64`.

Cette boîte de dialogue affiche la stratégie configurée dans le cadre *Password policy*.

☐ Ajustez les valeurs correspondant à vos exigences.

- Les valeurs comprises dans un intervalle compris entre `1` et `16` sont autorisées.
  La valeur `0` permet de désactiver la stratégie concernée.

Pour appliquer les entrées spécifiées dans les cadres *Configuration* et *Password policy*, cochez la case dans la colonne *Policy check* destinée à un utilisateur particulier.

☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`passwords min-length 6`	Indique la stratégie de longueur minimale du mot de passe.

`passwords min-lowercase-chars 1`	Indique la stratégie de nombre minimum de lettre minuscules dans le mot de passe.
`passwords min-numeric-chars 1`	Indique la stratégie de nombre minimum de chiffres dans le mot de passe.
`passwords min-special-chars 1`	Indique la stratégie de nombre minimum de caractères spéciaux dans le mot de passe.
`passwords min-uppercase-chars 1`	Indique la stratégie de nombre minimum de lettre majuscules dans le mot de passe.
`show passwords`	Affiche les stratégies configurées.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

3.5 LDAP

Les administrateurs de serveurs gèrent des Active Directory qui contiennent les identifiants de connexion des utilisateurs pour les applications utilisées dans l'environnement de bureau. De structure hiérarchique, l'Active Directory contient les noms d'utilisateurs, les mots de passe et les niveaux de permission de lecture et d'écriture autorisés pour chaque utilisateur.

Cet équipement utilise le protocole LDAP (Lightweight Directory Access Protocol) pour récupérer les informations de connexion et les niveaux de permission des utilisateurs à partir d'un Active Directory. Cela permet une « authentification unique » pour les équipements de réseau. La récupération des identifiants de connexion à partir d'un Active Directory permet à l'utilisateur de se connecter avec les mêmes identifiants de connexion que ceux utilisés dans l'environnement de bureau.

Lorsqu'une session LDAP est créée, l'équipement contacte le Directory System Agent (DSA) pour effectuer une recherche dans l'Active Directory d'un serveur LDAP. Si le serveur trouve plusieurs entrées dans l'Active Directory pour un utilisateur, il envoie le niveau de permission le plus élevé trouvé. Le DSA est à l'écoute des requêtes d'information et envoie des réponses sur le port TCP `389` pour LDAP ou sur le port TCP `636` pour LDAP sur SSL (LDAPS). Les clients et les serveurs codent les requêtes et les réponses LDAPS à l'aide des règles de codage de base (BER). L'équipement ouvre une nouvelle connexion pour chaque requête et ferme la connexion après avoir reçu une réponse du serveur.

L'équipement vous permet de charger un certificat CA afin de valider le serveur pour les sessions Secure Socket Level (SSL) et Transport Layer Security (TLS). Le certificat est cependant facultatif pour les sessions TLS.

L'équipement peut mettre en mémoire cache les identifiants de connexion de 1024 utilisateurs au maximum. Si les serveurs Active Directory ne sont pas accessibles, les utilisateurs ont la possibilité de se connecter à l'aide de leurs identifiants de connexion bureau.

3.5.1 Coordination avec l'administrateur du serveur

Pour configurer la fonction *LDAP*, l'administrateur réseau doit demander les informations suivantes à l'administrateur du serveur :

- Le nom ou l'adresse IP du serveur
- L'emplacement de l'Active Directory sur le serveur
- Le type de connexion utilisé
- Le port d'écoute TCP
- Si nécessaire, l'emplacement du certificat CA
- Le nom de l'attribut contenant le nom de connexion de l'utilisateur
- Les noms de l'attribut contenant les niveaux de permission de l'utilisateur

L'administrateur du serveur peut attribuer des niveaux de permission sur une base individuelle en utilisant un attribut tel que `description` ou à un groupe en utilisant l'attribut `memberOf`. Dans la boîte de dialogue *Device Security > LDAP > Role Mapping*, vous spécifiez quels attributs reçoivent les différents niveaux de permission.

Vous avez également la possibilité de récupérer le nom des attributs contenant le nom de connexion de l'utilisateur et les niveaux de permission à l'aide d'un navigateur LDAP tel que JXplorer ou Softerra.

3.5.2 Exemple de configuration

L'équipement est en mesure d'établir un lien chiffré avec un serveur local en utilisant uniquement le nom du serveur ou avec un serveur sur un réseau différent en utilisant une adresse IP. L'administrateur du serveur utilise des attributs pour définir les identifiants de connexion d'un utilisateur et affecter des niveaux de permission à des individus et à des groupes.

À l'aide des informations reçues de l'administrateur du serveur, spécifiez quels attributs de l'Active Directory contiennent les identifiants de connexion de l'utilisateur et le niveau de permission. L'équipement compare alors les identifiants de connexion de l'utilisateur avec les niveaux de permission spécifiés dans l'équipement avant d'autoriser la connexion de l'utilisateur au niveau de permission attribué.

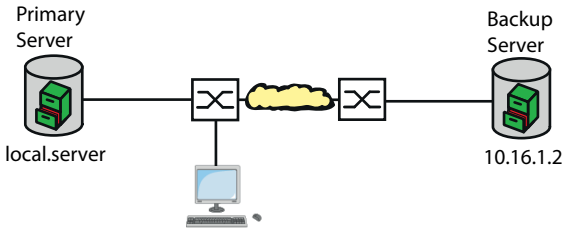


Figure 18 : Exemple de configuration LDAP

Dans cet exemple, l'administrateur du serveur a envoyé les informations suivantes :

Informations	Primary Server	Backup Server
Le nom ou l'adresse IP du serveur	`local.server`	`10.16.1.2`
L'emplacement de l'Active Directory sur le serveur	`Country/City/User`	`Country/Company/User`
Le type de connexion utilisé	`TLS` (avec certificat)	`SSL`
L'administrateur du serveur a envoyé le certificat CA par e-mail.	Certificat CA pour le serveur primaire enregistré localement	Certificat CA pour le serveur de sauvegarde enregistré localement
Le port d'écoute TCP	`389 (tls)`	`636 (ssl)`
Le nom de l'attribut contenant le nom de l'utilisateur	`userPrincipalName`	`userPrincipalName`
Les noms de l'attribut contenant les niveaux de permission de l'utilisateur	`OPERATOR` `ADMINISTRATOR`	`OPERATOR` `ADMINISTRATOR`

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Authentication List*.
- ☐ Pour configurer l'équipement afin qu'il récupère les identifiants de connexion de l'utilisateur au cours de la connexion à l'aide de l'interface utilisateur graphique à partir d'Active Directory d'abord, spécifiez pour la liste `defaultLoginAuthList` la valeur `ldap` dans la colonnePolicy 1.
- ☐ Ouvrez la boîte de dialogue *Device Security > LDAP > Configuration*.

- ☐ L'équipement vous permet de spécifier la durée pendant laquelle il enregistre les identifiants de connexion de l'utilisateur dans le cache. Pour mettre en cache les identifiants de connexion de l'utilisateur pendant une journée, entrez la valeur `1440` dans le champ *Client cache timeout [min]* du cadre *Configuration*.
- ☐ L'entrée *Bind user* est facultative. Lorsqu'elle est spécifiée, les utilisateurs saisissent uniquement leur nom d'utilisateur pour se connecter. L'utilisateur du service peut être toute personne ayant des identifiants de connexion répertoriés dans l'Active Directory sous l'attribut spécifié dans la colonne *User name attribute*. Dans la colonne *Bind user*, saisissez le nom d'utilisateur et le domaine.
- ☐ Le *Base DN* est une combinaison du composant de domaine (DC) et de l'unité d'organisation (OU). Le *Base DN* permet à l'équipement de localiser un serveur dans un domaine (DC) et de trouver l'Active Directory (OU). Spécifiez l'emplacement de l'Active Directory. Dans la colonne *Base DN*, spécifiez la valeur `ou=Users,ou=City,ou=Country,dc=server,dc=local`.
- ☐ Dans la colonne *User name attribute*, saisissez la valeur `userPrincipalName` pour spécifier l'attribut sous lequel l'administrateur du serveur répertorie les utilisateurs.

L'équipement utilise un certificat CA pour vérifier le serveur.

- ☐ Lorsque le certificat est stocké sur votre PC ou sur un lecteur réseau, glissez-déposez le certificat dans la zone  . Vous pouvez également cliquer sur la zone pour sélectionner le certificat.
- ☐ Pour transférer le certificat CA sur l'équipement, cliquez sur le bouton *Start*.
- ☐ Pour ajouter une entrée de tableau, cliquez sur le bouton  .
- ☐ Pour spécifier une description, saisissez la valeur `Primary AD Server` dans la colonne *Description*.
- ☐ Pour spécifier le nom de serveur et le domaine du serveur primaire, saisissez la valeur `local.server` dans la colonne *Address*.
- ☐ Pour communiquer, le serveur primaire utilise le port TCP `389` qui correspond à la valeur par défaut *Destination TCP port*.
- ☐ Le serveur primaire utilise TLS pour chiffrer la communication et un certificat CA pour valider le serveur. Dans la colonne *Connection security*, spécifiez la valeur `startTLS`.
- ☐ Pour activer l'entrée, cochez la case dans la colonne *Active*.
- ☐ En utilisant les informations reçues de l'administrateur du serveur pour le serveur de sauvegarde, ajoutez, configurez et activez une autre ligne.

- ☐ Ouvrez la boîte de dialogue *Device Security > LDAP > Role Mapping*.
- ☐ Pour ajouter une entrée de tableau, cliquez sur le bouton  .

Lorsqu'un utilisateur qui a été configuré et activé pour utiliser LDAP se connecte, l'équipement recherche dans l'Active Directory les identifiants de connexion de l'utilisateur. Si l'équipement identifie le nom d'utilisateur et le mot de passe comme étant correct, il recherche la valeur spécifiée dans la colonne *Type*. Si l'équipement trouve l'attribut et que le texte de la colonne *Parameter* correspond au texte de l'Active Directory, l'équipement permet à l'utilisateur de se connecter selon le niveau de permission attribué. Lorsque la valeur `attribute` est spécifiée dans la colonne *Type*, spécifiez la valeur dans la colonne *Parameter* sous la forme suivante : `attributeName=attributeValue`.

- ☐ Dans la colonne *Role*, saisissez la valeur `operator` pour spécifier le rôle d'utilisateur.
- ☐ Pour activer l'entrée, cochez la case dans la colonne *Active*.

- ☐ Cliquez sur le bouton  .
  La boîte de dialogue affiche la fenêtre *Create*.
  Saisissez les valeurs reçues de l'administrateur du serveur pour le rôle `administrator`.
  Pour activer l'entrée, cochez la case dans la colonne *Active*.
- ☐ Ouvrez la boîte de dialogue *Device Security > LDAP > Configuration*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.

Le tableau suivant décrit comment configurer la fonction *LDAP* dans l'équipement à l'aide de l'interface de ligne de commande. Le tableau affiche les commandes pour `Index 1`. Pour configurer `Index 2`, appliquez les mêmes commandes et remplacez les informations correspondantes.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`ldap cache-timeout 1440`	Spécifiez que l'équipement doit vider la mémoire non volatile après un jour.
`ldap client server add 1 local.server port 389`	Ajoutez une connexion au serveur client d'authentification à distance avec le nom d'hôte `local.server` et le port UDP `389`.
`ldap client server modify 1 security startTLS`	Spécifiez le type de sécurité utilisé pour la connexion.
`ldap client server modify 1 description Primary_AD_Server`	Spécifiez le nom de configuration de l'entrée.
`ldap basedn ou=Users,ou=City,ou=Country,dc=server, dc=local`	Spécifiez le nom de domaine de base utilisé pour trouver l'Active Directory sur le serveur.
`ldap search-attr userPrincipalName`	Spécifiez l'attribut à rechercher dans l'Active Directory qui contient les identifiants de connexion des utilisateurs.
`ldap bind-user user@company.com`	Spécifiez le nom et le domaine de l'utilisateur du service.
`ldap bind-passwd Ur-123456`	Spécifiez le mot de passe de l'utilisateur du service.
`ldap client server enable 1`	Activez la connexion au serveur client d'authentification à distance.
`ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR`	Ajoutez une entrée de mappage de rôle d'authentification à distance pour le rôle `Operator`. Mettez en correspondance le rôle `operator` avec l'attribut contenant le mot `OPERATOR`.
`ldap mapping enable 1`	Activez l'entrée de mappage de rôle d'authentification à distance.
`ldap operation`	Activez la fonction d'authentification à distance.

3.6 Accès via SNMP

Le protocole SNMP vous permet de travailler avec un système d'administration de réseau afin de surveiller l'équipement sur le réseau et de modifier ses réglages.

3.6.1 Accès SNMPv1/v2

Lorsque SNMPv1 ou SNMPv2 est utilisé, les communications entre le système d'administration de réseau et l'équipement ne sont pas chiffrées. Chaque paquet SNMP contient le noms de communauté en texte clair et l'adresse IP de l'expéditeur.

Les noms de communauté `user` dédiés aux accès en lecture et les noms de communauté `admin` dédiés aux accès en écriture sont réglés par défaut dans l'équipement. Lorsque SNMPv1/v2 est activé, l'équipement permet à tout utilisateur connaissant le nom de communauté d'accéder à l'équipement.

Rendez plus difficile tout accès indésirable à l'équipement. Pour ce faire, exécutez les étapes suivantes :

- ☐ Modifiez les noms de communauté par défaut dans l'équipement.
  Traitez les noms de communauté avec discrétion.
  Toute personne connaissant le nom de communauté dédié aux droits en écriture a les moyens de modifier les réglages de l'équipement.
- ☐ Spécifiez un nom de communauté dédié à l'accès en lecture/écriture différent du nom de communauté dédié à l'accès en lecture.
- ☐ Utilisez uniquement SNMPv1 ou SNMPv2 dans des environnements protégés contre l'écoute clandestine. Les protocoles n'utilisent pas le chiffrement.
- ☐ Dans l'équipement, nous recommandons d'utiliser SNMPv3 et de désactiver l'accès via SNMPv1 et SNMPv2.

3.6.2 Accès via SNMPv3

Lorsque SNMPv3 est utilisé, les communications entre le système d'administration de réseau et l'équipement sont chiffrées. Le système d'administration de réseau s'authentifie sur l'équipement à l'aide des identifiants de connexion d'un utilisateur. La condition préalable à l'accès via SNMPv3 est que le système d'administration de réseau utilise des réglages identiques à ceux de l'équipement.

L'équipement vous permet de spécifier le *SNMP auth type* et les paramètres *SNMP encryption type* pour chaque compte d'utilisateur individuel.

Lorsque vous configurez un nouveau compte d'utilisateur dans l'équipement, les paramètres sont réglés par défaut de manière à ce que le système d'administration de réseau ConneXium Network Manager puisse joindre l'équipement immédiatement.

Les comptes d'utilisateur configurés dans l'équipement utilisent les mêmes mots de passe dans l'interface utilisateur graphique, dans l'interface de ligne de commande et avec SNMPv3.

Pour adapter les paramètres SNMPv3 des réglages du compte d'utilisateur aux réglages de votre système d'administration de réseau, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > User Management*.

La boîte de dialogue affiche les comptes d'utilisateur configurés.

- ☐ Cliquez sur la ligne du compte d'utilisateur concerné dans le champ *SNMP auth type*. Sélectionnez le réglage souhaité.
- ☐ Cliquez sur la ligne du compte d'utilisateur concerné dans le champ *SNMP encryption type*. Sélectionnez le réglage souhaité.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`users snmpv3 authentication <user> md5 | sha1`	Affectation du protocole HMAC-MD5 ou HMACSHA dédié aux requêtes d'authentification destinées au compte d'utilisateur `<user>`.
`users snmpv3 encryption <user> des | aescfb128 | none`	Affecte l'algorithme DES ou AES-128 au compte d'utilisateur `<user>`. Avec cet algorithme, l'équipement chiffre les requêtes d'authentification. La valeur `none` supprime le chiffrement.
`show users`	Affiche les comptes d'utilisateur qui ont été configurés.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

3.7 Accès Out of Band

L'équipement s'accompagne d'un port séparé permettant l'accès out-of-band à l'administration de l'équipement. En cas de charge in-band élevée sur les ports de commutation, vous pouvez utiliser ce port séparé pour accéder à l'administration de l'équipement.

Il convient pour cela que vous connectiez préalablement la station d'administration réseau directement au port USB. Lorsque vous utilisez Microsoft Windows, installez le pilote RNDIS si nécessaire. Une fois que vous avez connecté la station d'administration réseau, celle-ci peut communiquer avec l'administration de l'équipement via une connexion de réseau virtuelle.

Avec le réglage par défaut, vous pouvez accéder à l'administration de l'équipement via ce port en utilisant les paramètres IP suivants :
- *IP address* `91.0.0.100`
- *Netmask* `255.255.255.0`

L'équipement vous permet d'accéder à l'administration de l'équipement en utilisant les protocoles suivants :
- SNMP
- Telnet
- SSH
- HTTP
- HTTPS
- FTP
- SCP
- TFTP
- SFTP

3.7.1 Spécification des paramètres IP

Lorsque vous connectez la station d'administration réseau via le port USB, l'équipement affecte l'adresse IP de l'interface réseau USB incrémentée de 1 à la station d'administration réseau (`91.0.0.101` dans le réglage par défaut). L'équipement vous permet de modifier les paramètres IP pour adapter l'équipement aux exigences de votre environnement.

Vérifiez que le sous-réseau IP de cette interface réseau ne chevauche aucun sous-réseau connecté à une autre interface de l'équipement :
- Interface d'administration

Si la station d'administration réseau accède à l'administration de l'équipement via le port USB, l'équipement déconnecte l'interface utilisateur graphique et l'interface de ligne de commande immédiatement dès que les modifications ont été effectuées.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Out of Band over USB*.
- ☐ Écrasez l'adresse IP dans le champ *IP parameter* du cadre *IP address*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

```
enable
```
Basculez sur le mode Privileged EXEC.

```
network usb parms 192.168.1.1
255.255.255.0
```
Spécifier l'adresse IP `192.168.1.1` et le masque réseau `255.255.255.0` pour l'interface réseau USB.

```
show network usb
```
Afficher les réglages de l'interface réseau USB.

```
Out-of-band USB management settings
-----------------------------------
Management operation.....................enabled
IP address..............................192.168.1.1
Subnet mask.............................255.255.255.0
Host MAC address........................64:60:38:1f:85:85
Device MAC address......................64:60:38:1f:85:86
```

```
save
```
Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

3.7.2 Désactiver l'interface réseau USB

Dans le réglage par défaut, l'interface réseau USB est activée. Si vous souhaitez empêcher l'accès à l'administration de l'équipement via le port USB, l'équipement vous permet de désactiver l'interface réseau USB.

Si la station d'administration réseau accède à l'administration de l'équipement via le port USB, l'équipement déconnecte l'interface utilisateur graphique et l'interface de ligne de commande immédiatement dès que les modifications ont été effectuées.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Out of Band over USB*.
- ☐ Pour désactiver l'interface réseau USB, sélectionnez le bouton radio *Off* dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

```
enable
```
Basculez sur le mode Privileged EXEC.

```
no network usb operation
```
Désactiver l'interface réseau USB.

```
Out-of-band USB management settings
-----------------------------------
Management operation....................disabled
IP address..............................192.168.1.1
Subnet mask.............................255.255.255.0
Host MAC address........................64:60:38:1f:85:85
Device MAC address......................64:60:38:1f:85:86
```

```
save
```
Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

4 Synchronisation de l'heure système dans le réseau

De nombreuses applications dépendent de la précision la plus élevée possible de l'heure système. La précision nécessaire et l'écart admissible avec l'heure réelle dépendent du domaine d'application.

Les domaines d'application sont par exemple :
- Les entrées de log
- L'horodatage de données de production
- Le contrôle des processus

L'équipement vous permet de synchroniser l'heure sur le réseau à l'aide des options suivantes :
- Le protocole SNTP (Simple Network Time Protocol) est une solution simple pour les domaines d'application exigeant une faible précision. Dans des conditions idéales, SNTP permet d'atteindre une précision de l'ordre de la milliseconde. La précision dépend du retard du signal.
- La norme IEEE 1588 associée au Precision Time Protocol (PTP) permet d'atteindre des précisions de l'ordre de fractions de microsecondes. Cette méthode convient même aux applications exigeantes, y compris le contrôle des processus.

Lorsque les équipements concernés prennent en charge le protocole PTP, c'est le meilleur choix. PTP est plus précis, dispose de méthodes avancées de correction des erreurs et entraîne une faible charge du réseau. La mise en œuvre de PTP est relativement facile.

Commentaire : Selon les normes PTP et SNTP, les deux protocoles fonctionnent en parallèle dans le même réseau. Cependant, comme les deux protocoles influencent l'heure système de l'équipement, des situations peuvent se produire dans lesquelles les deux protocoles sont en conflit l'un avec l'autre.

4.1 Réglages de base

La boîte de dialogue *Time > Basic Settings* vous permet de spécifier les réglages généraux relatifs à l'heure.

4.1.1 Réglage de l'heure

Lorsqu'aucune source d'heure de référence n'est disponible, vous avez la possibilité de régler vous-même l'heure sur l'équipement.

Après un démarrage à froid ou un redémarrage, lorsqu'aucune horloge en temps réel n'est disponible ou que l'horloge en temps réel contient une heure non valide, l'équipement initialise son horloge sur le 1er janvier, 00:00. Après la mise hors tension, l'équipement stocke les réglages dans la mémoire tampon de l'horloge en temps réel pendant un maximum de 24 heures.

Vous pouvez également configurer les réglages dans l'équipement de manière à obtenir automatiquement l'heure actuelle depuis une horloge PTP ou un serveur SNTP.

Vous pouvez également configurer les réglages dans l'équipement de manière à obtenir automatiquement l'heure actuelle depuis un serveur SNTP.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Time > Basic Settings*.
- ▶ Le champ *System time (UTC)* affiche l'UTC (temps universel coordonné) actuel de l'équipement. L'UTC correspond à l'heure relative à la mesure du temps universel coordonné. L'UTC est le même dans le monde entier et ne prend pas en compte les décalages horaires locaux.
- ▶ L'heure figurant dans le champ *System time* est obtenue à partir de l'heure du champ *System time (UTC)* additionnée à la valeur du champ *Local offset [min]* et un éventuel ajustement dû à l'heure d'été.

Commentaire : PTP envoie le temps atomique international (TAI). Depuis le 1er juillet 2020, l'heure TAI a 37 secondes d'avance sur l'heure UTC. Lorsque la source de temps de référence PTP du décalage UTC est réglée correctement, l'équipement corrige automatiquement cette différence sur l'affichage dans le champ *System time (UTC)*.

- ☐ Pour que l'équipement applique l'heure de votre PC au champ *System time*, cliquez sur le bouton *Set time from PC*.
  En fonction de la valeur du champ *Local offset [min]*, l'équipement calcule l'heure dans le champ *System time (UTC)*. L'heure du champ *System time (UTC)* est obtenue à partir de l'heure du champ *System time* moins la valeur du champ *Local offset [min]* et un éventuel ajustement dû à l'heure d'été.
- ▶ Le champ *Time source* affiche l'origine des données temporelles. L'équipement sélectionne automatiquement la source la plus précise.
  La source est tout d'abord `local`.
  Lorsque SNTP est activé et que l'équipement reçoit un paquet SNTP valide, il règle sa source d'heure sur `sntp`.
  Lorsque PTP est activé et que l'équipement reçoit un message PTP valide, il règle sa source d'heure sur `ptp`. L'équipement donne la priorité au PTP par rapport au SNTP.
- ▶ La valeur *Local offset [min]* permet de spécifier la différence entre l'heure locale et l'heure du champ *System time (UTC)*.
- ☐ Pour que l'équipement utilise le fuseau horaire de votre PC, cliquez sur le bouton *Set time from PC*. L'équipement calcule la différence entre l'heure locale et l'UTC et saisit la valeur obtenue dans le champ *Local offset [min]*.

Commentaire : L'équipement fournit l'option pour obtenir le décalage local depuis un serveur DHCP.

- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`clock set <YYYY-MM-DD> <HH:MM:SS>`	Régler l'heure système de l'équipement.
`clock timezone offset <-780..840>`	Saisir la différence en minutes entre l'heure locale et l'UTC reçu.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

4.1.2 Passage automatique à l'heure d'été

Lorsque vous utilisez l'équipement dans un fuseau horaire pour lequel un passage à l'heure d'été est prévu, vous pouvez régler le passage automatique à l'heure d'été dans l'onglet *Daylight saving time*.

Lorsque l'heure d'été est activée, l'équipement avance l'heure système locale d'1 heure au moment du passage à l'heure d'été. À la fin de l'heure d'été, l'équipement recule l'heure système locale d'1 heure. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Time > Basic Settings*, onglet *Daylight saving time*.
- ☐ Afin de sélectionner un profil préréglé dédié au début et à la fin de l'heure d'été, cliquez sur le bouton *Profile...* dans le cadre *Operation*.
- ☐ Lorsqu'aucun profil d'heure d'été correspondant n'est disponible, vous pouvez spécifier les moments auxquels les changements d'heure sont effectués dans les champs *Summertime begin* et *Summertime end*.
  Pour ces deux points de référence temporels, spécifiez le mois, la semaine du mois, le jour de la semaine et l'heure du jour.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`clock summer-time mode <disable|recurring|eu|usa>`	Configurer le passage automatique à l'heure d'été : activer/désactiver la fonction correspondante ou utiliser un profil.
`clock summer-time recurring start`	Saisir le début de l'heure d'été.
`clock summer-time recurring end`	Saisir la fin de l'heure d'été.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

4.2 SNTP

Le protocole SNTP (Simple Network Time Protocol) vous permet de synchroniser l'heure du système sur votre réseau. L'équipement prend en charge la fonction de client SNTP et de serveur SNTP.

Le serveur SNTP fournit le temps universel coordonné (UTC). L'UTC correspond à l'heure relative à la mesure du temps universel coordonné. L'UTC est le même dans le monde entier et ne prend pas en compte les décalages horaires locaux.

SNTP est une version simplifiée du protocole NTP (Network Time Protocol). Les paquets de données des protocoles SNTP et NTP sont identiques. Les serveurs NTP et SNTP servent donc de source d'heure pour les clients SNTP.

Commentaire : Les informations relatives aux serveurs SNTP fournies dans ce chapitre s'appliquent également aux serveurs NTP.

SNTP prend en charge les modes opérationnels suivants pour la transmission de l'heure :

- *Unicast*
  En mode opérationnel *Unicast*, un client SNTP envoie une requête à un serveur SNTP et attend une réponse de la part de ce serveur.
- *Broadcast*
  En mode opérationnel *Broadcast*, un serveur SNTP envoie des messages SNTP au réseau selon des intervalles spécifiés. Les clients SNTP reçoivent ces messages SNTP et les évaluent.

Dans un environnement IPv6, le mode de fonctionnement *Broadcast* fonctionne comme suit :

- Le client SNTP écoute uniquement les messages du serveur SNTP dont l'adresse *Multicast*IPv6 est définie sur `ff05::101` comme adresse cible IPv6.
- Le serveur SNTP envoie uniquement des messages SNTP à l'adresse *Multicast*`ff05::101`. Le serveur SNTP n'envoie pas de messages SNTP dont l'adresse de lien local est l'adresse source IPv6.

Tableau 16 : Classes d'adresses IPv4 cibles pour le mode opérationnel Broadcast

Adresse IPv4 cible	Envoi de paquets SNTP à
`0.0.0.0`	Personne
`224.0.1.1`	Adresse *Multicast* pour les messages SNTP
`255.255.255.255`	Adresse *Broadcast*

Commentaire : Un serveur SNTP en mode opérationnel *Broadcast* répond également aux requêtes directes issues de clients SNTP en mode *Unicast*. Les clients SNTP travaillent quant à eux soit en mode opérationnel *Unicast* soit en mode opérationnel *Broadcast*.

4.2.1 Préparation

Exécutez les étapes suivantes :

- ☐ Tracez un plan du réseau comprenant les équipements utilisant le SNTP afin d'avoir une vue d'ensemble de la transmission de l'heure.
  Lors de la planification, veuillez noter que la précision de l'heure dépend des temps de retard des messages SNTP. Afin de minimiser les temps de retard et leur variance, placez un serveur SNTP dans chaque segment de serveur. Chacun de ces serveurs SNTP synchronise sa propre heure système en tant que client SNTP avec son serveur SNTP parent (cascade SNTP). Le serveur SNTP placé le plus haut dans la cascade SNTP dispose de l'accès le plus direct à l'heure source de référence.

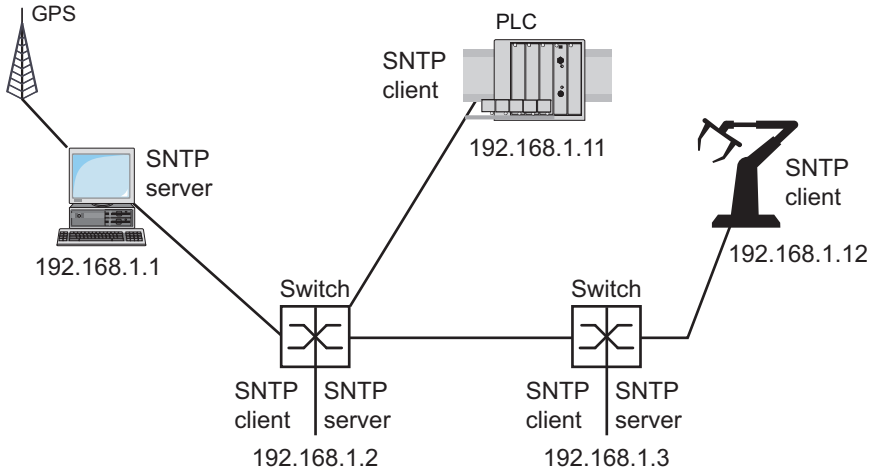


Figure 19 : Exemple de cascade SNTP

Commentaire : Pour une distribution précise de l'heure, utilisez de préférence des composants de réseau qui transmettent les paquets SNTP avec un temps de transmission faible et uniforme (latence) entre les serveurs SNTP et des clients SNTP (routeurs et commutateurs).

- Un client SNTP envoie ses requêtes à un maximum de 4 serveurs SNTP configurés. En l'absence de réponse de la part du 1er serveur SNTP, le client SNTP envoie ses requêtes au second serveur SNTP. Lorsque cette requête échoue également, elle envoie la requête au 3e et enfin au 4e serveur SNTP. Si aucun de ces serveurs SNTP ne répond, le client SNTP perd sa synchronisation. Le client SNTP envoie périodiquement des requêtes de manière cyclique à chaque serveur jusqu'à ce qu'un serveur SNTP lui fournisse une heure valide.

Commentaire : L'équipement offre la possibilité d'obtenir une liste d'adresses IP de serveurs SNTP de la part d'un serveur DHCP.

- Lorsqu'aucune source d'heure de référence n'est disponible, définissez un équipement doté d'un serveur SNTP comme source d'heure de référence. Ajustez l'heure système à intervalles réguliers.

4.2.2 Définition des réglages du client SNTP

En tant que client SNTP, l'équipement obtient les informations temporelles de la part des serveurs SNTP ou NTP et synchronise son horloge système en conséquence. Pour ce faire, exécutez les étapes suivantes :

- Ouvrez la boîte de dialogue *Time > SNTP > Client*.
- Réglez le mode opérationnel SNTP.
  Dans le cadre *Configuration*, sélectionnez l'une des valeurs suivantes dans le champ *Mode* :
  - `unicast`
    L'équipement envoie une requête à un serveur SNTP et attend une réponse de la part de ce serveur.
  - `broadcast`
    L'équipement attend les messages *Broadcast* ou *Multicast* de la part des serveurs SNTP sur le réseau.
- Pour synchroniser l'heure une seule fois, cochez la case *Disable client after successful sync*. Après la synchronisation, l'équipement désactive la fonction *SNTP Client*.
- Le tableau affiche le serveur SNTP auquel le client SNTP envoie une requête en mode opérationnel *Unicast*. Le tableau contient jusqu'à 4 définitions de serveur SNTP.
- Pour ajouter une entrée de tableau, cliquez sur le bouton .
- Spécifiez les données de connexion du serveur SNTP.
- Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .
- Le champ *State* affiche l'état actuel de la fonction *SNTP Client*.

Tableau 17 : Réglages du client SNTP pour l'exemple

Équipement	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Fonction *SNTP Client*	`Off`	`On`	`On`	`On`	`On`

Tableau 17 : Réglages du client SNTP pour l'exemple (cont

Équipement	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Configuration: *Mode*	unicast	unicast	unicast	unicast	unicast
Request interval [s]	30	30	30	30	30
Adresse(s) *SNTP Server*	–	192.168.1.1	192.168.1.2 192.168.1.1	192.168.1.2 192.168.1.1	192.168.1.3 192.168.1.2 192.168.1.1

4.2.3 Définition des réglages de serveur SNTP

Lorsque l'équipement fonctionne en tant que serveur SNTP, il distribue son heure système en temps universel coordonné (UTC) sur le réseau. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Time > SNTP > Server*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Afin d'activer le mode opérationnel *Broadcast*, sélectionnez le bouton radio *Broadcast admin mode* dans le cadre *Configuration*.
  En mode opérationnel *Broadcast*, le serveur SNTP envoie des messages SNTP au réseau selon des intervalles spécifiés. Le serveur SNTP répond également aux requêtes issues de clients SNTP en mode opérationnel *Unicast*.
  - ☐ Dans le champ *Broadcast destination address*, spécifiez l'adresse IPv4 à laquelle le serveur SNTP envoie les paquets SNTP. Définissez une adresse *Broadcast* ou une adresse *Multicast*.
    Dans un environnement IPv6, vous ne pouvez pas définir l'adresse IPv6 à laquelle le serveur SNTP envoie les paquets SNTP. Le serveur SNTP utilise l'adresse *Multicast*-`ff05::101` comme adresse cible IPv6.
  - ☐ Dans le champ *Broadcast UDP port*, spécifiez le numéro du port UDP auquel le serveur SNTP envoie les paquets SNTP en mode opérationnel *Broadcast*.
  - ☐ Dans le champ *Broadcast VLAN ID*, spécifiez l'ID du VLAN auquel le serveur SNTP envoie les paquets SNTP en mode opérationnel *Broadcast*.
  - ☐ Dans le champ *Broadcast send interval [s]*, saisissez l'intervalle avec lequel le serveur SNTP de l'équipement envoie des paquets *Broadcast* SNTP.

Commentaire : À l'exception du champ *Broadcast destination address*, tous les autres réglages sont applicables aux serveurs SNTP IPv4 et IPv6.

- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.
- ▶ Le champ *State* affiche l'état actuel de la fonction *SNTP Server*.

Tableau 18 : Réglages pour l'exemple

Équipement	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Fonction *SNTP Server*	*On*	*On*	*On*	*Off*	*Off*
UDP port	123	123	123	123	123
Broadcast admin mode	case non cochée	case non cochée	case non cochée	case non cochée	case non cochée
Broadcast destination address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Broadcast UDP port	123	123	123	123	123

Tableau 18 : Réglages pour l'exemple (cont

Équipement	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Broadcast VLAN ID	1	1	1	1	1
Broadcast send interval [s]	128	128	128	128	128
Disable server at local time source	case non cochée	case non cochée	case non cochée	case non cochée	case non cochée

4.3 PTP

Afin que les applications contrôlées via LAN fonctionnent sans latence, une gestion précise du temps est nécessaire. Avec le protocole PTP (Precision Time Protocol), la norme IEEE 1588 décrit une méthode qui permet une synchronisation précise des horloges du réseau.

PTP permet une synchronisation avec une précision de quelques 100 ns. PTP utilise Multicasts pour les messages de synchronisation, ce qui permet de limiter la charge du réseau.

4.3.1 Types d'horloges

PTP définit les rôles de « maître » et d'« esclave » pour les horloges du réseau :
- Une horloge maîtresse (source de temps de référence) distribue ses informations temporelles.
- Une horloge esclave se synchronise avec le signal de temps reçu de l'horloge maîtresse.

Boundary Clock

Le délai de transmission (latence) dans les routeurs et les commutateurs a un effet mesurable sur la précision de la transmission. Pour corriger ces imprécisions, PTP définit ce que l'on appelle des Boundary Clocks.

Dans un segment de réseau, une Boundary Clock est la source de temps de référence (horloge maîtresse) sur laquelle les horloges esclaves subordonnées se synchronisent. En général, les routeurs et les commutateurs assument le rôle de Boundary Clock.

La Boundary Clock reçoit quant à elle l'heure d'une source de temps de référence de niveau supérieur (Grand Master).

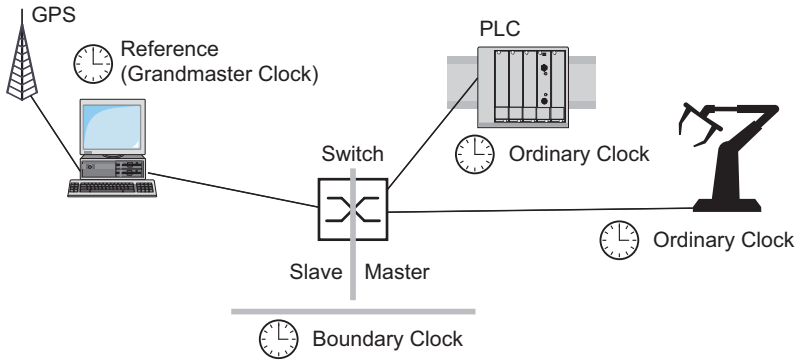


Figure 20 : Position de la Boundary Clock dans un réseau

Transparent Clock

Les commutateurs assument généralement le rôle de Transparent Clock pour permettre une grande précision en cascade. La Transparent Clock est une horloge Slave qui corrige son propre temps de transmission lorsqu'elle transmet les messages de synchronisation reçus.

Ordinary Clock

Le protocole PTP désigne l'horloge d'un équipement terminal par le terme « Ordinary Clock ». Une Ordinary Clock fonctionne soit comme une horloge maîtresse, soit comme une horloge esclave.

4.3.2 Algorithme de la meilleure horloge maîtresse

Les équipements participant au protocole PTP désignent un équipement du réseau comme source de temps de référence (Grand Master). L'algorithme « Best Master Clock » est utilisé pour déterminer la précision des horloges disponibles sur le réseau.

L'algorithme « Best Master Clock » évalue les critères suivants :
- *Priority 1*
- *Clock class*
- *Clock accuracy*
- *Clock variance*
- *Priority 2*

L'algorithme évalue d'abord la valeur du champ *Priority 1* des équipements participants. L'équipement ayant la plus petite valeur dans le champ *Priority 1* devient la source de temps de référence (Grandmaster). Si plusieurs équipements ont la même valeur, l'algorithme utilise le critère suivant. Lorsque cette valeur est également la même, l'algorithme utilise le critère qui suit celui-ci. Si ces valeurs sont les mêmes pour plusieurs équipements, la plus petite valeur du champ *Clock identity* détermine quel équipement est désigné comme source de temps de référence (Grandmaster).

Dans les réglages de la Boundary Clock, l'équipement vous permet de spécifier individuellement les valeurs de *Priority 1* et *Priority 2*. Cela vous permet d'influencer quel équipement sera la source de temps de référence (Grandmaster) dans le réseau.

4.3.3 Mesure du délai

Le délai des messages de synchronisation entre les équipements affecte la précision. La mesure du délai permet aux équipements de prendre en compte le délai moyen.

PTP version 2 offre les méthodes suivantes pour la mesure du délai :
- `e2e` (End to End)
  L'horloge esclave mesure le délai de transmission des messages de synchronisation à l'horloge maîtresse.

- *e2e-optimized*
  L'horloge esclave mesure le délai de transmission des messages de synchronisation à l'horloge maîtresse.
  Cette méthode n'est disponible que pour les Transparent Clocks. L'équipement transmet les messages de synchronisation envoyés par Multicast uniquement à l'horloge maîtresse, ce qui permet de limiter la charge du réseau. Lorsque l'équipement reçoit un message de synchronisation d'une autre horloge maîtresse, il transmet les messages de synchronisation uniquement à ce nouveau port.
  Lorsque l'équipement ne connaît pas d'horloge maîtresse, il transmet les messages de synchronisation à tous les ports.
- *p2p* (Peer to Peer)
  L'horloge esclave mesure le délai de transmission des messages de synchronisation à l'horloge maîtresse.
  En outre, l'horloge maîtresse mesure le délai de chaque horloge esclave, même à travers les ports bloqués. Cela présuppose que l'horloge maîtresse et l'horloge esclave supportent le mode pair à pair (*p2p*).
  En cas d'interruption d'un anneau redondant, par exemple, l'horloge esclave devient l'horloge maîtresse et l'horloge maîtresse devient l'horloge esclave. Cette commutation se fait sans perte de précision, car les horloges connaissent déjà le délai dans l'autre sens.

4.3.4 Domaines PTP

L'équipement transmet des messages de synchronisation uniquement depuis et vers les équipements du même domaine PTP. L'équipement vous permet de définir individuellement le domaine pour la Boundary Clock et pour la Transparent Clock.

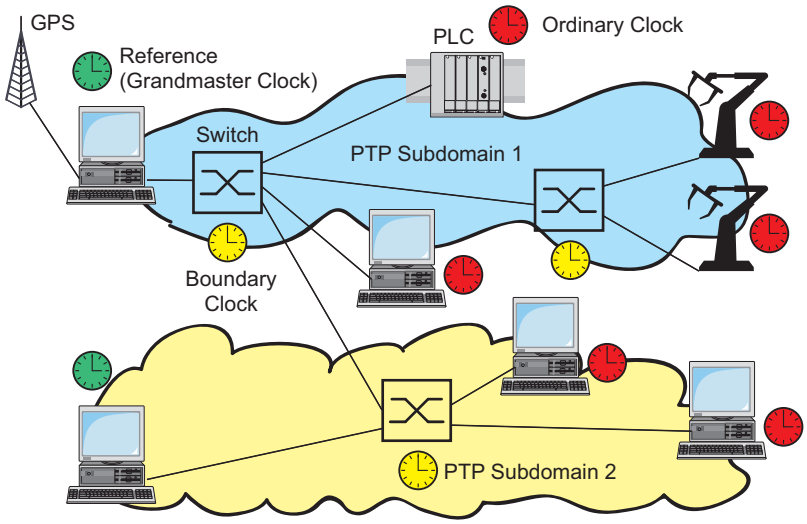


Figure 21 : Exemple de domaines PTP

4.3.5 Utilisation du PTP

Afin de synchroniser les horloges avec précision grâce au protocole PTP, n'utilisez que des commutateurs dotés d'une Boundary Clock ou d'une Transparent Clock comme nœuds.

Exécutez les étapes suivantes :

- ☐ Afin d'avoir une vue d'ensemble de la distribution des horloges, tracez un plan du réseau comprenant les équipements participants au PTP.
- ☐ Spécifiez le rôle de chaque commutateur participant (Boundary Clock ou Transparent Clock). Dans l'équipement, ce réglage est appelé *PTP mode*.

Tableau 19 : Réglages possibles du mode PTP

Mode PTP	Application
`v2-boundary-clock`	En tant que Boundary Clock, l'équipement distribue les messages de synchronisation aux horloges esclaves du segment de réseau subordonné. La Boundary Clock reçoit quant à elle l'heure d'une source de temps de référence de niveau supérieur (Grand Master).
`v2-transparent-clock`	En tant que Transparent Clock, l'équipement transmet les messages de synchronisation reçus après que ceux-ci aient été corrigés du délai de la Transparent Clock.

- ☐ Activez PTP sur chaque commutateur participant.
  PTP est alors configuré de manière largement automatique.
- ☐ Activez PTP sur les équipements terminaux.
- ☐ L'équipement vous permet d'influencer quel équipement du réseau est désigné comme horloge de référence (Grand Master). Pour ce faire, modifiez la valeur par défaut dans les champs *Priority 1* et *Priority 2* pour la *Boundary Clock*.

5 Administration des profils de configuration

Si vous modifiez les réglages de l'équipement en cours de fonctionnement, ce dernier sauvegarde les modifications dans sa mémoire (*RAM*). Après redémarrage, les réglages sont perdus.

Pour conserver les modifications après un redémarrage, l'équipement vous permet de sauvegarder les réglages dans un profil de configuration dans la mémoire non volatile (*NVM*). Pour permettre un basculement rapide sur d'autres réglages, la mémoire non volatile offre un espace de stockage pour différents profils de configuration.

Si une mémoire externe est connectée, l'équipement sauvegarde automatiquement une copie du profil de configuration dans la mémoire externe (*ENVM*). Vous pouvez désactiver cette fonction.

5.1 Détection des réglages modifiés

L'équipement sauvegarde les modifications apportées aux réglages en cours de fonctionnement dans sa mémoire volatile (*RAM*). Le profil de configuration dans la mémoire non volatile (*NVM*) reste inchangé jusqu'à ce que vous sauvegardiez explicitement les réglages modifiés. En attendant, les profils de configuration dans la mémoire et dans la mémoire non volatile sont différents. L'équipement vous permet de détecter les réglages modifiés.

5.1.1 Mémoire volatile (RAM) et mémoire non volatile (NVM)

Vous pouvez reconnaître si le profil de configuration stocké dans la mémoire volatile (*RAM*) est différent du profil de configuration « selected » (sélectionné) dans la mémoire non volatile (*NVM*). Pour ce faire, exécutez les étapes suivantes :

- ☐ Vérifiez la barre d'état en haut du menu :
  - – Lorsqu'une icône clignote, les profils de configuration sont différents.
  - – Lorsqu'aucune icône n'est visible, les profils de configuration sont identiques.

Ou :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Load/Save*.
- ☐ Vérifiez l'état de la case à cocher dans le cadre *Information* :
  - – Lorsque la case n'est pas cochée, les profils de configuration sont différents.
  - – Lorsque la case est cochée, les profils de configuration sont identiques.

```
show config status

Configuration Storage sync State
--------------------------------
running-config to NV.....................out of sync
...
```

5.1.2 Mémoire externe (EAM) et mémoire non volatile (NVM)

Vous pouvez également reconnaître si la copie dans la mémoire externe (EAM) est différente du profil de configuration dans la mémoire non volatile (*NVM*). Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Load/Save*.
- ☐ Vérifiez l'état de la case à cocher dans le cadre *Information* :
  - Lorsque la case n'est pas cochée, les profils de configuration sont différents.
  - Lorsque la case est cochée, les profils de configuration sont identiques.

```
show config status

Configuration Storage sync State
--------------------------------
...
NV to EAM.................................out of sync
...
```

5.2 Sauvegarde des réglages

5.2.1 Sauvegarde du profil de configuration dans l'équipement

Si vous modifiez les réglages de l'équipement en cours de fonctionnement, ce dernier sauvegarde les modifications dans sa mémoire (RAM). Pour conserver les modifications après redémarrage, sauvegardez le profil de configuration dans la mémoire non volatile (*NVM*).

Sauvegarde d'un profil de configuration

L'équipement sauvegarde les réglages dans le profil de configuration « sélectionné » dans la mémoire non volatile (*NVM*).

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Load/Save*.
- ☐ Vérifiez que le profil de configuration requis est « sélectionné ».
  Le profil de configuration « sélectionné » se reconnaît à la case cochée dans la colonne *Selected*.
- ☐ Cliquez sur le bouton  .

`show config profiles nvm`	Affiche les profils de configuration contenus dans la mémoire non volatile (`nvm`).
`enable`	Basculez sur le mode Privileged EXEC.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

Copie de réglages dans un profil de configuration

L'équipement vous permet de sauvegarder les réglages en mémoire (RAM) dans un profil de configuration autre que le profil de configuration « sélectionné ». Ainsi, vous créez un nouveau profil de configuration dans la mémoire non volatile (*NVM*) ou vous en écrasez un existant.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Load/Save*.
- ☐ Cliquez sur le bouton  puis sur l'élément *Save as...*
  La boîte de dialogue affiche la fenêtre *Save as...*.
- ☐ Dans le champ *Name*, modifiez le nom du profil de configuration. Si vous conservez le nom proposé, l'équipement écrase un profil existant du même nom.
- ☐ Cliquez sur le bouton *Ok*.

Le nouveau profil de configuration a la désignation « Selected ».

`show config profiles nvm`	Affiche les profils de configuration contenus dans la mémoire non volatile (`nvm`).
`enable`	Basculez sur le mode Privileged EXEC.
`copy config running-config nvm profile <string>`	Sauvegardez les réglages actuels dans le profil de configuration nommé `<string>` dans la mémoire non volatile (`nvm`). Le cas échéant, l'équipement écrase un profil de configuration du même nom. Le nouveau profil de configuration a la désignation « Selected ».

Sélection d'un profil de configuration

Lorsque la mémoire non volatile (*NVM*) contient plusieurs profils de configuration, vous pouvez sélectionner n'importe quel de ces profils de configuration. L'équipement sauvegarde les réglages dans le profil de configuration « sélectionné ». Lors d'un redémarrage, l'équipement charge les réglages du profil de configuration « sélectionné » dans la mémoire (`RAM`).

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Load/Save*.

Le tableau affiche les profils de configuration présents dans l'équipement. Le profil de configuration « sélectionné » se reconnaît à la case cochée dans la colonne *Selected*.

- ☐ Dans le tableau, sélectionnez l'entrée du profil de configuration sauvegardé dans la mémoire non volatile (*NVM*).
- ☐ Cliquez sur le bouton ☰ puis sur l'élément *Select*.

Dans la colonne *Selected*, la case du profil de configuration est désormais `cochée`.

`enable`	Basculez sur le mode Privileged EXEC.
`show config profiles nvm`	Affiche les profils de configuration contenus dans la mémoire non volatile (`nvm`).
`configure`	Basculez sur le mode de configuration.
`config profile select nvm 1`	Identifiant du profil de configuration. Notez le nom adjacent du profil de configuration.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

5.2.2 Sauvegarde du profil de configuration dans la mémoire externe

Lorsqu'une mémoire externe est connectée et que vous sauvegardez un profil de configuration, l'équipement sauvegarde automatiquement une copie dans la *Selected external memory*. Dans le réglage par défaut, la fonction est activée. Vous pouvez désactiver cette fonction.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > External Memory*.
- ☐ Cochez la case dans la colonne *Backup config when saving* pour permettre à l'équipement de sauvegarder automatiquement une copie dans la mémoire externe durant le processus d'enregistrement.
- ☐ Pour désactiver la fonction, décochez la case dans la colonne *Backup config when saving*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`config envm config-save usb`	Activez la fonction. Lorsque vous sauvegardez un profil de configuration, l'équipement sauvegarde une copie dans la mémoire externe. `usb` = mémoire USB externe
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

5.2.3 Sauvegarde du profil de configuration sur un serveur distant

L'équipement vous permet de sauvegarder automatiquement le profil de configuration sur un serveur distant. La condition préalable est que vous activiez a fonction avant de sauvegarder le profil de configuration.

Après avoir sauvegardé le profil de configuration dans la mémoire non volatile (*NVM*), l'équipement envoie une copie à l'URL spécifiée.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Load/Save*.
  Dans le cadre *Backup config on a remote server when saving*, exécutez les étapes suivantes :
- ☐ Dans le champ *URL*, spécifiez le serveur ainsi que le chemin et le nom de fichier du profil de configuration sauvegardé.
- ☐ Cliquez sur le bouton *Set credentials*.
  La boîte de dialogue affiche la fenêtre *Credentials*.
- ☐ Saisissez les identifiants de connexion requis pour vous authentifier sur le serveur distant.
- ☐ Dans la liste d'options *Operation*, activez la fonction.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`show config remote-backup`	Vérifiez l'état de la fonction.
`configure`	Basculez sur le mode de configuration.
`config remote-backup destination`	Saisissez l'URL cible pour la sauvegarde du profil de configuration.
`config remote-backup username`	Saisissez le nom d'utilisateur pour vous authentifier sur le serveur distant.
`config remote-backup password`	Saisissez le mot de passe pour vous authentifier sur le serveur distant.
`config remote-backup operation`	Activez la fonction.

Si le transfert vers le serveur distant échoue, l'équipement consigne cet événement dans le fichier log (System Log).

5.2.4 Exportation d'un profil de configuration

Cet équipement vous permet de sauvegarder un profil de configuration sur un serveur sous forme de fichier XML. Si vous utilisez l'interface utilisateur graphique, vous pouvez sauvegarder le fichier XML directement sur votre PC.

Conditions préalables :
- Pour sauvegarder le fichier sur un serveur, vous avez besoin d'un serveur configuré sur le réseau.
- Pour sauvegarder le fichier sur un serveur SCP ou SFTP, vous avez aussi besoin du nom d'utilisateur et du mot de passe permettant d'accéder à ce serveur.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Load/Save*.
- ☐ Dans le tableau, sélectionnez l'entrée du profil de configuration requis.

Exportez le profil de configuration vers votre PC. Pour ce faire, exécutez les étapes suivantes :

- ☐ Cliquez sur le lien dans la colonne *Profile name*.
- ☐ Sélectionnez l'emplacement de stockage et spécifiez le nom du fichier.
- ☐ Cliquez sur le bouton *Ok*.

Le profil de configuration est désormais sauvegardé sous forme de fichier XML à l'emplacement spécifié.

Exportez le profil de configuration vers un serveur distant. Pour ce faire, exécutez les étapes suivantes :

- ☐ Cliquez sur le bouton puis sur l'élément *Export...*.
  La boîte de dialogue affiche la fenêtre *Export...*.
- ☐ Dans le champ *URL*, spécifiez l'URL du fichier sur le serveur distant.
  - ☐ Pour sauvegarder le fichier sur un serveur FTP, spécifiez l'URL pour le fichier au format suivant :
    `ftp://<utilisateur>:<mot de passe>@<adresse IP>:<port>/<nom du fichier>`
  - ☐ Pour sauvegarder le fichier sur un serveur TFTP, spécifiez l'URL pour le fichier au format suivant :
    `tftp://<adresse IP>/<chemin>/<nom du fichier>`
  - ☐ Pour sauvegarder le fichier sur un serveur SCP ou SFTP, spécifiez l'URL pour le fichier dans l'un des formats suivants :
    `scp://` ou `sftp://<utilisateur>:<mot de passe>@<adresse IP>/<chemin>/<nom du fichier>`
    `scp://` ou `sftp://<adresse IP>/<chemin>/<nom du fichier>`
    Lorsque vous cliquez sur le bouton *Ok*, l'équipement affiche la fenêtre *Credentials*. Vous y renseignez les champs *User name* et *Password* pour vous connecter au serveur.
- ☐ Cliquez sur le bouton *Ok*.
  Le profil de configuration est désormais sauvegardé sous forme de fichier XML à l'emplacement spécifié.

`show config profiles nvm`	Affiche les profils de configuration contenus dans la mémoire non volatile (`nvm`).
`enable`	Basculez sur le mode Privileged EXEC.
`copy config running-config remote tftp://<IP_address>/ <path>/<file_name>`	Sauvegardez les réglages actuels sur un serveur TFTP.
`copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>`	Sauvegardez le profil de configuration sélectionné dans la mémoire non volatile (`nvm`) sur un serveur FTP.
`copy config nvm profile config3 remote tftp://<IP_address>/ <path>/<file_name>`	Sauvegardez les profils de configuration `config3` dans la mémoire non volatile (`nvm`) sur un serveur TFTP.
`copy config nvm profile config3 remote ftp://<IP_address>:<port>/<path>/<file_name>`	Sauvegardez le profil de configuration `config3` dans la mémoire non volatile (`nvm`) sur un serveur FTP.

5.3 Chargement des réglages

Si vous sauvegardez plusieurs profils de configuration dans la mémoire, vous pouvez charger un profil de configuration différent.

5.3.1 Activation d'un profil de configuration

La mémoire non volatile de l'équipement peut contenir plusieurs profils de configuration. Si vous activez un profil de configuration sauvegardé dans la mémoire non volatile (*NVM*), vous modifiez immédiatement les réglages dans l'équipement. L'équipement n'a pas besoin de redémarrer.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Load/Save*.
- ☐ Dans le tableau, sélectionnez l'entrée du profil de configuration requis.
- ☐ Cliquez sur le bouton ☰ puis sur l'élément *Activate*.

L'équipement copie les réglages dans la mémoire (RAM) et se déconnecte de l'interface utilisateur graphique. L'équipement utilise immédiatement les réglages du profil de configuration.

- ☐ Rechargez l'interface utilisateur graphique.
- ☐ Connectez-vous de nouveau.

Dans la colonne *Selected*, la case du profil de configuration préalablement activé est cochée.

`show config profiles nvm`	Affiche les profils de configuration contenus dans la mémoire non volatile (nvm).
`enable`	Basculez sur le mode Privileged EXEC.
`copy config nvm profile config3 running-config`	Activez les réglages du profil de configuration config3 dans la mémoire non volatile (nvm). L'équipement copie les réglages dans la mémoire volatile et interrompt la connexion à l'interface de ligne de commande. L'équipement utilise immédiatement les réglages du profil de configuration config3.

5.3.2 Chargement du profil de configuration depuis la mémoire externe

Si une mémoire externe est connectée, l'équipement charge automatiquement un profil de configuration depuis la mémoire externe après redémarrage. L'équipement vous permet de sauvegarder ces réglages dans un profil de configuration dans la mémoire non volatile.

Lorsque la mémoire externe contient le profil de configuration d'un équipement identique, vous pouvez transférer les réglages d'un équipement à un autre.

Exécutez les étapes suivantes :

☐ Vérifiez que l'équipement charge un profil de configuration depuis la mémoire externe après redémarrage.
Dans le réglage par défaut, la fonction est activée. Si la fonction est désactivée, activez-la de nouveau comme suit :

☐ Ouvrez la boîte de dialogue *Basic Settings > External Memory*.

☐ Dans la colonne *Config priority*, sélectionnez la valeur `first`.

☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`config envm load-priority usb first`	Activez la fonction. Après redémarrage, l'équipement charge un profil de configuration depuis la mémoire externe. `usb` = mémoire USB externe
`show config envm settings`	Affiche les réglages de la mémoire externe (`envm`).

```
Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ----------------
usb    ok          [x]         [x]           first
```

`save`	Sauvegardez les réglages dans un profil de configuration dans la mémoire non volatile (*NVM*) de l'équipement.

A l'aide de l'interface de ligne de commande, l'équipement vous permet de copier les réglages depuis la mémoire externe directement dans la mémoire non volatile (*NVM*).

`show config profiles nvm`	Affiche les profils de configuration contenus dans la mémoire non volatile (`nvm`).
`enable`	Basculez sur le mode Privileged EXEC.
`copy config envm profile config3 nvm`	Copiez le profil de configuration `config3` de la mémoire externe (`envm`) dans la mémoire non volatile (`nvm`).

L'équipement peut aussi charger automatiquement un profil de configuration depuis un fichier script lors du processus de démarrage.

Conditions préalables :

- Vérifiez que la mémoire externe est connectée avec de démarrer l'équipement.
- Le répertoire racine de la mémoire externe contient un fichier texte `startup.txt` avec le contenu `script=<nom_fichier>`. La chaîne de substitution `<nom_fichier>` représente le fichier script que l'équipement exécute lors du processus de démarrage.
- Le répertoire racine de la mémoire externe contient le fichier script. Vous pouvez sauvegarder le script avec un nom spécifié par l'utilisateur. Sauvegardez le fichier avec l'extension `.cli`.

Commentaire : Vérifiez que le script sauvegardé dans la mémoire externe n'est pas vide. Si le script est vide, l'équipement charge le profil de configuration suivant conformément aux réglages de priorité de configuration.

Après application du script, l'équipement sauvegarde automatiquement le profil de configuration depuis le fichier script sous forme de fichier XML dans la mémoire externe. Lorsque vous saisissez la commande appropriée dans le fichier script, vous pouvez désactiver cette fonction :

☐ `no config envm config-save usb`
L'équipement ne crée pas de copie dans la mémoire USB externe.

Lorsque le fichier script contient une commande incorrecte, l'équipement n'applique pas cette commande durant le processus de démarrage. L'équipement consigne l'événement dans le fichier log (System Log).

5.3.3 Importation d'un profil de configuration

L'équipement vous permet d'importer depuis un serveur un profil de configuration sauvegardé sous forme de fichier XML. Si vous utilisez l'interface utilisateur graphique, vous pouvez importer le fichier XML directement depuis votre PC.

Conditions préalables :

- Pour sauvegarder le fichier sur un serveur, vous avez besoin d'un serveur configuré sur le réseau.
- Pour sauvegarder le fichier sur un serveur SCP ou SFTP, vous avez aussi besoin du nom d'utilisateur et du mot de passe permettant d'accéder à ce serveur.

Exécutez les étapes suivantes :

☐ Ouvrez la boîte de dialogue *Basic Settings > Load/Save*.

☐ Cliquez sur le bouton ☰ puis sur l'élément *Import...*.
La boîte de dialogue affiche la fenêtre *Import...*.

☐ Dans la liste déroulante *Select source*, sélectionnez l'emplacement d'où l'équipement importe le profil de configuration.
- *PC/URL*
  L'équipement importe le profil de configuration depuis le PC local ou depuis un serveur distant.
- *External memory*
  L'équipement importe le profil de configuration depuis la mémoire externe.

Importez le profil de configuration depuis le PC local ou depuis un serveur distant. Pour ce faire, exécutez les étapes suivantes :

- ☐ Importez le profil de configuration :
  - ☐ Lorsque le fichier se trouve sur un serveur FTP, spécifiez l'URL du fichier au format suivant :
    `ftp://<utilisateur>:<mot de passe>@<adresse IP>:<port>/<nom du fichier>`
  - ☐ Lorsque le fichier se trouve sur un serveur TFTP, spécifiez l'URL du fichier au format suivant :
    `tftp://<adresse IP>/<chemin>/<nom du fichier>`
  - ☐ Lorsque le fichier se trouve sur un serveur SCP ou SFTP, spécifiez l'URL du fichier dans l'un des formats suivants :
    `scp://` ou `sftp://<adresse IP>/<chemin>/<nom du fichier>`
    Lorsque vous cliquez sur le bouton *Start*, l'équipement affiche la fenêtre *Credentials*. Vous y renseignez les champs *User name* et *Password* pour vous connecter au serveur.
    `scp://` ou `sftp://<utilisateur>:<mot de passe>@<adresse IP>/<chemin>/<nom du fichier>`
- ☐ Dans le cadre *Destination*, spécifiez où l'équipement sauvegarde le profil de configuration importé :
  - ☐ Dans le champ *Profile name*, spécifiez le nom sous lequel l'équipement sauvegarde le profil de configuration.
  - ☐ Dans le champ *Storage type*, spécifiez l'emplacement de stockage pour le profil de configuration.
- ☐ Cliquez sur le bouton *Ok*.

L'équipement copie le profil de configuration dans la mémoire spécifiée.

Si vous spécifiez la valeur `ram` dans le cadre *Destination*, l'équipement déconnecte l'interface utilisateur graphique et utilise les réglages immédiatement.

Importez le profil de configuration depuis la mémoire externe. Pour ce faire, exécutez les étapes suivantes :

- ☐ Dans le cadre *Import profile from external memory*, liste déroulante *Profile name*, sélectionnez le nom du profil de configuration à importer.
  La condition préalable est que la mémoire externe contienne un profil de configuration exporté.
- ☐ Dans le cadre *Destination*, spécifiez où l'équipement sauvegarde le profil de configuration importé :
  - ☐ Dans le champ *Profile name*, spécifiez le nom sous lequel l'équipement sauvegarde le profil de configuration.
- ☐ Cliquez sur le bouton *Ok*.

L'équipement copie le profil de configuration dans la mémoire non volatile (*NVM*) de l'équipement.

Si vous spécifiez la valeur `ram` dans le cadre *Destination*, l'équipement déconnecte l'interface utilisateur graphique et utilise les réglages immédiatement.

`enable`	Basculez sur le mode Privileged EXEC.
`copy config remote ftp://<IP_address>:<port>/<path>/<file_name> running-config`	Importez et activez les réglages d'un profil de configuration sauvegardé sur un serveur FTP. L'équipement copie les réglages dans la mémoire volatile et interrompt la connexion à l'interface de ligne de commande. L'équipement utilise immédiatement les réglages du profil de configuration importé.
`copy config remote tftp://<IP_address>/ <path>/<file_name> running-config`	Importez et activez les réglages d'un profil de configuration sauvegardé sur un serveur TFTP. L'équipement copie les réglages dans la mémoire volatile et interrompt la connexion à l'interface de ligne de commande. L'équipement utilise immédiatement les réglages du profil de configuration importé.
`copy config remote sftp://<user name>:<password>@<IP_address>/<path>/<file_name> running-config`	Importez et activez les réglages d'un profil de configuration sauvegardé sur un serveur SFTP. L'équipement copie les réglages dans la mémoire volatile et interrompt la connexion à l'interface de ligne de commande. L'équipement utilise immédiatement les réglages du profil de configuration importé.
`copy config remote ftp://<IP_address>:<port>/<path>/<file_name> nvm profile config3`	Importez les réglages d'un profil de configuration sauvegardé sur un serveur FTP et sauvegardez les réglages dans le profil de configuration `config3` dans la mémoire non volatile (`nvm`).
`copy config remote tftp://<IP_address>/<path>/<file_name> nvm profile config3`	Importez les réglages d'un profil de configuration sauvegardé sur un serveur TFTP et sauvegardez les réglages dans le profil de configuration `config3` dans la mémoire non volatile (`nvm`).

5.4 Réinitialisation de l'équipement à l'état à la livraison

Si vous réinitialisez les réglages dans l'équipement à l'état à la livraison, l'équipement supprime les profils de configuration dans la mémoire volatile et dans la mémoire non volatile.

Si une mémoire externe est connectée, l'équipement supprime aussi les profils de configuration sauvegardés dans la mémoire externe.

Ensuite, l'équipement redémarre et charge les réglages d'usine.

5.4.1 Utilisation de l'interface utilisateur graphique ou de l'interface de ligne de commande

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Load/Save*.
- ☐ Cliquez sur le bouton , puis sur *Back to factory...*.
  La boîte de dialogue affiche un message.
- ☐ Cliquez sur le bouton *Ok*.

L'équipement supprime les profils de configuration dans la mémoire (`RAM`) et dans la mémoire non volatile (*`NVM`*).

Si une mémoire externe est connectée, l'équipement supprime aussi les profils de configuration sauvegardés dans la mémoire externe.

Après un court laps de temps, l'équipement redémarre et charge les réglages par défaut.

`enable`	Basculez sur le mode Privileged EXEC.
`clear factory`	Supprime les profils de configuration de la mémoire non volatile et de la mémoire externe. Si une mémoire externe est connectée, l'équipement supprime aussi les profils de configuration sauvegardés dans la mémoire externe. Après un court laps de temps, l'équipement redémarre et charge les réglages par défaut.

5.4.2 Utilisation du moniteur système

Prérequis :

- Votre PC est connecté avec la liaison série de l'équipement à l'aide d'un câble de terminaison.

Exécutez les étapes suivantes :

- ☐ Redémarrez l'équipement.
- ☐ Pour basculer sur le moniteur système, appuyez sur la touche <1> dans les 3 secondes lorsque vous y êtes invité durant le redémarrage.
  L'équipement charge le moniteur système.
- ☐ Pour basculer du menu principal sur le menu `Manage configurations`, appuyez sur la touche <4>.
- ☐ Pour exécuter la commande `Clear configs and boot params`, appuyez sur la touche <1>.

- Pour charger les réglages standard, appuyez sur la touche <Entrée>.
  L'équipement supprime les profils de configuration dans la mémoire (RAM) et dans la mémoire non volatile (*NVM*).
  Si une mémoire externe est connectée, l'équipement supprime aussi les profils de configuration sauvegardés dans la mémoire externe.
- Pour basculer sur le menu principal, appuyez sur la touche <q>.
- Pour redémarrer l'équipement avec les réglages standard, appuyez sur la touche <q>.

6 Chargement des mises à jour de logiciels

Schneider Electric œuvre en permanence à l'amélioration et au développement de ses logiciels. Vérifiez régulièrement s'il existe une version mise à jour des logiciels afin de bénéficier d'avantages supplémentaires. Vous trouverez des informations et des logiciels à télécharger dans les pages dédiées aux produits Schneider Electric sur Internet à l'adresse www.schneider-electric.com.

L'équipement vous offre les options suivantes pour mettre à jour le logiciel :
- Mise à jour du logiciel à partir du PC
- Mise à jour du logiciel depuis un serveur
- Mise à jour du logiciel depuis la mémoire externe
- Chargement d'une version précédente du logiciel

Commentaire : Les réglages de l'équipement sont conservés après la mise à jour du logiciel de l'équipement.

La version du logiciel installé sur l'équipement est affichée dans la boîte de dialogue de connexion de l'interface utilisateur graphique.

Pour afficher la version du logiciel installé lorsque vous êtes déjà connecté, exécutez les étapes suivantes :

☐ Ouvrez la boîte de dialogue *Basic Settings > Software*.
Le champ *Running version* affiche le numéro de version et la date de création du logiciel que l'équipement a chargé lors du dernier redémarrage et qu'il exécute actuellement.

`enable`	Basculez sur le mode Privileged EXEC.
`show system info`	Affiche les informations relatives au système, comme le numéro de version et la date de création du logiciel que l'équipement a chargé lors du dernier redémarrage et qu'il exécute actuellement.

6.1 Mise à jour du logiciel à partir du PC

La condition préalable est que le fichier image du logiciel de l'équipement soit sauvegardé sur un support de données qui soit accessible à partir d'un PC.

Exécutez les étapes suivantes :

☐ Accédez au dossier dans lequel le fichier image du logiciel de l'équipement est sauvegardé.

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Software*.
- ☐ Effectuez un glisser-déposer du fichier image dans la zone  . Vous pouvez également cliquer sur la zone pour sélectionner le fichier.
- ☐ Pour démarrer la procédure de mise à jour, cliquez sur le bouton *Start*.
  Dès que la procédure de mise à jour se termine correctement, l'équipement affiche un message indiquant que le logiciel a été mise à jour avec succès.
  Lors du redémarrage, l'équipement charge le logiciel de l'équipement installé.

6.2 Mise à jour du logiciel depuis un serveur

Pour mettre à jour le logiciel via SFTP ou SCP, vous avez besoin d'un serveur sur lequel le fichier image du logiciel de l'équipement est sauvegardé.

Pour mettre à jour le logiciel à l'aide de TFTP, SFTP ou SCP, vous avez besoin d'un serveur sur lequel le fichier image du logiciel de l'équipement est sauvegardé.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Software*.
- ☐ Dans le cadre *Software update*, champ*URL*, saisissez l'URL pour le fichier image au format suivant :
  - ▶ Lorsque le fichier image est sauvegardé sur un serveur FTP :
    `ftp://<adresse_IP>:<port>/<chemin>/<nom_fichier_image>.bin`
  - ▶ Lorsque le fichier image est sauvegardé sur un serveur TFTP :
    `tftp://<adresse_IP>/<chemin>/<nom_fichier_image>.bin`
  - ▶ Lorsque le fichier image est sauvegardé sur un serveur SCP ou SFTP :
    `scp://` ou `sftp://<adresse_IP>/<chemin>/<nom_fichier_image>.bin`
    `scp://` ou `sftp://<nom_utilisateur>:<mot_passe>@<adresse_IP>/<chemin>/<nom_fichier_image>.bin`
    Lorsque vous saisissez l'URL sans le nom d'utilisateur et le mot de passe, l'équipement affiche la fenêtre *Credentials*. Vous y saisissez les identifiants de connexion requis pour vous connecter au serveur.
- ☐ Pour démarrer la procédure de mise à jour, cliquez sur le bouton *Start*.
  L'équipement copie le logiciel actuellement exécuté sur l'équipement dans la mémoire de sauvegarde.
  Dès que la procédure de mise à jour se termine correctement, l'équipement affiche un message indiquant que le logiciel a été mise à jour avec succès.
  Lors du redémarrage, l'équipement charge le logiciel de l'équipement installé.

`enable`	Basculez sur le mode Privileged EXEC.
`copy firmware remote tftp://10.0.1.159/product.bin system`	Transférez le fichier `product.bin` du serveur TFTP avec l'adresse IP `10.0.1.159` à l'équipement.

6.3 Mise à jour du logiciel depuis la mémoire externe

6.3.1 Manuellement—initiée par l'administrateur

L'équipement vous permet de mettre à jour le logiciel de l'équipement en quelques clics. La condition préalable est que le fichier image du logiciel de l'équipement se trouve dans la mémoire externe.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Software*.
- ☐ Dans le tableau, mettez en surbrillance la ligne qui affiche le nom du fichier image choisi dans la mémoire externe.
- ☐ Effectuez un clic droit pour afficher le menu contextuel.
- ☐ Pour démarrer la procédure de mise à jour, cliquez sur l'élément *Update* dans le menu contextuel.
  L'équipement copie le logiciel actuellement exécuté sur l'équipement dans la mémoire de sauvegarde.
  Dès que la procédure de mise à jour se termine correctement, l'équipement affiche un message indiquant que le logiciel a été mise à jour avec succès.
  Lors du redémarrage, l'équipement charge le logiciel de l'équipement installé.

6.3.2 Automatiquement—initiée par l'équipement

Lorsque les fichiers suivants se trouvent dans la mémoire externe durant un redémarrage, l'équipement met à jour son logiciel automatiquement :

- le fichier image du logiciel de l'équipement,
- un fichier texte `startup.txt` avec le contenu `autoUpdate=<nom_fichier_image>.bin`.

La condition préalable est de cocher, dans la boîte de dialogue *Basic Settings > External Memory*, la case dans la colonne *Software auto update*. Il s'agit du réglage par défaut de l'équipement.

Exécutez les étapes suivantes :

- ☐ Copiez le fichier image du nouveau logiciel de l'équipement dans le répertoire principal de la mémoire externe. Utilisez uniquement un fichier image adapté pour l'équipement.
- ☐ Créez un fichier texte `startup.txt` dans le répertoire principal de la mémoire externe.
- ☐ Ouvrez le fichier `startup.txt` dans l'éditeur de texte et ajoutez la ligne suivante : `autoUpdate=<nom_fichier_image>.bin`
- ☐ Installez la mémoire externe dans l'équipement.

☐ Redémarrez l'équipement.
Durant le processus de démarrage, l'équipement vérifie automatiquement les critères suivants :
- Une mémoire externe est-elle connectée ?
- Y a-t-il un fichier `startup.txt` dans le répertoire principal de la mémoire externe ?
- Le fichier image spécifié dans le fichier `startup.txt` existe-t-il ?
- La version du logiciel du fichier image est-elle plus récente que celle du logiciel actuellement exécuté sur l'équipement ?

Lorsque les critères sont satisfaits, l'équipement démarre la procédure de mise à jour.
L'équipement copie le logiciel actuellement exécuté sur l'équipement dans la mémoire de sauvegarde.
Dès que la procédure de mise à jour se termine correctement, l'équipement redémarre automatiquement et charge la nouvelle version du logiciel.

☐ Vérifiez le résultat de la procédure de mise à jour. Le fichier log dans la boîte de dialogue *Diagnostics > Report > System Log* contient l'un des messages suivants :
- `S_watson_AUTOMATIC_SWUPDATE_SUCCESS`
  Mise à jour du logiciel terminée correctement
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED`
  Mise à jour du logiciel annulée
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE`
  Mise à jour du logiciel annulée parce que le fichier image est incorrect
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
  Mise à jour du logiciel annulée parce que l'équipement n'a pas sauvegardé le fichier image

6.4 Chargement d'une version précédente du logiciel

L'équipement vous permet de remplacer le logiciel de l'équipement par une version précédente. Les réglages de base dans l'équipement sont conservés une fois le logiciel de l'équipement remplacé.

Commentaire : Seuls les réglages des fonctions disponibles dans le nouveau logiciel de l'équipement sont perdus.

7 Configuration des ports

Les fonctions de configuration de port suivantes sont disponibles.
- Activation/désactivation d'un port
- Sélection du mode opérationnel
- Mode Gigabit Ethernet pour les ports

7.1 Activation/désactivation d'un port

Dans le réglage par défaut, chaque port est activé. Pour un niveau de sécurité d'accès accru, désactivez les ports non connectés. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.
- ☐ Pour activer un port, cochez la case dans la colonne *Port on*.
- ☐ Pour désactiver un port, décochez la case dans la colonne *Port on*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`no shutdown`	Activez l'interface.

7.2 Sélection du mode opérationnel

Dans le réglage par défaut, les ports sont définis sur le mode opérationnel *Automatic configuration*.

Commentaire : La configuration automatique active est prioritaire sur la configuration manuelle.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.
- ☐ Si l'équipement connecté sur ce port requiert un réglage fixe, exécutez les étapes suivantes :
  - ☐ Désactivez la fonction. Décochez la case dans la colonne *Automatic configuration*.
  - ☐ Dans la colonne *Manual configuration*, saisissez le mode opérationnel souhaité (débit de transmission, mode duplex).
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`no auto-negotiate`	Désactivez le mode de configuration automatique.
`speed 100 full`	Vitesse du port 100 MBit/s, full duplex

7.3 Mode Gigabit Ethernet pour les ports

L'équipement prend en charge 2.5 Gbit/s sur différentes interfaces avec l'un des transceivers SFP suivants :

- M-SFP-2.5-MM/LC EEC
- M-SFP-2.5-SM-/LC EEC
- M-SFP-2.5-SM/LC EEC
- M-SFP-2.5-SM+/LC EEC

Le type de transceiver raccordé détermine la vitesse du port. L'équipement ne permet pas de définir la vitesse manuellement. Les ports avec 2,5 Gbit/s de vitesse ne peuvent pas prendre en charge des débits de données de 100 Mbit/s.

Commentaire : Vous trouverez plus d'informations sur les numéros de commande des transceivers au chapitre « Accessoires » du manuel d'utilisation dédié à l'installation.

7.3.1 Exemple

Vous utilisez le mode Gigabit Ethernet pour bénéficier d'une bande passante accrue pour les uplinks. Pour utiliser cette fonction, insérez un transceiver adapté à l'emplacement approprié.

Exécutez les étapes suivantes :

☐ Ouvrez la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.

La colonne *Manual configuration* affiche la valeur `2.5 Gbit/s FDX` pour les ports avec un transceiver 2.5 Gbit/s SFP raccordé.

Vous ne pouvez pas modifier la vitesse.

```
show port 1/1
```

Affiche les paramètres pour l'emplacement `1` port `1`. L'entrée de liste `Physical Mode` affiche la valeur `2500 full` pour les ports avec un transceiver 2.5 Gbit/s SFP inséré.

```
Interface.....................1/1
Name..........................My interface
--
Cable-crossing Setting........-
Physical Mode.................2500 full
Physical Status...............-
```

8 Assistance relative à la protection contre l'accès non autorisé

L'équipement offre diverses fonctions contribuant à la protection de l'équipement contre l'accès non autorisé.

Une fois que vous avez configuré l'équipement, procédez aux étapes suivantes afin de réduire le risque d'accès non autorisé à l'équipement.

- Modification de la communauté SNMPv1/v2
- Désactivation de SNMPv1/v2
- Désactivation de HTTP
- Utilisation de vos propres certificats HTTPS
- Utilisation de votre propre clé SSH
- Désactivation de Telnet
- Désactivation de Ethernet Switch Configurator
- Activation de la restriction d'accès IP
- Ajustement des délais d'expiration de session

8.1 Modification de la communauté SNMPv1/v2

SNMPv1/v2 n'utilise pas le chiffrement. Chaque paquet SNMP contient l'adresse IP de l'expéditeur et le nom de communauté en texte clair avec lequel l'expéditeur accède à l'équipement. Lorsque SNMPv1/v2 est activé, l'équipement permet à tout utilisateur connaissant le nom de communauté d'accéder à l'équipement.

Les noms de communauté `user` dédiés aux accès en lecture et les noms de communauté `admin` dédiés aux accès en écriture sont réglés par défaut dans l'équipement. Si vous utilisez SNMPv1 ou SNMPv2, modifiez le noms de communauté par défaut. Traitez les noms de communauté avec discrétion. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > SNMPv1/v2 Community*.

La boîte de dialogue affiche les communautés configurées.

- ☐ Pour la communauté `Write`, spécifiez le nom de communauté dans la colonne *Name*.
  - Jusqu'à 32 caractères alphanumériques sont autorisés.
  - L'équipement fait la distinction entre majuscules et minuscules.
  - Spécifiez un nom de communauté différent du nom de communauté défini pour l'accès en écriture.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`snmp community rw <community name>`	Spécifier la communauté pour l'accès en lecture/écriture.
`show snmp community`	Afficher les communautés qui ont été configurées.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

8.2 Désactivation de SNMPv1/v2

Si vous avez besoin de SNMPv1 ou SNMPv2, utilisez ces protocoles uniquement dans des environnements protégés contre l'écoute clandestine. SNMPv1 et SNMPv2 n'utilisent pas le chiffrement. Les paquets SNMP contiennent la communauté en texte clair. Nous recommandons d'utiliser SNMPv3 dans l'équipement et de désactiver l'accès via SNMPv1 et SNMPv2. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > Server*, onglet *SNMP*.

La boîte de dialogue affiche les réglages du serveur SNMP.

- ☐ Pour désactiver le protocole SNMPv1, décochez la case *SNMPv1*.
- ☐ Pour désactiver le protocole SNMPv2, décochez la case *SNMPv2*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`no snmp access version v1`	Désactiver le protocole SNMPv1.
`no snmp access version v2`	Désactiver le protocole SNMPv2.
`show snmp access`	Afficher les réglages du serveur SNMP.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

8.3 Désactivation de HTTP

Le serveur Web fournit le protocole HTTP ou HTTPS à l'interface utilisateur graphique. Les connexions HTTPS sont chiffrées, alors que les connexions HTTP ne le sont pas.

Le protocole HTTP est activé par défaut. Si vous désactivez le protocole HTTP, aucun accès non chiffré à l'interface utilisateur graphique n'est possible. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > Server*, onglet *HTTP*.
- ☐ Pour désactiver le protocole HTTP, sélectionnez le bouton radio `Off` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`no http server`	Désactiver le protocole HTTP.

Lorsque le protocole HTTP est désactivé, vous pouvez uniquement accéder à l'interface utilisateur graphique de l'équipement via HTTPS. Dans la barre d'adresse du navigateur Web, saisissez `https://` avant l'adresse IP de l'équipement.

Lorsque le protocoles HTTPS est désactivé et que vous désactivez également HTTP, l'interface utilisateur graphique est inaccessible. Pour l'interface utilisateur graphique, activez le serveur HTTPS à l'aide de l'interface de ligne de commande. Pour ce faire, exécutez les étapes suivantes :

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`https server`	Activer le protocole HTTPS.

8.4 Désactivation de Telnet

L'équipement vous permet d'accéder à distance à l'administration de l'équipement à l'aide de Telnet ou SSH. Les connexions Telnet ne sont pas chiffrées, alors que les connexions SSH sont chiffrées.

Le serveur Telnet est activé par défaut dans l'équipement. Si vous désactivez Telnet, l'accès à distance non chiffré à l'interface de ligne de commande n'est plus possible. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > Server*, onglet *Telnet*.
- ☐ Pour désactiver le serveur Telnet, sélectionnez le bouton radio `Off` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`no telnet server`	Désactiver le serveur Telnet.

Lorsque le serveur SSH est désactivé et que vous désactivez également Telnet, l'accès à l'interface de ligne de commande n'est possible qu'à travers l'interface série de l'équipement. Pour travailler à distance avec l'interface de ligne de commande, activez SSH. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > Server*, onglet *SSH*.
- ☐ Afin d'activer le serveur *SSH*, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`ssh server`	Activez le serveur SSH.

8.5 Désactiver la restriction de l'accès à Ethernet Switch Configurator

Ethernet Switch Configurator vous permet d'affecter les paramètres IP à l'équipement via le réseau lors de la mise en service. Ethernet Switch Configurator communique dans le VLAN d'administration de l'équipement sans chiffrement ni authentification.

Une fois que l'équipement a été mis en service, nous recommandons de régler Ethernet Switch Configurator sur lecture seule ou de désactiver entièrement l'accès à Ethernet Switch Configurator. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Network*.
- ☐ Pour retirer l'autorisation en écriture du logiciel Ethernet Switch Configurator, spécifiez la valeur `readOnly` dans le champ *Access* du cadre *Ethernet Switch Configurator protocol v1/v2*.
- ☐ Pour désactiver entièrement l'accès à Ethernet Switch Configurator, sélectionnez le bouton radio `Off` dans le cadre *Ethernet Switch Configurator protocol v1/v2*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

`enable`	Basculez sur le mode Privileged EXEC.
`network ethernet-switch-conf mode read-only`	Désactiver l'autorisation en écriture du logiciel Ethernet Switch Configurator.
`no network ethernet-switch-conf operation`	Désactiver l'accès à Ethernet Switch Configurator.

8.6 Activation de la restriction de l'accès IP

Avec le réglage par défaut, vous pouvez accéder à l'administration de l'équipement depuis une adresse IP quelconque et avec les protocoles pris en charge.

La restriction de l'accès IP vous permet de limiter l'accès à l'administration de l'équipement aux plages d'adresses IP sélectionnées et aux protocoles basés sur IP sélectionnés.

Exemple :

L'équipement doit être accessible uniquement depuis le réseau d'entreprise à l'aide de l'interface utilisateur graphique. L'administrateur dispose également d'un accès à distance via SSH. Le réseau d'entreprise dispose de la plage d'adresses `192.168.1.0/24` et de l'accès à distance depuis un réseau mobile à l'aide de la plage d'adresses IP `109.237.176.0/24`. Le programme de l'application SSH connaît l'empreinte de la clé RSA.

Tableau 20 : Paramètres de la restriction de l'accès IP

Paramètre	Réseau d'entreprise	Réseau de téléphonie mobile
Adresse de réseau	`192.168.1.0`	`109.237.176.0`
Masque réseau	`24`	`24`
Protocoles souhaités	https, snmp	ssh

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > IP Access Restriction*.
- ☐ Cochez la case située dans la colonne *Active* pour l'entrée.
  Cette entrée permet aux utilisateurs d'accéder à l'équipement depuis une adresse IP quelconque et à l'aide des protocoles pris en charge.

La plage d'adresses du réseau d'entreprise :

- ☐ Pour ajouter une entrée de tableau, cliquez sur le bouton  .
- ☐ Spécifiez la plage d'adresses du réseau d'entreprise dans la colonne *IP address range* : `192.168.1.0/24`
- ☐ Pour l'intervalle d'adresses du réseau d'entreprise, désactivez les protocoles non souhaités. Les cases à cocher *HTTPS*, *SNMP* et *Active* restent cochées.

La plage d'adresses du réseau de téléphonie mobile :

- ☐ Pour ajouter une entrée de tableau, cliquez sur le bouton  .
- ☐ Spécifiez la plage d'adresses du réseau mobile dans la colonne *IP address range* : `109.237.176.0/24`
- ☐ Pour l'intervalle d'adresses du réseau mobile, désactivez les protocoles non souhaités. Les cases à cocher *SSH* et *Active* restent cochées.

Avant d'activer cette fonction, vérifiez qu'au moins une entrée active du tableau vous permet l'accès. Sinon, la connexion à l'équipement prend fin lorsque vous modifiez les réglages. L'accès à l'administration de l'équipement n'est possible qu'à l'aide de l'interface de ligne de commande via l'interface série de l'équipement.

- ☐ Afin d'activer la restriction de l'accès IP, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

`enable`	Basculez sur le mode Privileged EXEC.
`show network management access global`	Indique si la restriction de l'accès IP est activée ou désactivée.
`show network management access rules`	Afficher les entrées qui ont été configurées.
`no network management access operation`	Désactiver la restriction de l'accès IP.
`network management access add 2`	Créer l'entrée pour la plage d'adresses du réseau d'entreprise. Numéro du prochain index disponible dans cet exemple : `2`.
`network management access modify 2 ip 192.168.1.0`	Spécifier l'adresse IP du réseau d'entreprise.
`network management access modify 2 mask 24`	Spécifier le masque réseau du réseau d'entreprise.
`network management access modify 2 ssh disable`	Désactiver SSH pour la plage d'adresses du réseau d'entreprise. Répéter l'opération pour chaque protocole non souhaité.
`network management access add 3`	Créer une entrée pour la plage d'adresses du réseau mobile. Numéro du prochain index disponible dans cet exemple : `3`.
`network management access modify 3 ip 109.237.176.0`	Spécifier l'adresse IP du réseau mobile.
`network management access modify 3 mask 24`	Spécifier le masque réseau du réseau de téléphonie mobile.
`network management access modify 3 snmp disable`	Désactiver SNMP pour la plage d'adresses du réseau de téléphonie mobile. Répéter l'opération pour chaque protocole non souhaité.
`no network management access status 1`	Désactiver l'entrée par défaut. Cette entrée permet aux utilisateurs d'accéder à l'équipement depuis une adresse IP quelconque et à l'aide des protocoles pris en charge.
`network management access status 2`	Activer une entrée pour la plage d'adresses du réseau d'entreprise.
`network management access status 3`	Activer une entrée pour la plage d'adresses du réseau mobile.
`show network management access rules`	Afficher les entrées qui ont été configurées.
`network management access operation`	Activer la restriction de l'accès IP.

8.7 Ajustement des délais d'expiration de session

L'équipement vous permet de mettre automatiquement fin à la session suite à l'inactivité de l'utilisateur connecté. Le délai d'expiration est la période d'inactivité écoulée depuis la dernière action de l'utilisateur.

Vous pouvez spécifier un délai d'expiration pour les applications suivantes :
- Sessions d'interface de ligne de commande à l'aide d'une connexion SSH
- Sessions d'interface de ligne de commande via une connexion Telnet
- Sessions d'interface de ligne de commande à l'aide d'une connexion série
- Interface utilisateur graphique

Délai d'expiration pour les sessions d'interface de ligne de commande à l'aide d'une connexion SSH

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > Server*, onglet *SSH*.
- ☐ Spécifiez le délai d'expiration en minutes dans le champ *Session timeout [min]* du cadre *Configuration*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`ssh timeout <0..160>`	Spécifier le délai d'expiration en minutes pour les sessions d'interface de ligne de commande à l'aide une connexion SSH.

Délai d'expiration pour les sessions d'interface de ligne de commande via une connexion Telnet

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > Server*, onglet *Telnet*.
- ☐ Spécifiez le délai d'expiration en minutes dans le champ *Session timeout [min]* du cadre *Configuration*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`telnet timeout <0..160>`	Spécifier le délai d'expiration en minutes pour les sessions d'interface de ligne de commande à l'aide d'une connexion Telnet.

Délai d'expiration pour les sessions d'interface de ligne de commande à l'aide d'une connexion série

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > CLI*, onglet *Global*.
- ☐ Spécifiez le délai d'expiration en minutes dans le champ *Serial interface timeout [min]* du cadre *Configuration*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`cli serial-timeout <0..160>`	Spécifier le délai d'expiration en minutes pour les sessions d'interface de ligne de commande à l'aide d'une connexion série.

Délai d'expiration de l'interface utilisateur graphique

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > Web*.
- ☐ Spécifiez le délai d'expiration en minutes dans le champ *Web interface session timeout [min]* du cadre *Configuration*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`network management access web timeout <0..160>`	Spécifier la période d'expiration en minutes pour les sessions de l'interface utilisateur graphique

9 Commande du trafic de données

L'équipement vérifie les paquets de données à transférer conformément aux règles définies. Les paquets de données auxquels les règles s'appliquent sont soit transférés par l'équipement, soit bloqués. Si des paquets de données ne correspondent à aucune règle, l'équipement les bloque.

Les ports de routage auxquels aucune règle n'est affectée laissent passer les paquets. Dès que des règles sont affectées, elles sont traitées en priorité. Ensuite, l'action standard spécifiée de l'équipement est exécutée.

L'équipement fournit les fonctions suivantes pour la commande du flux de données :
- Commande de requête de service (Denial of Service, DoS)
- Accès refusé aux équipements en fonction de leur adresse IP ou MAC (Access Control List)

L'équipement observe et surveille le flux de données. L'équipement prend les résultats de l'observation et de la surveillance et les associe aux règles de sécurité du réseau pour générer ce que l'on appelle un tableau d'état. Sur la base de ce tableau d'état, l'équipement décide d'accepter, de dénier ou de rejeter les données.

Les paquets de données sont filtrés par l'équipement selon la séquence suivante :
- DoS … si `permit` ou `accept`, passage à la règle suivante
- ACL … si `permit` ou `accept`, passage à la règle suivante

9.1 Protection contre un accès non autorisé

Avec cette fonction, l'équipement vous aide à vous protéger contre des paquets de données non valides ou falsifiés destinés à certains services ou équipements. Vous avez la possibilité de spécifier des filtres afin de restreindre le flux de données à des fins de protection contre des attaques de type Denial of Service. Les filtres activés vérifient les paquets de données entrants et les rejettent dès qu'une correspondance avec le critère du filtre est trouvée.

La boîte de dialogue *Network Security > DoS > Global* contient 2 cadres dans lesquels vous activez les différents filtres. Pour les activer, cochez les cases correspondantes.

Dans le cadre *TCP/UDP*, vous activez jusqu'à 4 filtres qui n'influent que sur les paquets TCP et UDP. À l'aide de ce filtre, vous désactivez les scans des ports utilisés par les attaquants pour essayer de détecter les équipements et services proposés. Les filtres fonctionnent comme décrit ci-dessous :

Tableau 21 : Filtres DoS pour paquets TCP

Filtre	Action
Activate Null Scan Filter	L'équipement détecte et rejette les paquets TCP entrants présentant les propriétés suivantes : - Aucun drapeau TCP n'est défini. - Le numéro de séquence TCP est 0.

Tableau 21 : Filtres DoS pour paquets TCP

Filtre	Action
Activate Xmas Filter	L'équipement détecte et rejette les paquets TCP entrants présentant les propriétés suivantes : ▶ Les drapeaux TCP *FIN*, *URG* et *PSH* sont définis simultanément. ▶ Le numéro de séquence TCP est 0.
Activate SYN/FIN Filter	L'équipement détecte et rejette les paquets TCP entrants dans lesquels les drapeaux TCP *SYN* et *FIN* sont définis simultanément.
Activate Minimal Header Filter	L'équipement détecte et rejette les paquets TCP entrants dans lesquels l'en-tête TCP est trop court.

Le cadre *ICMP* propose 2 options de filtre pour les paquets ICMP. La fragmentation des paquets ICMP est le signe d'une attaque. Si vous activez ce filtre, l'équipement détecte les paquets ICMP fragmentés et les rejette. À l'aide du paramètre *Allowed payload size [byte]*, vous pouvez également spécifier la taille maximale admissible des données utiles pour les paquets ICMP. L'équipement rejette les paquets de données qui excèdent cette spécification en octets.

Commentaire : Vous pouvez combiner les filtres comme vous le souhaitez dans la boîte de dialogue *Network Security > DoS > Global*. Lorsque plusieurs filtres sont sélectionnés, un Ou logique s'applique : si le premier ou le deuxième (ou le troisième, etc.) filtre s'applique à un paquet de données, l'équipement le rejette.

9.2 ACL

Dans ce menu, vous pouvez saisir les paramètres des listes de contrôle d'accès (ACL).

L'équipement utilise les ACL pour filtrer les paquets de données reçus sur des VLAN ou sur des ports individuels ou multiples. Dans une ACL, vous spécifiez les règles que l'équipement utilise pour filtrer les paquets de données. Lorsque l'une de ces règles s'applique à un paquet, l'équipement applique au paquet les actions spécifiées dans la règle. Les actions disponibles sont les suivantes :
- autoriser (`permit`)
- rejeter (`deny`)
- rediriger sur un port donné (voir le champ *Redirection port*)
- copier en miroir (voir le champ *Mirror port*)

La liste ci-dessous contient des critères que vous pouvez appliquer pour filtrer les paquets de données :
- Adresse source ou cible d'un paquet (MAC)
- Adresse source ou cible d'un paquet de données (IPv4)
- Port source ou cible d'un paquet de données (IPv4)

Vous pouvez spécifier les types d'ACL suivants :
- ACL IP pour VLAN
- ACL IP pour ports
- ACL MAC pour VLAN
- ACL MAC pour ports

Lorsque vous affectez une ACL IP et une ACL MAC à la même interface, l'équipement utilise d'abord l'ACL IP pour filtre le flux de données. L'équipement applique les règles de l'ACL MAC une fois les paquets filtrés à l'aide de l'ACL IP. La priorité d'une ACL est indépendante de l'index d'une règle.

Au sein d'une ACL, l'équipement traite les règles dans l'ordre. L'index de chaque règle détermine l'ordre dans lequel l'équipement filtre le flux de données. Lorsque vous affectez une ACL à un port ou à un VLAN, vous pouvez spécifier sa priorité avec l'index. Plus le nombre est petit, plus la priorité est élevée. L'équipement traite d'abord la règle avec la priorité la plus élevée.

Si aucune des règles spécifiées dans une ACL ne s'applique à un paquet de données, la règle `deny` implicite s'applique. Ainsi, l'équipement rejette les paquets de données reçus.

Gardez à l'esprit que l'équipement met directement en œuvre la règle `deny` implicite.

Commentaire : Le nombre d'ACL disponibles dépend de l'équipement. Vous trouverez plus d'informations sur les valeurs des ACL au chapitre « Caractéristiques techniques » à la page 383.

Commentaire : Vous pouvez affecter une même ACL à un nombre quelconque de ports ou VLAN.

Le menu *ACL* contient les boîtes de dialogue suivantes :
- *ACL IPv4 Rule*
- *ACL MAC Rule*
- *ACL Assignment*

Ces boîtes de dialogue offrent les options suivantes :
- Spécification des règles des différents types d'ACL.
- Affectation des priorités requises aux règles.
- Affectation des ACL aux ports ou aux VLAN.

9.2.1 Création et modification de règles IPv4

Lors du filtrage des paquets de données IPv4, l'équipement vous permet de :
- créer de nouveaux groupes et règles ;
- ajouter de nouvelles règles à des groupes existants ;
- modifier une règle existante ;
- activer et désactiver des groupes et des règles ;
- supprimer des groupes et règles existants ;
- modifier l'ordre des règles existantes.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Network Security > ACL > IPv4 Rule*.
- ☐ Cliquez sur le bouton  .
  La boîte de dialogue affiche la fenêtre *Create*.
- ☐ Pour créer un groupe, spécifiez un nom évocateur dans le champ *Group name*. Vous pouvez combiner plusieurs règles dans un groupe.
- ☐ Pour ajouter une règle à un groupe existant, sélectionnez le nom du groupe dans le champ *Group name*.
- ☐ Dans le champ *Index*, vous spécifiez le numéro de la règle au sein de l'ACL.
  Ce numéro définit la priorité de la règle.
- ☐ Cliquez sur le bouton *Ok*.
  L'équipement ajoute la règle au tableau.
  Le groupe et le rôle sont immédiatement actifs.
  Pour désactiver un groupe ou des règles, décochez la case dans la colonne *Active*.
  Pour supprimer une règle, mettez en surbrillance l'entrée de tableau concernée et cliquez sur le bouton  .
- ☐ Modifiez les paramètres de la règle dans le tableau.
  Pour modifier une valeur, double-cliquez dans le champ concerné.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

Commentaire : L'équipement vous permet d'utiliser des caractères génériques avec les paramètres *Source IP address* et *Destination IP address*. Par exemple, si vous saisissez `192.168.?.?`, l'équipement autorise les adresses commençant par `192.168`.

Commentaire : La condition préalable pour modifier les valeurs dans les colonnes *Source TCP/UDP port* et *Destination TCP/UDP port* est de spécifier la valeur `tcp` ou `udp` dans la colonne *Protocol*.

Commentaire : La condition préalable pour modifier la valeur dans les colonnes *Redirection port* et *Mirror port* est de spécifier la valeur `permit` dans la colonne *Action*.

9.2.2 Création et configuration d'une ACL IP à l'aide de l'interface de ligne de commande

Dans l'exemple suivant, vous configurez des ACL pour bloquer les communications depuis les ordinateurs B et C vers l'ordinateur A via IP (TCP, UDP, etc.).

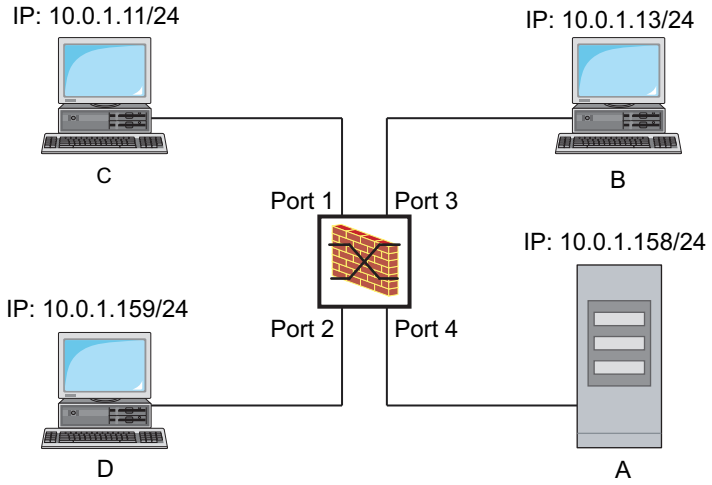


Figure 22 : Exemple d'une ACL IP

Exécutez les étapes suivantes :

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`ip access-list extended name filter1 deny src 10.0.1.11-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	Ajoutez une ACL IP avec le nom `filter1`. Ajoutez une règle refusant les paquets de données IP de `10.0.1.11` à `10.0.1.158`. Priorité `1` (priorité la plus haute).
`ip access-list extended name filter1 permit src any dst any`	Ajoutez une règle à l'ACL IP autorisant les paquets de données IP.
`show access-list ip filter1`	Affichez les règles de l'ACL IP `filter1`.
`ip access-list extended name filter2 deny src 10.0.1.13-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	Ajoutez une ACL IP avec le nom `filter2`. Ajoutez une règle refusant les paquets de données IP de `10.0.1.13` à `10.0.1.158`. Priorité `1` (priorité la plus haute).
`show access-list ip filter2`	Affichez les règles de l'ACL IP `filter2`.

9.2.3 Création et modification de règles MAC

Lors du filtrage des paquets de données MAC, l'équipement vous permet de :
- créer de nouveaux groupes et règles ;
- ajouter de nouvelles règles à des groupes existants ;
- modifier une règle existante ;
- activer et désactiver des groupes et des règles ;
- supprimer des groupes et règles existants ;
- modifier l'ordre des règles existantes.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Network Security > ACL > MAC Rule*.
- ☐ Cliquez sur le bouton  .
  La boîte de dialogue affiche la fenêtre *Create*.
- ☐ Pour créer un groupe, spécifiez un nom évocateur dans le champ *Group name*. Vous pouvez combiner plusieurs règles dans un groupe.
- ☐ Pour ajouter une règle à un groupe existant, sélectionnez le nom du groupe dans le champ *Group name*.
- ☐ Dans le champ *Index*, vous spécifiez le numéro de la règle au sein de l'ACL.
  Ce numéro définit la priorité de la règle.
- ☐ Cliquez sur le bouton *Ok*.
  L'équipement ajoute la règle au tableau.
  Le groupe et le rôle sont immédiatement actifs.
  Pour désactiver un groupe ou des règles, décochez la case dans la colonne *Active*.
  Pour supprimer une règle, mettez en surbrillance l'entrée de tableau concernée et cliquez sur le bouton  .
- ☐ Modifiez les paramètres de la règle dans le tableau.
  Pour modifier une valeur, double-cliquez dans le champ concerné.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

Commentaire : Dans les champs *Source MAC address* et *Destination MAC address*, vous pouvez utiliser des caractères génériques au format `FF:??:??:??:??:??` ou `??:??:??:??:00:01`. Utilisez des majuscules ici.

9.2.4 Création et configuration d'une ACL MAC à l'aide de l'interface de ligne de commande

Dans l'exemple suivant, AppleTalk et IPX doivent être exclus de tout le réseau. Pour ce faire, exécutez les étapes suivantes :

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`mac acl add 1 macfilter`	Ajoute une ACL MAC avec l'ID `1` et le nom `macfilter`.
`mac acl rule add 1 1 deny src any any dst any any etype appletalk`	Ajoute une règle en position `1` de l'ACL MAC avec l'ID `1` rejetant les paquets avec EtherType `0x809B (AppleTalk)`.
`mac acl rule add 1 2 deny src any any dst any any etype ipx-old`	Ajoute une règle en position `2` de l'ACL MAC avec l'ID `1` rejetant les paquets avec EtherType `0x8137 (IPX alt)`.
`mac acl rule add 1 3 deny src any any dst any any etype ipx-new`	Ajoute une règle en position `3` de l'ACL MAC avec l'ID `1` rejetant les paquets avec EtherType `0x8138 (IPX)`.
`mac acl rule add 1 4 permit src any any dst any any`	Ajoute une règle en position `4` de l'ACL MAC avec l'ID `1` transférant les paquets.
`show acl mac rules 1`	Affiche les règles de l'ACL MAC avec l'ID `1`.
`interface 1/1,1/2,1/3,1/4,1/5,1/6`	Basculez en mode de configuration des interfaces `1/1` à `1/6`.

`acl mac assign 1 in 1`	Affecte l'ACL MAC avec l'ID `1` à des paquets de données entrants (`1/1`) sur les interfaces `1/6` à `in`.
`exit`	Quitte le mode d'interface.
`show acl mac assignment 1`	Affiche l'affectation de l'ACL MAC avec l'ID `1` à des interfaces ou des VLAN.

9.2.5 Affectation d'ACL à un port ou un VLAN

Lorsque vous affectez des ACL à un port ou un VLAN, l'équipement offre les options suivantes :
- Sélection du port ou du VLAN.
- Spécification de la priorité de l'ACL.
- Sélection de l'ACL à l'aide du nom de groupe.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Network Security > ACL > Assignment*.
- ☐ Cliquez sur le bouton .
  La boîte de dialogue affiche la fenêtre *Create*.
  - ☐ Dans le champ *Port/VLAN*, spécifiez le port ou le VLAN souhaité.
  - ☐ Dans le champ *Priority*, spécifiez la priorité.
  - ☐ Dans le champ *Direction*, spécifiez les paquets de données auxquels l'équipement applique la règle.
  - ☐ Dans le champ *Group name*, spécifiez la règle que l'équipement affecte au port ou au VLAN.
- ☐ Cliquez sur le bouton *Ok*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

9.3 Contournement de l'authentification MAC

La fonction *MAC authorized bypass* permet aux clients ne prenant pas en charge la norme technique IEEE 802.1X, tels que les imprimantes et les fax, de s'authentifier sur le réseau à l'aide de leur adresse MAC. L'équipement vous permet de spécifier le format de l'adresse MAC utilisée pour authentifier les clients sur le serveur RADIUS.

Exemple :

Divisez l'adresse MAC en 6 groupes de 2 caractères. Utilisez des lettres majuscules et un double point en tant que séparateur : `AA:BB:CC:DD:EE:FF`

Utilisez la forme `xY-45uM_e` Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Network Security > 802.1X Port Authentication > Global*.
  Dans le cadre *MAC authentication bypass format options*, exécutez les étapes suivantes :
- ☐ Dans la liste déroulante *Group size*, sélectionnez la valeur `2`.
  L'équipement divise l'adresse MAC en 6 groupes de 2 caractères.
- ☐ Dans la liste déroulante *Group separator*, sélectionnez le caractère `:`.
- ☐ Dans la liste déroulante *Upper or lower case*, sélectionnez l'élément `upper-case`.
- ☐ Dans le champ *Password*, saisissez le mot de passe `xY-45uM_e`.
  L'équipement utilise ce mot de passe pour chaque client qui s'authentifie sur le serveur RADIUS. Si vous laissez le champ vide, l'équipement utilise l'adresse MAC formatée comme mot de passe.
- ☐ Pour sauvegarder temporairement les réglages, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`dot1x mac-authentication-bypass format group-size 2`	Spécifiez la taille du groupe `2`.
`dot1x mac-authentication-bypass format group-separator :`	Spécifiez le séparateur de groupe `:`.
`dot1x mac-authentication-bypass format letter-case upper-case`	Indique que l'équipement formate les données d'authentification en majuscules.
`dot1x mac-authentication-bypass password xY-45uM_e`	Spécifiez le mot de passe `xY-45uM_e`. L'équipement utilise ce mot de passe pour authentifier chaque client sur le serveur RADIUS.

10 Monitorage de la charge du réseau

L'équipement dispose de plusieurs fonctions qui vous permettent de réduire la charge du réseau :
- Distribution directe des paquets
- Multicasts
- Limiteur de charge
- Priorisation - QoS
- Contrôle de flux

10.1 Distribution directe des paquets

L'équipement réduit la charge du réseau avec la distribution directe des paquets.

Sur chacun de ses ports, l'équipement apprend l'adresse MAC de l'expéditeur des paquets de données reçus. L'équipement sauvegarde la combinaison « port et adresse MAC » dans son tableau d'adresses MAC (FDB).

En appliquant la méthode « Store and Forward », l'équipement met en mémoire tampon les données reçues et vérifie leur validité avant de les transférer. L'équipement rejette les paquets de données non valides et défectueux.

10.1.1 Apprentissage des adresses MAC

Lorsque l'équipement reçoit un paquet de données, il vérifie si l'adresse MAC de l'expéditeur est déjà sauvegardée dans le tableau des adresses MAC (FDB). Lorsque l'adresse MAC de l'expéditeur est inconnue, l'équipement génère une nouvelle entrée. L'équipement compare alors l'adresse MAC cible du paquet de données avec les entrées sauvegardées dans le tableau des adresses MAC (FDB) :
- L'équipement transfère les paquets avec une adresse MAC cible connue directement aux ports qui ont déjà reçu des paquets de données de cette adresse MAC.
- L'équipement transfère les paquets de données avec des adresses cibles inconnues, c'est-à-dire que l'équipement transfère ces paquets de données à chaque port.

10.1.2 Vieillissement des adresses MAC apprises

Les adresses qui n'ont pas été détectées par l'équipement pendant un laps de temps configurable (durée de vieillissement) sont supprimées du tableau des adresses MAC (FSB) par l'équipement. Un redémarrage ou une réinitialisation du tableau des adresses MAC supprime les entrées dans le tableau des adresses MAC (FDB).

10.1.3 Entrées d'adresses statiques

Outre l'apprentissage de l'adresse MAC de l'expéditeur, l'équipement permet également de définir manuellement les adresses MAC. Ces adresses MAC restent configurées et sont conservées en cas de réinitialisation du tableau des adresses MAC (FDB) ou de redémarrage de l'équipement.

Les entrées d'adresses statiques permettent à l'équipement de transférer des paquets de données directement aux ports sélectionnés. Si vous ne spécifiez aucun port cible, l'équipement rejette les paquets de données correspondants.

Vous pouvez gérer les entrées d'adresses statiques dans l'interface utilisateur graphique ou dans l'interface de ligne de commande.

Exécutez les étapes suivantes :

☐ Créez une entrée d'adresse statique.

☐ Ouvrez la boîte de dialogue *Switching > Filter for MAC Addresses*.

☐ Ajoutez une adresse MAC configurable par l'utilisateur :

- Cliquez sur le bouton  .
  La boîte de dialogue affiche la fenêtre *Create*.
- Dans le champ *Address*, spécifiez l'adresse MAC cible.
- Dans le champ *VLAN ID*, spécifiez l'ID du VLAN.
- Dans la liste *Port*, sélectionnez les ports auxquels l'équipement transfère les paquets de données avec l'adresse MAC cible spécifiée dans le VLAN indiqué.
  Si vous avez défini une adresse MAC Unicast dans le champ *Address*, sélectionnez un seul port.
  Si vous avez défini une adresse MAC Multicast dans le champ *Address*, sélectionnez un ou plusieurs ports.
  Si vous souhaitez que l'équipement rejette les paquets de données avec l'adresse MAC cible, ne sélectionnez aucun port.
- Cliquez sur le bouton *Ok*.

☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`mac-filter <MAC address>  <VLAN ID>`	Créez le filtre d'adresse MAC, qui comprend une adresse MAC et un VLAN-ID.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`mac-filter <MAC address>  <VLAN ID>`	Affectez le port à un filtre d'adresse MAC préalablement créé.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

☐ Convertissez une adresse MAC apprise en une entrée d'adresse statique.

- ☐ Ouvrez la boîte de dialogue *Switching > Filter for MAC Addresses*.
- ☐ Pour convertir une adresse MAC apprise en une entrée d'adresse statique, sélectionnez la valeur `permanent` dans la colonne *Status*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

☐ Désactivez une entrée d'adresse statique.

- ☐ Ouvrez la boîte de dialogue *Switching > Filter for MAC Addresses*.
- ☐ Pour désactiver une entrée d'adresse statique, sélectionnez la valeur `invalid` dans la colonne *Status*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`no mac-filter <MAC address>  <VLAN ID>`	Annulez l'affectation du filtre d'adresse MAC sur le port.
`exit`	Basculez sur le mode de configuration.
`no mac-filter <MAC address>  <VLAN ID>`	Supprimez le filtre d'adresse MAC, qui comprend un adresse MAC et un VLAN-ID.
`exit`	Basculez sur le mode Privileged EXEC.
`save`	Sauvegarder les réglages dans la mémoire non volatile (`nvm`) du profil sélectionné (« selected »).

☐ Supprimez les adresses MAC apprises.

- ☐ Pour supprimer les adresses apprises du tableau des adresses MAC (FDB), ouvrez la boîte de dialogue *Basic Settings > Restart* et cliquez sur le bouton *Reset MAC address table*.

`clear mac-addr-table`	Supprimez les adresses MAC apprises du tableau d'adresses MAC (FDB).

10.2 Multicasts

Par défaut, l'équipement transfère les paquets de données avec une adresse Multicast, c'est-à-dire que l'équipement transfère les paquets de données à chaque port. Cela entraîne une charge accrue du réseau.

L'utilisation de la fonction IGMP snooping peut réduire la charge du réseau générée par le trafic de données Multicast. IGMP snooping permet à l'équipement d'envoyer des paquets de données Multicast uniquement sur les ports auxquels les équipements « intéressés » par le Multicast sont connectés.

10.2.1 Exemple d'application Multicast

Des caméras de surveillance transmettent des images aux moniteurs dans la salle des machines et dans la salle de contrôle. Avec une transmission IP Multicast, les caméras transmettent leurs données graphiques via le réseau dans des paquets Multicast.

L'Internet Group Management Protocol (IGMP) organise le trafic de données Multicast entre les routeurs Multicast et les moniteurs. Les commutateurs réseau entre les routeurs Multicast et les moniteurs surveillent le trafic de données IGMP en permanence (« IGMP Snooping »).

Les commutateurs réseau sauvegardent les connexions pour recevoir un flux Multicast (rapport IGMP). L'équipement crée ensuite une entrée dans le tableau d'adresses MAC (FDB) et transfère les paquets Multicast uniquement aux ports sur lesquels il a précédemment reçu des reports IGMP.

10.2.2 IGMP Snooping

L'Internet Group Management Protocol (IGMP) décrit la distribution des informations Multicast entre les routeurs et les récepteurs sur la couche 3. IGMP Snooping décrit la fonction d'un commutateur réseau qui surveille en permanence le trafic IGMP et optimise ses propres réglages de transmission pour ce trafic de données.

La fonction *IGMP Snooping* dans l'équipement obéit à la norme technique RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).

Les routeurs Multicast avec une fonction *IGMP* activée demandent périodiquement (requête) l'enregistrement de flux Multicast afin de déterminer les membres du groupe Multicast IP associés. Les membres du groupe Multicast IP répondent avec un message Report (Rapport). Ce message Report (Rapport) contient les paramètres requis par la fonction *IGMP*. Le routeur Multicast saisit l'adresse du groupe Multicast IP tirée du message Report (Rapport) dans sa table de routage. Ainsi, il transfère les paquets de données avec ce groupe Multicast IP dans le champ d'adresse cible conformément à sa table de routage.

Lorsqu'ils quittent un groupe Multicast (IGMP version 2 et supérieures), les récepteurs se déconnectent avec un message « Leave » (Quitter) et n'envoient plus de messages Report (Rapport). S'il ne reçoit plus de messages Report (Rapport) de ce récepteur dans un délai donné (durée de vieillissement), le routeur Multicast supprime l'entrée d'un récepteur dans la table de routage.

Lorsque plusieurs routeurs Multicast IGMP sont dans le même réseau, l'équipement avec l'adresse IP la plus petite reprend la fonction de requête. En l'absence de tout routeur Multicast sur le réseau, vous pouvez activer la fonction de requête dans un commutateur réseau équipé en conséquence.

Un commutateur réseau qui connecte un récepteur Multicast à un routeur Multicast analyse les informations IGMP avec la méthode IGMP Snooping.

La méthode IGMP Snooping permet également aux commutateurs réseau d'utiliser la fonction *IGMP*. Un commutateur réseau sauvegarde les adresses MAC dérivées des adresses IP des récepteurs Multicast en tant qu'adresses Multicast reconnues dans son tableau d'adresses MAC (FDB). De plus, le commutateur réseau identifie les ports sur lesquels il a reçu des rapports pour une adresse Multicast spécifique. De cette manière, le commutateur réseau transfère les paquets Multicast uniquement aux ports auxquels des récepteurs Multicast sont connectés. Les autres ports ne reçoivent pas ces paquets.

Une fonctionnalité spéciale de l'équipement est la possibilité de déterminer le traitement de paquets de données avec des adresses Multicast inconnues. En fonction du réglage, l'équipement rejette ces paquets de données ou les transfère à chaque port. Par défaut, l'équipement transmet les paquets de données uniquement aux ports avec des équipements connectés, qui à leur tour reçoivent des paquets de requête. Vous pouvez aussi d'envoyer en outre les paquets Multicast connus aux ports de requête.

Réglage de l'IGMP Snooping

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > IGMP Snooping > Global*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.

Lorsque la fonction *IGMP Snooping* est désactivée, l'équipement se comporte comme suit :
- ▶ L'équipement ignore la requête reçue et les messages Report (Rapport).
- ▶ L'équipement transfère les paquets de données reçus avec une adresse Multicast en tant qu'adresse cible à chaque port.

- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

☐ Spécification des réglages pour un port :

- ☐ Ouvrez la boîte de dialogue *Switching > IGMP Snooping > Configuration*, onglet *Port*.
- ☐ Pour activer la fonction *IGMP Snooping* sur un port, cochez la case dans la colonne *Active* pour le port concerné.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

☐ Spécification des réglages pour un VLAN :

- ☐ Ouvrez la boîte de dialogue *Switching > IGMP Snooping > Configuration*, onglet *VLAN ID*.
- ☐ Pour activer la fonction *IGMP Snooping* pour un VLAN spécifique, cochez la case dans la colonne *Active* pour le VLAN concerné.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

Réglage de la fonction IGMP Querier

L'équipement lui-même envoie, à titre facultatif, des messages de requête actifs ; sinon, il répond aux messages de requête ou détecte d'autres requérants Multicast dans le réseau (fonction *IGMP Snooping Querier*).

Prérequis :

La fonction *IGMP Snooping* est activée globalement.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > IGMP Snooping > Querier*.
- ☐ Dans le cadre *Operation*, activez/désactivez la fonction *IGMP Snooping Querier* de l'équipement de manière globale.
- ☐ Pour activer la fonction *IGMP Snooping Querier* pour un VLAN spécifique, cochez la case dans la colonne *Active* pour le VLAN concerné.
- ▶ L'équipement exécute un simple processus de sélection : lorsque l'adresse IP source de l'autre requérant Multicast est plus petite que la sienne, il bascule sur l'état passif, dans lequel il n'envoie plus de requêtes.
- ▶ Dans la colonne *Address*, vous spécifiez l'adresse IP Multicast que l'équipement insère dans l'adresse de l'expéditeur dans les requêtes générées. Vous utilisez l'adresse du routeur Multicast.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

Améliorations de la fonction IGMP Snooping (tableau)

La boîte de dialogue *Switching > IGMP Snooping > Snooping Enhancements* vous permet d'accéder aux réglages améliorés de la fonction *IGMP Snooping*. Vous activez ou désactivez les réglages pour chaque port dans un VLAN.

Les réglages suivants sont possibles :

- ▶ `Static`
  Utilisez ce réglage pour définir le port en tant que port de requête statique. L'équipement transfère chaque message IGMP sur un port de requête statique, même s'il n'a préalablement reçu aucun message de requête sur ce port. Lorsque l'option statique est désactivée et que l'équipement a préalablement reçu des messages de requête IGMP, il transfère les messages IGMP sur ce port. Lorsque c'est le cas, l'entrée affiche `L` (« learned »).
- ▶ `Learn by LLDP`
  Un port avec ce réglage détecte automatiquement d'autres équipements Schneider Electric utilisant LLDP (Link Layer Discovery Protocol). L'équipement apprend alors l'état de requête IGMP de ce port auprès de ces équipements Schneider Electric et configure la fonction *IGMP Snooping Querier* en conséquence. L'entrée `ALA` indique que la fonction `Learn by LLDP` est activée. Lorsque l'équipement trouve un autre équipement Schneider Electric sur ce port dans ce VLAN, l'entrée affiche également `A` (« automatic » (automatique)).
- ▶ `Forward All`
  Avec ce réglage, l'équipement transfère les paquets de données destinés à une adresse Multicast à ce port. Le réglage est adapté dans les situations suivantes, par exemple :
  - À des fins de diagnostic.
  - Pour les équipements dans un anneau MRP : après la commutation de l'anneau, la fonction `Forward All` permet de reconfigurer le réseau rapidement pour les paquets de données avec adresses cibles Multicast enregistrées. Activez la fonction `Forward All` sur chaque port d'anneau.

Prérequis :

La fonction *IGMP Snooping* est activée globalement.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > IGMP Snooping > Snooping Enhancements*.
- ☐ Double-cliquez sur le port choisi dans le VLAN choisi.
- ☐ Pour activer une ou plusieurs fonctions, sélectionnez les options correspondantes.
- ☐ Cliquez sur le bouton *Ok*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`vlan database`	Passer en mode de configuration VLAN.
`igmp-snooping vlan-id 1 forward-all 1/1`	Activez la fonction `Forward All` pour le port `1/1` dans le VLAN `1`.

Configuration de Multicasts

L'équipement vous permet de configurer l'échange de paquets de données Multicast. L'équipement propose différentes options selon si les paquets de données doivent être envoyés à des destinataires Multicast inconnus ou connus.

Les réglages pour les adresses Multicast inconnues sont globaux pour tout l'équipement. Les options suivantes peuvent être sélectionnées :
- L'équipement rejette les Multicasts inconnus.
- L'équipement transfère les Multicasts inconnus à tous les ports.

Commentaire : Les réglages d'échange pour les adresses Multicast inconnues s'appliquent également aux adresses IP réservées à partir du « Local Network Control Block » (`224.0.0.0..224.0.0.255`). Ce comportement peut influer sur les protocoles de routage de niveau supérieur.

Pour chaque VLAN, vous spécifiez individuellement l'envoi de paquets Multicast à des adresses Multicast connues. Les options suivantes peuvent être sélectionnées :
- L'équipement transfère des Multicasts connus aux ports ayant préalablement reçu des messages de requête (ports de requête) et aux ports enregistrés. Les ports enregistrés sont des ports avec destinataires Multicast enregistrés auprès du groupe Multicast correspondant. Cette option garantit que le transfert fonctionne avec des applications basiques sans configuration supplémentaire.
- L'équipement transfère des Multicasts connus uniquement aux ports enregistrés. Ce réglage présente l'avantage d'utiliser de manière optimale la bande passante disponible grâce à une distribution directe.

Prérequis :

La fonction *IGMP Snooping* est activée globalement.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > IGMP Snooping > Multicasts*.
- ☐ Dans le cadre *Configuration*, vous spécifiez comment l'équipement envoie des paquets de données à des adresses Multicast inconnues.
  - ▶ *send to registered ports*
    L'équipement transfère les paquets avec une adresse Multicast inconnue à tous les ports de requête.
- ☐ Dans la colonne *Known multicasts*, vous spécifiez comment l'équipement envoie des paquets de données à des adresses Multicast connues dans le VLAN correspondant. Cliquez dans le champ de votre choix et sélectionnez la valeur souhaitée.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

10.3 Limiteur de charge

La fonction de limiteur de charge garantit un fonctionnement stable, même avec des volumes de trafic importants, en limitant le trafic sur les ports. La limitation de la charge est réalisée individuellement pour chaque port, ainsi que séparément pour les trafics entrant et sortant.

Si le débit de données sur un port excède la limite définie, l'équipement rejette la surcharge sur ce port.

La limitation de la charge intervient exclusivement sur la couche 2. Dans le cadre de ce processus, la fonction de limiteur de charge ignore les informations des protocoles des niveaux supérieurs, comme IP ou TCP. Cela peut influer sur le trafic TCP.

Pour minimiser ces effets, utilisez les options suivantes :
- Restreignez la limitation de la charge à certains types de paquets, par exemple Broadcasts, Multicasts et Unicasts, avec une adresse cible inconnue.
- Limitez le trafic de données sortant plutôt que le trafic entrant. La limitation de la charge sortante fonctionne mieux avec le contrôle de débit TCP du fait de la mise en tampon interne des paquets de données dans l'équipement.
- Augmentez la durée de vieillissement des adresses Unicast apprises.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > Rate Limiter*.
- Activez le limiteur de charge et définissez les limites du débit de données. Les réglages s'appliquent par port et se subdivisent par type de trafic :
  - Paquets de données Broadcast reçus
  - Paquets de données Multicast reçus
  - Paquets de données Unicast reçus avec une adresse cible inconnue

  Pour activer le limiteur de charge sur un port, cochez la case d'au moins une catégorie. Dans la colonne *Threshold unit*, vous spécifiez si l'équipement interprète les valeurs seuil en tant que pourcentage de la bande passante du port ou en tant que paquets par seconde. La valeur seuil `0` désactive le limiteur de charge.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

10.4 QoS/priorité

QoS (Quality of Service) est une procédure définie dans IEEE 802.1D utilisée pour distribuer les ressources dans le réseau. QoS vous permet de prioriser les données des applications nécessaires.

Lorsque la charge du réseau est élevée, la priorisation permet d'éviter que le trafic de données de priorité inférieure n'interfère avec le trafic des données sensibles au temps. Le trafic des données sensibles au temps comprend, par exemple, la voix, la vidéo et les données en temps réel.

10.4.1 Description de la priorisation

Pour la priorisation du trafic de données, des classes de trafic sont définies dans l'équipement. L'équipement donne la priorité aux classes de trafic supérieures par rapport aux classes de trafic inférieures. Le nombre de classes de trafic dépend du type de l'équipement.

Pour un flux optimal des données sensibles au temps, vous affectez les classes de trafic supérieures à ces données. Vous affectez les classes de trafic inférieures aux données moins sensibles au temps.

Affectation de classes de trafic aux données

L'équipement affecte automatiquement des classes de trafic aux données entrantes (classification du trafic). L'équipement prend en compte les critères de classification suivants :

- Méthodes selon lesquelles l'équipement procède à l'affectation des paquets de données reçus à des classes de trafic :
  - `trustDot1p`
    L'équipement utilise la priorité du paquet de données contenu dans le tag de VLAN.
  - `trustIpDscp`
    L'équipement utilise les informations QoS contenues dans l'en-tête IP (ToS/DiffServ).
  - `untrusted`
    L'équipement ignore les informations de priorité possible contenues dans les paquets de données et utilise directement la priorité du port destinataire.
- La priorité affectée au port destinataire.

Les deux critères de classification sont configurables.

Durant la classification du trafic, l'équipement utilise les règles suivantes :

- Lorsque le port destinataire est défini sur `trustDot1p` (réglage par défaut), l'équipement utilise la priorité du paquet de données contenue dans le tag de VLAN. Lorsque les paquets de données ne contiennent pas de tag de VLAN, l'équipement est guidé par la priorité du port destinataire.
- Lorsque le port destinataire est défini sur `trustIpDscp`, l'équipement utilise les informations QoS (ToS/DiffServ) dans l'en-tête IP. Lorsque les paquets de données ne contiennent pas de paquet IP, l'équipement est guidé par la priorité du port destinataire.
- Lorsque le port destinataire est défini sur `untrusted`, l'équipement est guidé par la priorité du port destinataire.

Priorisation des classes de trafic

Pour la priorisation des classes de trafic, l'équipement utilise les méthodes suivantes :

- `Strict`
  Lorsque la transmission des données d'une classe de trafic supérieure est terminée ou que les données concernées sont toujours dans la file d'attente, l'équipement envoie les données de la classe de trafic correspondante. Si chaque classe de trafic est priorisée selon la méthode `Strict`, l'équipement peut bloquer de manière permanente les données des classes de trafic inférieures en cas de charge élevée du réseau.
- `Weighted Fair Queuing`
  Une bande passante spécifique est affectée à la classe de trafic. Cela permet de garantir l'envoi par l'équipement du trafic de données de cette classe, même si le trafic de données dans les classes supérieures est élevé.

10.4.2 Traitement des informations de priorité reçues

Les applications étiquettent les paquets de données avec les informations de priorisation suivantes :

- Priorité VLAN sur la base de la norme technique IEEE 802.1Q/ 802.1D (couche 2)
- Type-of-Service (ToS) ou DiffServ (DSCP) pour les paquets IP d'administration de VLAN (couche 3)

L'équipement vous permet d'évaluer ces informations de priorité à l'aide des options suivantes :

- `trustDot1p`
  L'équipement affecte des paquets de données taggés VLAN aux différentes classes de trafic conformément à leurs priorités VLAN. L'attribution correspondante est configurable. L'équipement affecte la priorité du port destinataire aux paquets de données qu'il reçoit sans tag de VLAN.
- `trustIpDscp`
  L'équipement affecte les paquets IP aux différentes classes conformément à la valeur DSCP dans l'en-tête IP, même si le paquet a également un tag de VLAN. L'attribution correspondante est configurable. L'équipement priorise les paquets non-IP conformément à la priorité du port destinataire.
- `untrusted`
  L'équipement ignore les informations de priorité dans les paquets de données et leur affecte la priorité du port destinataire.

10.4.3 Taggage VLAN

Pour les fonctions de VLAN et de priorisation, la norme technique IEEE 802.1Q fournit pour intégration un cadre MAC dans le tag de VLAN. Le tag de VLAN se compose de 4 octets et se trouve entre le champ de l'adresse source (« Champ Adresse source ») et le champ de type (« Champ Longueur / Type »).

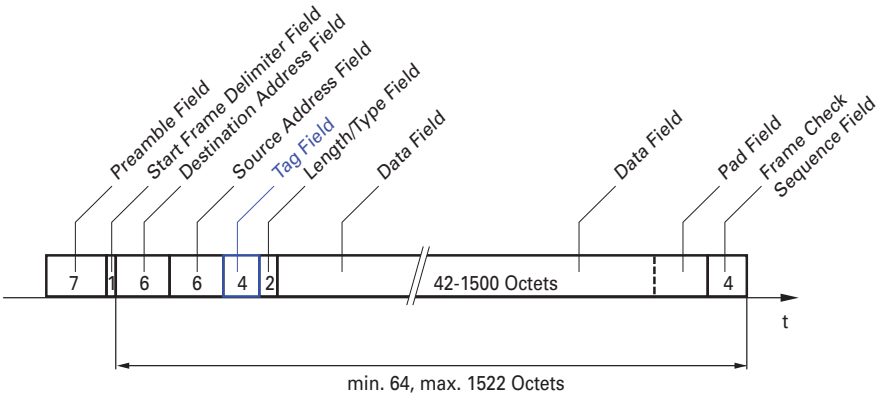


Figure 23 : Paquet de données Ethernet avec tag

Pour les paquets de données avec tags de VLAN, l'équipement évalue les informations suivantes :
- Informations de priorité
- Lorsque des VLAN sont configurés, taggage VLAN

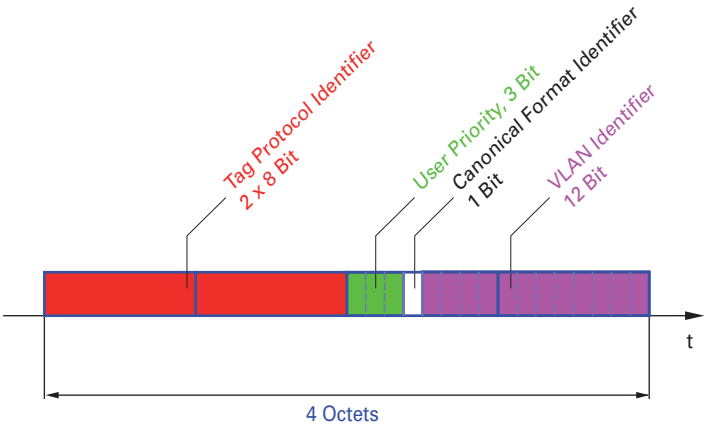


Figure 24 : Structure du taggage VLAN

Les paquets de données avec tags de VLAN contenant des informations de priorité mais aucune information de VLAN (VLAN-ID = 0) sont appelés des Priority Tagged Frames (cadres taggés de priorité).

Commentaire : Les protocoles réseau et les mécanismes de redondance utilisent la classe de trafic 7, qui est la plus élevée. Aussi, sélectionnez une autre classe de trafic pour les données d'application.

Lorsque vous utilisez la priorisation VLAN, tenez compte des fonctionnalités spéciales suivantes :
- La priorisation de bout en bout requiert que les tags de VLAN soient transmis à tout le réseau. La condition préalable est que chaque composant du réseau soit compatible VLAN.
- Les routeurs ne sont pas à même d'envoyer et de recevoir des paquets avec des tags de VLAN par le biais d'interfaces de routeur basées sur des ports.

10.4.4 IP ToS (Type of Service)

Le champ Type-of-Service (ToS) dans l'en-tête IP fait partie du protocole IP depuis le début et est utilisé pour distinguer les différents services dans les réseaux IP. La tendance était déjà au traitement différencié des paquets IP, du fait des limites de la bande passante disponible et du manque de fiabilité des liaisons. Grâce à l'augmentation continue de la bande passante disponible, l'utilisation du champ ToS était inutile.

Ce sont finalement les besoins en termes de temps réel des réseaux d'aujourd'hui qui ont redonné de l'importance au champ ToS. La sélection de l'octet ToS de l'en-tête IP vous permet de distinguer les différents services. Cependant, ce champ reste peu utilisé dans la pratique.

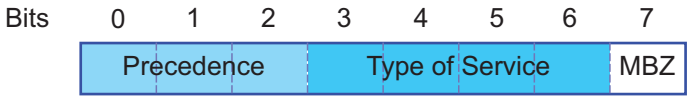


Tableau 22 : Champ ToS dans l'en-tête IP

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Zero
110 - Internetwork Control	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput	
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immediate		
001 - Priority		
000 - Routine		

10.4.5 Traitement des classes de trafic

L'équipement fournit les options suivantes pour le traitement des classes de trafic :
- Strict Priority
- Weighted Fair Queuing
- Strict Priority en combinaison avec Weighted Fair Queuing
- Gestion des files d'attente

Description de Strict Priority

Avec le réglage Strict Priority, l'équipement transmet d'abord les paquets de données avec une classe de trafic élevée (priorité élevée) avant de transmettre un paquet de données avec la classe de trafic immédiatement la plus élevée. Lorsqu'il ne reste aucun autre paquet de données dans la file d'attente, l'équipement transmet un paquet de données avec la classe de trafic la plus basse (priorité la plus basse). Dans les cas défavorables, en présence d'un volume important de trafic à priorité élevée en attente d'envoi sur ce port, l'équipement n'envoie pas les paquets avec une priorité basse.

Dans les applications sensibles au temps, comme la VoIP ou la vidéo, Strict Priority permet d'envoyer les données immédiatement.

Description de Weighted Fair Queuing

Avec Weighted Fair Queuing, également appelé Weighted Round Robin (WRR), vous affectez une bande passante minimale ou réservée à chaque classe de trafic. Cela garantit que les paquets de données avec une priorité inférieure sont également envoyés, même si le réseau est très chargé.

Les valeurs réservées sont comprises entre 0 % et 100 % de bande passante disponible, par incréments de 1 %.
- Une valeur de 0 équivaut à un réglage « aucune bande passante ».
- Le total des bandes passantes individuelles ne peut pas dépasser 100 %.

Lorsque vous affectez Weighted Fair Queuing à chaque classe de trafic, toute la bande passante du port correspondant est disponible pour vous.

Combinaison de Strict Priority et Weighted Fair Queuing

Lorsque vous combinez Weighted Fair Queuing avec Strict Priority, vérifiez que la classe de trafic la plus élevée de Weighted Fair Queuing est inférieure à la classe de trafic la plus basse de Strict Priority.

Si vous combinez Weighted Fair Queuing avec Strict Priority, une charge Strict Priority élevée du réseau peut réduire de manière significative la bande passante disponible pour Weighted Fair Queuing.

10.4.6 Gestion des files d'attente

Queue Shaping

Queue Shaping régule le débit auquel les files d'attente transmettent les paquets de données. Par exemple, l'utilisation du Queue Shaping vous permet de limiter le débit d'une file d'attente de haute priorité stricte de manière à permettre à une file d'attente de priorité stricte inférieure d'envoyer des paquets avant que tous les paquets de priorité supérieure aient été transmis. L'équipement vous permet de configurer le Queue Shaping pour toutes les files d'attente. Spécifiez le Queue Shaping en tant que débit maximum auquel le trafic traverse une file d'attente en lui affectant un pourcentage de la bande passante disponible.

Définition des réglages pour la gestion des files d'attente

Exécutez les étapes suivantes :

☐ Ouvrez la boîte de dialogue *Switching > QoS/Priority > Queue Management*.

La bande passante totale affectée dans la colonne *Min. bandwidth [%]* est de 100 %.

☐ Pour activer Weighted Fair Queuing pour *Traffic class* = `0`, procédez comme suit :
- Décochez la case dans la colonne *Strict priority*.
- Dans la colonne *Min. bandwidth [%]*, spécifiez la valeur `5`.

☐ Pour activer Weighted Fair Queuing pour *Traffic class* = `1`, procédez comme suit :
- Décochez la case dans la colonne *Strict priority*.
- Dans la colonne *Min. bandwidth [%]*, spécifiez la valeur `20`.

- ☐ Pour activer Weighted Fair Queuing pour *Traffic class* = 2, procédez comme suit :
  - ▶ Décochez la case dans la colonne *Strict priority*.
  - ▶ Dans la colonne *Min. bandwidth [%]*, spécifiez la valeur 30.
- ☐ Pour activer Weighted Fair Queuing pour *Traffic class* = 3, procédez comme suit :
  - ▶ Décochez la case dans la colonne *Strict priority*.
  - ▶ Dans la colonne *Min. bandwidth [%]*, spécifiez la valeur 20.
- ☐ Pour activer Weighted Fair Queuing et Queue Shaping pour *Traffic class* = 4, procédez comme suit :
  - ▶ Décochez la case dans la colonne *Strict priority*.
  - ▶ Dans la colonne *Min. bandwidth [%]*, spécifiez la valeur 10.
  - ▶ Dans la colonne *Max. bandwidth [%]*, spécifiez la valeur 10.

  Lorsque vous utilisez une combinaison entre Weighted Fair Queuing et Queue Shaping pour une classe de trafic spécifique, dans la colonne *Max. bandwidth [%]*, spécifiez une valeur supérieure à la valeur spécifiée dans la colonne *Min. bandwidth [%]*.
- ☐ Pour activer Weighted Fair Queuing pour *Traffic class* = 5, procédez comme suit :
  - ▶ Décochez la case dans la colonne *Strict priority*.
  - ▶ Dans la colonne *Min. bandwidth [%]*, spécifiez la valeur 5.
- ☐ Pour activer Weighted Fair Queuing pour *Traffic class* = 6, procédez comme suit :
  - ▶ Décochez la case dans la colonne *Strict priority*.
  - ▶ Dans la colonne *Min. bandwidth [%]*, spécifiez la valeur 10.
- ☐ Pour activer Strict Priority et Queue Shaping pour *Traffic class* = 7, procédez comme suit :
  - ▶ Cochez la case dans la colonne *Strict priority*.
  - ▶ Dans la colonne *Max. bandwidth [%]*, spécifiez la valeur 10.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`cos-queue weighted 0`	Activation de Weighted Fair Queuing pour la classe de trafic 0.
`cos-queue min-bandwidth: 0 5`	Affectation d'une pondération de 5 % à la classe de trafic 0.
`cos-queue weighted 1`	Activation de Weighted Fair Queuing pour la classe de trafic 1.
`cos-queue min-bandwidth: 1 20`	Affectation d'une pondération de 20 % à la classe de trafic 1.
`cos-queue weighted 2`	Activation de Weighted Fair Queuing pour la classe de trafic 2.
`cos-queue min-bandwidth: 2 30`	Affectation d'une pondération de 30 % à la classe de trafic 2.

```
cos-queue weighted 3
```
Activation de Weighted Fair Queuing pour la classe de trafic 3.

```
cos-queue min-bandwidth: 3 20
```
Affectation d'une pondération de 20 % à la classe de trafic 3.

```
show cos-queue
Queue Id  Min. bandwidth  Max. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         0               0               strict
5         0               0               strict
6         0               0               strict
7         0               0               strict
```

Combinaison de Weighted Fair Queuing et Queue Shaping

Exécutez les étapes suivantes :

```
enable
```
Basculez sur le mode Privileged EXEC.

```
configure
```
Basculez sur le mode de configuration.

```
cos-queue weighted 4
```
Activation de Weighted Fair Queuing pour la classe de trafic 4.

```
cos-queue min-bandwidth: 4 10
```
Affectation d'une pondération de 10 % à la classe de trafic 4.

```
cos-queue max-bandwidth: 4 10
```
Affectation d'une pondération de 10 % à la classe de trafic 4.

```
cos-queue weighted 5
```
Activation de Weighted Fair Queuing pour la classe de trafic 5.

```
cos-queue min-bandwidth: 5 5
```
Affectation d'une pondération de 5 % à la classe de trafic 5.

```
cos-queue weighted 6
```
Activation de Weighted Fair Queuing pour la classe de trafic 6.

```
cos-queue min-bandwidth: 6 10
```
Affectation d'une pondération de 10 % à la classe de trafic 6.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               0               strict
```

Réglage du Queue Shaping

Exécutez les étapes suivantes :

```
enable
```
Basculez sur le mode Privileged EXEC.

```
configure
```
Basculez sur le mode de configuration.

```
cos-queue max-bandwidth: 7 10
```
Affectation d'une pondération de 10 % à la classe de trafic 7.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               10              strict
```

10.4.7 Priorisation de l'administration

Pour avoir toujours accès à l'administration de l'équipement même en cas de charge réseau élevée, l'équipement vous permet de prioriser les paquets d'administration.

Lors de la priorisation des paquets d'administration, l'équipement envoie les paquets d'administration avec des informations de priorité.

- Dans la couche 2, l'équipement modifie la priorité de VLAN dans le tag.
  La condition préalable à cette fonction est que les ports correspondants soient définis pour permettre l'envoi de paquets avec un tag de VLAN.
- Dans la couche 3, l'équipement modifie la valeur IP-DSCP.

10.4.8 Réglage de la priorisation

Attribution de la priorité de port

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > QoS/Priority > Port Configuration*.
- ☐ Dans la colonne *Port priority*, vous spécifiez la priorité avec laquelle l'équipement transfère les paquets de données reçus sur ce port sans tag de VLAN.
- ☐ Dans la colonne *Trust mode*, vous spécifiez les critères que l'équipement utilise pour affecter une classe de trafic aux paquets de données reçus.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`vlan priority 3`	Affectation à l'interface `1/1` de la priorité de port `3`.
`exit`	Basculez sur le mode de configuration.

Affectation de la priorité de VLAN à une classe de trafic

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > QoS/Priority > 802.1D/p Mapping*.
- ☐ Pour affecter une classe de trafic à une priorité de VLAN, insérez la valeur associée dans la colonne *Traffic class*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`classofservice dot1p-mapping 0 2`	Affectation d'une priorité de VLAN de `0` à la classe de trafic `2`.
`classofservice dot1p-mapping 1 2`	Affectation d'une priorité de VLAN de `1` à la classe de trafic `2`.
`exit`	Basculez sur le mode Privileged EXEC.
`show classofservice dot1p-mapping`	Affichez l'affectation.

Affecter la priorité de port aux paquet de données reçus

Exécutez les étapes suivantes :

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`classofservice trust untrusted`	Affectation du mode `untrusted` à l'interface.
`classofservice dot1p-mapping 0 2`	Affectation d'une priorité de VLAN de `0` à la classe de trafic `2`.
`classofservice dot1p-mapping 1 2`	Affectation d'une priorité de VLAN de `1` à la classe de trafic `2`.
`vlan priority 1`	Spécification de la valeur `1` pour la priorité de port.
`exit`	Basculez sur le mode de configuration.

```
exit
```
Basculez sur le mode Privileged EXEC.

```
show classofservice trust
```
Affichage du mode Trust des ports/interfaces.

```
 Interface Trust Mode
 --------- -------------
 1/1       untrusted
 1/2       dot1p
 1/3       dot1p
 1/4       dot1p
 1/5       dot1p
 1/6       dot1p
 1/7       dot1p
```

Affectation DSCP à une classe de trafic

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > QoS/Priority > IP DSCP Mapping*.
- ☐ Spécifiez la valeur désirée dans la colonne *Traffic class*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

```
enable
```
Basculez sur le mode Privileged EXEC.

```
configure
```
Basculez sur le mode de configuration.

```
classofservice  ip-dscp-mapping cs1 1
```
Affectation de la valeur DSCP `CS1` à la classe de trafic `1`.

```
show classofservice  ip-dscp-mapping
```
Affichage des affectations IP-DSCP

```
    IP DSCP       Traffic Class
 -------------    -------------
   be                  2
   1                   2
   .                   .
   .                   .
   (cs1)               1
   .                   .
```

Affecter la priorité DSCP aux paquets de données IP reçus

Exécutez les étapes suivantes :

```
enable
```
Basculez sur le mode Privileged EXEC.

```
configure
```
Basculez sur le mode de configuration.

```
interface 1/1
```
Basculez sur le mode de configuration de l'interface `1/1`.

```
classofservice trust ip-dscp
```
Affectation globale du mode `trust ip-dscp`.

```
exit
```
Basculez sur le mode de configuration.

```
show classofservice trust
```
Affichage du mode Trust des ports/interfaces.

```
 Interface     Trust Mode
 ----------    -------------
 1/1           ip-dscp
 1/2           dot1p
 1/3           dot1p
 .             .
 .             .
 1/5           dot1p
 .             .
```

Configuration de la régulation du trafic sur un port

Exécutez les étapes suivantes :

```
enable
```
Basculez sur le mode Privileged EXEC.

```
configure
```
Basculez sur le mode de configuration.

```
interface 1/2
```
Basculez sur le mode de configuration de l'interface `1/2`.

```
traffic-shape bw 50
```
Limitation de la bande passante maximale du port `1/2` à 50 %.

```
exit
```
Basculez sur le mode de configuration.

```
exit
```
Basculez sur le mode Privileged EXEC.

```
show traffic-shape
```
Affiche la configuration de la régulation du trafic.

```
Interface  Shaping rate
---------  ------------
1/1        0  %
1/2        50 %
1/3        0  %
1/4        0  %
```

Configuration de la priorité d'administration de couche 2

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > QoS/Priority > Global*.
- ☐ Dans le champ *VLAN priority for management packets*, spécifiez la priorité de VLAN avec laquelle l'équipement envoie les paquets de données d'administration.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

```
enable
```
Basculez sur le mode Privileged EXEC.

```
network management priority dot1p 7
```
Affectation de la priorité de VLAN 7 aux paquets d'administration. L'équipement envoie les paquets d'administration avec la priorité la plus élevée.

```
show network parms
```
Affichage de la priorité du VLAN dans lequel s'effectue l'administration de l'équipement.

```
IPv4 Network
------------
...
Management VLAN priority.....................7
...
```

Configuration de la priorité d'administration de couche 3

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > QoS/Priority > Global*.
- ☐ Dans le champ *IP DSCP value for management packets*, spécifiez la valeur DSCP avec laquelle l'équipement envoie les paquets de données d'administration.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

```
enable
```
Basculez sur le mode Privileged EXEC.

```
network management priority ip-dscp 56
```
Affectation de la valeur DSCP 56 aux paquets d'administration. L'équipement envoie les paquets d'administration avec la priorité la plus élevée.

```
show network parms
```
Affichage de la priorité du VLAN dans lequel s'effectue l'administration de l'équipement.

```
IPv4 Network
------------
...
Management IP-DSCP value....................56
```

10.5 Contrôle de flux

Si de nombreux paquets de données sont reçus simultanément dans la file d'attente priorisée d'un port, cela peut entraîner un débordement de capacité de la mémoire du port. Cela se produit, par exemple, lorsque l'équipement reçoit des données sur un port gigabit et les transfère vers un port avec une bande passante moindre. L'équipement rejette les paquets de données excédentaires.

Le mécanisme de contrôle de flux décrit dans la norme technique IEEE 802.3 permet d'éviter la perte de tout paquet de données en raison d'un débordement de capacité de la mémoire d'un port. Un peu avant que la mémoire d'un port ne soit totalement pleine, l'équipement signale aux équipements connectés qu'il ne peut plus accepter aucun paquet de données de leur part.

- En mode full duplex, l'équipement envoie un paquet de données de pause.
- En mode half duplex, l'équipement simule une collision.

La figure suivante présente le fonctionnement du contrôle de flux. Les stations de travail 1, 2 et 3 souhaitent simultanément transmettre une grande quantité de données à la station de travail 4. La bande passante combinée des stations de travail 1, 2 et 3 est supérieure à la bande passante de la station 4. Cela entraîne un débordement sur la file d'attente de réception du port 4. L'entonnoir à gauche symbolise cet état.

Lorsque la fonction de contrôle de flux sur les ports 1, 2 et 3 de l'équipement est activée, l'équipement réagit avant que l'entonnoir ne déborde. L'entonnoir à droite représente les ports 1, 2 et 3 envoyant un message aux équipements émetteurs afin de contrôler la vitesse de transmission. Ainsi, le port destinataire n'est plus débordé et est à même de traiter le trafic entrant.

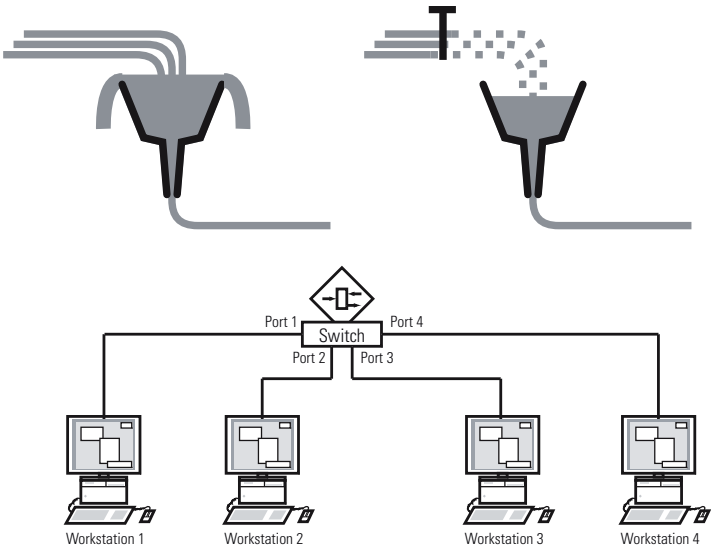


Figure 25 : Exemple de contrôle de flux

10.5.1 Liaison half duplex ou full duplex

Contrôle de flux avec liaison half duplex

Dans cet exemple, il existe une liaison half duplex entre la station de travail 2 et l'équipement.

Avant que la file d'attente d'envoi du port 2 ne déborde, l'équipement renvoie des données à la station de travail 2. La station de travail 2 détecte une collision et interrompt la transmission.

Contrôle de flux avec une liaison full duplex

Dans cet exemple, il existe une liaison full duplex entre la station de travail 2 et l'équipement.

Avant que la file d'attente d'envoi du port 2 ne déborde, l'équipement envoie une requête à la station de travail 2 pour insérer une petite pause dans la transmission des données.

10.5.2 Réglage du contrôle de flux

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > Global*.
- ☐ Cochez la case *Flow control*.
  Avec ce réglage, vous activez le contrôle de flux dans l'équipement.
- ☐ Ouvrez la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.
- ☐ Pour activer le contrôle de flux sur un port, cochez la case dans la colonne *Flow control*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

Commentaire : Si vous utilisez une fonction de redondance, désactivez le contrôle de flux sur les ports impliqués. Si le contrôle de flux et la fonction de redondance sont activés simultanément, la fonction de redondance peut ne pas fonctionner comme prévu.

11 Configuration de la TSN basée sur des modèles

11.1 Faits de base

Lorsque vous utilisez la fonction *TSN*, les conditions de base suivantes s'appliquent :

- L'équipement fonctionne selon la méthode « Store and Forward ». Ainsi, l'équipement doit recevoir le paquet de données complet avant de prendre une décision de transfert.
- Vous spécifiez une fois le Base time et le Cycle time dans l'équipement. Les deux réglages sont valables pour chaque port participant au TSN.
- Vous configurez une Gate Control List par port sur la base de modèles prédéfinis pour faciliter la configuration.
- Vérifiez que la somme des temps d'entrée de la Gate Control List est inférieure ou égale au Cycle time spécifié.
- L'équipement utilise une guard band permettant de protéger la tranche de temps pour les paquets à haute priorité contre les paquets de la tranche de temps précédente qui empiètent. Le facteur décisif pour la longueur de l'intervalle de la guard band est la vitesse du port d'envoi. Nous recommandons les longueurs d'intervalle suivantes pour la guard band. Les valeurs sont basées sur la vitesse du port et la taille maximale autorisée pour les paquets Ethernet :
  - 2.5 Gbit/s: 5 µs
  - 1 Gbit/s: 13 µs
  - 100 Mbit/s: 124 µs
- La plage de Cycle time est 50 000..10 000 000 ns.
- La plage d'intervalles de la Gate Control List est 1 000..10 000 000 ns.
- Vérifiez que le Cycle time ainsi que les intervalles de la Gate Control List sont des multiples de 1 µs, 2 µs ou 4 µs.

Tableau 23 : Dépendance entre le Cycle time et la granularité

Cycle time	Granularité
50 µs..4 ms	1 µs
4.002 ms..8 ms	2 µs
8.004 ms..10 ms	4 µs

11.2 Exemple

Cet exemple décrit comment configurer les équipements pour un scénario avec les conditions suivantes :
- Cycle time = 1 ms
- Tranche de temps pour les paquets de haute priorité = 500 µs
- Tranche de temps pour les paquets de faible priorité = 487 µs

Dans cet exemple, chaque équipement est connecté au réseau avec une vitesse de port de 1 Gbit/s.

Tableau 24 : Structure du cycle

Tranche de temps	Classes de trafic	Durée
Paquets de haute priorité	7	500 µs
Paquets de faible priorité	0,1,2,3,4,5,6	487 µs
Guard band	–	13 µs

11.2.1 Calcul du temps

L'équipement calcule automatiquement la durée de la tranche de temps pour les paquets de faible priorité. Le calcul est basé sur les paramètres suivants :
- Cycle time
- Durée de la tranche de temps pour les paquets de haute priorité
- Durée de la guard band

11.2.2 Configuration des équipements

En utilisant les temps spécifiés précédemment, vous configurez les équipements à l'aide de l'interface utilisateur graphique ou de l'interface de ligne de commande. Pour chaque équipement concerné, exécutez les étapes suivantes.

Vérifier et ajuster le Cycle time

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > TSN > Configuration*.
- ☐ Dans le cadre *Configuration*, vérifiez la valeur dans le champ *Cycle time [ns]*.
- ☐ Si nécessaire, ajustez la valeur.

- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

```
enable                                          Basculez sur le mode Privileged EXEC.
configure                                       Basculez sur le mode de configuration.
show tsn configuration
Port  Status                 Conf. cycle time[ns]  Conf. base time
      Default gate states    Curr. cycle time[ns]  Curr. base time
      Config change pending                        Time of last activation
----  ---------------------  --------------------  ------------------------------
 1/1  [x]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                     1000000  1970-01-01 00:00:00.000000000
      [ ]                                          2018-07-12 08:10:58.813000000

 1/2  [x]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                     1000000  1970-01-01 00:00:00.000000000
      [ ]                                          2018-07-11 07:24:35.204000000

 1/3  [ ]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                           0  1970-01-01 00:00:00.000000000
      [ ]                                          1970-01-01 00:00:00.000000000

 1/4  [ ]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                           0  1970-01-01 00:00:00.000000000
      [ ]                                          1970-01-01 00:00:00.000000000

tsn cycle-time 1000000                          Si nécessaire, ajustez la valeur.
```

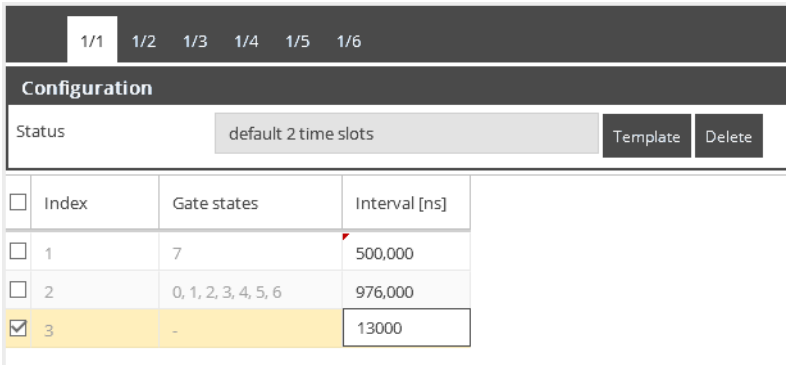
Sélectionner un modèle et configurer la Gate Control List

L'équipement fournit des modèles prédéfinis pour vous aider à configurer la Gate Control List. Dans cet exemple, nous utilisons le modèle *default 2 time slots*. Après avoir sélectionné le modèle, vous pouvez ajuster la durée des tranches de temps. Exécutez les étapes suivantes pour chaque port pour lequel vous souhaitez utiliser la fonction *TSN*.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > TSN > Gate Control List > Configured*.
- ☐ Sélectionnez l'onglet correspondant au port pour lequel vous souhaitez spécifier les réglages.

- ☐ Sélectionnez un modèle dans le cadre *Configuration*.
  Exécutez les étapes suivantes :
  - Cliquez sur le bouton *Template*.
  - Sélectionnez l'élément `default 2 time slots`.
  - Cliquez sur le bouton *Ok*.
- ☐ Ajustez les valeurs dans la colonne *Interval [ns]* :
  - Saisissez la valeur `500000` dans la ligne pour les paquets de haute priorité.
  - Saisissez la valeur `13000` dans la ligne pour la guard band.
  - L'équipement calcule automatiquement la troisième valeur lors de l'enregistrement des modifications.



- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`tsn gcl modify 1 interval 500000`	Ajustez la durée en nanosecondes de la tranches de temps pour les paquets de haute priorité.
`tsn gcl modify 3 interval 13000`	Ajustez la durée en nanosecondes de la tranches de temps pour la guard band. L'équipement calcule automatiquement la durée de la tranche de temps pour les paquets de faible priorité. Vous ne pouvez pas définir la tranche de temps pour les paquets de faible priorité.

12 VLAN

Dans le cas le plus simple, un réseau local virtuel (VLAN) se compose d'un groupe de participants à un réseau dans un segment donné, capables de communiquer entre eux comme s'ils appartenaient à un réseau local distinct.

Les VLAN plus complexes s'étendent sur plusieurs segments de réseau et se basent en outre sur des connexions logiques (et non uniquement physiques) entre participants au réseau. Les VLAN sont des éléments de conception flexible de réseau. Il est plus facile de reconfigurer des connexions logiques de manière centralisée que des connexions câblées.

L'équipement prend en charge l'apprentissage de VLAN indépendant conformément à la norme technique IEEE 802.1Q, qui définit la fonction *VLAN*.

L'utilisation de VLAN présente de nombreux avantages. La liste suivante répertorie les principaux :

- Limitation de la charge du réseau
  Les VLAN réduisent considérablement la charge du réseau car les équipements ne transmettent les paquets Broadcast, Multicast et Unicast avec des adresses cibles inconnues (non apprises) qu'au sein du LAN virtuel. Concernant le reste des données, le réseau transmet le trafic normalement.
- Flexibilité
  Vous avez la possibilité de former des groupes d'utilisateurs sur la base de la fonction des participants, indépendamment de leur emplacement ou support physique.
- Clarté
  Les VLAN donnent aux réseaux une structure claire et facilitent la maintenance.

12.1 Exemples de VLAN

Les exemples suivants sont tirés de la pratique et vous donnent un rapide aperçu de la structure d'un VLAN.

Commentaire : Lors de la configuration des VLAN, vous utilisez une interface pour accéder à l'administration de l'équipement qui reste inchangée. Dans cet exemple, vous utilisez soit l'interface 1/6, soit la connexion série pour configurer les VLAN.

12.1.1 Exemple 1

Cet exemple présente une configuration de VLAN minimale (VLAN basé sur des ports). Un administrateur a connecté plusieurs équipements terminaux à un équipement de transmission et les a affectés à 2 VLAN. Cela empêche efficacement toute transmission de données entre les VLAN, dont les membres ne communiquent qu'au sein de leur propre VLAN.

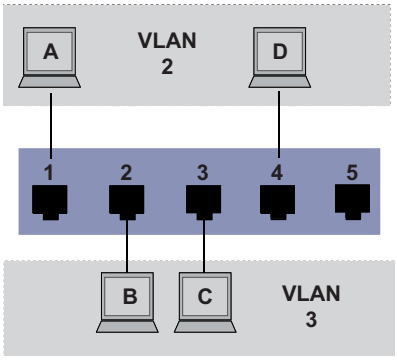


Figure 26 : Exemple de VLAN simple basé sur des ports

Lors de la définition des VLAN, vous créez des règles de communication pour chaque port, que vous saisissez dans les tableaux d'entrée et de sortie.

Le tableau d'entrée spécifie le VLAN-ID qu'un port affecte aux paquets de données entrants. Ainsi, vous utilisez l'adresse de port de l'équipement terminal pour l'affecter à un VLAN.

Le tableau de sortie spécifie à quels ports l'équipement envoie les paquets depuis ce VLAN.
- `T` = taggé (avec un champ de tag, coché)
- `U` = non taggé (sans champ de tag, case non cochée)

Pour cet exemple, l'état du champ TAG des paquets de données n'est pas pertinent ; aussi, vous utilisez le réglage `U`.

Tableau 25 : Tableau d'entrée

Équipement terminal	Port	ID du VLAN du port (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Tableau 26 : Tableau de sortie

VLAN-ID	Port				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

Exécutez les étapes suivantes :

☐ Définition du VLAN

- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Configuration*.
- ☐ Cliquez sur le bouton .
  La boîte de dialogue affiche la fenêtre *Create*.
- ☐ Dans le champ *VLAN ID*, spécifiez la valeur `2`.
- ☐ Cliquez sur le bouton *Ok*.
- ☐ Pour le VLAN, spécifiez le nom `VLAN2` :
  Double-cliquez dans la colonne *Name* et spécifiez le nom.
  Pour le VLAN `1`, dans la colonne *Name*, modifiez la valeur `Default` en `VLAN1`.
- ☐ Répétez les étapes précédentes pour créer un VLAN `3` avec le nom `VLAN3`.

`enable`	Basculez sur le mode Privileged EXEC.
`vlan database`	Passer en mode de configuration VLAN.
`vlan add 2`	Crée un nouveau VLAN avec le VLAN-ID `2`.
`name 2 VLAN2`	Affecte le nom `2` au VLAN `VLAN2`.
`vlan add 3`	Crée un nouveau VLAN avec le VLAN-ID `3`.
`name 3 VLAN3`	Affecte le nom `3` au VLAN `VLAN3`.
`name 1 VLAN1`	Affecte le nom `1` au VLAN `VLAN1`.
`exit`	Basculez sur le mode Privileged EXEC.
`show vlan brief`	Affiche la configuration de VLAN actuelle.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 128
Number of currently configured VLANs............ 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ Définition des ports

- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Port*.
- ☐ Pour affecter le port à un VLAN, spécifiez la valeur souhaitée dans la colonne correspondante.
  Valeurs possibles :
  - `T` = Le port est un membre du VLAN. Le port transmet des paquets de données taggés.
  - `U` = Le port est un membre du VLAN. Le port transmet des paquets de données non taggés.
  - `F` = Le port n'est pas un membre du VLAN.
    Les modifications à l'aide de la fonction *GVRP* sont désactivées.
  - `-` = Le port n'est pas un membre de ce VLAN.
    Les modifications à l'aide de la fonction *GVRP* sont autorisées.

  Les équipements terminaux interprétant généralement les paquets de données non taggés, vous spécifiez la valeur `U`.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Port*.
- ☐ Dans la colonne *Port-VLAN ID*, spécifiez le VLAN-ID du VLAN concerné : `2` ou `3`
- ☐ Les équipements terminaux interprétant généralement les paquets de données non taggés, vous spécifiez, dans la colonne *Acceptable packet types*, la valeur `admitAll` pour les ports de l'équipement terminal.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

La valeur dans la colonne *Ingress filtering* n'influe pas sur le fonctionnement de cet exemple.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`vlan participation include 2`	Le port `1/1` devient un membre du VLAN `2` et transmet les paquets de données sans tag de VLAN.
`vlan pvid 2`	Affectez le VLAN-ID du port `1/1` au port `2`.
`exit`	Basculez sur le mode de configuration.
`interface 1/2`	Basculez sur le mode de configuration de l'interface `1/2`.
`vlan participation include 3`	Le port `1/2` devient un membre du VLAN `3` et transmet les paquets de données sans tag de VLAN.
`vlan pvid 3`	Affectez le VLAN-ID du port `1/2` au port `3`.
`exit`	Basculez sur le mode de configuration.
`interface 1/3`	Basculez sur le mode de configuration de l'interface `1/3`.
`vlan participation include 3`	Le port `1/3` devient un membre du VLAN `3` et transmet les paquets de données sans tag de VLAN.
`vlan pvid 3`	Affectez le VLAN-ID du port `1/3` au port `3`.
`exit`	Basculez sur le mode de configuration.
`interface 1/4`	Basculez sur le mode de configuration de l'interface `1/4`.
`vlan participation include 2`	Le port `1/4` devient un membre du VLAN `2` et transmet les paquets de données sans tag de VLAN.
`vlan pvid 2`	Affectez le VLAN-ID du port `1/4` au port `2`.
`exit`	Basculez sur le mode de configuration.

```
exit                                    Basculez sur le mode Privileged EXEC.
show vlan id 3                          Affiche les détails du VLAN 3.
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1            -      Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4            -      Autodetect   Tagged
1/5            -      Autodetect   Tagged
```

12.1.2 Exemple 2

Le deuxième exemple présente une configuration plus complexe à 3 VLAN (1 à 3). Outre le commutateur de l'exemple 1, vous utilisez un 2ème commutateur (sur la droite dans cet exemple).

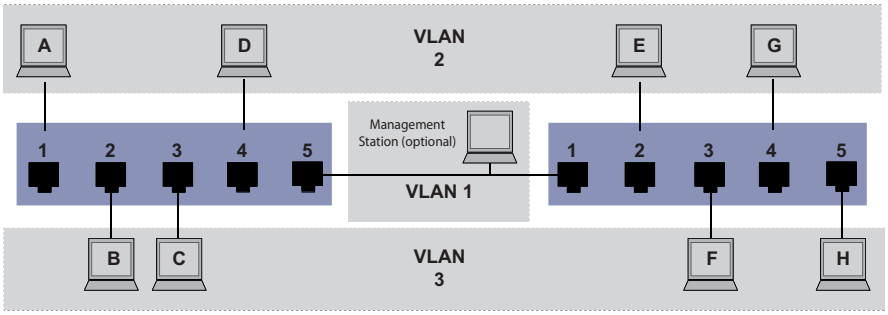


Figure 27 : Exemple d'une configuration de VLAN plus complexe

Les équipements terminaux des VLAN individuels (A à H) sont répartis sur 2 équipements de transmission (commutateurs). C'est pourquoi les VLAN de ce type s'appellent VLAN distribués. Si le VLAN est configuré correctement, une station d'administration réseau optionnelle est également indiquée et permet d'accéder à chaque composant du réseau.

Commentaire : Dans ce cas, le VLAN 1 n'est pas pertinent pour la communication des équipements terminaux, mais il est requis pour l'administration des équipements de transmission via ce que l'on appelle le VLAN d'administration.

Comme dans l'exemple précédent, affectez de manière univoque les ports et leurs équipements terminaux connectés à un VLAN. Avec la connexion directe entre les 2 équipements de transmission (uplink), les ports transportent des paquets pour les deux VLAN. Pour distinguer ces uplinks, vous utilisez le « taggage VLAN », qui traite les paquets de données en conséquence. Ainsi, vous gérez l'affectation aux VLAN respectifs.

Exécutez les étapes suivantes :
- ☐ Ajoutez le port uplink 5 aux tableaux d'entrée et de sortie de l'exemple 1.
- ☐ Créez de nouveaux tableaux d'entrée et de sortie pour le commutateur de droite, comme décrit dans le premier exemple.

Le tableau de sortie spécifie à quels ports l'équipement envoie les paquets depuis ce VLAN.
- ▶ `T` = taggé (avec un champ de tag, coché)
- ▶ `U` = non taggé (sans champ de tag, case non cochée)

Dans cet exemple, des paquets taggés sont utilisés dans la communication entre les équipements de transmission (Uplink), les paquets pour les différents VLAN étant différenciés au niveau de ces ports.

Tableau 27 : Tableau d'entrée de l'équipement de gauche

Équipement terminal	Port	ID du VLAN du port (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Tableau 28 : Tableau d'entrée de l'équipement de droite

Équipement terminal	Port	ID du VLAN du port (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

Tableau 29 : Tableau de sortie de l'équipement de gauche

VLAN-ID	Port				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Tableau 30 : Tableau de sortie de l'équipement de droite

VLAN-ID	Port				
	1	2	3	4	5
1	U				
2	T	U		U	
3	T		U		U

Les relations de communication sont ici les suivantes : les équipements terminaux sur les ports 1 et 4 de l'équipement de gauche et les équipements terminaux 2 et 4 de l'équipement de droite sont des membres du VLAN 2 et peuvent ainsi communiquer entre eux. Le comportement est le même pour les équipements terminaux sur les ports 2 et 3 de l'équipement de gauche et les équipements terminaux sur les ports 3 et 5 de l'équipement de droite. Ces éléments appartiennent au VLAN 3.

Les équipements terminaux « voient » leur partie respective du réseau. Les participants en dehors de ce VLAN sont inaccessibles. L'équipement envoie aussi des paquets Broadcast, Multicast et Unicast avec des adresses cibles inconnues (non apprises) uniquement au sein d'un VLAN.

Ici, les équipements utilisent le taggage de VLAN (IEEE 801.1Q) au sein du VLAN avec l'ID 1 (Uplink). La lettre T dans le tableau de sortie des ports indique le taggage de VLAN.

La configuration de l'exemple est identique pour l'équipement de droite. Procédez de la même façon, en utilisant les tableaux d'entrée et de sortie créés ci-dessus, pour adapter au nouvel environnement l'équipement de gauche déjà configuré.

Exécutez les étapes suivantes :

- ☐ Définition du VLAN

- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Configuration*.
- ☐ Cliquez sur le bouton  .
  La boîte de dialogue affiche la fenêtre *Create*.
- ☐ Dans le champ *VLAN ID*, spécifiez le VLAN-ID, par exemple `2`.
- ☐ Cliquez sur le bouton *Ok*.
- ☐ Pour le VLAN, spécifiez le nom `VLAN2` :
  Double-cliquez dans la colonne *Name* et spécifiez le nom.
  Pour le VLAN `1`, dans la colonne *Name*, modifiez la valeur `Default` en `VLAN1`.
- ☐ Répétez les étapes précédentes pour créer un VLAN `3` avec le nom `VLAN3`.

`enable`	Basculez sur le mode Privileged EXEC.
`vlan database`	Passer en mode de configuration VLAN.
`vlan add 2`	Crée un nouveau VLAN avec le VLAN-ID `2`.
`name 2 VLAN2`	Affecte le nom `2` au VLAN `VLAN2`.
`vlan add 3`	Crée un nouveau VLAN avec le VLAN-ID `3`.
`name 3 VLAN3`	Affecte le nom `3` au VLAN `VLAN3`.
`name 1 VLAN1`	Affecte le nom `1` au VLAN `VLAN1`.
`exit`	Basculez sur le mode Privileged EXEC.
`show vlan brief`	Affiche la configuration de VLAN actuelle.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 128
Number of currently configured VLANs........... 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                      VLAN Type VLAN Creation Time
---- --------------------------------- --------- ------------------
1       VLAN1                          default    0 days, 00:00:05
2       VLAN2                          static     0 days, 02:44:29
3       VLAN3                          static     0 days, 02:52:26
```

☐ Définition des ports

- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Port*.
- ☐ Pour affecter le port à un VLAN, spécifiez la valeur souhaitée dans la colonne correspondante.
  Valeurs possibles :
  - `T` = Le port est un membre du VLAN. Le port transmet des paquets de données taggés.
  - `U` = Le port est un membre du VLAN. Le port transmet des paquets de données non taggés.
  - `F` = Le port n'est pas un membre du VLAN.
    Les modifications à l'aide de la fonction *GVRP* sont désactivées.
  - `-` = Le port n'est pas un membre de ce VLAN.
    Les modifications à l'aide de la fonction *GVRP* sont désactivées.

  Les équipements terminaux interprétant généralement les paquets de données non taggés, vous spécifiez la valeur `U`.
  Vous spécifiez le réglage `T` sur le port uplink sur lequel les VLAN communiquent entre eux.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.
- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Port*.
- ☐ Dans la colonne *Port-VLAN ID*, spécifiez le VLAN-ID du VLAN concerné :
  `1`, `2` ou `3`
- ☐ Les équipements terminaux interprétant généralement les paquets de données non taggés, vous spécifiez, dans la colonne *Acceptable packet types*, la valeur `admitAll` pour les ports de l'équipement terminal.
- ☐ Pour le port uplink, dans la colonne *Acceptable packet types*, spécifiez la valeur `admitOnlyVlanTagged`.
- ☐ Cochez la case dans la colonne *Ingress filtering* pour les ports uplink afin d'évaluer les tags de VLAN sur ce port.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`vlan participation include 1`	Le port `1/1` devient un membre du VLAN `1` et transmet les paquets de données sans tag de VLAN.
`vlan participation include 2`	Le port `1/1` devient un membre du VLAN `2` et transmet les paquets de données sans tag de VLAN.
`vlan tagging 2 enable`	Le port `1/1` devient un membre du VLAN `2` et transmet les paquets de données avec un tag de VLAN.
`vlan participation include 3`	Le port `1/1` devient un membre du VLAN `3` et transmet les paquets de données sans tag de VLAN.
`vlan tagging 3 enable`	Le port `1/1` devient un membre du VLAN `3` et transmet les paquets de données avec un tag de VLAN.
`vlan pvid 1`	Affectez le VLAN-ID du port `1` au port `1/1`.
`vlan ingressfilter`	Activez le filtrage à l'entrée sur le port `1/1`.
`vlan acceptframe vlanonly`	Le port `1/1` ne transfère que les paquets avec un tag de VLAN.
`exit`	Basculez sur le mode de configuration.
`interface 1/2`	Basculez sur le mode de configuration de l'interface `1/2`.
`vlan participation include 2`	Le port `1/2` devient un membre du VLAN `2` et transmet les paquets de données sans tag de VLAN.
`vlan pvid 2`	Affectez le VLAN-ID du port `2` au port `1/2`.
`exit`	Basculez sur le mode de configuration.
`interface 1/3`	Basculez sur le mode de configuration de l'interface `1/3`.
`vlan participation include 3`	Le port `1/3` devient un membre du VLAN `3` et transmet les paquets de données sans tag de VLAN.
`vlan pvid 3`	Affectez le VLAN-ID du port `3` au port `1/3`.
`exit`	Basculez sur le mode de configuration.
`interface 1/4`	Basculez sur le mode de configuration de l'interface `1/4`.
`vlan participation include 2`	Le port `1/4` devient un membre du VLAN `2` et transmet les paquets de données sans tag de VLAN.
`vlan pvid 2`	Affectez le VLAN-ID du port `2` au port `1/4`.
`exit`	Basculez sur le mode de configuration.
`interface 1/5`	Basculez sur le mode de configuration de l'interface `1/5`.
`vlan participation include 3`	Le port `1/5` devient un membre du VLAN `3` et transmet les paquets de données sans tag de VLAN.

```
vlan pvid 3                                          Affectez le VLAN-ID du port 3 au port 1/5.
exit                                                 Basculez sur le mode de configuration.
exit                                                 Basculez sur le mode Privileged EXEC.
show vlan id 3                                       Affiche les détails du VLAN 3.
VLAN ID.....................3
VLAN Name...................VLAN3
VLAN Type...................Static
VLAN Creation Time...........0 days, 00:07:47 (System Uptime)
VLAN Routing.................disabled

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         -         Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         -         Autodetect   Untagged
1/5         Include   Include      Untagged
```

12.2 Guest VLAN / Unauthenticated VLAN

Un Guest VLAN permet à un équipement de fournir un contrôle d'accès au réseau basé sur des ports (IEEE 802.1x) à des demandeurs non compatibles 802.1x. Cette fonctionnalité constitue un mécanisme que permet aux invités d'accéder aux réseaux externes uniquement. Si vous connectez des demandeurs non compatibles 802.1x à un port 802.1x non autorisé actif, les demandeurs n'envoient aucune réponse aux requêtes 802.1x. Les demandeurs n'envoyant aucune réponse, le port reste à l'état non autorisé. Les demandeurs n'ont pas accès aux réseaux externes.

Le demandeur Guest VLAN correspond à une configuration de base par port. Lorsque vous configurez un port en tant que Guest VLAN et que vous connectez des demandeurs non compatibles 802.1x à ce port, l'équipement affecte les demandeurs au Guest VLAN. L'ajout de demandeurs à un Guest VLAN entraîne le passage du port à l'état autorisé, permettant ainsi aux demandeurs d'accéder aux réseaux externes.

Un Unauthenticated VLAN permet à l'équipement de fournir des services aux demandeurs compatibles 802.1x qui ne s'authentifient pas correctement. Cette fonction permet aux demandeurs non autorisés d'accéder à des services limités. Si vous configurez un Unauthenticated VLAN sur un port avec authentification de port 802.1x et que le fonctionnement global est activé, l'équipement place le port dans un Unauthenticated VLAN. Lorsqu'un demandeur compatible 802.1x s'authentifie de manière incorrecte sur le port, l'équipement ajoute le demandeur au Unauthenticated VLAN. Si vous configurez également un Guest VLAN sur le port, les demandeurs non compatibles 802.1x utilisent le Guest VLAN.

Si le port a un Unauthenticated VLAN affecté, le compte à rebours de réauthentification s'enclenche. Lorsque le délai spécifié dans la colonne *Reauthentication period [s]* est écoulé et que des demandeurs sont présents sur le port, le Unauthenticated VLAN se réauthentifie. Si aucun demandeur n'est présent, l'équipement place le port dans le Guest VLAN configuré.

L'exemple suivant explique comment créer un Guest VLAN. Créez un Unauthorized VLAN de la même manière.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Configuration*.
- ☐ Cliquez sur le bouton  .
  La boîte de dialogue affiche la fenêtre *Create*.
- ☐ Dans le champ *VLAN ID*, spécifiez la valeur `10`.
- ☐ Cliquez sur le bouton *Ok*.
- ☐ Pour le VLAN, spécifiez le nom `Guest`:
  Double-cliquez dans la colonne *Name* et spécifiez le nom.
- ☐ Cliquez sur le bouton  .
  La boîte de dialogue affiche la fenêtre *Create*.
- ☐ Dans le champ *VLAN ID*, spécifiez la valeur `20`.
- ☐ Cliquez sur le bouton *Ok*.
- ☐ Pour le VLAN, spécifiez le nom `Not authorized`:
  Double-cliquez dans la colonne *Name* et spécifiez le nom.
- ☐ Ouvrez la boîte de dialogue *Network Security > 802.1X Port Authentication > Global*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

- ☐ Ouvrez la boîte de dialogue *Network Security > 802.1X Port Authentication > Port Configuration*.
- ☐ Spécifiez les réglages suivants pour le port `1/4` :
  - La valeur `auto` dans la colonne *Port control*
  - La valeur `10` dans la colonne *Guest VLAN ID*
  - La valeur `20` dans la colonne *Unauthenticated VLAN ID*
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`vlan database`	Passer en mode de configuration VLAN.
`vlan add 10`	Crée le VLAN `10`.
`vlan add 20`	Crée le VLAN `20`.
`name 10 Guest`	Renomme le VLAN `10` en `Guest`.
`name 20 Unauth`	Renomme le VLAN `20` en `Unauth`.
`exit`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`dot1x system-auth-control enable`	Active la fonction *802.1X Port Authentication* globalement.
`dot1x port-control auto`	Active le contrôle de port sur le port `1/4`.
`interface 1/4`	Basculez sur le mode de configuration de l'interface `1/4`.
`dot1x guest-vlan 10`	Affectez le guest vlan au port `1/4`.
`dot1x unauthenticated-vlan 20`	Affectez le unauthorized vlan au port `1/4`.
`exit`	Basculez sur le mode de configuration.

12.3 Affectation du VLAN RADIUS

La fonctionnalité d'affectation du VLAN RADIUS permet d'associer un VLAN-ID RADIUS à un client authentifié. Lorsqu'un client s'authentifie correctement et que le serveur RADIUS envoie un attribut de VLAN, l'équipement associe le client au VLAN affecté à RADIUS. Ainsi, l'équipement ajoute le port physique en tant que membre au VLAN correspondant et définit le VLAN-ID du port (PVID) avec la valeur donnée. Le port transmet les paquets de données sans tag de VLAN.

12.4 Création d'un Voice VLAN

Utilisez la fonctionnalité Voice VLAN pour séparer les trafics de voix et de données sur un port, par VLAN et/ou par priorité. L'un des principaux avantages de l'utilisation d'un Voice VLAN est la préservation de la qualité sonore d'un téléphone IP en cas de trafic de données élevé sur le port.

L'équipement utilise l'adresse MAC source pour identifier et prioriser le flux de données voix. L'utilisation d'une adresse MAC pour identifier les équipements permet d'éviter qu'un client malveillant ne se connecte au même port, entraînant ainsi la détérioration du trafic voix.

Un autre avantage de la fonctionnalité Voice VLAN est qu'un téléphone VoIP obtient un VLAN-ID ou des informations de priorité via LLDP-MED. Par conséquent, le téléphone VoIP envoie des données de voix taggées, taggées en priorité ou bien non taggées. Cela dépend de la configuration de l'interface du Voice VLAN.

Les modes suivants sont possibles pour l'interface du Voice VLAN. Les 3 premières méthodes distinguent et priorisent les trafics de voix et de données. La distinction des trafics se traduit par une qualité accrue du trafic de voix lors des périodes de trafic élevé.

- Configurer le port pour utiliser le mode `vlan` permet à l'équipement de tagger les données de voix provenant d'un téléphone VoIP avec le VLAN-ID voix défini par l'utilisateur. L'équipement affecte des données régulières au VLAN-ID du port par défaut.
- Configurer le port pour utiliser le mode `dot1p-priority` permet à l'équipement de tagger les données provenant d'un téléphone VoIP avec le VLAN 0 et la priorité définie par l'utilisateur. L'équipement affecte la priorité par défaut du port aux données régulières.
- Configurez le VLAN-ID voix et la priorité à l'aide du mode `vlan/dot1p-priority`. Dans ce mode, le téléphone VoIP envoie les données de voix avec le VLAN-ID voix et les informations de priorité définis par l'utilisateur. L'équipement affecte le PVID et la priorité par défaut du port aux données régulières.
- S'il est configuré comme `untagged`, le téléphone envoie des paquets non taggés.
- S'il est configuré comme `none`, le téléphone utilise sa propre configuration pour envoyer le trafic de voix.

13 Redondance

13.1 Topologie de réseau comparée aux protocoles de redondance

Lors de l'utilisation d'Ethernet, une condition préalable importante est que les paquets de données suivent un chemin unique de l'expéditeur au destinataire. Les topologies de réseau suivantes satisfont à cette condition requise :

- Topologie en ligne
- Topologie en étoile
- Topologie arborescente

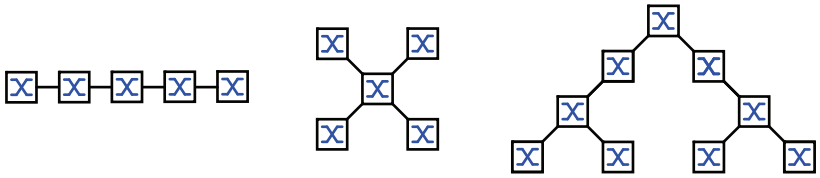


Figure 28 : Réseau avec topologies en ligne, en étoile et arborescente

Pour conserver la communication en cas de détection d'une défaillance de la liaison, installez des liaisons physiques supplémentaires entre les nœuds du réseau. Les protocoles de redondance permettent de s'assurer que les liaisons supplémentaires restent désactivées tant que la liaison initiale fonctionne. Lorsqu'une défaillance de la liaison est détectée, le protocole de redondance génère un nouveau chemin entre l'expéditeur et le destinataire via la liaison alternative.

Pour introduire de la redondance dans la couche 2, vous définissez d'abord de quelle topologie de réseau vous avez besoin. En fonction de la topologie de réseau sélectionnée, vous choisissez ensuite les protocoles de redondance qui peuvent être utilisés avec cette topologie de réseau.

13.1.1 Topologies de réseau

Topologie maillée

Pour les réseaux avec des topologies en étoile ou arborescentes, les procédures de redondance ne sont possibles qu'en liaison avec la création d'une boucle physique. Le résultat est une topologie maillée.

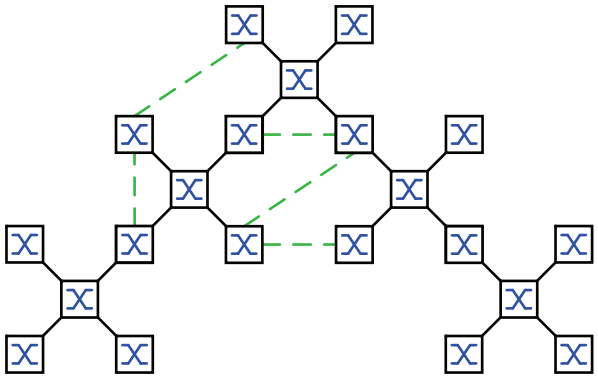


Figure 29 : Topologie maillée : topologie arborescente avec des boucles physiques

Pour fonctionner dans cette topologie de réseau, l'équipement vous fournit les protocoles de redondance suivants :

- Rapid Spanning Tree (RSTP)

Topologie en anneau

Dans les réseaux avec une topologie en ligne, vous pouvez utiliser des procédures de redondance en connectant les extrémités de la ligne. Cela génère une topologie en anneau.

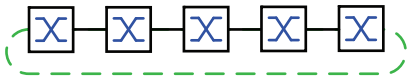


Figure 30 : Topologie en anneau : topologie en ligne avec extrémités connectées

Pour fonctionner dans cette topologie de réseau, l'équipement vous fournit les protocoles de redondance suivants :

- Media Redundancy Protocol (MRP)
- Rapid Spanning Tree (RSTP)

13.1.2 Protocoles de redondance

Pour fonctionner dans différentes topologies de réseau, l'équipement vous fournit les protocoles de redondance suivants :

Tableau 31 : Vue d'ensemble des protocoles de redondance

Protocole de redondance	Topologie de réseau	Remarques
MRP	Anneau	Le temps de commutation peut être sélectionné et est pratiquement indépendant du nombre d'équipements. Un anneau MRP comprend jusqu'à 50 équipements qui prennent en charge le protocole MRP conformément à la norme technique IEC 62439. Si vous n'utilisez que des équipements Schneider Electric, jusqu'à 100 équipements sont possibles dans l'anneau MRP.
Sous-anneau	Anneau	La fonction *Sub Ring* vous permet de coupler facilement des segments de réseau à des couplages d'anneaux redondants.
Ring/Network Coupling	Anneau	
RCP	Anneau	
RSTP	Structure aléatoire	Le temps de commutation dépend de la topologie de réseau et du nombre d'équipements. ▶ typ. < 1 s avec RSTP ▶ typ. < 30 s avec STP
Agrégation de liens	Structure aléatoire	Un groupe d'agrégation de liens est la combinaison d'au moins 2 liaisons point à point full duplex fonctionnant avec le même débit sur un commutateur réseau unique pour augmenter la bande passante.
Link Backup	Structure aléatoire	Lorsque l'équipement détecte une erreur sur la liaison principale, il transfère le trafic sur la liaison de secours. Link Backup s'utilise typiquement dans les réseaux de prestataires de services ou d'entreprises.
Client HIPER Ring	Anneau	Étend un HIPER Ring existant ou remplace un équipement participant déjà en tant que client dans un HIPER Ring.
HIPER Ring sur LAG	Anneau	Relie les équipements entre eux par l'intermédiaire d'un groupe d'agrégation de liens (LAG). Les clients de l'anneau et le gestionnaire d'anneau se comportent de la même manière qu'un anneau sans instance LAG.

Si le contrôle de flux et la fonction de redondance sont activés simultanément, la fonction de redondance peut ne pas fonctionner comme prévu.

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Si vous utilisez une fonction de redondance, désactivez le contrôle de flux sur les ports impliqués de l'équipement.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

13.1.3 Combinaisons de redondances

Tableau 32 : Vue d'ensemble des protocoles de redondance

	MRP	RSTP	Link Aggreg.	Link Backup	Sous-anneau	HIPER Ring
MRP	▲	– – –	– – –	– – –	– – –	– – –
RSTP	▲ 1)	▲	– – –	– – –	– – –	– – –
Link Aggreg.	▲ 2)	▲ 2)	▲	– – –	– – –	– – –
Link Backup	▲	▲	▲	▲	– – –	– – –
Sous-anneau	▲	▲	▲ 2)	▲	▲	– – –
HIPER Ring	▲	▲ 1)	▲ 2)	▲	▲	▲

▲ Combinaison possible

1) Un couplage redondant entre ces topologies de réseau est susceptible de générer des boucles.
Pour coupler ces topologies de manière redondante, reportez-vous au chapitre « FuseNet » à la page 226.

2) Combinaison possible sur le même port

13.2 Media Redundancy Protocol (MRP)

Depuis mai 2008, le Media Redundancy Protocol (MRP) est une solution standardisée pour la redondance d'anneau dans les environnements industriels.

MRP est compatible avec le couplage d'anneau redondant, prend en charge les VLAN et se distingue par des temps de reconfiguration très courts.

Un anneau MRP comprend jusqu'à 50 équipements qui prennent en charge le protocole MRP conformément à la norme technique IEC 62439. Si vous n'utilisez que des équipements Schneider Electric, jusqu'à 100 équipements sont possibles dans l'anneau MRP.

Lorsque vous utilisez le port redondant MRP fixe (Fixed Backup) et qu'une défaillance de la liaison d'anneau principale est détectée, le gestionnaire d'anneau transfère les données sur la liaison de l'anneau secondaire. Une fois la liaison principale restaurée, la liaison secondaire continue d'être utilisée.

13.2.1 Structure du réseau

Le concept de redondance d'anneau vous permet de réaliser des structures de réseaux en anneau hautement disponibles.

Grâce à la fonction RM (**R**ing**M**anager, ou gestionnaire d'anneau), les deux extrémités d'une dorsale dans une structure linéaire peuvent être connectées en un couplage d'anneau redondant. Le gestionnaire d'anneau conserve la ligne redondante ouverte tant que la structure linéaire est intacte. En cas de défaillance d'un segment, le gestionnaire d'anneau ferme immédiatement la ligne redondante, et la structure linéaire est de nouveau intacte.

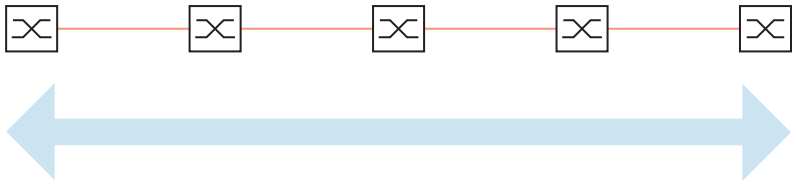


Figure 31 : Structure linéaire

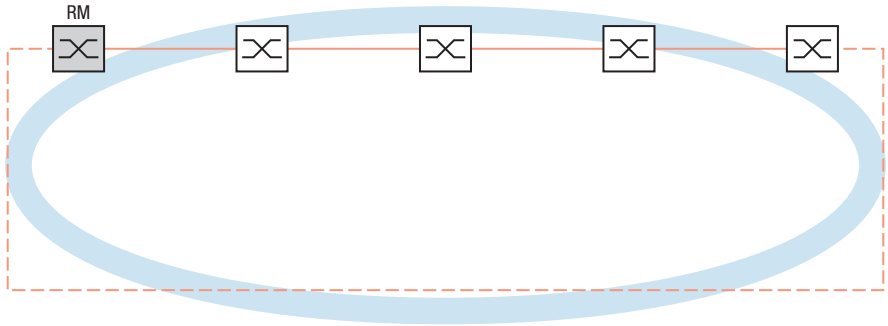


Figure 32 : Structure en couplage d'anneau redondant
RM = gestionnaire d'anneau
—— ligne principale
- - - ligne redondante

13.2.2 Temps de reconfiguration

Lorsqu'une défaillance de la section de ligne est détectée, le gestionnaire d'anneau rétablit la structure linéaire de l'anneau MRP. Vous définissez le délai maximum pour la reconfiguration de la ligne dans le gestionnaire d'anneau.

Valeurs possibles pour le délai maximum :
- *500ms*
- *30ms*

Commentaire : Si chaque équipement dans l'anneau prend en charge un délai plus court, vous pouvez configurer le temps de reconfiguration avec une valeur inférieure à *500ms*.

Sinon, les équipements qui ne prennent en charge que des délais plus longs peuvent ne pas être accessibles en raison d'une surcharge. Cela peut entraîner la génération de boucles.

13.2.3 Mode avancé

Pour les délais encore plus courts que les temps de reconfiguration spécifiés, l'équipement fournit le mode avancé. Lorsque les participants à l'anneau informent le gestionnaire d'anneau des interruptions dans l'anneau via des notifications de défaillance de la liaison, le mode avancé accélère la détection de la défaillance de la liaison.

Les équipements Schneider Electric prennent en charge les notifications de défaillance de liaison. Aussi, vous activez généralement le mode avancé dans le gestionnaire d'anneau.

Lorsque vous utilisez des équipements qui ne prennent pas en charge les notifications de défaillance de liaison, le gestionnaire d'anneau reconfigure la ligne dans le temps de reconfiguration maximum défini.

13.2.4 Conditions préalables pour MRP

Avant de définir un anneau MRP, vérifiez que les conditions suivantes sont remplies :
- Tous les participants à l'anneau prennent en charge MRP.
- Les participants à l'anneau sont interconnectés via les ports d'anneau. Outre les voisins de l'équipement, aucun autre participant à l'anneau n'est connecté à l'équipement concerné.
- Tous les participants à l'anneau prennent en charge le temps de configuration spécifié dans le gestionnaire d'anneau.
- Il n'y a qu'un seul gestionnaire d'anneau dans l'anneau.

Si vous utilisez des VLAN, configurez chaque port d'anneau avec les réglages suivants :

- ☐ Désactivez le filtrage à l'entrée - voir la boîte de dialogue *Switching > VLAN > Port*.
- ☐ Définissez le VLAN-ID du port (PVID) - voir la boîte de dialogue *Switching > VLAN > Port*.
  - PVID = `1` dans les cas où l'équipement transmet les paquets de données MRP non taggés (VLAN-ID = `0` dans la boîte de dialogue *Switching > L2-Redundancy > MRP*)
    En définissant le PVID = `1`, l'équipement affecte automatiquement les paquets non taggés reçus au VLAN 1.
  - PVID = `any` dans les cas où l'équipement transmet les paquets de données MRP dans un VLAN (VLAN-ID ≥ `1` dans la boîte de dialogue *Switching > L2-Redundancy > MRP*)
- ☐ Définissez les règles à la sortie - voir la boîte de dialogue *Switching > VLAN > Configuration*.
  - `U` (non taggé) pour les ports d'anneau du VLAN 1 dans les cas où l'équipement transmet les paquets de données MRP non taggés (VLAN-ID = `0` dans la boîte de dialogue *Switching > L2-Redundancy > MRP*, l'anneau MRP n'est pas affecté à un VLAN).
  - `T` (taggé) pour les ports d'anneau du VLAN que vous affectez à l'anneau MRP. Sélectionnez `T` dans les cas où l'équipement transmet les paquets de données MRP dans un VLAN (VLAN-ID ≥ `1` dans la boîte de dialogue *Switching > L2-Redundancy > MRP*).

13.2.5 Exemple de configuration

Un réseau dorsal contient 3 équipements dans une structure linéaire. Pour augmenter la disponibilité du réseau, vous convertissez la structure linéaire en une structure en couplage d'anneau redondant. Des équipements de différents constructeurs sont utilisés. Tous les équipements prennent en charge MRP. Sur chaque équipement, vous définissez les ports 1.1 et 1.2 comme ports d'anneau.

Lorsqu'une défaillance de la liaison d'anneau principale est détectée, le gestionnaire d'anneau envoie les données sur la liaison d'anneau secondaire. Lorsque la liaison principale est restaurée, la liaison secondaire bascule de nouveau en mode de secours.

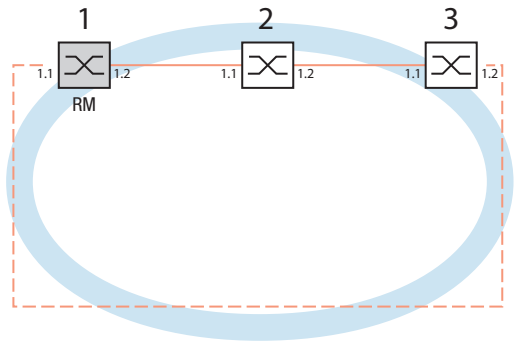


Figure 33 : Exemple d'anneau MRP
RM = gestionnaire d'anneau
—— ligne principale
- - - ligne redondante

L'exemple de configuration suivant décrit la configuration de l'équipement du gestionnaire d'anneau (1). Vous configurez les deux autres équipements (2 à 3) de la même manière, mais sans activer la fonction *Ring manager*. Cet exemple n'utilise pas de VLAN. Vous spécifiez la valeur *30ms* comme temps de restauration de l'anneau. Chaque équipement prend en charge le mode avancé du gestionnaire d'anneau.

- ☐ Définissez le réseau en fonction de vos besoins.
- ☐ Configurez chaque port de manière à ce que la vitesse de transmission et les réglages duplex des lignes correspondent au tableau suivant :

Tableau 33 : Réglages des ports d'anneau

Type de port	Débit	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	coché	case non cochée	*100 Mbit/s FDX*
TX	1 Gbit/s	coché	coché	–
Optique	100 Mbit/s	coché	case non cochée	*100 Mbit/s FDX*
Optique	1 Gbit/s	coché	coché	–
Optique	2.5 Gbit/s	coché	–	*2.5 Gbit/s FDX*

Commentaire : Vous configurez des ports optiques sans prise en charge de l'auto-négociation (configuration automatique) avec 100 Mbit/s full duplex (FDX) ou 1000 Mbit/s full duplex (FDX).

Commentaire : Vous configurez des ports optiques sans prise en charge de l'auto-négociation (configuration automatique) avec 100 Mbit/s full duplex (FDX).

Commentaire : Configurez chaque équipement de l'anneau MRP individuellement. Avant de raccorder la ligne redondante, vérifiez que vous avez terminé la configuration de chaque équipement de l'anneau MRP. Vous évitez ainsi les boucles pendant la phase de configuration.

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Pour éviter les boucles durant la phase de configuration, configurez chaque équipement de la configuration *MRP* individuellement. Avant de raccorder les lignes redondantes, terminez la configuration des autres équipements de la configuration de l'anneau.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Vous désactivez le contrôle de flux sur les ports impliqués.

Si le contrôle de flux et la fonction de redondance sont activés simultanément, la fonction de redondance peut ne pas fonctionner comme prévu. (Réglage par défaut : contrôle de flux désactivé globalement et activé sur chaque port.)

Désactivez la fonction *Spanning Tree* function dans chaque équipement du réseau. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Désactivez la fonction.
  Dans l'état à la livraison, Spanning Tree est activé sur l'équipement.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`no spanning-tree operation`	Désactive Spanning Tree.
`show spanning-tree global`	Affiche les paramètres pour la vérification.

Activez MRP sur chaque équipement dans le réseau. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > MRP*.
- ☐ Spécifiez les ports d'anneau de votre choix.

Dans l'interface de ligne de commande, vous définissez d'abord un paramètre supplémentaire, l'ID de domaine MRP. Configurez chaque participant à l'anneau avec le même ID de domaine MRP. L'ID de domaine MRP est une séquence de 16 blocs de chiffres (valeurs de 8 bits).

Lors de la configuration avec l'interface utilisateur graphique, l'équipement utilise la valeur par défaut `255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255`.

`mrp domain add default-domain`	Crée un nouveau domaine MRP avec l'ID `default-domain`.
`mrp domain modify port primary 1/1`	Spécifie le port *1/1* en tant que port d'anneau `1`.
`mrp domain modify port secondary 1/2`	Spécifie le port *1/2* en tant que port d'anneau `2`.

Activez le port *Fixed backup*. Pour ce faire, exécutez les étapes suivantes :

- ☐ Activez le gestionnaire d'anneau.
  Pour les autres équipements dans l'anneau, conservez le réglage *Off*.
- ☐ Pour permettre à l'équipement de continuer à envoyer des données sur le port secondaire une fois l'anneau restauré, cochez la case *Fixed backup*.

Commentaire : Lorsque l'équipement bascule de nouveau sur le port principal, le délai de restauration maximal de l'anneau peut être dépassé.

Lorsque vous décochez la case *Fixed backup* et que l'anneau est restauré, le gestionnaire d'anneau bloque le port secondaire et débloque le port principal.

`mrp domain modify port secondary 1/2 fixed-backup enable`	Active la fonction *Fixed backup* sur le port secondaire. Le port secondaire continue de transférer des données une fois l'anneau restauré.

☐ Activez le gestionnaire d'anneau.
Pour les autres équipements dans l'anneau, conservez le réglage *Off*.

```
mrp domain modify mode   manager
```

Spécifie que l'équipement fonctionne en tant que *Ring manager*. Pour les autres équipements dans l'anneau, conservez le réglage par défaut.

☐ Cochez la case dans le champ *Advanced mode*.

```
mrp domain modify   advanced-mode
enabled
```

Active le mode avancé.

☐ Dans le champ *Ring recovery*, sélectionnez la valeur *30ms*.

```
mrp domain modify   recovery-delay
200ms
```

Spécifie la valeur *30ms* comme étant le délai maximal pour la reconfiguration de l'anneau.

Commentaire : Si sélectionner la valeur *30ms* pour la restauration de l'anneau ne permet pas d'atteindre la stabilité requise pour satisfaire aux besoins de votre réseau, sélectionnez la valeur *500ms*.

☐ Activez la fonction de l'anneau MRP.
☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

```
mrp domain modify operation   enable
```

Active l'anneau MRP.

Lorsque chaque participant à l'anneau est configuré, fermez la ligne en un anneau. Pour cela, connectez les équipements aux extrémités de la ligne via leurs ports d'anneau.

Vérifiez les messages émis par l'équipement. Pour ce faire, exécutez les étapes suivantes :

```
show mrp
```

Affiche les paramètres pour la vérification.

Le champ *Operation* affiche le mode opérationnel du port d'anneau.

Valeurs possibles :

- `forwarding`
  Le port est activé, la liaison est établie.
- `blocked`
  Le port est bloqué, la liaison est établie.
- `disabled`
  Le port est désactivé.
- `not-connected`
  Aucune liaison n'est établie.

Le champ *Information* affiche les messages pour la configuration de la redondance et les causes possibles des erreurs détectées.

Lorsque l'équipement fonctionne en tant que client de l'anneau ou gestionnaire de l'anneau, les messages suivants sont possibles :

- *Redundancy available*
  La redondance est définie. Lorsqu'un composant de l'anneau est défaillant, la ligne redondante prend le relais.
- *Configuration error: Error on ringport link.*
  Une erreur est détectée dans le câblage des ports de l'anneau.

Lorsque l'équipement fonctionne en tant que gestionnaire de l'anneau, les messages suivants sont possibles :

- *Configuration error: Packets from another ring manager received.*
  Il existe un autre équipement dans l'anneau qui fonctionne en tant que gestionnaire de l'anneau.
  Activez la fonction *Ring manager* sur un seul équipement dans l'anneau.
- *Configuration error: Ring link is connected to wrong port.*
  Une ligne dans l'anneau est connectée avec un port autre que le port de l'anneau. L'équipement ne reçoit que les paquets de données de test sur un port de l'anneau.

Si possible, intégrez l'anneau MRP dans un VLAN. Pour ce faire, exécutez les étapes suivantes :

- ☐ Dans le champ *VLAN ID*, définissez le VLAN-ID MRP. Le VLAN-ID MRP détermine dans lequel des VLAN configurés l'équipement transmet les paquets MRP.
  Pour définir le VLAN-ID MRP, configurez d'abord les VLAN et les règles à la sortie dans la boîte de dialogue *Switching > VLAN > Configuration*.
  - Si l'anneau MRP n'est pas affecté à un VLAN (comme dans cet exemple), laissez le VLAN-ID défini sur `0`.
    Dans la boîte de dialogue *Switching > VLAN > Configuration*, spécifiez l'appartenance au VLAN avec `U` (non taggé) pour les ports d'anneau dans le VLAN `1`.
  - Si l'anneau MRP est affecté à un VLAN, saisissez un VLAN-ID >`0`.
    Dans la boîte de dialogue *Switching > VLAN > Configuration*, spécifiez l'appartenance au VLAN avec `T` (taggé) pour les ports d'anneau dans le VLAN sélectionné.

`mrp domain modify vlan <0..4042>`	Affecte le VLAN-ID.

13.2.6 MRP sur LAG

Les équipements Schneider Electric vous permettent de combiner des groupes d'agrégation de liens (LAG) pour augmenter la bande passante avec le Media Redundancy Protocol (MRP) assurant la redondance. Cette fonction vous permet d'augmenter la bande passante sur des segments individuels ou sur l'ensemble du réseau.

La fonction *Link Aggregation* vous permet de surmonter les restrictions inhérentes à la bande passante des ports individuels. LAG vous permet de combiner au moins 2 liaisons en parallèle, créant ainsi une liaison logique entre 2 équipements. Les liaisons parallèles augmentent la bande passante pour le flux de données entre les 2 équipements.

Un anneau MRP comprend jusqu'à 50 équipements qui prennent en charge le protocole MRP conformément à la norme technique IEC 62439. Si vous n'utilisez que des équipementsSchneider Electric, le protocole vous permet de configurer des anneaux MRP avec un maximum de 100 équipements.

Vous utilisez MRP sur LAG dans les cas suivants :
- pour augmenter la bande passante uniquement sur des segments spécifiques d'un anneau MRP
- pour augmenter la bande passante sur l'ensemble de l'anneau MRP

Structure du réseau

Lors de la configuration d'un anneau MRP avec des LAG, le gestionnaire d'anneau (RM) surveille la continuité des deux extrémités de la dorsale. Le RM bloque les données sur le port secondaire (redondant) tant que la dorsale est intacte. Lorsque le RM détecte une interruption du flux de données sur l'anneau, il commence à transmettre les données sur le port secondaire, ce qui rétablit la continuité de la dorsale.

Vous utilisez les instances LAG dans les anneaux MRP uniquement pour augmenter la bande passante ; dans ce cas, MRP assure la redondance.

Afin que le RM puisse détecter une interruption sur l'anneau, MRP requiert qu'un équipement bloque chaque port de l'instance LAG si un port de l'instance est défaillant.

LAG sur un segment unique d'un anneau MRP

L'équipement vous permet de configurer une instance LAG sur des segments spécifiques d'un anneau MRP.

Vous utilisez la méthode de commutation simple LAG pour les équipements de l'anneau MRP. La méthode de commutation simple constitue un moyen peu onéreux d'étendre votre réseau en utilisant un seul équipement de chaque côté d'un segment pour fournir les ports physiques. Vous regroupez les ports de l'équipement dans une instance LAG afin de fournir une bande passante accrue sur des segments spécifiques selon les besoins.

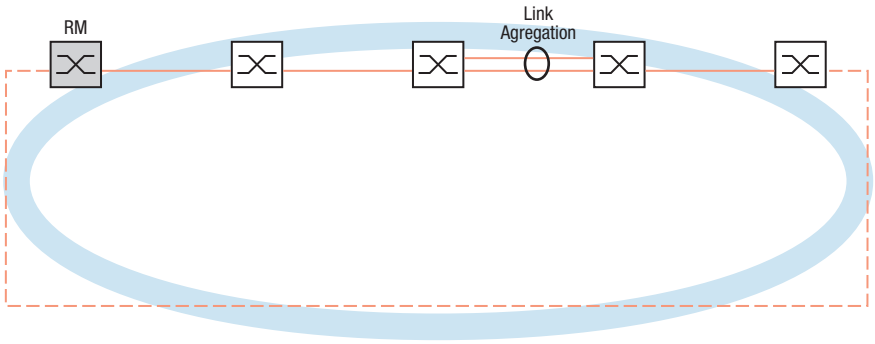


Figure 34 : Agrégation de liens sur un segment unique d'un anneau MRP.

LAG sur un anneau MRP entier

Outre la possibilité de configurer une instance LAG sur des segments spécifiques d'un anneau MRP, les équipements Schneider Electric vous permettent également de configurer des instances LAG sur chaque segment, ce qui augmente la bande passante sur l'ensemble de l'anneau MRP.

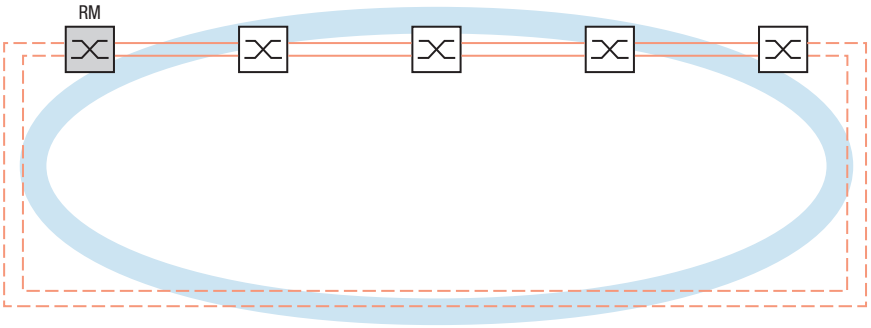


Figure 35 : Agrégation de liens sur l'ensemble de l'anneau MRP.

Détection des interruptions sur l'anneau

Lors de la configuration de l'instance LAG, spécifiez la valeur *Active ports (min.)* pour qu'elle soit égale au nombre total de ports utilisés dans l'instance LAG. Lorsqu'un équipement détecte une interruption sur un port de l'instance LAG, il bloque les données sur les autres ports de l'instance. Avec chaque port d'une instance bloqué, le RM détecte que l'anneau est ouvert et se met à transmettre les données sur le port secondaire. De cette façon, le RM est en mesure de rétablir la continuité des équipements de l'autre côté du segment interrompu.

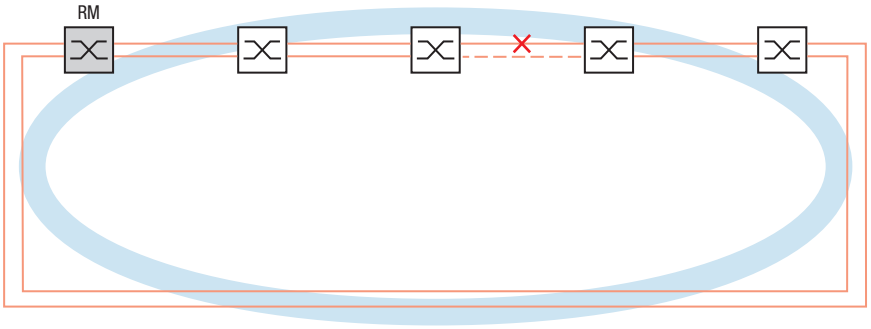


Figure 36 : Interruption d'une liaison dans un anneau MRP.

Exemple de configuration

Dans l'exemple suivant, le commutateur A et le commutateur B relient deux segments entre eux. Les segments produisent un trafic trop important pour que la bande passante des ports individuels puisse le gérer. Vous configurez une instance LAG pour le segment unique de l'anneau MRP, augmentant ainsi la bande passante du segment.

La condition préalable à cet exemple de configuration est que vous commenciez avec un anneau MRP opérationnel.

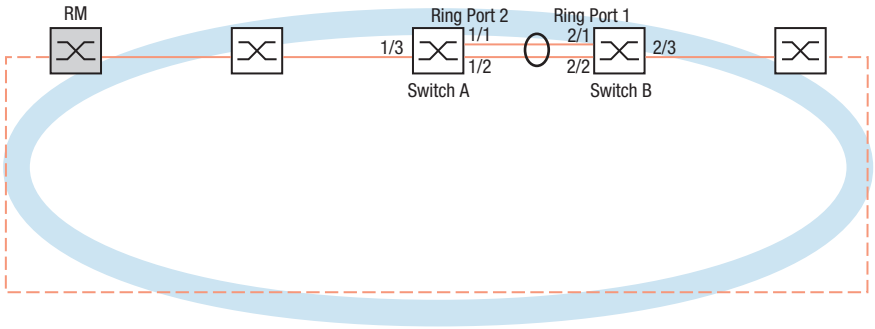


Figure 37 : Exemple de configuration MRP sur LAG

Configurez d'abord le commutateur A. Pour ce faire, exécutez les étapes suivantes. Puis, configurez le commutateur B en suivant les mêmes étapes mais en substituant les numéros de port et de port d'anneau correspondants.

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Link Aggregation*.
- ☐ Cliquez sur le bouton .
  La boîte de dialogue affiche la fenêtre *Create*.
- ☐ Dans la liste déroulante *Trunk port*, sélectionnez le numéro d'instance du groupe d'agrégation de liens.
- ☐ Dans la liste déroulante *Port*, sélectionnez le port *1/1*.

- ☐ Cliquez sur le bouton *Ok*.
- ☐ Répétez les étapes précédentes et sélectionnez le port *1/2*.
- ☐ Cliquez sur le bouton *Ok*.
- ☐ Dans la colonne *Active ports (min.)*, saisissez `2`, ce qui correspond dans ce cas au nombre total de ports de l'instance. Lorsque vous combinez MRP et LAG, vous spécifiez le nombre total de ports comme *Active ports (min.)*. Lorsque l'équipement détecte une interruption sur un port, il bloque les autres ports de l'instance, ce qui entraîne l'ouverture de l'anneau. Le gestionnaire d'anneau détecte que l'anneau est ouvert et se met à transmettre les données sur son port d'anneau secondaire, ce qui rétablit la connectivité avec les autres équipements du réseau.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.
- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > MRP*.
- ☐ Dans le cadre *Ring port 2*, sélectionnez le port `lag/1` dans la liste déroulante *Port*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`link-aggregation add lag/1`	Crée un groupe d'agrégation de liens `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Ajoute le port *1/1* au groupe d'agrégation de liens.
`link-aggregation modify lag/1 addport 1/2`	Ajoute le port *1/2* au groupe d'agrégation de liens.
`mrp domain modify port secondary lag/1`	Spécifie le port `lag/1` en tant que port d'anneau `2`.
`copy config running-config nvm`	Sauvegardez les réglages actuels dans la mémoire non volatile (`nvm`) dans le profil de configuration « Selected » (Sélectionné).

13.3 Client HIPER Ring

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Pour éviter les boucles durant la phase de configuration, configurez chaque équipement de la configuration *HIPER Ring* individuellement. Avant de raccorder les lignes redondantes, terminez la configuration des autres équipements de la configuration de l'anneau.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Le concept de redondance en HIPER Ring permet d'établir des structures réseau annulaires et hautement disponibles. La fonction Client *HIPER Ring* permet à l'administrateur réseau d'étendre un HIPER Ring existant ou de remplacer un équipement client déjà impliqué dans un HIPER Ring.

Lorsque l'équipement détecte un défaillance de la liaison sur un port d'anneau, il envoie un paquet LinkDown au gestionnaire d'anneau (RM) et vide la table FDB. Lorsque le RM reçoit le paquet LinkDown, il transmet immédiatement le flux de données via les ports d'anneau principal et secondaire. Ainsi, le RM est à même de maintenir l'intégrité du HIPER Ring.

L'équipement ne prend en charge que les ports Fast Ethernet et Gigabit Ethernet en tant que ports d'anneau. De plus, vous pouvez inclure les ports d'anneau dans une instance LAG.

À l'état par défaut, le HIPER Ring est désactivé et les ports principal et secondaire sont définis sur `no Port`.

Commentaire : Désactivez le Spanning Tree Protocol (STP) pour les ports d'anneau dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*, car STP et HIPER Ring ont des temps de réaction différents.

Tableau 34 : Réglages des ports d'anneau

Type de port	Débit	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`coché`	`case non cochée`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`coché`	`coché`	–
Optique	100 Mbit/s	`coché`	`case non cochée`	*`100 Mbit/s FDX`*
Optique	1 Gbit/s	`coché`	`coché`	–
Optique	2.5 Gbit/s	`coché`	–	*`2.5 Gbit/s FDX`*

13.3.1 VLAN sur le HIPER Ring

L'équipement vous permet de transférer les données du VLAN via le HIPER Ring. Ainsi, l'équipement assure la redondance pour vos données de VLAN. L'équipement de l'anneau transfère les données d'administration autour de l'anneau, par exemple sur le VLAN 1. Pour que les données atteignent la station d'administration réseau, les équipements de l'anneau transfèrent les données d'administration non taggées sur les ports d'anneau. Aussi, spécifiez les ports d'anneau en tant que membres du VLAN 1.

Lorsque d'autres VLAN traversent vos équipements d'anneau, ces derniers transfèrent les données des autres VLAN sous forme taggée.

Spécifiez les réglages de VLAN. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Configuration*.
- ☐ Transférer les données d'administration VLAN non taggées sur les ports d'anneau.
  Dans la ligne VLAN 1, sélectionnez l'élément `U` dans la liste déroulante dans les colonnes relatives au port d'anneau.
- ☐ Empêcher le transfert des paquets d'administration à des ports hors anneau.
  Dans la ligne VLAN 1, sélectionnez l'élément `-` dans la liste déroulante dans les colonnes **non** relatives au port d'anneau.
- ☐ Permettre à un équipement d'anneau de transférer des données de VLAN à et depuis des ports appartenant au VLAN.
  Dans la ligne VLAN 1, sélectionnez l'élément `T` dans la liste déroulante dans les colonnes relatives au port d'anneau.
- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Port*.
- ☐ Affecter l'appartenance au VLAN 1 aux ports d'anneau.
  Saisissez la valeur `1` dans la colonne *Port-VLAN ID* des lignes des ports d'anneau.
- ☐ Affecter l'appartenance au VLAN 1 aux ports hors anneau.
  Saisissez le VLAN-ID approprié dans la colonne *Port-VLAN ID* des lignes des ports hors anneau.

13.3.2 HIPER Ring sur LAG

La fonction *HIPER Ring* permet de relier les équipements entre eux par l'intermédiaire d'un groupe d'agrégation de liens (LAG). Les clients de l'anneau et le gestionnaire d'anneau se comportent de la même manière qu'un anneau sans instance LAG.

Si un lien LAG est défaillant, l'autre lien de l'instance l'est également, ce qui entraîne une interruption de l'anneau. Après avoir détecté une interruption de l'anneau, les ports concernés envoient un paquet Link Down au gestionnaire de l'anneau. Le gestionnaire d'anneau débloque le port secondaire, en envoyant des données dans les deux sens autour de l'anneau, et répond par un paquet Delete. À la réception d'un paquet Delete, l'anneau participe au vidage de sa FDB.

13.4 Spanning Tree

Commentaire : Spanning Tree Protocol est un protocole conçu pour les commutateurs réseau MAC. C'est la raison pour laquelle la description suivante utilise le terme de commutateur réseau pour l'équipement.

Les réseaux locaux ne cessent de s'étendre. Cette extension s'entend aussi bien sur le plan géographique qu'en nombre de participants. Aussi, il est avantageux d'utiliser plusieurs commutateurs réseau, par exemple :

- pour réduire la charge du réseau dans les sous-zones,
- pour définir des connexions redondantes et
- pour surmonter les restrictions liées à la distance.

Toutefois, l'utilisation de plusieurs commutateurs réseau avec plusieurs connexions redondantes entre les sous-réseaux peut générer des boucles, et ainsi l'interruption de la communication à travers le réseau. Pour éviter cela, vous pouvez mettre en œuvre Spanning Tree. Spanning Tree permet une commutation sans boucle grâce à la désactivation systématique des connexions redondantes. La redondance permet la réactivation systématique des liaisons individuelles selon les besoins.

RSTP est un développement de Spanning-Tree Protocol (STP) et est compatible avec ce dernier. Lorsqu'une liaison ou un commutateur réseau présente une défaillance, STP requiert au maximum 30 secondes pour procéder à une reconfiguration. Cela n'est plus acceptable pour les applications sensibles au temps. RSTP atteint des temps de reconfiguration moyens de moins d'une seconde. Lorsque vous utilisez RSTP dans une topologie en anneau avec 10 ou 20 équipements, vous pouvez même atteindre des temps de reconfiguration de l'ordre de quelques millisecondes.

Commentaire : RSTP réduit une topologie de réseau de couche 2 avec chemins redondants en une structure arborescente (Spanning Tree) ne contenant plus aucun chemin redondant. L'un des équipements assume ici le rôle du root bridge. Le nombre maximum d'équipements autorisés dans une branche active (du root bridge jusqu'au bout de la branche) est spécifié par la variable *Max age* pour le root bridge actuel. La valeur prédéfinie pour *Max age* est de `20` et peut être augmentée jusqu'à `40`.

Si l'équipement fonctionnant en tant que racine subit une défaillance et qu'un autre équipement reprend sa fonction, le réglage *Max age* du nouveau root bridge détermine le nombre maximum d'équipements autorisés dans une branche.

Commentaire : La norme technique RSTP requiert que chaque équipement dans un réseau fonctionne avec l'algorithme (Rapid) Spanning Tree. Lorsque STP et RSTP sont utilisés simultanément, les avantages de la reconfiguration plus rapide avec RSTP sont perdus dans les segments du réseau qui fonctionnent en combinaison.

Un équipement qui ne prend en charge que RSTP fonctionne avec des équipements MSTP en ne s'affectant pas une zone MST à lui-même, mais plutôt le CST (Common Spanning Tree).

13.4.1 Principes de base

RSTP étant un développement de STP, chacune des descriptions suivantes de STP s'applique aussi à RSTP.

Tâches de STP

L'algorithme Spanning Tree réduit les topologies de réseau constituées de commutateurs réseau et contenant des structures en anneau du fait des liaisons redondantes en une structure arborescente. Ainsi, STP ouvre des structures en anneau conformément aux règles prédéfinies en désactivant les chemins redondants. Lorsqu'un chemin est interrompu en raison de la défaillance d'un composant du réseau, STP réactive le chemin précédemment désactivé. Ainsi, les liaisons redondantes augmentent la disponibilité de la communication.

STP détermine un commutateur réseau qui représente la base de la structure arborescente STP. Ce commutateur réseau est appelé root bridge.

Caractéristiques de l'algorithme STP :
- reconfiguration automatique de la structure arborescente en cas de défaillance d'un commutateur réseau ou d'interruption d'un chemin de données,
- stabilisation de la structure arborescente jusqu'à la taille maximale du réseau,
- stabilisation de la topologie sur une courte période,
- possibilité pour l'administrateur de spécifier et de reproduire la topologie,
- transparence pour les équipements terminaux,
- faible charge réseau par rapport à la capacité de transmission disponible du fait de la structure arborescente crée.

Paramètres du commutateur réseau

Dans le contexte de Spanning Tree, chaque commutateur réseau est ses liaisons sont décrits de manière univoque par les paramètres suivants :
- Identifiant de commutateur réseau
- Coût du chemin racine pour les ports de commutateur réseau
- Identifiant de port

Identifiant de commutateur réseau

L'identifiant de commutateur réseau se compose de 8 octets. Les 2 octets avec la valeur la plus élevée sont prioritaires. Lors de la configuration du réseau, l'administrateur peut modifier le réglage par défaut pour le nombre prioritaire, qui est 32768 (8000H). Les 6 octets avec la valeur la moins élevée de l'identifiant de commutateur réseau constituent l'adresse MAC du commutateur réseau. L'adresse MAC permet à chaque commutateur réseau d'avoir un identifiant unique.

Le commutateur réseau dont l'identifiant présente la plus petite valeur est celui avec la priorité la plus élevée.

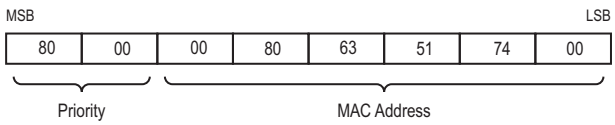


Figure 38 : Identifiant de commutateur réseau, exemple (valeurs en notation hexadécimale)

Coût du chemin racine

À chaque chemin qui connecte 2 commutateurs réseau est affecté un coût pour la transmission (coût du chemin). L'équipement détermine cette valeur sur la base de la vitesse de transmission (voir le tableau 35). L'équipement affecte un coût de chemin plus élevé aux chemins avec des vitesses de transmission plus basses.

Alternativement, l'administrateur peut définir le coût du chemin. Comme l'équipement, l'administrateur affecte un coût plus élevé aux chemins avec des vitesses de transmission plus basses. Cette valeur pouvant toutefois être choisie librement, l'administrateur dispose d'un outil lui permettant de donner la préférence à un chemin spécifique parmi les chemins redondants.

Le coût du chemin racine est la somme des coûts individuels des chemins qu'un paquet de données doit traverser depuis un port de commutateur réseau connecté jusqu'au root bridge.

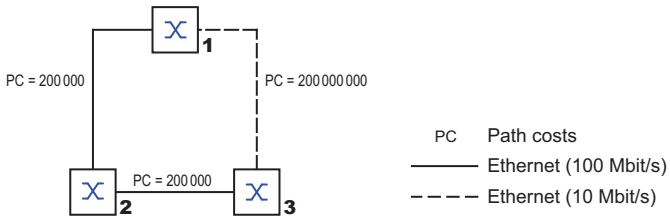


Figure 39 : Coûts des chemins

Tableau 35 : Coûts des chemins recommandés pour RSTP sur la base du débit de données.

Débit de données	Valeur recommandée	Plage recommandée	Plage possible
≤100 kbit/s	200 000000[1]	20000000-200000000	1-200000000
1 Mbit/s	20000000[a]	2000000-200000000	1-200000000
10 Mbit/s	2000000[a]	200000-20000000	1-200000000
100 Mbit/s	200000[a]	20000-2000000	1-200000000
1 Gbit/s	20000	2000-200000	1-200000000
10 Gbit/s	2000	200-20000	1-200000000
100 Gbit/s	200	20-2000	1-200000000
1 TBit/s	20	2-200	1-200000000
10 TBit/s	2	1-20	1-200000000

1. Vérifiez que les commutateurs réseau conformes à la norme technique IEEE 802.1D-1998 et prenant en charge uniquement les valeurs 16 bits pour les coûts des chemins, utilisent la valeur 65535 (FFFFH) pour les chemins des coûts lorsqu'ils sont utilisés en combinaison avec des commutateurs réseau prenant en charge des valeurs 32 bits pour les coûts des chemins.

Identifiant de port

L'identifiant de port se compose de 2 octets. Une partie, l'octet de valeur la plus basse, contient le numéro de port physique. Ce dernier constitue un identifiant unique pour le port de ce commutateur réseau. La deuxième partie de valeur plus élevée est la priorité du port, déterminée par l'administrateur (valeur par défaut : 128). Ici aussi, le port avec le plus petit numéro d'identifiant a la priorité la plus élevée.

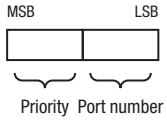


Figure 40 : Identifiant de port

Max Age (Âge max) et Diameter (Diamètre)

Les valeurs « Max Age » (Âge max) et « Diameter » (Diamètre) déterminent pour une large part l'extension maximale d'un réseau Spanning Tree.

Diameter

Le nombre de liaisons entre les équipements dans le réseau qui sont les plus éloignés les uns des autres s'appelle le diamètre du réseau.

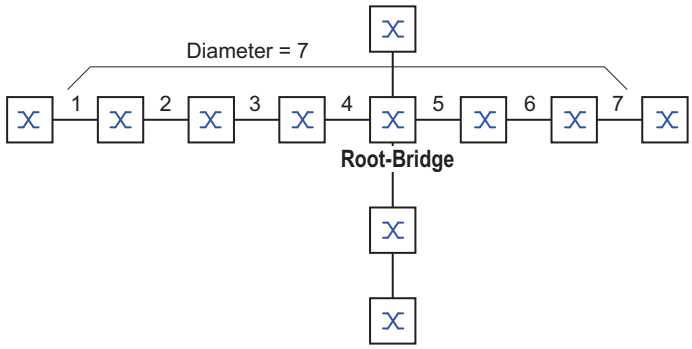


Figure 41 : Définition de diamètre

Le diamètre de réseau qui peut être atteint dans le réseau est MaxAge-1.

Dans l'état à la livraison, MaxAge = 20 et le diamètre maximum qui peut être atteint = 19. Si vous définissez la valeur maximale de 40 pour MaxAge, le diamètre maximum qui peut être atteint = 39.

MaxAge

Chaque STP-BPDU contient un compteur « MessageAge ». Lorsqu'un commutateur réseau est traversé, le compteur est incrémenté de 1.

Avant de transférer une STP-BPDU, le commutateur réseau compare le compteur « MessageAge » et la valeur « MaxAge » spécifiée dans l'équipement :
- Si MessageAge < MaxAge, le commutateur réseau transfère la STP-BPDU au commutateur réseau suivant.
- Si MessageAge = MaxAge, le commutateur réseau rejette la STP-BPDU.

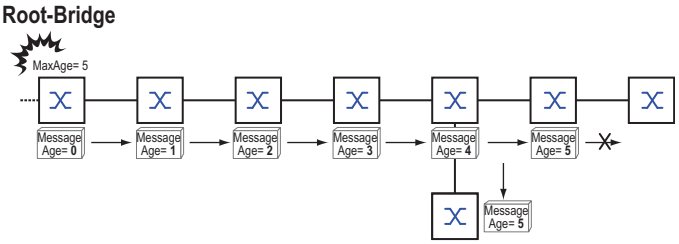


Figure 42 : Transmission d'une STP-BPDU en fonction de MaxAge

13.4.2 Règles de création de la structure arborescente

Informations sur les commutateurs réseau

Pour déterminer la structure arborescente, les commutateurs réseau ont besoin d'informations plus détaillées sur les autres commutateurs réseau dans le réseau.

Pour obtenir ces informations, chaque commutateur réseau envoie une BPDU (Bridge Protocol Data Unit) aux autres commutateurs réseau.

Le contenu d'une BPDU comprend :
- Identifiant de commutateur réseau
- Coûts de chemin racine
- Identifiant de port

(voir IEEE 802.1D)

Définition de la structure arborescente

Le commutateur réseau dont l'identifiant a le plus petit nombre est appelé root bridge. Il est (ou va devenir) la racine de la structure arborescente.

La structure de l'arborescence dépend des coûts de chemin racine. Spanning Tree sélectionne la structure de manière à ce que les coûts des chemins entre chaque commutateur réseau individuel et le root bridge soient les plus réduits possible.

- Lorsque plusieurs chemins ont les mêmes coûts de chemin racine, le commutateur réseau le plus éloigné de la racine décide quel port bloquer. Pour cela, il utilise l'identifiant du commutateur réseau le plus proche de la racine. Le commutateur réseau bloque le port menant au commutateur réseau avec l'ID numériquement plus élevé (un ID numériquement plus élevé est logiquement pire). Si 2 commutateurs réseau ont la même priorité, le commutateur réseau avec l'adresse MAC numériquement plus grande a l'ID numériquement plus élevé, qui est logiquement pire.
- Lorsque plusieurs chemins avec les mêmes coûts de chemin racine conduisent d'un commutateur réseau jusqu'à ce même commutateur réseau, le commutateur réseau le plus éloigné de la racine utilise l'identifiant de port de l'autre commutateur réseau comme dernier critère (voir la figure 40). Dans ce processus, le commutateur réseau bloque le port menant au port avec l'ID numériquement plus élevé (un ID numériquement plus élevé est logiquement pire). Si 2 ports ont la même priorité, le port avec le numéro de port plus élevé a l'ID numériquement plus élevé, qui est logiquement pire.

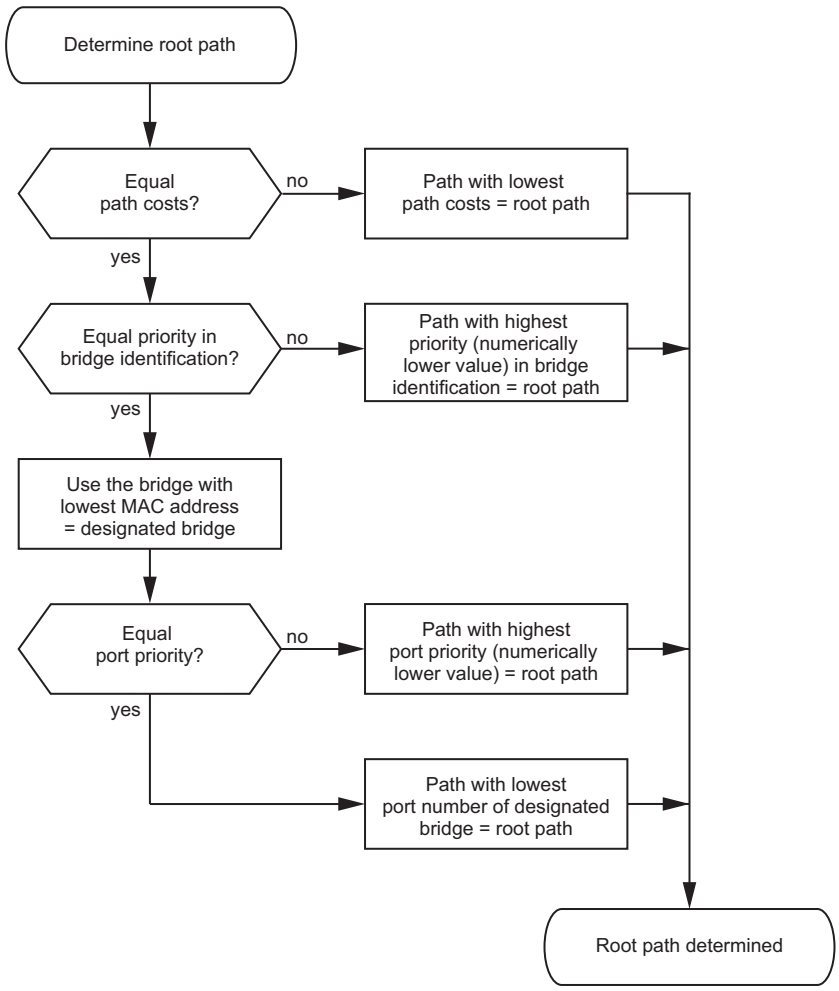


Figure 43 : Organigramme permettant de spécifier le chemin racine

13.4.3 Exemples

Exemple de détermination du chemin racine

Vous pouvez utiliser le plan réseau (voir la figure 44) pour suivre l'organigramme (voir la figure 43) permettant de déterminer le chemin racine. L'administrateur a spécifié une priorité dans l'identification de chaque commutateur réseau. Le commutateur réseau dont l'identifiant a la plus petite valeur numérique assume le rôle de root bridge, soit dans le cas présent le commutateur réseau 1. Dans l'exemple, chaque sous-chemin a le même coût de chemin. Le protocole bloque le chemin entre le commutateur réseau 2 et le commutateur réseau 3 car une liaison du commutateur réseau 3 via le commutateur réseau 2 jusqu'au root bridge entraînerait des coûts de chemin plus élevés.

Le chemin depuis le commutateur réseau 6 jusqu'au root bridge est intéressant :
- Le chemin via le commutateur réseau 5 et le commutateur réseau 3 génère les mêmes coûts de chemin racine que le chemin via le commutateur réseau 4 et le commutateur réseau 2.
- STP sélectionne le chemin utilisant le commutateur réseau avec l'adresse MAC la plus petite dans l'identifiant de commutateur réseau (commutateur réseau 4 dans l'illustration).
- Il y a aussi 2 chemins entre le commutateur réseau 6 et le commutateur réseau 4. Ici, l'identifiant de port est décisif (Port 1 < Port 3).

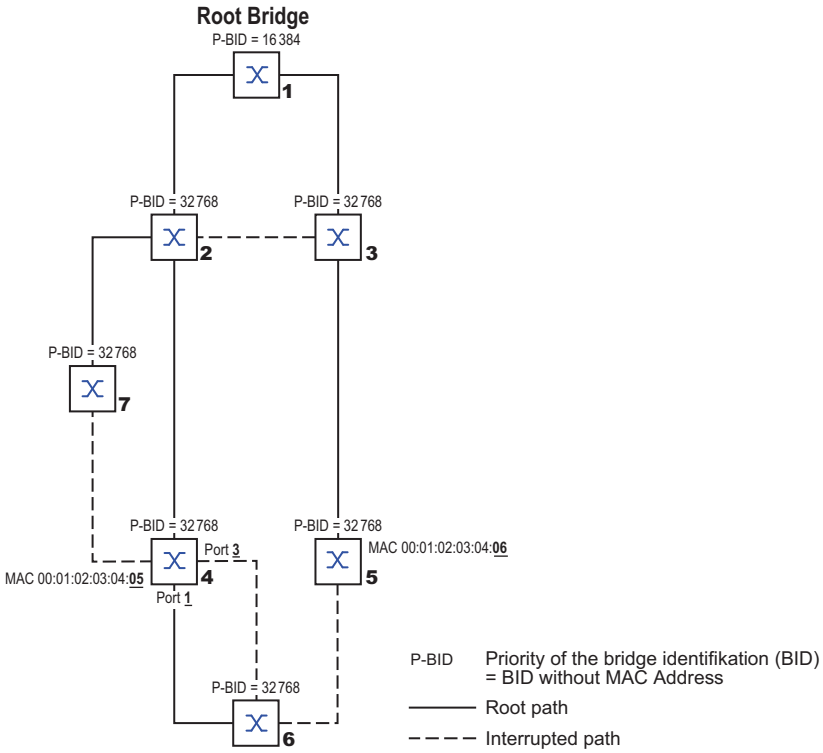


Figure 44 : Exemple de détermination du chemin racine

Commentaire : En cas de défaillance du root bridge actuel, l'adresse MAC dans l'identifiant de commutateur réseau détermine seuls quel commutateur réseau devient le nouveau root bridge, car l'administrateur ne modifie pas les valeurs par défaut des commutateurs réseau dans l'identifiant de commutateur réseau, sauf la valeur pour le root bridge.

Exemple de manipulation du chemin racine

Vous pouvez utiliser le plan réseau (voir la figure 45) pour suivre l'organigramme (voir la figure 43) permettant de déterminer le chemin racine. L'administrateur a effectué ce qui suit :

- conservé la valeur par défaut de 32768 (8000H) pour chaque commutateur réseau, sauf pour le commutateur réseau 1 et le commutateur réseau 5, et
- affecté au commutateur réseau 1 la valeur 16384 (4000H), ce qui en fait le root bridge.
- Au commutateur réseau 5, il a affecté la valeur 28672 (7000H).

Le protocole bloque le chemin entre le commutateur réseau 2 et le commutateur réseau 3, car une liaison du commutateur réseau 3 via le commutateur réseau 2 jusqu'au root bridge impliquerait des coûts de chemin plus élevés.

Le chemin du commutateur réseau 6 jusqu'au root bridge est intéressant :

▶ Les commutateurs réseau sélectionnent le chemin via le commutateur réseau 5 car la valeur 28672 pour la priorité dans l'identifiant de commutateur réseau est inférieure à la valeur 32768.

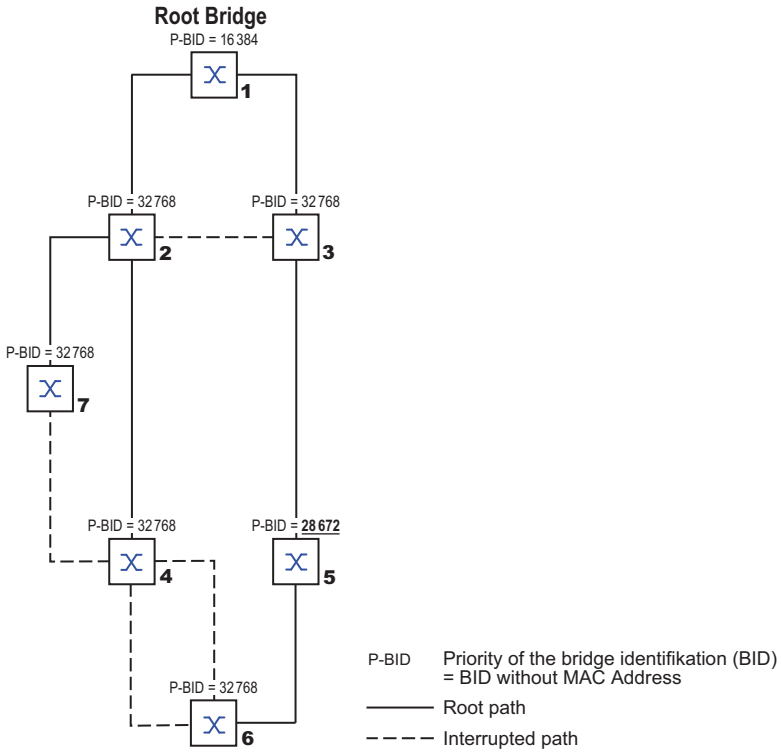


Figure 45 : Exemple de manipulation du chemin racine

Exemple de manipulation de la structure arborescente

L'administrateur décèle rapidement que cette configuration avec le commutateur réseau 1 en tant que root bridge n'est pas valide. Sur les chemins du commutateur réseau 1 au commutateur réseau 2 et du commutateur réseau 1 au commutateur réseau 3, les paquets de commande envoyés par le root bridge à tous les autres commutateurs réseau s'accumulent.

Lorsque l'administrateur configure le commutateur réseau 2 en tant que root bridge, la charge des paquets de commande sur les sous-réseaux est répartie plus régulièrement. Le résultat est la configuration présentée ici (voir la figure 46). Les coûts de chemin de la plupart des commutateurs réseau vers le root bridge ont diminué.

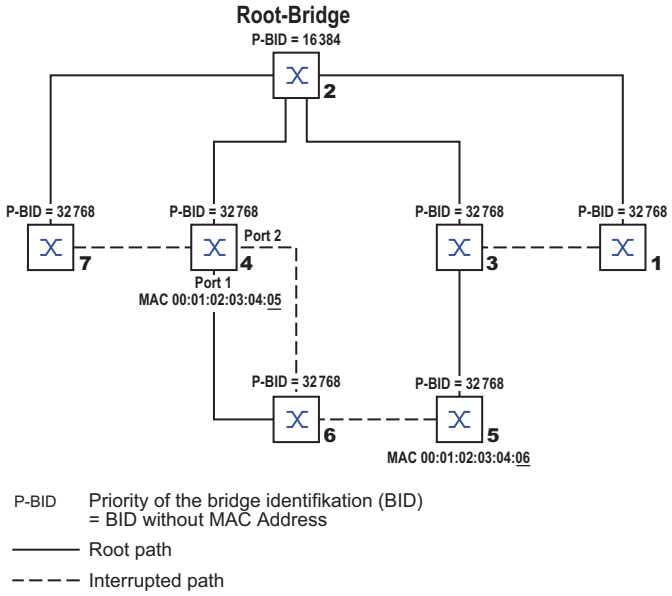


Figure 46 : Exemple de manipulation de la structure arborescente

13.5 Rapid Spanning Tree Protocol

RSTP utilise le même algorithme que STP pour déterminer la structure arborescente. En cas de défaillance d'une liaison ou d'un commutateur réseau, RSTP modifie simplement les paramètres et ajoute de nouveaux paramètres et mécanismes qui accélèrent la reconfiguration.

Les ports jouent un rôle significatif dans ce contexte.

13.5.1 Rôle des ports

RSTP affecte à chaque port de commutateur réseau l'un des rôles suivants (voir la figure 47) :

- Port racine :
  Il s'agit du port sur lequel un commutateur réseau reçoit des paquets de données avec les coûts de chemin les plus bas depuis le root bridge.
  Lorsque plusieurs ports ont des coûts de chemin aussi bas, l'ID du port conduisant à la racine (commutateur réseau désigné) détermine lequel de ses ports se voit attribuer le rôle de port racine par le commutateur réseau le plus distant de la racine.
  Lorsqu'un commutateur réseau a plusieurs ports avec des coûts de chemin aussi bas vers le même commutateur réseau, le commutateur réseau utilise l'ID de port du commutateur réseau conduisant à la racine (commutateur réseau désigné) pour déterminer quel port sélectionner localement en tant que port racine (voir la figure 43).
  Le root bridge lui-même n'a pas de port racine.
- Port désigné :
  Dans un segment de réseau, le commutateur réseau avec les coûts de chemin racine les plus bas est le commutateur réseau désigné.
  Lorsque plus d'un commutateur réseau ont les mêmes coûts de chemin racine, le commutateur réseau avec l'identifiant de commutateur réseau le plus petit devient le commutateur réseau désigné. Le port désigné sur ce commutateur réseau est le port connecté à un segment de réseau s'éloignant du root bridge. Lorsqu'un commutateur réseau est connecté à un segment de réseau avec plusieurs ports (via un hub, par exemple), le commutateur réseau attribue le rôle de port désigné au port avec le meilleur ID de port.
- Port marginal
  Chaque segment de réseau sans commutateur réseau RSTP supplémentaire est connecté avec exactement un port désigné. Dans ce cas, le port désigné est également un port marginal. Un port marginal se distingue par le fait qu'il ne reçoit aucune RST BPDU (Rapid Spanning Tree Bridge Protocol Data Units).
- Port alternatif
  Lorsque la liaison avec le root bridge est perdue, ce port bloqué reprend le rôle de port racine. Le port alternatif constitue un port de secours pour la liaison avec le root bridge.

- Port de secours
  Il s'agit d'un port bloqué qui sert de port de secours en cas de perte de la liaison avec le port désigné de ce segment de réseau (sans commutateur réseau RSTP).
- Port désactivé
  Il s'agit d'un port qui ne participe pas au fonctionnement Spanning Tree, c'est-à-dire que le port est éteint ou n'a aucune liaison.

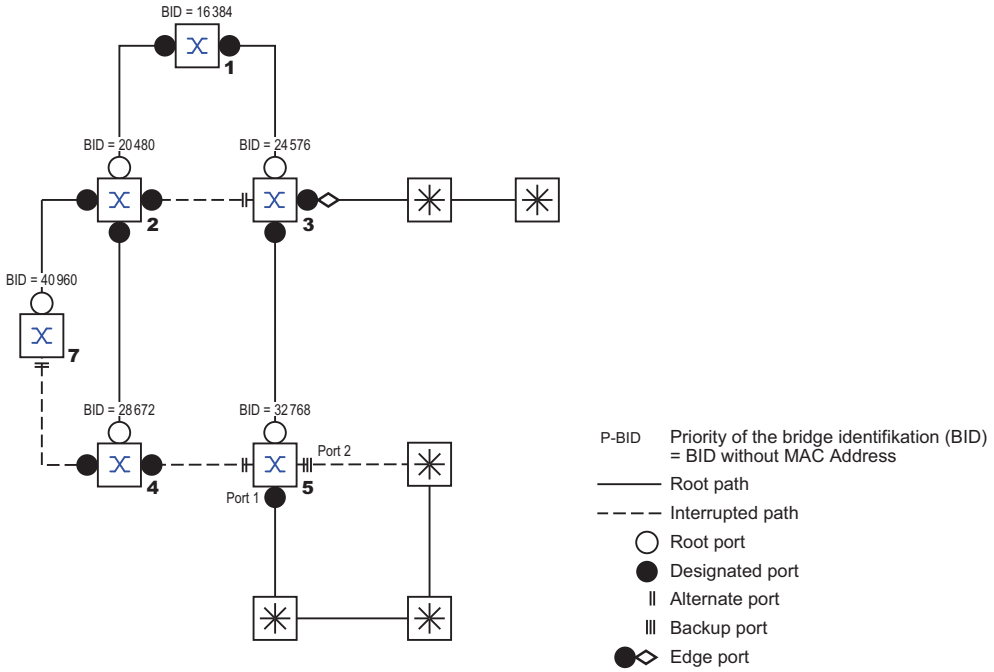


Figure 47 : Affectation d'un rôle à un port

13.5.2 États de port

En fonction de la structure arborescente et de l'état des chemins de liaison sélectionnés, RSTP affecte aux ports leurs états.

Tableau 36 : Relation ente les valeurs d'état de port pour STP et RSTP

État de port STP	État de port commutateur réseau administratif	MAC opérationnel	État de port RSTP	Topologie active (rôle de port)
DISABLED	Disabled	FALSE	Discarding[1]	Excluded (désactivé)
DISABLED	Enabled	FALSE	Discarding[a]	Excluded (désactivé)
BLOCKING	Enabled	TRUE	Discarding[2]	Excluded (alternatif, de secours)
LISTENING	Enabled	TRUE	Discarding[b]	Included (racine, désigné)
LEARNING	Enabled	TRUE	Learning	Included (racine, désigné)
FORWARDING	Enabled	TRUE	Forwarding	Included (racine, désigné)

1. La dot1d-MIB affiche « Disabled » (Désactivé)
2. La dot1d-MIB affiche « Blocked » (Bloqué)

Signification des états de port RSTP :
- Disabled (Désactivé) : le port n'appartient pas à la topologie active
- Discarding (Rejet) : aucun apprentissage d'adresse dans FDB, aucun trafic de données sauf pour les STP-BPDU
- Learning (Apprentissage) : apprentissage d'adresse actif (FDB), aucun trafic de données à par les STP-BPDU
- Forwarding (Transfert) : apprentissage d'adresse actif (FDB), envoi et réception de tous les types de paquets (pas uniquement les STP-BPDU)

13.5.3 Spanning Tree Priority Vector

Pour attribuer des rôles aux ports, les commutateurs réseau RSTP échangent des informations de configuration entre eux. Ces informations sont connues sous le nom de « Spanning Tree Priority Vector ». Elles font partie des RSTP-BPDU et contiennent les données suivantes :
- Identifiant de commutateur réseau du root bridge
- Coûts de chemin racine du commutateur réseau expéditeur
- Identifiant du commutateur réseau expéditeur
- Identifiants des ports via lesquels le message a été envoyé
- Identifiants des ports via lesquels le message a été reçu

Sur la base de ces informations, les commutateurs réseau participant à RSTP sont à même de déterminer les rôles des ports eux-mêmes et de définir les états de leurs propres ports.

13.5.4 Reconfiguration rapide

Pourquoi la réaction de RSTP est-elle plus rapide que celle de STP en cas d'interruption du chemin racine ?
- Introduction de ports marginaux :
  Durant une reconfiguration, RSTP définit un port marginal dans le mode de transmission après 3 secondes (réglage par défaut). Pour s'assurer qu'aucun commutateur réseau envoyant des BPDU n'est connecté, RSTP attend que le « Hello Time » soit écoulé.
  Lorsque vous vérifiez qu'un équipement terminal est et reste connecté à ce port, il n'y a pas de délai d'attente sur ce port en cas de reconfiguration.
- Introduction de ports alternatifs :
  Les rôles des ports étant déjà distribués en mode opérationnel normal, un commutateur réseau peut basculer immédiatement du port racine sur le port alternatif lorsque la liaison au root bridge est perdue.
- Communication avec des commutateurs réseau voisins (liaisons point à point) :
  La communication directe décentralisée entre commutateurs réseau voisins permet des réactions sans périodes d'attente pour les changements d'état dans la topologie Spanning Tree.
- Tableau d'adresses :
  Avec STP, l'âge des entrées dans le FDB détermine la mise à jour de la communication. RSTP supprime immédiatement les entrées dans les ports concernés par une reconfiguration.
- Réaction aux événements :
  Sans avoir à adhérer à aucune spécification de temps, RSTP réagit immédiatement aux événements comme des interruptions de connexion, des rétablissements de connexion, etc.

Commentaire : Les paquets de données peuvent être dupliqués pendant la phase de reconfiguration de la topologie RSTP et/ou arriver désordonnés sur le récepteur. Vous pouvez également utiliser le Spanning Tree Protocol ou sélectionner un autre procédé de redondance décrit dans ce manuel.

13.5.5 Configuration de l'équipement

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Pour éviter les boucles durant la phase de configuration, configurez chaque équipement de la configuration *Spanning Tree* individuellement. Avant de raccorder les lignes redondantes, terminez la configuration des autres équipements de la configuration de *Spanning Tree*.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

RSTP configure la topologie de réseau de manière totalement autonome. L'équipement avec la priorité de commutateur réseau la plus basse devient automatiquement le root bridge. Toutefois, pour définir une structure de réseau spécifique de manière indépendante, vous spécifiez un équipement comme étant le root bridge. Généralement, un équipement dans la dorsale assume ce rôle.

Exécutez les étapes suivantes :

- ☐ Définissez le réseau en fonction de vos besoins, initialement sans lignes redondantes
- ☐ Vous désactivez le contrôle de flux sur les ports impliqués.
  Si le contrôle de flux et la fonction de redondance sont activés simultanément, la fonction de redondance peut ne pas fonctionner comme prévu. (Réglage par défaut : contrôle de flux désactivé globalement et activé sur chaque port.)
- ☐ Désactivez MRP sur chaque équipement.
- ☐ Activez Spanning Tree sur chaque équipement dans le réseau.
  Dans l'état à la livraison, Spanning Tree est activé sur l'équipement.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Activez la fonction.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`spanning-tree operation`	Active Spanning Tree.
`show spanning-tree global`	Affiche les paramètres pour la vérification.

À présent, raccordez les lignes redondantes.

Définissez les réglages pour l'équipement qui assume le rôle de root bridge.

Exécutez les étapes suivantes :

- ☐ Dans le champ *Priority*, saisissez une valeur numériquement inférieure.
  Le commutateur réseau avec l'ID de commutateur réseau numériquement le plus bas a la priorité la plus élevée et devient le root bridge du réseau.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`spanning-tree mst priority 0 <0..61440>`	Spécifie la priorité du commutateur réseau de l'équipement. **Commentaire :** Spécifiez la priorité du commutateur réseau dans la plage `0..61440` par incréments de 4096.

Après la sauvegarde, la boîte de dialogue affiche les informations suivantes :
- La case *Bridge is root* est cochée.
- Le champ *Root port* affiche la valeur `0.0`.
- Le champ *Root path cost* affiche la valeur `0`.

`show spanning-tree global`	Affiche les paramètres pour la vérification.

- ☐ Si nécessaire, modifiez ensuite les valeurs dans les champs *Forward delay [s]* et *Max age*.
  - Le root bridge transmet les valeurs modifiées aux autres équipements.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`spanning-tree forward-time <4..30>`	Spécifie le délai en secondes pour le changement d'état.
`spanning-tree max-age <6..40>`	Spécifie la longueur de branche maximum admissible, par exemple le nombre d'équipements pour le root bridge.
`show spanning-tree global`	Affiche les paramètres pour la vérification.

Commentaire : Les paramètres *Forward delay [s]* et *Max age* ont la relation suivante :

Forward delay [s] ≥ (*Max age*/2) + 1

Si vous saisissez dans les champs des valeurs en conflit avec cette relation, l'équipement remplace ces valeurs par les dernières valeurs valides ou par la valeurs par défaut.

Commentaire : Si possible, ne modifiez pas la valeur dans le champ « Hello Time ».

Vérifiez les valeurs suivantes pour les autres équipements :
- L'ID de commutateur réseau (priorité de commutateur réseau et adresse MAC) de l'équipement correspondant et le root bridge.
- Le numéro du port de l'équipement qui mène au root bridge.
- Le coûts du chemin entre le port racine de l'équipement et le root bridge.

Exécutez les étapes suivantes :

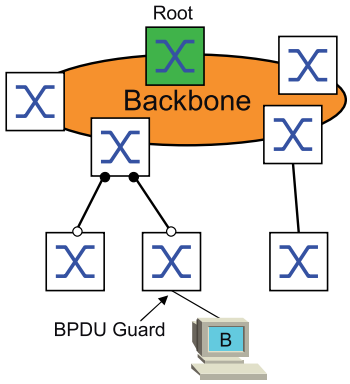
`show spanning-tree global`	Affiche les paramètres pour la vérification.

13.5.6 Protections

L'équipement vous permet d'activer différentes fonctions de protection dans les ports de l'équipement.

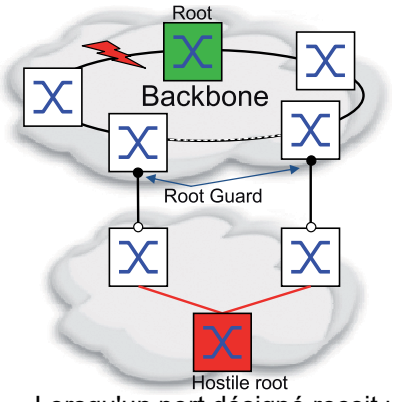
Les fonctions de protection suivantes vous permettent de protéger votre réseau contre les configurations incorrectes, les boucles et les attaques à l'aide de STP-BPDU :

- BPDU Guard – pour les ports marginaux spécifiés manuellement (ports d'équipement terminal)
  Vous activez cette fonction de protection de manière globale dans l'équipement.



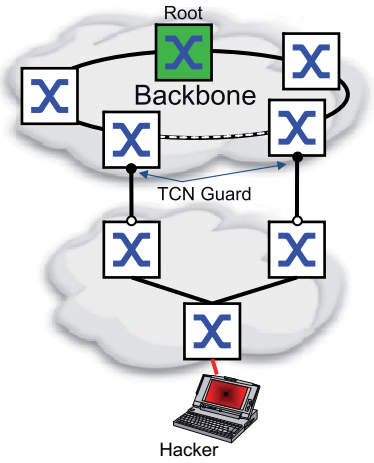
Normalement, les ports de l'équipement terminal ne reçoivent pas de STP-BPDU. Si une attaque tente d'envoyer des STP-BPDU sur ce port, l'équipement désactive le port.

- Root Guard – pour les ports désignés
  Vous activez cette fonction de protection séparément pour chaque port d'équipement.



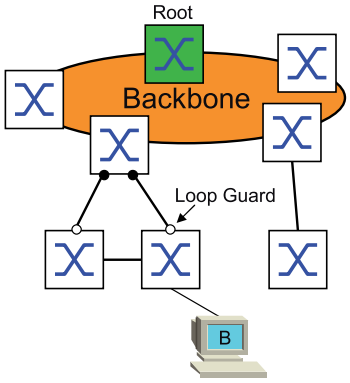
Lorsqu'un port désigné reçoit une STP-BPDU avec de meilleures informations de chemin jusqu'au root bridge, l'équipement rejette la STP-BPDU et définit l'état de transmission du port sur `discarding` au lieu de `root`.
En l'absence de STP-BPDU avec de meilleures informations de chemin jusqu'au root bridge, après 2 × *Hello time [s]*, l'équipement rétablit l'état du port sur une valeur conforme au rôle du port.

- TCN Guard – pour les ports recevant des STP-BPDU avec une marque Modification de la topologie
  Vous activez cette fonction de protection séparément pour chaque port d'équipement.



Si la fonction de protection est activée, l'équipement ignore les marques Modification de la topologie dans les STP-BPDU reçues. Cela ne modifie pas le contenu du tableau d'adresses (FDB) du port de l'équipement. Toutefois, des informations supplémentaires dans la BPDU modifiant la topologie sont traitées par l'équipement.

- Loop Guard – pour les ports racines, alternatifs et de secours
  Vous activez cette fonction de protection séparément pour chaque port d'équipement.



Si le port ne reçoit plus de STP-BPDU, cette fonction de protection permet de prévenir la modification involontaire de l'état de transmission d'un port en `forwarding`. Si cette situation se produit, l'équipement désigne l'état de boucle du port comme étant incohérent mais ne transfère aucun paquet de données.

Activation de BPDU Guard

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Cochez la case *BPDU guard*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`spanning-tree bpdu-guard`	Active BPDU Guard.
`show spanning-tree global`	Affiche les paramètres pour la vérification.

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*.
- ☐ Basculez sur l'onglet *CIST*.
- ☐ Pour les ports d'équipement terminal, cochez la case dans la colonne *Admin edge port*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`interface <x/y>`	Basculez sur le mode de configuration de l'interface `<x/y>`.
`spanning-tree edge-port`	Désigne le port en tant port d'équipement terminal (port marginal).
`show spanning-tree port x/y`	Affiche les paramètres pour la vérification.
`exit`	Quitte le mode d'interface.

Lorsqu'un port marginal reçoit une STP-BPDU, l'équipement se comporte comme suit :

- ▶ L'équipement désactive ce port.
  Dans la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*, la case pour ce port dans la colonne *Port on* est `décochée`.
- ▶ L'équipement désigne le port.

Vous pouvez déterminer si un port s'est désactivé en raison d'une BPDU reçue. Pour ce faire, exécutez les étapes suivantes :

Dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*, onglet *Guards*, la case dans la colonne *BPDU guard effect* est `cochée`.

`show spanning-tree port x/y`	Affiche les paramètres du port pour vérification. La valeur du paramètre *BPDU guard effect* est `enabled`.

Rétablissez l'état du port de l'équipement à la valeur `forwarding`. Pour ce faire, exécutez les étapes suivantes :

- ☐ Lorsque le port reçoit encore des BPDU :
  - – Supprimez la définition manuelle en tant que port marginal (port d'équipement terminal).
    ou
  - – Désactivez BPDU Guard.
- ☐ Activez de nouveau le port d'équipement.

Activation de Root Guard / TCN Guard / Loop Guard

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*.
- ☐ Basculez sur l'onglet *Guards*.
- ☐ Pour les ports désignés,cochez la case dans la colonne *Root guard*.
- ☐ Pour les ports qui reçoivent des STP-BPDU avec une marque Modification de la topologie, cochez la case dans la colonne *TCN guard*.
- ☐ Pour les ports racines, alternatifs ou de secours, cochez la case dans la colonne *Loop guard*.

Commentaire : Les fonctions *Root guard* et *Loop guard* sont mutuellement exclusives. Si vous tentez d'activer la fonction *Root guard* alors que la fonction *Loop guard* est activée, l'équipement désactive la fonction *Loop guard*.

- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface <x/y>`	Basculez sur le mode de configuration de l'interface `<x/y>`.
`spanning-tree guard-root`	Active Root Guard sur le port désigné.
`spanning-tree guard-tcn`	Active TCN Guard sur le port qui reçoit des STP-BPDU avec une marque Modification de la topologie.
`spanning-tree guard-loop`	Active Loop Guard sur un port racine, alternatif ou de secours.
`exit`	Quitte le mode d'interface.
`show spanning-tree port x/y`	Affiche les paramètres du port pour vérification.

13.6 Dual RSTP (MCSESM-E)

Les applications industrielles requièrent une tolérance fautive de vos réseaux. Cela implique aussi la gestion de temps d'interruption courts et déterministes pour la communication lorsque l'un des composants de réseau est défaillant.

Une topologie en anneau permet des temps d'interruption courts avec une utilisation minimale des ressources. Avec le protocole *Spanning Tree*, le temps d'interruption dépend de la taille du réseau. Pour optimiser le temps d'interruption, vous pouvez diviser les grands réseaux *Spanning Tree* en petits segments d'anneau.

La fonction *Dual RSTP* est utilisée avec la fonction *RCP*. À l'aide de la fonction *RCP*, vous avez la possibilité de coupler un ou plusieurs anneaux RSTP à l'instance RSTP dans un anneau principal. En cas de couplage de deux segments *Spanning Tree*, l'anneau secondaire représente une instance RSTP à laquelle les réglages de la fonction *Dual RSTP* s'appliquent. Cette instance *Dual RSTP* fonctionne indépendamment de l'instance RSTP de l'anneau principal et des autres anneaux secondaires. Lorsque RSTP est le protocole utilisé dans un seul des anneaux à coupler, vous n'avez pas besoin de la fonction *Dual RSTP*.

13.7 Agrégation de liens

La fonction *Link Aggregation* par la méthode de commutation simple vous permet de surmonter 2 restrictions inhérentes aux liaisons Ethernet, à savoir la bande passante et la redondance.

La fonction *Link Aggregation* vous permet de surmonter les restrictions inhérentes à la bande passante des ports individuels. La fonction *Link Aggregation* vous permet de combiner au moins 2 liaisons en parallèle, créant ainsi 1 liaison logique entre 2 équipements. Les liaisons parallèles augmentent la bande passante pour le trafic entre les 2 équipements.

La fonction *Link Aggregation* s'utilise généralement sur la dorsale du réseau. Cette fonction constitue une manière peu onéreuse d'augmenter la bande passante de manière progressive.

De plus, la fonction *Link Aggregation* offre une redondance avec une reprise en toute transparence. Lorsqu'une liaison est défaillante, avec au moins 2 liaisons configurées en parallèle, les autres liaisons du groupe continuent de transférer le trafic.

Les réglages par défaut d'une nouvelle instance *Link Aggregation* sont les suivants :
- Dans la colonne *Active*, la case est cochée.
- Dans la colonne *Send trap (Link up/down)*, la case est cochée.
- Dans la colonne *Static link aggregation*, la case est décochée.
- Dans la colonne *Active ports (min.)*, la valeur est `1`.

13.7.1 MÉTHODES DE FONCTIONNEMENT

L'équipement fonctionne selon la méthode de commutation simple. La méthode de commutation simple constitue un moyen peu onéreux d'étendre votre réseau. La méthode de commutation simple établit que vous avez besoin d'un équipement de chaque côté d'une liaison pour fournir les ports physiques. L'équipement équilibre la charge du trafic sur les ports membres du groupe.

L'équipement utilise également la méthode de la même vitesse de liaison, selon laquelle les ports membres du groupe sont full duplex, les liaisons point à point ayant le même débit de transmission. Le premier port que vous ajoutez au groupe est le port maître et détermine la bande passante pour les autres ports membres du groupe d'agrégation de liens.

L'équipement vous permet de définir jusqu'à 2 groupes d'agrégation de liens. Le nombre de ports utilisables par groupe d'agrégation de liens dépend de l'équipement.

13.7.2 Exemple d'agrégation de liens

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Pour éviter les boucles durant la phase de configuration, configurez chaque équipement de la configuration *Link Aggregation* individuellement. Avant de raccorder les lignes redondantes, terminez la configuration des autres équipements de la configuration de *Link Aggregation*.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Connectez plusieurs stations de travail à l'aide d'un groupe de liens agrégés entre les commutateurs réseau 1 et 2. En agrégeant plusieurs liens, il est possible d'atteindre des vitesses supérieures sans mise à niveau du matériel.

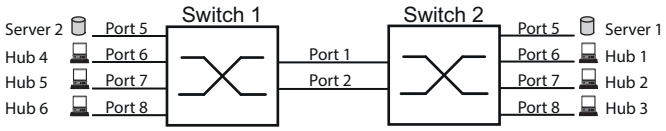


Figure 48 : Agrégation de liens entre commutateurs réseau

Configurez les commutateurs 1 et 2 dans l'interface utilisateur graphique. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Link Aggregation*.
- ☐ Cliquez sur le bouton .
  La boîte de dialogue affiche la fenêtre *Create*.
- ☐ Dans la liste déroulante *Trunk port*, sélectionnez le numéro d'instance du groupe d'agrégation de liens.
- ☐ Dans la liste déroulante *Port*, sélectionnez le port *1/1*.
- ☐ Cliquez sur le bouton *Ok*.
- ☐ Répétez les étapes précédentes et sélectionnez le port *1/2*.
- ☐ Cliquez sur le bouton *Ok*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`link-aggregation add lag/1`	Crée un groupe d'agrégation de liens `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Ajoute le port *1/1* au groupe d'agrégation de liens.
`link-aggregation modify lag/1 addport 1/2`	Ajoute le port *1/2* au groupe d'agrégation de liens.

13.8 Link Backup

Link Backup fournit une liaison redondante pour le trafic sur les équipements de couche 2. Lorsque l'équipement détecte une erreur sur la liaison principale, il transfère le trafic sur la liaison de secours. Link Backup s'utilise typiquement dans les réseaux de prestataires de services ou d'entreprises.

Vous définissez les liaisons de secours par paires, soit une liaison principale et une liaison de secours. Dans le cas d'une redondance pour réseaux d'entreprise, par exemple, l'équipement vous permet de définir plus de une paire. Le nombre maximal de paires de secours correspond au nombre total de ports physiques / 2. De plus, lorsque l'état d'un port participant à une paire de secours se modifie, l'équipement envoie un trap SNMP.

Lors de la configuration des paires de secours, observez les règles suivantes :
- Une paire de liaisons se compose de n'importe quelle combinaison de ports physiques. Par exemple, un port est un port 100 Mbit et l'autre est un port 1000 Mbit SFP.
- Un port spécifique est toujours membre d'une paire de secours.
- Vérifiez que les ports d'une paire de secours sont membres du même VLAN avec le même VLAN-ID. Lorsque le port principal ou le port de secours est membre d'un VLAN, affectez le deuxième port au même VLAN.

Le réglage par défaut pour cette fonction est désactivé sans aucune paire de secours.

Commentaire : Vérifiez que Spanning Tree Protocol est désactivé sur les ports Link Backup.

13.8.1 Description d'une défaillance

Link Backup vous permet également de définir une option Fail Back. Lorsque vous activez la fonction de retour et que la liaison principale reprend son fonctionnement normal, l'équipement bloque le trafic sur le port de secours, puis le transfère vers le port principal. Cette procédure contribue à éviter que l'équipement ne génère des boucles dans le réseau.

Lorsque le port principal rétablit la liaison et un état actif, l'équipement prend en charge 2 modes de fonctionnement :
- Lorsque vous désactivez *Fail back*, le port principal reste à l'état bloqué jusqu'à une défaillance de la liaison de secours.
- Lorsque vous activez *Fail back* et une fois le temporisateur *Fail back delay [s]*, le port principal retourne à l'état de transfert et le port de secours est de nouveau désactivé.

Dans les cas répertoriés ci-dessus, le port force sa liaison à transférer le trafic et envoie d'abord un paquet « flush FDB » (vidage FDB) à l'équipement distant. Le paquet de vidage permet à l'équipement distant de réapprendre rapidement les adresses MAC.

13.8.2 Exemple de configuration

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Pour éviter les boucles durant la phase de configuration, configurez chaque équipement de la configuration *Link Backup* individuellement. Avant de raccorder les lignes redondantes, terminez la configuration des autres équipements de la configuration de *Link Backup*.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Dans l'exemple de réseau ci-dessous, vous connectez les ports *2/3* et *2/4* sur le commutateur réseau A aux commutateurs réseau uplink B et C. Lorsque vous définissez les ports en tant que paire de secours, un des ports transfère le trafic et l'autre port est en mode de blocage.

Le port principal *2/3* sur le commutateur réseau A est le port actif et transfère le trafic au port 1 sur le commutateur réseau B. Le port *2/4* sur le commutateur réseau A est le port de secours et bloque le trafic.

Lorsque le commutateur réseau A désactive le port *2/3* en raison d'une erreur détectée, le port *2/4* sur le commutateur réseau A commence à transférer le trafic vers le port 2 sur le commutateur réseau C.

Lorsque le port *2/3* bascule de nouveau sur l'état actif « no shutdown » (pas d'interruption), *Fail back* est activé et *Fail back delay [s]* est défini sur 30 secondes. Une fois le temporisateur expiré, le port *2/4* bloque le trafic, puis le port *2/3* commence à transférer le trafic.

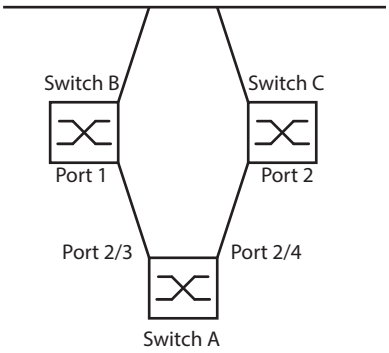


Figure 49 : Exemple de réseau Link Backup

Les tableaux suivants contiennent des exemples de paramètres pour configurer le commutateur réseau A.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Link Backup*.
- ☐ Saisissez une nouvelle paire de secours dans le tableau :
  - ☐ Cliquez sur le bouton  .
    La boîte de dialogue affiche la fenêtre *Create*.
  - ☐ Dans la liste déroulante *Primary port*, sélectionnez le port *2/3*.
    Dans la liste déroulante *Backup port*, sélectionnez le port *2/4*.
  - ☐ Cliquez sur le bouton *Ok*.
- ☐ Dans le cadre *Description*, saisissez `Link_Backup_1` comme nom pour la paire de secours.
- ☐ Pour activer la fonction *Fail back* pour la paire de secours, cochez la case *Fail back*.
- ☐ Définissez le temporisateur de reprise pour la paire de secours en saisissant `30` s dans *Fail back delay [s]*.
- ☐ Pour activer la paire de secours, cochez la case *Active*.
- ☐ Pour activer la fonction, sélectionnez le bouton radio *On* dans le cadre *Operation*.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 2/3`	Basculez sur le mode de configuration de l'interface *2/3*.
`link-backup add 2/4`	Crée une instance Link Backup avec le port *2/3* en port principal et le port *2/4* en port de secours.
`link-backup modify 2/4 description Link_Backup_1`	Spécifie la chaîne `Link_Backup_1` comme nom de la paire de secours.
`link-backup modify 2/4 failback-status enable`	Active le temporisateur de reprise.
`link-backup modify 2/4 failback-time 30`	Définit le délai de reprise sur `30` s.
`link-backup modify 2/4 status enable`	Active l'instance Link Backup.
`exit`	Basculez sur le mode de configuration.
`link-backup operation`	Active la fonction *Link Backup* globalement dans l'équipement.

13.9 FuseNet

Les protocoles *FuseNet* vous permettent de coupler des anneaux fonctionnant avec l'un des protocoles de redondance suivants :

- MRP
- HIPER ring
- RSTP

Commentaire : La condition préalable au couplage d'un réseau à l'anneau principal à l'aide du protocole *Ring/Network Coupling* est que le réseau connecté ne contienne que des équipements de réseau prenant en charge le protocole *Ring/Network Coupling*.

Utilisez le tableau suivant pour sélectionne le protocole de couplage *FuseNet* à utiliser dans votre réseau :

Anneau principal	**Réseau connecté**		
	MRP	**HIPER ring**	**RSTP**
MRP	*Sub Ring*[1)]	– *Redundant Coupling Protocol* – *Ring/Network Coupling*	– *Redundant Coupling Protocol* – *Ring/Network Coupling*
HIPER ring	*Sub Ring*	*Ring/Network Coupling*	– *Redundant Coupling Protocol* – *Ring/Network Coupling*
RSTP	*Redundant Coupling Protocol*	*Redundant Coupling Protocol*	*Dual RSTP* + *Redundant Coupling Protocol*

– aucun protocole de couplage adapté

1) avec *MRP* configuré sur différents VLAN

13.10 Sous-anneau

La fonction *Sub Ring* est une extension de Media Redundancy Protocol (MRP). Cette fonction vous permet de coupler un sous-anneau à un anneau principal par le biais de différentes structures de réseau.

Le protocole Subring assure la redondance pour les équipements en couplant les deux extrémités d'un réseau linéaire en un anneau principal.

La définition de sous-anneaux présente les avantages suivants :
- Par le biais du processus de couplage, vous incluez le nouveau segment de réseau dans le concept de redondance.
- Les sous-anneaux permettent l'intégration facile de nouvelles zones dans des réseaux existants.
- Les sous-anneaux permettent le mappage facile de la structure organisationnelle d'une zone dans une topologie de réseau.
- Dans un anneau MRP, les temps de reprise du sous-anneau en cas de redondance sont généralement < 100 ms.

13.10.1 Description d'un sous-anneau

Le concept de sous-anneau vous permet de coupler des segments de réseau à des équipements adaptés dans un anneau existant (anneau principal). Les équipements avec lesquels vous couplez le sous-anneau à l'anneau principal sont des gestionnaires de sous-anneau (SRM).

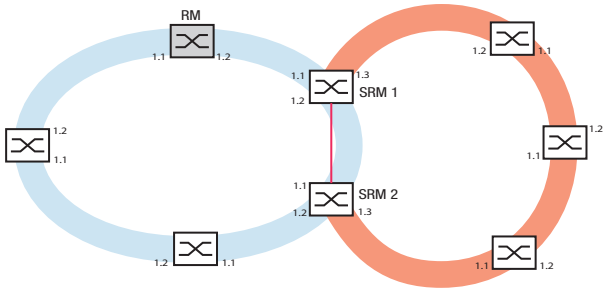


Figure 50 : Exemple d'une structure de sous-anneau
Anneau bleu = anneau principal
Anneau orange = sous-anneau
Ligne rouge = liaison redondante du sous-anneau
SRM = gestionnaire de sous-anneau
RM = gestionnaire d'anneau

Les équipements aptes à être des gestionnaires de sous-anneau prennent en charge jusqu'à 8 instances et gèrent donc jusqu'à 8 sous-anneaux simultanément.

La fonction *Sub Ring* vous permet d'intégrer des équipements prenant en charge MRP en tant que participants. Les équipements avec lesquels vous couplez le sous-anneau à l'anneau principal requièrent la fonction de gestionnaire *Sub Ring*.

Chaque sous-anneau peut comprendre jusqu'à 200 participants, à l'exclusion des gestionnaires de sous-anneaux eux-mêmes et des équipements entre les gestionnaires de sous-anneaux dans l'anneau principal.

Les figures suivantes présentent des exemples de topologies de sous-anneau possibles :

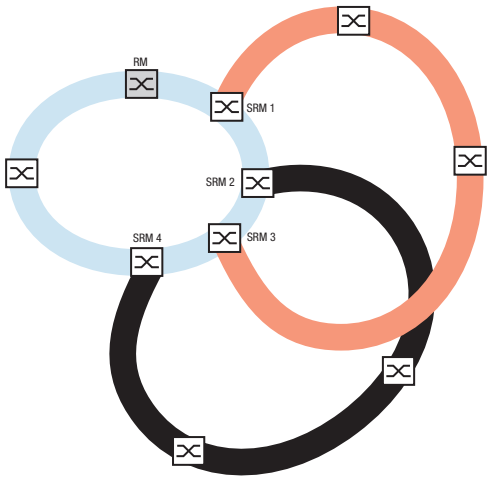


Figure 51 : Exemple d'une structure de sous-anneau avec chevauchement

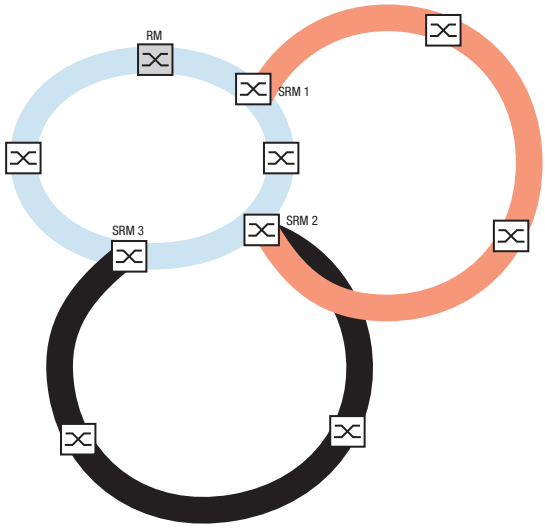


Figure 52 : Cas spécial : un gestionnaire de sous-anneau administre 2 sous-anneaux (2 instances). Le gestionnaire de sous-anneau peut administrer jusqu'à 8 instances.

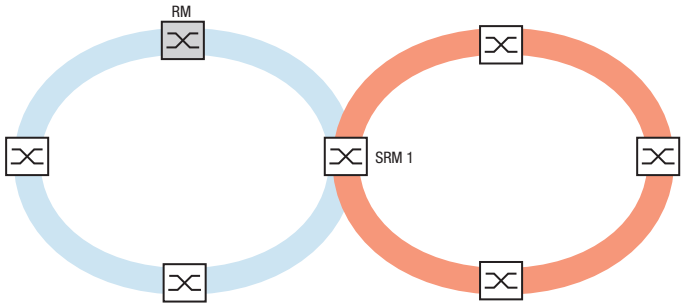


Figure 53 : Cas spécial : un gestionnaire de sous-anneau administre les deux extrémités d'un sous-anneau sur différents ports (gestionnaire de sous-anneau unique).

Commentaire : Dans les exemples précédents, les gestionnaires de sous-anneaux ne couplent les sous-anneaux qu'à des anneaux principaux existants. La fonction *Sub Ring* interdit les sous-anneaux en cascade, par exemple le couplage d'un nouveau sous-anneau à un autre sous-anneau existant.

Si vous utilisez MRP pour l'anneau principal et le sous-anneau, spécifiez les réglages VLAN comme suit :

- VLAN X pour l'anneau principal
  - sur les ports d'anneau des participants à l'anneau principal
  - sur les ports d'anneau du gestionnaire de sous-anneau
- VLAN Y pour le sous-anneau
  - sur les ports d'anneau des participants au sous-anneau
  - sur les ports de sous-anneau du gestionnaire de sous-anneau

  Vous pouvez utiliser le même VLAN pour plusieurs sous-anneaux.

13.10.2 Exemple de sous-anneau

Dans l'exemple suivant, vous couplez un nouveau segment de réseau avec 3 équipements à un anneau principal existant utilisant le protocole MRP. Lorsque vous couplez le réseau aux deux extrémités au lieu d'une extrémité, le sous-anneau offre une disponibilité accrue avec la configuration correspondante.

Vous couplez le nouveau segment de réseau en tant que sous-anneau. Vous couplez le sous-anneau aux équipements existants de l'anneau principal à l'aide des types de configuration suivants.

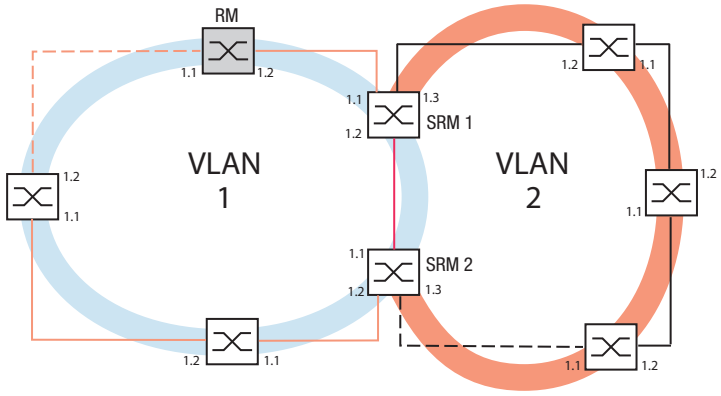


Figure 54 : Exemple d'une structure de sous-anneau
Ligne orange = membres de l'anneau principal dans VLAN 1
Ligne noire = membres du sous-anneau dans VLAN 2
Ligne pointillée orange = boucle de l'anneau principal ouverte
Ligne pointillée noire = boucle de sous-anneau ouverte
Ligne rouge = membre de liaison redondante dans VLAN 1
SRM = gestionnaire de sous-anneau
RM = gestionnaire d'anneau

Pour configurer le sous-anneau, exécutez les étapes suivantes :

- ☐ Configurez les trois équipements du nouveau segment de réseau en tant que participants à un anneau MRP :
  - Configurez le débit de transmission et le mode duplex pour les ports d'anneau conformément au tableau suivant :

Tableau 37 : Réglages des ports de sous-anneau

Type de port	Débit	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	coché	case non cochée	*100 Mbit/s FDX*
TX	1 Gbit/s	coché	coché	–
Optique	100 Mbit/s	coché	case non cochée	*100 Mbit/s FDX*
Optique	1 Gbit/s	coché	coché	–
Optique	2.5 Gbit/s	coché	–	*2.5 Gbit/s FDX*

Les étapes suivantes contiennent des réglages supplémentaires pour la configuration de sous-anneau :

- ☐ Pour prévenir les boucles durant la configuration, désactivez la fonction du gestionnaire de sous-anneau sur l'anneau principal et les équipements de sous-anneau. Après avoir entièrement configuré chaque équipement participant à l'anneau principal et aux sous-anneaux, activez la fonction *Sub Ring* globale et les gestionnaires de sous-anneaux.
- ☐ Désactivez la fonction RSTP sur les ports d'anneau MRP utilisés dans le sous-anneau.
- ☐ Vérifiez que la fonction *Link Aggregation* est inactive sur les ports participant à l'anneau principal et au sous-anneau.
- ☐ Spécifiez une appartenance à un VLAN différent pour les ports de l'anneau principal et les ports de sous-anneau, bien que l'anneau principal utilise le protocole MRP. Par exemple, utilisez le VLAN-ID `1` pour l'anneau principal et la liaison redondante, puis utilisez le VLAN-ID `2` pour le sous-anneau.
  - Pour les équipements participant à l'anneau principal, par exemple, ouvrez la boîte de dialogue *Switching > VLAN > Configuration*. Créez le VLAN `1` dans le tableau VLAN statique. Pour tagger les ports de l'anneau principal dans le VLAN `1`, sélectionnez l'élément `T` dans la liste déroulante des colonnes de port appropriées.
  - Pour les équipements participant au sous-anneau, exécutez l'étape ci-dessus et ajoutez les ports au VLAN `2` dans le tableau VLAN statique.
- ☐ Activez la fonction *MRP* pour les équipements de l'anneau principal et du sous-anneau.
  - Dans la boîte de dialogue *Switching > L2-Redundancy > MRP*, configurez les 2 ports d'anneau participant à l'anneau principal sur les équipements de l'anneau principal.
  - Pour les équipements participant au sous-anneau, exécutez l'étape ci-dessus et configurez les 2 ports d'anneau participant au sous-anneau sur les équipements de sous-anneau.
  - Affectez le même ID de domaine MRP aux équipement de l'anneau principal et du sous-anneau. Si vous n'utilisez que des équipements Schneider Electric, les valeurs par défaut conviennent pour l'ID de domaine MRP.

Commentaire : Le *MRP domain* est une séquence de 16 nombres compris dans une plage de `0` à `255`. La valeur par défaut est `255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255`. Un *MRP domain* constitué uniquement de zéros n'est pas valide.

La boîte de dialogue *Sub Ring* vous permet de modifier l'ID de domaine MRP. Vous pouvez également utiliser l'interface de ligne de commande. Pour ce faire, exécutez les étapes suivantes :

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`mrp domain delete`	Supprime le domaine MRP actuel.
`mrp domain add domain-id 0.0.1.1.2.2.3.4.4.111.222.123.0.0.66.99`	Crée un nouveau domaine MRP avec l'ID de domaine MRP spécifié. Toute modification ultérieure du domaine MRP s'appliquera à cet ID de domaine.

13.10.3 Exemple de configuration de sous-anneau

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Pour éviter les boucles durant la phase de configuration, configurez chaque équipement de la configuration *Sub Ring* individuellement. Avant de raccorder les lignes redondantes, terminez la configuration des autres équipements de la configuration de l'anneau.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Commentaire : Évitez les boucles durant la configuration. Configurez chaque équipement du sous-anneau individuellement. Avant d'activer la liaison redondante, configurez entièrement chaque équipement de sous-anneau.

Configurez les 2 gestionnaires de sous-anneau dans l'exemple. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching* > *L2-Redundancy* > *Sub Ring*.
- ☐ Pour ajouter une entrée de tableau, cliquez sur le bouton  .
- ☐ Dans la colonne *Port*, sélectionnez le port qui couple l'équipement au sous-anneau. Utilisez le port *1/3* pour cet exemple.
  Pour le couplage, utilisez l'un des ports disponibles à l'exception des ports déjà connectés à l'anneau principal.
- ☐ Dans la colonne *Name*, affectez un nom au sous-anneau.
  Pour cet exemple, saisissez `Test`.

- ☐ Dans la colonne *SRM mode*, sélectionnez le mode Gestionnaire de sous-anneau.
  Vous spécifiez ainsi quel port pour le couplage du sous-anneau à l'anneau principal devient le gestionnaire redondant.
  Les options pour le couplage sont les suivantes :
  - `manager`
    Lorsque vous spécifiez les deux gestionnaires de sous-anneau avec la même valeur, l'équipement avec l'adresse MAC plus élevée administre la liaison redondante.
  - `redundant manager`
    Cet équipement administre la liaison redondante si vous avez spécifié l'autre gestionnaire de sous-anneau en tant que `manager`. Sinon, l'équipement avec l'adresse MAC plus élevée administre la liaison redondante.

  Spécifiez le gestionnaire de sous-anneau 1 en tant que `manager`, conformément à la figure illustrant cet exemple.
- ☐ Laissez les valeurs dans la colonne *VLAN* et dans la colonne *MRP domain* inchangées.
  Les valeurs par défaut sont correctes pour l'exemple de configuration.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`sub-ring add 1`	Crée un nouveau sous-anneau avec l'ID de sous-anneau `1`.
`sub-ring modify 1 port 1/3`	Spécifier le port *1/3* en tant que port de sous-anneau.
`sub-ring modify 1 name Test`	Affecter le nom `Test` au sous-anneau `1`.
`sub-ring modify 1 mode manager`	Affecter le mode `manager` au sous-anneau `1`.
`show sub-ring ring`	Afficher l'état des sous-anneaux sur cet équipement.
`show sub-ring global`	Afficher l'état global du sous-anneau sur cet équipement.

- ☐ Configurez le 2ème gestionnaire de sous-anneau de la même manière.
  Spécifiez le gestionnaire de sous-anneau 2 en tant que `redundant manager`, conformément à la figure illustrant cet exemple.

- ☐ Pour activer la fonction Gestionnaire de sous-anneau, cochez la case *Active* dans la ligne appropriée.
- ☐ Après avoir configuré les deux gestionnaires de sous-anneau et les équipements participant au sous-anneau, activez la fonction et fermez la liaison redondante.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`sub-ring enable 1`	Activez le sous-anneau `1`.
`sub-ring enable 2`	Activez le sous-anneau `2`.
`exit`	Basculez sur le mode Privileged EXEC.

`show sub-ring ring <Domain ID>`	Affichez les réglages des sous-anneaux sélectionnés.
`show sub-ring global`	Affichez les réglages de sous-anneau globaux.
`copy config running-config nvm profile Test`	Sauvegardez les réglages actuels dans le profil de configuration nommé `Test` dans la mémoire non volatile (`nvm`).

13.11 Sous-anneau avec LAG

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Pour éviter les boucles durant la phase de configuration, configurez chaque équipement de la configuration *Sub Ring* individuellement. Avant de raccorder les lignes redondantes, terminez la configuration des autres équipements de la configuration de l'anneau.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Lorsqu'il existe au moins deux lignes de connexion redondantes parallèles (appelées trunk) entre deux équipements, et que ces lignes sont combinées en une seule connexion logique, il s'agit d'une connexion d'agrégation de liens (LAG).

L'équipement vous permet d'utiliser les ports LAG comme ports d'anneau avec le protocole *Sub Ring*.

13.11.1 Exemple

L'exemple suivant montre une configuration simple entre un anneau MRP et un sous-anneau.

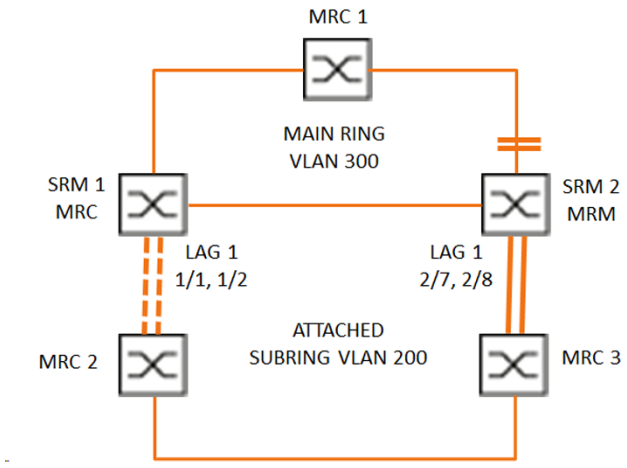


Figure 55 : Sous-anneau avec agrégation de liens

Le tableau suivant décrit les rôles des équipements comme illustré dans la figure ci-dessus. Le tableau décrit comment utiliser les ports d'anneau et les ports de sous-anneau comme ports LAG.

Tableau 38 : Équipements, ports et rôles

Nom de l'équipement	Port d'anneau	Rôle d'anneau principal	Rôle de sous-anneau	Port de sous-anneau
MRC1	1/3, 1/4	Client MRP	-	-
SRM1	1/3, 1/4	Client MRP	Gestionnaire redondant	lag/1
SRM2	2/4, 2/5	Gestionnaire MRP	Gestionnaire	lag/1
MRC2	lag/1, 1/3	-	Client MRP	-
MRC3	lag/1, 1/3	-	Client MRP	-

Configuration de l'anneau MRP

Les équipements participant à l'anneau principal sont membres du VLAN 300.

Exécutez les étapes suivantes :

`SRM2`

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`mrp domain add default-domain`	Crée un nouveau domaine MRP avec l'ID `default-domain`.
`mrp domain modify port primary 2/4`	Spécifie le port *2/4* en tant que port d'anneau `1`.
`mrp domain modify port secondary 2/5`	Spécifie le port *2/5* en tant que port d'anneau `2`.
`mrp domain modify mode manager`	Spécifie que l'équipement fonctionne en tant que *Ring manager*. N'activez pas la fonction *Ring manager* sur un autre équipement.
`mrp domain modify operation enable`	Active l'anneau MRP.
`mrp domain modify vlan 300`	Spécifie le VLAN-ID comme `300`.
`mrp operation`	Activez la fonction *MRP* dans l'équipement.

`MRC1, SRM1`

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`mrp domain add default-domain`	Crée un nouveau domaine MRP avec l'ID `default-domain`.
`mrp domain modify port primary 1/3`	Spécifie le port *1/3* en tant que port d'anneau `1`.
`mrp domain modify port secondary 1/4`	Spécifie le port *1/4* en tant que port d'anneau `2`.
`mrp domain modify mode client`	Spécifie le rôle de l'équipement en tant que client de l'anneau.
`mrp domain modify operation enable`	Active l'anneau MRP.
`mrp domain modify vlan 300`	Spécifie le VLAN-ID comme `300`.
`mrp operation`	Activez la fonction *MRP* dans l'équipement.

Configuration du sous-anneau

Les équipements participant au sous-anneau attaché sont membres du VLAN 200.

Exécutez les étapes suivantes :

SRM1

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`link-aggregation add lag/1`	Crée un groupe d'agrégation de liens `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Ajoute le port *1/1* au groupe d'agrégation de liens.
`link-aggregation modify lag/1 addport 1/2`	Ajoute le port *1/2* au groupe d'agrégation de liens.
`link-aggregation modify lag/1 adminmode`	Activez le groupe d'agrégation de liens.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`sub-ring add 1`	Crée un nouveau sous-anneau avec l'ID de sous-anneau `1`.
`sub-ring modify 1 name SRM1`	Affectez le nom `SRM1` au sous-anneau `1`.
`sub-ring modify 1 mode redundant-manager vlan 200 port lag/1`	Affectez à l'équipement le rôle de `Sub-ring redundant manager` dans le sous-anneau `1`. Si le sous-anneau est fermé, l'équipement bloque le port de l'anneau. VLAN `200` est défini pour le VLAN-ID du domaine. Le port `lag/1` est défini comme membre du VLAN `200`.
`sub-ring enable 1`	Activez le sous-anneau `1`.
`sub-ring operation`	Activez la fonctionnalité globale Gestionnaire de sous-anneau sur cet équipement.

SRM2

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`link-aggregation add lag/1`	Crée un groupe d'agrégation de liens `lag/1`.
`link-aggregation modify lag/1 addport 2/7`	Ajoute le port *2/7* au groupe d'agrégation de liens.
`link-aggregation modify lag/1 addport 2/8`	Ajoute le port *2/8* au groupe d'agrégation de liens.
`link-aggregation modify lag/1 adminmode`	Activez le groupe d'agrégation de liens.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`sub-ring add 1`	Crée un nouveau sous-anneau avec l'ID de sous-anneau `1`.

`sub-ring modify 1 mode manager vlan 200 port lag/1`	Affectez à l'équipement le rôle de `Subring manager` dans le sous-anneau `1`. VLAN `200` est défini pour le VLAN-ID du domaine. Le port `lag/1` est défini comme membre du VLAN `200`.
`sub-ring modify 1 name SRM2`	Affecter le nom `SRM2` au sous-anneau `1`.
`sub-ring enable 1`	Activez le sous-anneau `1`.
`sub-ring operation`	Activez la fonctionnalité globale Gestionnaire de sous-anneau sur cet équipement.

`MRC 2, 3`

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`mrp domain add default-domain`	Crée un nouveau domaine MRP avec l'ID `default-domain`.
`mrp domain modify port primary lag/1`	Spécifie le port `lag/1` en tant que port d'anneau `1`.
`mrp domain modify port secondary 1/3`	Spécifie le port *1/3* en tant que port d'anneau `2`.
`mrp domain modify mode client`	Spécifie le rôle de l'équipement en tant que client de l'anneau.
`mrp domain modify operation enable`	Active l'anneau MRP.
`mrp domain modify vlan 200`	Spécifie le VLAN-ID comme `200`.
`mrp operation`	Activez la fonction *MRP* dans l'équipement.

Désactiver STP

Désactivez la fonction *Spanning Tree* sur chaque port que vous avez spécifié en tant que port MRP ou port de sous-anneau. L'exemple suivant utilise le port *1/3*.

Exécutez les étapes suivantes :

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/3`	Basculez sur le mode de configuration de l'interface *1/3*.
`no spanning-tree operation`	Désactivez la fonction *Spanning Tree* sur le port.

13.12 Ring/Network Coupling

Basée sur un anneau, la fonction *Ring/Network Coupling* couple les anneaux ou les segments de réseau de manière redondante. *Ring/Network Coupling* connecte 2 anneaux/segments de réseau via 2 chemins distincts.

Lorsque les équipements dans le réseau couplé sont des équipements Schneider Electric, la fonction *Ring/Network Coupling* prend en charge le couplage selon des protocoles d'anneau dans les anneaux principal et secondaires :

- HIPER Ring
- Fast HIPER Ring
- MRP

La fonction *Ring/Network Coupling* peut également coupler des segments de réseau de structures en bus et maillées.

13.12.1 Méthodes de Ring/Network Coupling

Couplage à un commutateur réseau

Deux ports d'**un** équipement dans le premier anneau/réseau se connectent à un port chacun de deux équipements dans le deuxième anneau/réseau (voir la figure 56). Dans la méthode de couplage à un commutateur réseau, la ligne principale transfère les données et l'équipement bloque la ligne redondante.

Lorsque la ligne principale ne fonctionne plus, l'équipement débloque immédiatement la ligne redondante. Lorsque la ligne principale est restaurée, l'équipement bloque les données sur la ligne redondante. La ligne principale transfère de nouveau les données.

Le couplage d'anneau détecte et traite une erreur dans un laps de 500 ms (généralement 150 ms).

Couplage à deux commutateurs réseau

Un port de **deux** équipements dans le premier anneau/réseau se connectent chacun à un port de deux équipements dans le deuxième anneau/segment de réseau (voir la figure 58).

L'équipement dans la ligne redondante et l'équipement dans la ligne principale utilisent des paquets de commande pour s'informer mutuellement de leur mode opérationnel, via Ethernet ou une ligne de commande.

Lorsque la ligne principale ne fonctionne plus, l'équipement redondant (standby) débloque immédiatement la ligne redondante. Dès que la ligne principale est restaurée, l'équipement sur la ligne principale en informe l'équipement redondant. L'équipement en standby bloque les données sur la ligne redondante. La ligne principale transfère de nouveau les données.

Le couplage d'anneau détecte et traite une erreur dans un laps de 500 ms (généralement 150 ms).

Le type de configuration de couplage est principalement déterminé par la topologie de réseau et par le niveau de disponibilité souhaité (voir le tableau 39).

Tableau 39 : Critères de sélection pour les types de configuration du couplage redondant

	Couplage à un commutateur réseau	**Couplage à deux commutateurs réseau**	**Couplage à deux commutateurs réseau avec ligne de commande**
Application	Les 2 équipements sont dans des positions topologiques non pratiques. Aussi, l'établissement d'une liaison entre eux impliquerait beaucoup d'efforts pour le couplage à deux commutateurs réseau.	Les 2 équipements sont dans des positions topologiques pratiques. L'installation d'une ligne de commande impliquerait beaucoup d'efforts	Les 2 équipements sont dans des positions topologiques pratiques. L'installation d'une ligne de commande n'impliquerait pas beaucoup d'efforts.
Inconvénient	Si le commutateur réseau configuré pour le couplage redondant subit une défaillance, il ne reste aucune liaison entre les réseaux.	Plus d'efforts pour connecter les 2 équipements au réseau (par rapport au couplage à un commutateur réseau).	Plus d'efforts pour connecter les deux équipements au réseau (par rapport au couplage à un commutateur réseau et au couplage à deux commutateurs réseau).
Avantage	Moins d'efforts impliqués pour connecter les 2 équipements au réseau (par rapport au couplage à deux commutateurs réseau).	Lorsque l'un des équipements configurés pour le couplage redondant subit une défaillance, les réseaux couplés restent connectés.	Lorsque l'un des équipements configurés pour le couplage redondant subit une défaillance, les réseaux couplés restent connectés. La détermination de partenaire entre les équipements de couplage s'effectue de manière plus sûre et rapide que sans la ligne de commande.

13.12.2 Préparation du Ring/Network Coupling

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Pour éviter les boucles durant la phase de configuration, configurez chaque équipement de la configuration *Ring/Network Coupling* individuellement. Avant de raccorder les lignes redondantes, terminez la configuration des autres équipements de la configuration de l'anneau.

Pour éviter les boucles, utilisez la fonction *Ring/Network Coupling* uniquement sur les ports pour lesquels le protocole Rapid Spanning Tree est désactivé.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

À l'aide des images dans la boîte de dialogue, vous définissez le rôle des équipements dans le *Ring/Network Coupling*.

Dans les captures d'écrans et diagrammes suivants, les conventions ci-dessous sont utilisées :
- Les cadres et lignes bleus indiquent les équipements ou connexions des éléments actuellement décrits.
- Les lignes continues indiquent une liaison principale.
- Les lignes tiretées indiquent une liaison en standby.
- Les lignes pointillées indiquent la ligne de commande.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Dans le cadre *Mode*, liste d'options *Type*, sélectionnez le bouton radio approprié.
  - *one-switch coupling*
  - *two-switch coupling, master*
  - *two-switch coupling, slave*
  - *two-switch coupling with control line, master*
  - *two-switch coupling with control line, slave*

Couplage à un commutateur réseau

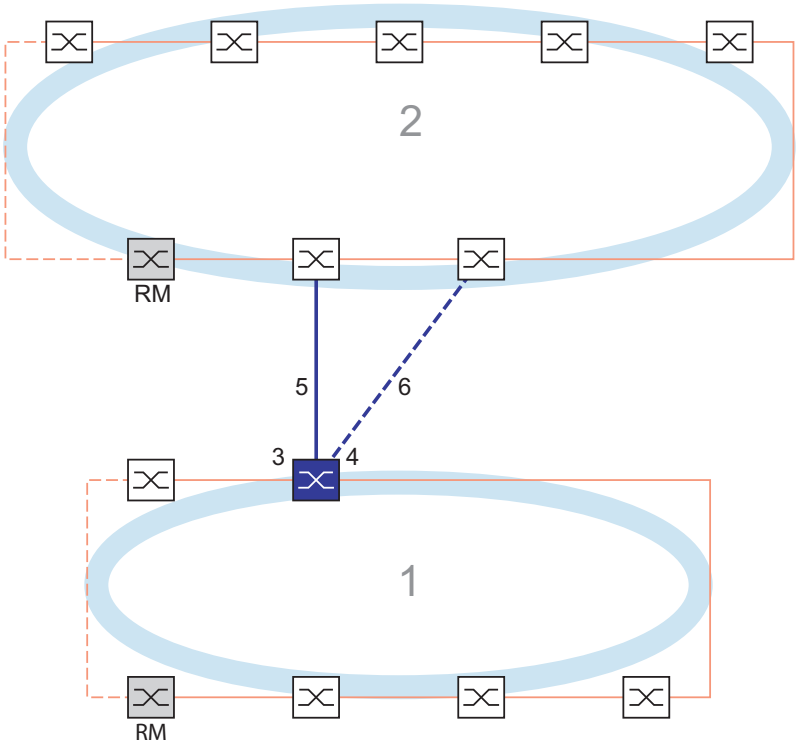


Figure 56 : Exemple de couplage à un commutateur réseau
1 : anneau
2 : backbone
3 : port de couplage partenaire
4 : port de couplage
5 : ligne principale
6 : ligne redondante

La ligne principale, indiquée par la ligne continue bleue connectée au port de couplage partenaire, permet un couplage entre les deux réseaux en mode de fonctionnement normal. Si la ligne principale est défaillante, la ligne redondante, indiquée par la ligne tiretée bleue connectée au port de couplage, assure le couplage en anneau/réseau. **Un** commutateur réseau assure la commutation du couplage.

Les réglages suivants s'appliquent à l'équipement affiché en bleu dans le graphique sélectionné.

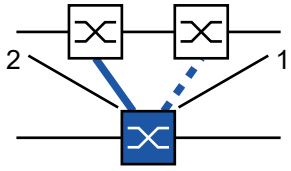


Figure 57 : Couplage à un commutateur réseau
1 : port de couplage
2 : port de couplage partenaire

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Dans le cadre *Mode*, liste d'options *Type*, sélectionnez le bouton radio `one-switch coupling`.

Commentaire : Configurez le *Partner coupling port* et les ports d'anneau sur différents ports.

- ☐ Dans le cadre *Coupling port*, sélectionnez le port sur lequel vous connectez la ligne redondante dans la liste déroulante *Port*.
- ☐ Dans le cadre *Partner coupling port*, sélectionnez le port sur lequel vous connectez la ligne principale dans la liste déroulante *Port*.
- ☐ Pour activer la fonction, sélectionnez le bouton radio *On* dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.
- ☐ Connectez la ligne redondante au port de couplage partenaire.
  Dans le cadre *Partner coupling port*, le champ *State* affiche l'état du port de couplage partenaire.
- ☐ Connectez la ligne principale au port de couplage.
  Dans le cadre *Coupling port*, le champ *State* affiche l'état du port de couplage.

Dans le cadre *Information*, le champ *Redundancy available* affiche si la redondance est disponible. Le champ *Configuration failure* affiche si les réglages sont complets et corrects.

Pour les ports de couplage, exécutez les étapes suivantes :

Commentaire : Les réglages suivants sont requis pour les ports de couplage.

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.
- ☐ Pour les ports sélectionnés en tant que ports de couplage, spécifiez les réglages conformément aux paramètres dans le tableau suivant.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

Tableau 40 : Réglages des ports d'anneau

Type de port	Débit	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	coché	case non cochée	*100 Mbit/s FDX*
TX	1 Gbit/s	coché	coché	–
Optique	100 Mbit/s	coché	case non cochée	*100 Mbit/s FDX*
Optique	1 Gbit/s	coché	coché	–
Optique	2.5 Gbit/s	coché	–	*2.5 Gbit/s FDX*

Si vous avez configuré des VLAN sur les ports de couplage, alors vous spécifiez les réglages VLAN sur les ports de couplage et de couplage partenaire. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Port*.
- ☐ Modifiez le réglage *Port-VLAN ID* avec la valeur du VLAN-ID configuré sur les ports.
- ☐ Décochez la case *Ingress filtering* pour les deux ports de couplage.
- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Configuration*.
- ☐ Pour tagger les connexions redondantes pour `VLAN 1` et l'appartenance au VLAN, saisissez la valeur `T` dans les cellules correspondant aux deux ports de couplage dans la ligne `VLAN 1`.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

Les équipements de couplage envoient des paquets de redondance avec la priorité la plus élevée sur `VLAN 1`.

- ☐ Dans le cadre *Configuration*, liste d'options *Redundancy mode*, spécifiez le type de redondance :
  - ▶ Avec le réglage *redundant ring/network coupling*, la ligne principale ou la ligne redondante est active. Le réglage permet aux équipements de basculer entre les deux lignes.
  - ▶ Lorsque vous activez le réglage *extended redundancy*, la ligne principale et la ligne redondante sont actives simultanément. Le réglage vous permet d'ajouter de la redondance au réseau de couplage. Lorsque la liaison entre les équipements de couplage dans le deuxième réseau subit une défaillance, les équipements de couplage continuent de transmettre et de recevoir des données.

Commentaire : Durant la période de reconfiguration, des dédoublements de paquets peuvent se produire. Aussi, si vos équipements détectent les dédoublements de paquets, sélectionnez ce réglage.

Le *Coupling mode* décrit le type de réseau dorsal auquel vous connectez le réseau en anneau (voir la figure 56).

- ☐ Dans le cadre *Configuration*, liste d'options *Coupling mode*, spécifiez le type du deuxième réseau :
  - ☐ Si vous le connectez à un réseau en anneau, sélectionnez le bouton radio *ring coupling*.
  - ☐ Si vous le connectez à une structure en bus ou maillée, sélectionnez le bouton radio *network coupling*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

Réinitialisez les réglages de couplage à l'état par défaut. Pour ce faire, exécutez les étapes suivantes :

- ☐ Cliquez sur le bouton ☰ puis sur l'élément *Reset*.

Couplage à deux commutateurs réseau

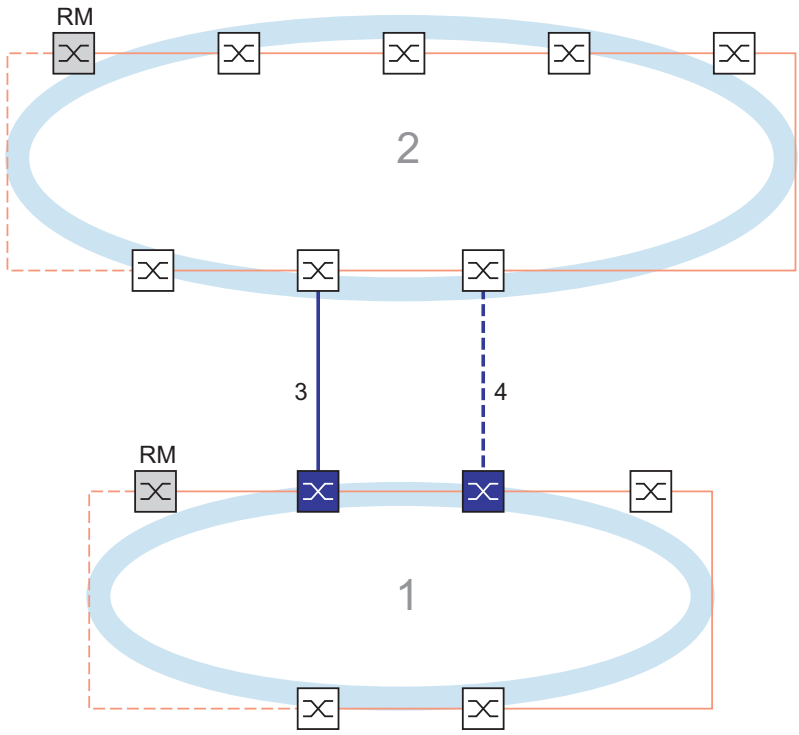


Figure 58 : Exemple de couplage à deux commutateurs réseau
1 : anneau
2 : backbone
3 : ligne principale
4 : ligne redondante

Le couplage entre 2 réseaux est effectué par la ligne principale, indiquée par la ligne continue bleue. En cas de défaillance de la ligne principale ou de l'un des équipements adjacents, la ligne redondante, indiquée par la ligne tiretée noire, assure le couplage du réseau. Le couplage est effectué par 2 équipements.

Les équipements s'envoient mutuellement des paquets de commande via Ethernet.

L'équipement principal connecté à la ligne principale et l'équipement en standby connecté à la ligne redondante sont partenaires dans le cadre du couplage.
☐ Connectez les 2 partenaires à l'aide des ports d'anneau.

Couplage à deux commutateurs réseau, équipement principal

Les réglages suivants s'appliquent à l'équipement affiché en bleu dans le graphique sélectionné.

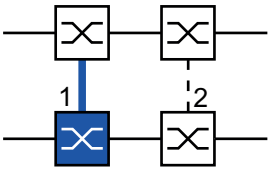


Figure 59 : Couplage à deux commutateurs réseau, équipement principal
1 : port de couplage
2 : port de couplage partenaire

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Dans le cadre *Mode*, liste d'options *Type*, sélectionnez le bouton radio `two-switch coupling, master`.
- ☐ Dans le cadre *Coupling port*, sélectionnez le port sur lequel vous connectez les segments de réseau dans la liste déroulante *Port*.
  Configurez le *Coupling port* et les ports d'anneau sur différents ports.
- ☐ Pour activer la fonction, sélectionnez le bouton radio *On* dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.
- ☐ Connectez la ligne principale au *Coupling port*.
  Dans le cadre *Coupling port*, le champ *State* affiche l'état du port de couplage.
  Lorsque le partenaire est déjà présent dans le réseau, le champ *IP address* dans le cadre *Partner coupling port* affiche l'adresse IP du port partenaire.

Dans le cadre *Information*, le champ *Redundancy available* affiche si la redondance est disponible. Le champ *Configuration failure* affiche si les réglages sont complets et corrects.

Commentaire : Si vous utilisez la fonction *Ring manager* et une fonction de couplage à deux commutateurs réseau sur le même équipement, il existe un risque de générer une boucle.

Pour prévenir les boucles continues alors que les liaisons sont opérationnelles sur les ports de couplage d'anneau, exécutez l'une des actions suivantes. L'équipement définit l'état du port de couplage sur « off » :
- désactivez le fonctionnement
- modifiez la configuration

Pour les ports de couplage, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.
- ☐ Pour les ports sélectionnés en tant que ports de couplage, spécifiez les réglages conformément aux paramètres dans le tableau suivant.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

Tableau 41 : Réglages des ports d'anneau

Type de port	Débit	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	coché	case non cochée	*100 Mbit/s FDX*
TX	1 Gbit/s	coché	coché	–
Optique	100 Mbit/s	coché	case non cochée	*100 Mbit/s FDX*
Optique	1 Gbit/s	coché	coché	–
Optique	2.5 Gbit/s	coché	–	*2.5 Gbit/s FDX*

Si vous avez configuré des VLAN sur les ports de couplage, alors vous spécifiez les réglages VLAN sur les ports de couplage et de couplage partenaire. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Port*.
- ☐ Modifiez le réglage *Port-VLAN ID* avec la valeur du VLAN-ID configuré sur les ports.
- ☐ Décochez la case *Ingress filtering* pour les deux ports de couplage.
- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Configuration*.
- ☐ Pour tagger les connexions redondantes pour `VLAN 1` et l'appartenance au VLAN, saisissez la valeur `T` dans les cellules correspondant aux deux ports de couplage dans la ligne `VLAN 1`.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

Les équipements de couplage envoient des paquets de redondance avec la priorité la plus élevée sur `VLAN 1`.

Couplage à deux commutateurs réseau, équipement en standby

Les réglages suivants s'appliquent à l'équipement affiché en bleu dans le graphique sélectionné.

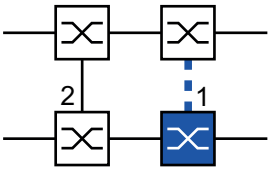


Figure 60 : Couplage à deux commutateurs réseau, équipement en standby
1 : port de couplage
2 : port de couplage partenaire

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Dans le cadre *Mode*, liste d'options *Type*, sélectionnez le bouton radio *two-switch coupling, slave*.
- ☐ Dans le cadre *Coupling port*, sélectionnez le port sur lequel vous connectez les segments de réseau dans la liste déroulante *Port*.
  Configurez le *Coupling port* et les ports d'anneau sur différents ports.
- ☐ Pour activer la fonction, sélectionnez le bouton radio *On* dans le cadre *Operation*.

- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.
- ☐ Connectez la ligne redondante au *Coupling port*.
  Dans le cadre *Coupling port*, le champ *State* affiche l'état du port de couplage.
  Lorsque le partenaire est déjà présent dans le réseau, le champ *IP address* dans le cadre *Partner coupling port* affiche l'adresse IP du port partenaire.

Dans le cadre *Information*, le champ *Redundancy available* affiche si la redondance est disponible. Le champ *Configuration failure* affiche si les réglages sont complets et corrects.

Commentaire : Si vous utilisez la fonction *Ring manager* et une fonction de couplage à deux commutateurs réseau sur le même équipement, il existe un risque de générer une boucle.

Pour prévenir les boucles continues alors que les liaisons sont opérationnelles sur les ports de couplage d'anneau, exécutez l'une des actions suivantes. L'équipement définit l'état du port de couplage sur « off » :

- désactivez le fonctionnement
- modifiez la configuration

Pour les ports de couplage, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.
- ☐ Pour les ports sélectionnés en tant que ports de couplage, spécifiez les réglages conformément aux paramètres dans le tableau suivant.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

Tableau 42 : Réglages des ports d'anneau

Type de port	Débit	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	coché	case non cochée	*100 Mbit/s FDX*
TX	1 Gbit/s	coché	coché	–
Optique	100 Mbit/s	coché	case non cochée	*100 Mbit/s FDX*
Optique	1 Gbit/s	coché	coché	–
Optique	2.5 Gbit/s	coché	–	*2.5 Gbit/s FDX*

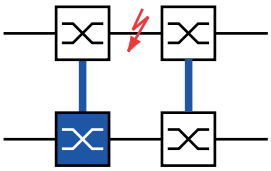
Si vous avez configuré des VLAN sur les ports de couplage, alors vous spécifiez les réglages VLAN sur les ports de couplage et de couplage partenaire. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Port*.
- ☐ Modifiez le réglage *Port-VLAN ID* avec la valeur du VLAN-ID configuré sur les ports.
- ☐ Décochez la case *Ingress filtering* pour les deux ports de couplage.
- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Configuration*.
- ☐ Pour tagger les connexions redondantes pour `VLAN 1` et l'appartenance au VLAN, saisissez la valeur `T` dans les cellules correspondant aux deux ports de couplage dans la ligne `VLAN 1`.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

Les équipements de couplage envoient des paquets de redondance avec la priorité la plus élevée sur `VLAN 1`.

Spécifiez les réglages *Redundancy mode* et *Coupling mode*. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Dans le cadre *Configuration*, liste d'options *Redundancy mode*, sélectionnez l'un des boutons radio suivants :
  - ▶ `redundant ring/network coupling`
    Avec ce réglage, la ligne principale ou la ligne redondante est active. Le réglage permet aux équipements de basculer entre les deux lignes.
  - ▶ `extended redundancy`
    Avec ce réglage, la ligne principale et la ligne redondante sont actives simultanément. Le réglage vous permet d'ajouter de la redondance au deuxième réseau. Lorsque la liaison entre les équipements de couplage dans le deuxième réseau subit une défaillance, les équipements de couplage continuent de transmettre et de recevoir des données.

    Durant la période de reconfiguration, des dédoublements de paquets peuvent se produire. Aussi, sélectionnez ce réglage uniquement si vos équipements détectent les dédoublements de paquets.
- ☐ Dans le cadre *Configuration*, liste d'options *Coupling mode*, sélectionnez l'un des boutons radio suivants :
  - ☐ Si vous le connectez à un réseau en anneau, sélectionnez le bouton radio *ring coupling*.
  - ☐ Si vous le connectez à une structure en bus ou maillée, sélectionnez le bouton radio *network coupling*.

  Le *Coupling mode* décrit le type de réseau dorsal auquel vous connectez le réseau en anneau (voir la figure 58).
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

Réinitialisez les réglages de couplage à l'état par défaut. Pour ce faire, exécutez les étapes suivantes :

- ☐ Cliquez sur le bouton puis sur l'élément *Reset*.

Couplage à deux commutateurs réseau avec ligne de commande

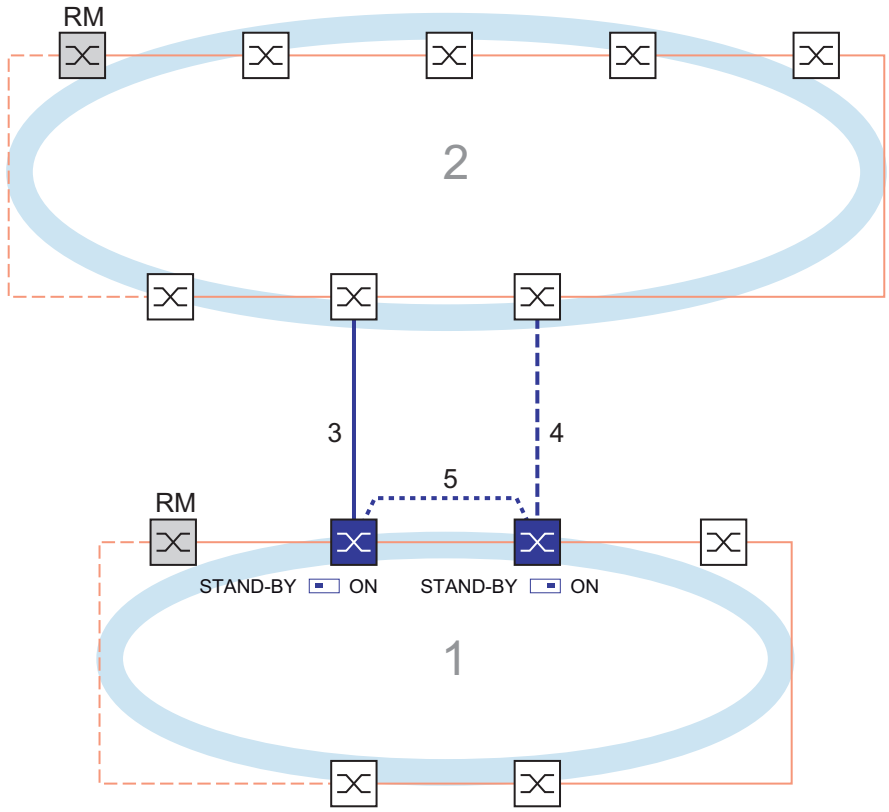


Figure 61 : Exemple de couplage à deux commutateurs réseau avec ligne de commande
1 : anneau
2 : backbone
3 : ligne principale
4 : ligne redondante
5 : ligne de commande

Le couplage entre 2 réseaux est effectué par la ligne principale, indiquée par la ligne continue bleue. En cas de défaillance de la ligne principale ou de l'un des équipements adjacents, la ligne redondante, indiquée par la ligne tiretée bleue, assure le couplage des 2 réseaux. Le couplage d'anneau est effectué par 2 équipements.

Les équipements envoient des paquets de commande via une ligne de commande, indiquée par la ligne pointillée bleue dans la figure ci-dessous (voir la figure 62).

L'équipement principal connecté à la ligne principale et l'équipement en standby connecté à la ligne redondante sont partenaires dans le cadre du couplage.
☐ Connectez les 2 partenaires à l'aide des ports d'anneau.

Couplage à deux commutateurs réseau avec ligne de commande, équipement principal

Les réglages suivants s'appliquent à l'équipement affiché en bleu dans le graphique sélectionné.

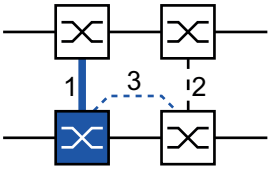


Figure 62 : Couplage à deux commutateurs réseau avec ligne de commande, équipement principal
1 : port de couplage
2 : port de couplage partenaire
3 : ligne de commande

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Dans le cadre *Mode*, liste d'options *Type*, sélectionnez le bouton radio `two-switch coupling with control line, master`.
- ☐ Dans le cadre *Coupling port*, sélectionnez le port sur lequel vous connectez les segments de réseau dans la liste déroulante *Port*.
  Configurez le *Coupling port* et les ports d'anneau sur différents ports.
- ☐ Dans le cadre *Control port*, sélectionnez le port sur lequel vous connectez la ligne de contrôle dans la liste déroulante *Port*.
  Configurez le *Coupling port* et les ports d'anneau sur différents ports.
- ☐ Pour activer la fonction, sélectionnez le bouton radio *On* dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.
- ☐ Connectez la ligne redondante au port de couplage.
  Dans le cadre *Coupling port*, le champ *State* affiche l'état du port de couplage.
  Lorsque le partenaire est déjà présent dans le réseau, le champ *IP address* dans le cadre *Partner coupling port* affiche l'adresse IP du port partenaire.
- ☐ Connectez la ligne de commande au port de commande.
  Dans le cadre *Control port*, le champ *State* affiche l'état du port de commande.
  Lorsque le partenaire est déjà présent dans le réseau, le champ *IP address* dans le cadre *Partner coupling port* affiche l'adresse IP du port partenaire.

Dans le cadre *Information*, le champ *Redundancy available* affiche si la redondance est disponible. Le champ *Configuration failure* affiche si les réglages sont complets et corrects.

Commentaire : Si vous utilisez la fonction *Ring manager* et une fonction de couplage à deux commutateurs réseau sur le même équipement, il existe un risque de générer une boucle.

Pour prévenir les boucles continues alors que les liaisons sont opérationnelles sur les ports de couplage d'anneau, exécutez l'une des actions suivantes. L'équipement définit l'état du port de couplage sur « off » :
- désactivez le fonctionnement
- modifiez la configuration

Pour les ports de couplage, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.
- ☐ Pour les ports sélectionnés en tant que ports de couplage, spécifiez les réglages conformément aux paramètres dans le tableau suivant.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

Tableau 43 : Réglages des ports d'anneau

Type de port	Débit	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	coché	case non cochée	*100 Mbit/s FDX*
TX	1 Gbit/s	coché	coché	–
Optique	100 Mbit/s	coché	case non cochée	*100 Mbit/s FDX*
Optique	1 Gbit/s	coché	coché	–
Optique	2.5 Gbit/s	coché	–	*2.5 Gbit/s FDX*

Si vous avez configuré des VLAN sur les ports de couplage, alors vous spécifiez les réglages VLAN sur les ports de couplage et de couplage partenaire. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Port*.
- ☐ Modifiez le réglage *Port-VLAN ID* avec la valeur du VLAN-ID configuré sur les ports.
- ☐ Décochez la case *Ingress filtering* pour les deux ports de couplage.
- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Configuration*.
- ☐ Pour tagger les connexions redondantes pour `VLAN 1` et l'appartenance au VLAN, saisissez la valeur `T` dans les cellules correspondant aux deux ports de couplage dans la ligne `VLAN 1`.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

Les équipements de couplage envoient des paquets de redondance avec la priorité la plus élevée sur `VLAN 1`.

Couplage à deux commutateurs réseau avec ligne de commande, équipement en standby

Les réglages suivants s'appliquent à l'équipement affiché en bleu dans le graphique sélectionné.

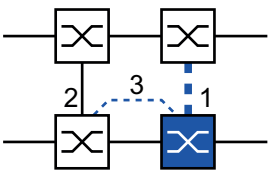


Figure 63 : Couplage à deux commutateurs réseau avec ligne de commande, équipement en standby
1 : port de couplage
2 : port de couplage partenaire
3 : ligne de commande

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Dans le cadre *Mode*, liste d'options *Type*, sélectionnez le bouton radio `two-switch coupling with control line, slave`.
- ☐ Dans le cadre *Coupling port*, sélectionnez le port sur lequel vous connectez les segments de réseau dans la liste déroulante *Port*.
  Configurez le *Coupling port* et les ports d'anneau sur différents ports.
- ☐ Dans le cadre *Control port*, sélectionnez le port sur lequel vous connectez la ligne de contrôle dans la liste déroulante *Port*.
  Configurez le *Coupling port* et les ports d'anneau sur différents ports.
- ☐ Pour activer la fonction, sélectionnez le bouton radio *On* dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.
- ☐ Connectez la ligne redondante au port de couplage.
  Dans le cadre *Coupling port*, le champ *State* affiche l'état du port de couplage.
  Lorsque le partenaire est déjà présent dans le réseau, le champ *IP address* dans le cadre *Partner coupling port* affiche l'adresse IP du port partenaire.
- ☐ Connectez la ligne de commande au port de commande.
  Dans le cadre *Control port*, le champ *State* affiche l'état du port de commande.
  Lorsque le partenaire est déjà présent dans le réseau, le champ *IP address* dans le cadre *Partner coupling port* affiche l'adresse IP du port partenaire.

Dans le cadre *Information*, le champ *Redundancy available* affiche si la redondance est disponible. Le champ *Configuration failure* affiche si les réglages sont complets et corrects.

Commentaire : Si vous utilisez la fonction *Ring manager* et une fonction de couplage à deux commutateurs réseau sur le même équipement, il existe un risque de générer une boucle.

Pour prévenir les boucles continues alors que les liaisons sont opérationnelles sur les ports de couplage d'anneau, exécutez l'une des actions suivantes. L'équipement définit l'état du port de couplage sur « off » :

- désactivez le fonctionnement
- modifiez la configuration

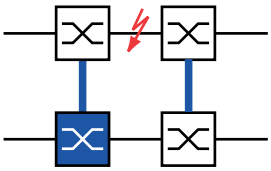
Pour les ports de couplage, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Port*.
- ☐ Modifiez le réglage *Port-VLAN ID* avec la valeur du VLAN-ID configuré sur les ports.
- ☐ Décochez la case *Ingress filtering* pour les deux ports de couplage.
- ☐ Ouvrez la boîte de dialogue *Switching > VLAN > Configuration*.
- ☐ Pour tagger les connexions redondantes pour `VLAN 1` et l'appartenance au VLAN, saisissez la valeur `T` dans les cellules correspondant aux deux ports de couplage dans la ligne `VLAN 1`.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

Les équipements de couplage envoient des paquets de redondance avec la priorité la plus élevée sur `VLAN 1`.

Spécifiez les réglages *Redundancy mode* et *Coupling mode*. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Ring/Network Coupling*.
- ☐ Dans le cadre *Configuration*, liste d'options *Redundancy mode*, sélectionnez l'un des boutons radio suivants :
  - ▶ `redundant ring/network coupling`
    Avec ce réglage, la ligne principale ou la ligne redondante est active. Le réglage permet aux équipements de basculer entre les deux lignes.
  - ▶ `extended redundancy`
    Avec ce réglage, la ligne principale et la ligne redondante sont actives simultanément. Le réglage vous permet d'ajouter de la redondance au deuxième réseau. Lorsque la liaison entre les équipements de couplage dans le deuxième réseau subit une défaillance, les équipements de couplage continuent de transmettre et de recevoir des données.

    Durant la période de reconfiguration, des dédoublements de paquets peuvent se produire. Aussi, sélectionnez ce réglage uniquement si vos équipements détectent les dédoublements de paquets.
- ☐ Dans le cadre *Configuration*, liste d'options *Coupling mode*, sélectionnez l'un des boutons radio suivants :
  - ☐ Si vous le connectez à un réseau en anneau, sélectionnez le bouton radio *ring coupling*.
  - ☐ Si vous le connectez à une structure en bus ou maillée, sélectionnez le bouton radio *network coupling*.

  Le *Coupling mode* décrit le type de réseau dorsal auquel vous connectez le réseau en anneau (voir la figure 61).
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

Réinitialisez les réglages de couplage à l'état par défaut. Pour ce faire, exécutez les étapes suivantes :

- ☐ Cliquez sur le bouton ☰ puis sur l'élément *Reset*.

13.13 RCP

Les applications industrielles requièrent une tolérance fautive de vos réseaux. Cela implique aussi la gestion de temps d'interruption courts et déterministes pour la communication lorsque l'un des équipements du réseau est défaillant.

Une topologie en anneau fournit des délais de transition courts avec une utilisation minimale des ressources. Toutefois, la topologie en anneau pose le problème du couplage de ces anneaux entre eux de manière redondante.

Redundant Coupling Protocol *RCP* vous permet de coupler les anneaux fonctionnant avec l'un des protocoles de redondance suivants :
- MRP
- HIPER ring
- RSTP

La fonction *RCP* vous permet de coupler plusieurs anneaux secondaires à un anneau principal (voir la figure 64). Seuls les commutateurs réseau qui couplent les anneaux requièrent la fonction *RCP*.

Vous pouvez aussi utiliser des équipements autres que Schneider Electric dans les réseaux couplés.

La fonction *RCP* utilise un équipement master et un slave pour transporter les données entre les réseaux. Seul l'équipement master transfère les trames entre les anneaux.

Lorsque des messages multicast Schneider Electric propriétaires sont utilisés, les équipements *RCP* master et slave s'informent mutuellement de leur mode opérationnel. Configurez les équipements dans l'anneau qui ne sont pas des équipements de couplage pour qu'ils transfèrent les adresses multicast suivantes :
- `01:80:63:07:00:09`
- `01:80:63:07:00:0A`

Connectez les équipements master et slave en tant que voisins directs.

Vous utilisez 4 ports par équipement pour créer le couplage redondant. Installez les équipements de couplage avec 2 ports intérieurs et 2 ports extérieurs dans chaque réseau.

- Le port intérieur connecte les équipements master et slave entre eux.
- Le port extérieur connecte les équipements au réseau.

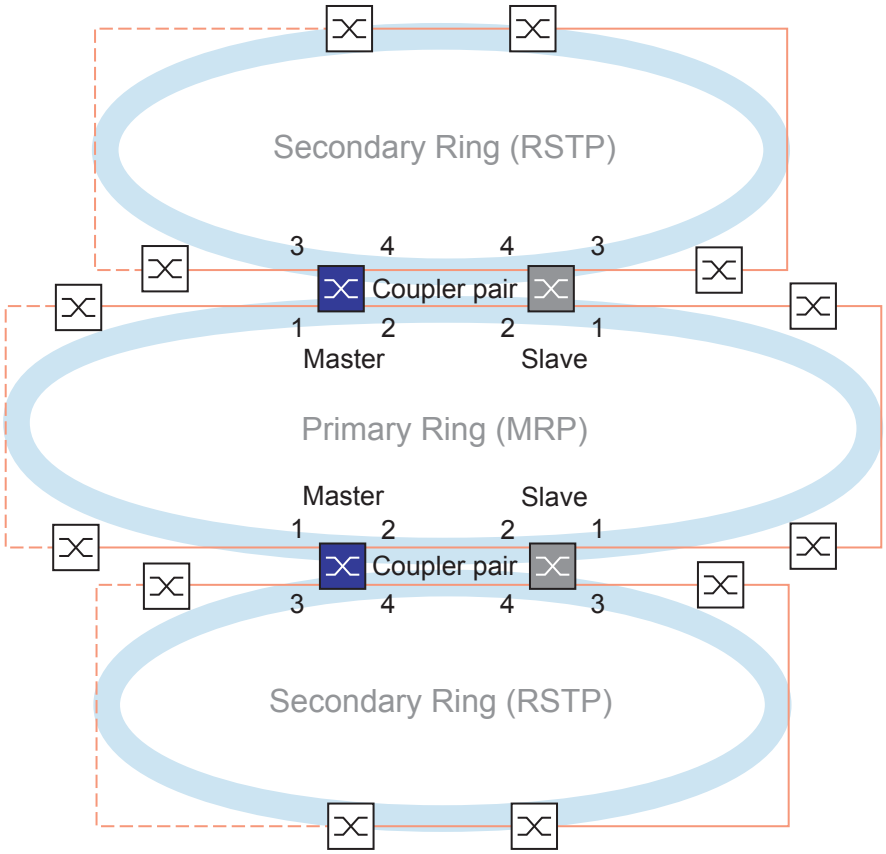


Figure 64 : Exemple de couplage redondant à deux commutateurs réseau
1 : port de couplage extérieur dans l'anneau principal
2 : port de couplage intérieur dans l'anneau principal
3 : port de couplage extérieur dans l'anneau secondaire
4 : port de couplage intérieur dans l'anneau secondaire

Lorsque le rôle est défini sur la valeur *auto*, les équipements coupleurs sélectionnent automatiquement leur rôle en tant que *master* ou *slave*. Si vous souhaitez un équipement master ou slave permanent, configurez les rôles manuellement.

Commentaire : Le rôle `single` n'est utilisé qu'avec la fonction *Dual RSTP*. Voir « Couplage de 2 anneaux RSTP à l'aide de la fonction Dual RSTP » à la page 259.

Si le maître n'est plus accessible à l'aide des ports de couplage intérieurs, l'équipement esclave attend l'expiration du délai de temporisation avant de reprendre le rôle de maître. Durant le délai de temporisation spécifié, l'esclave tente d'atteindre le maître via les ports de couplage extérieurs. Si le maître n'est toujours pas accessible, l'esclave assume le rôle de maître. Pour maintenir la stabilité dans le réseau connecté aux ports de couplage extérieurs, configurez un délai de temporisation plus long que le temps de restauration dans les anneaux couplés.

Commentaire : Désactivez RSTP sur les ports intérieurs et extérieurs de couplage redondant *RCP* non connectés à l'anneau RSTP. Dans l'exemple de configuration, vous désactivez RSTP sur les ports `1` et `2` de chaque équipement.

13.13.1 Exemple d'application pour le couplage RCP

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Pour éviter les boucles durant la phase de configuration, configurez chaque équipement de la configuration *RCP* individuellement. Avant de raccorder les lignes redondantes, terminez la configuration des autres équipements de la configuration de l'anneau.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Les équipements Schneider Electric prennent en charge la méthode Redundant Coupling Protocol à deux commutateurs réseau. Vous pouvez utiliser la fonction *RCP* pour fournir un réseau installé dans un train, par exemple. Le réseau fournit des informations aux passagers concernant la position du train ou les différents arrêts sur la ligne. Le réseau peut aussi améliorer la sécurité des passagers, par exemple avec la vidéosurveillance.

Les anneaux principaux dans la figure représentent un réseau en anneau *MRP* dans une voiture. Les anneaux secondaires dans la figure sont des réseaux en anneau RSTP. Chaque anneau contient 4 équipements (voir la figure 65).

Pour simplifier la topologie du train dans la figure, les ports d'anneau *MRP* et les ports intérieurs et extérieurs *RCP* sont affectés aux mêmes numéros de port. Spécifiez les mêmes valeurs pour les paramètres des ports conformément à leur fonction dans le réseau. Par exemple, spécifiez les ports *1/1* et *1/2* sur les commutateurs réseaux 1D et 1C en tant que ports d'anneau MRP. Port *1/4* en tant que port intérieur *RCP* et port *1/3* en tant que port extérieur *RCP*.

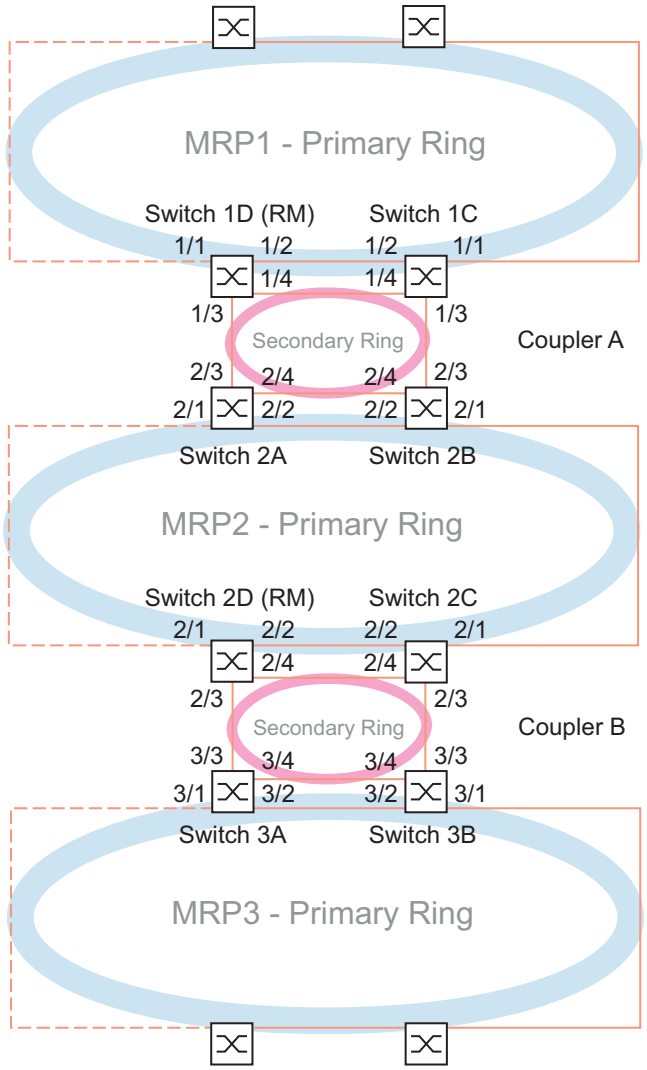


Figure 65 : Topologie de train Redundant Coupling Protocol

La liste suivante indique les rôles des ports sur chaque équipement.
1 : les ports 1 et 2 sont des ports d'anneau MRP
2 : le port 3 est un port extérieur RCP
3 : le port 4 est un port intérieur RCP

Les étapes suivantes décrivent comment spécifier les paramètres pour le commutateur réseau 1D dans Coupler A. Configurez les autres équipements utilisés pour Coupler A et les équipements utilisés dans Coupler B de la même manière.

Désactivez la fonction RSTP dans l'anneau MRP.

MRP et RSTP ne sont pas compatibles. Aussi, désactivez la fonction RSTP sur les ports *RCP* utilisés dans l'anneau *MRP*. Dans l'exemple de configuration, les ports `x/1` et `x/2` sont utilisés pour l'anneau *MRP*. Activez la fonction RSTP uniquement sur les ports intérieurs et extérieurs *RCP* utilisés dans l'anneau secondaire. Par exemple, activez la fonction RSTP sur les ports `x/3` et `x/4`.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port*, onglet *CIST*.
- ☐ Dans le réglage par défaut, la fonction RSTP est active sur les ports. Pour désactiver la fonction RSTP sur les ports d'anneau *MRP*, décochez les cases *STP active* pour les ports `x/1` et `x/2`.
- ☐ Ouvrez la boîte de dialogue *Switching* > *L2-Redundancy* > *Spanning Tree* > *Global*.
- ☐ Pour activer la fonction, sélectionnez le bouton radio *On* dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface x/1`	Basculez sur le mode de configuration de l'interface `x/1`.
`no spanning-tree mode`	Désactivez la fonction *Spanning Tree* sur le port.
`exit`	Basculez sur le mode de configuration.
`interface x/2`	Basculez sur le mode de configuration de l'interface `x/2`.
`no spanning-tree mode`	Désactivez la fonction *Spanning Tree* sur le port.
`exit`	Basculez sur le mode de configuration.
`spanning-tree operation`	Activer la fonction *Spanning Tree*.

Spécifiez le maître de l'anneau dans l'anneau MRP.

Dans la figure, le commutateur réseau D de chaque anneau *MRP* est désigné comme le ring manger (voir la figure 65). Spécifiez les autres commutateurs réseau dans les années comme étant des clients d'anneau.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching* > *L2-Redundancy* > *MRP*.
- ☐ Spécifiez le premier port d'anneau dans le cadre *Ring port 1*.
  Dans la liste déroulante *Port*, sélectionnez le port `x/1`.
- ☐ Spécifiez le deuxième port d'anneau dans le cadre *Ring port 2*.
  Dans la liste déroulante *Port*, sélectionnez le port `x/2`.
- ☐ Pour désigner l'équipement en tant que Ring Manager, activez la fonction dans le cadre *Ring manager*.
- ☐ Pour activer la fonction, sélectionnez le bouton radio *On* dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`mrp domain add default-domain`	Créez un nouveau domaine *MRP* avec l'ID `default-domain`.
`mrp domain modify port primary x/1`	Spécifiez le port `x/1` en tant que port d'anneau `1`.
`mrp domain modify port secondary x/2`	Spécifiez le port `x/2` en tant que port d'anneau `2`.
`mrp domain modify mode manager`	Spécifiez que l'équipement fonctionne en tant que *Ring manager*. Pour les autres équipements dans l'anneau, conservez le réglage par défaut.
`mrp domain modify operation enable`	Activer la fonction *MRP*.

Spécification des équipements dans le coupleur redondant

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > RCP*.
- ☐ Spécifiez le *Inner port* dans le cadre *Primary ring/network*. Sélectionnez le port `x/2`.
- ☐ Spécifiez le *Outer port* dans le cadre *Primary ring/network*. Sélectionnez le port `x/1`.
- ☐ Spécifiez le *Inner port* dans le cadre *Secondary ring/network*. Sélectionnez le port `x/4`.
- ☐ Spécifiez le *Outer port* dans le cadre *Secondary ring/network*. Sélectionnez le port `x/3`.

- ☐ Pour activer la fonction, sélectionnez le bouton radio *On* dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`redundant-coupling port primary inner x/2`	Spécifiez le port `x/2` en tant que port intérieur principal.
`redundant-coupling port primary outer x/1`	Spécifiez le port `x/1` en tant que port extérieur principal.
`redundant-coupling port secondary inner x/4`	Spécifiez le port `x/4` en tant que port intérieur secondaire.
`redundant-coupling port secondary outer x/3`	Spécifiez le port `x/3` en tant que port extérieur secondaire.
`redundant-coupling operation`	Activez la fonction *RCP* dans l'équipement.
`copy config running-config nvm`	Sauvegardez les réglages actuels dans la mémoire non-volatile (`nvm`) dans le profil de configuration « selected ».

13.13.2 Couplage de 2 anneaux RSTP à l'aide de la fonction Dual RSTP

Si vous souhaitez utiliser RSTP pour les anneaux principal et secondaire, la fonction *RCP* affecte les ports de l'anneau secondaire à l'instance *Dual RSTP*. Cela crée deux réseaux RSTP indépendants couplés par *RCP*.

Vous pouvez mettre en œuvre jusqu'à 16 équipements MCSESM-E dans un anneau secondaire. Les 2 équipements de l'anneau principal qui couplent l'anneau secondaire font partie de ce nombre. En cas de défaillance d'un composant de réseau dans l'anneau secondaire, la fonction *RCP* peut généralement atteindre un délai de reconfiguration inférieur à 50 ms.

Vous pouvez également mettre en œuvre jusqu'à 16 équipements MCSESM-E dans un anneau principal. Ainsi, les fonctions *RCP* et *Dual RSTP* peuvent aussi généralement atteindre un délai de reconfiguration inférieur à 50 ms dans l'anneau principal. Vous pouvez connecter jusqu'à 8 anneaux secondaires à un anneau principal. Ainsi, vous pouvez connecter jusqu'à 128 commutateurs réseau (8 × 14 + 16). Dans ce réseau, vous pouvez généralement atteindre un délai de reconfiguration de bout en bout inférieur à 50 ms avec redondance des équipements.

Lorsque les exigences en matière de délai de reconfiguration dans l'anneau principal sont moindres, vous disposez des options suivantes :
- Augmenter le nombre de commutateurs réseau dans l'anneau principal.
- Connecter plus d'anneaux secondaires à l'anneau principal.

Vous pouvez aussi utiliser des équipements autres que MCSESM-E dans les anneaux, mais uniquement dans les cas où les équipements mettent à jour les modifications de la topologie RSTP suffisamment rapidement. Par exemple, si un composant de réseau subit une défaillance.

Propriétés des ports principal et secondaire de l'instance

Pour les ports d'une instance principale ou secondaire, tenez compte des remarques suivantes :
- Seuls les ports du commutateur réseau *RCP* qui sont configurés en tant que ports d'anneau extérieurs et intérieurs appartiennent à l'instance *Dual RSTP*. Les autres ports appartiennent à l'instance principale du commutateur réseau.
- Vous pouvez connecter des équipements terminaux ou des réseaux qui n'exécutent pas *Spanning Tree* sur un port appartenant implicitement à une instance principale du commutateur réseau *RCP*.
  Ces topologies ne fournissent ni la redondance d'équipement ni la redondance de liaison.
- Vous pouvez réaliser un réseau maillé dans l'anneau principal ou secondaire en établissant plus de liaisons entre les ports de la même instance.
  Dans ces topologies, un délai de reconfiguration de bout en bout maximum défini de 50 ms ne s'applique pas.

Couplage de 2 anneaux RSTP à l'aide d'un seul commutateur réseau RCP

Si vous souhaitez coupler 2 anneaux RSTP à l'aide d'un seul commutateur réseau, utilisez le rôle `single`.

Pour le commutateur réseau *RCP* avec le rôle `single`, les ports intérieurs et extérieurs ont la même fonction. Vous pouvez intervertir les ports intérieurs et extérieurs d'une instance spécifique.

Si vous utilisez un commutateur réseau pour connecter les anneaux, vous pouvez connecter jusqu'à 16 anneaux secondaires à un anneau principal. Cela inclut le commutateur réseau *RCP* qui connecte les anneaux. Ainsi, vous pouvez connecter jusqu'à 256 commutateurs réseau (16 × 15 + 16). Dans ce réseau, vous pouvez atteindre un délai de reconfiguration de bout en bout maximum de 50 ms dans un réseau avec redondance des équipements.

Lorsque les exigences en matière de délai de reconfiguration dans l'anneau principal sont moindres, vous disposez des options suivantes :

- Augmenter le nombre de commutateurs réseau dans l'anneau principal.
- Connecter plus d'anneaux secondaires à l'anneau principal.

Options en matière de topologie pour la fonction Dual RSTP

L'exemple suivant montre la structure de base d'un anneau principal connecté à 3 anneaux secondaires. Les anneaux secondaires 1 et 2 sont connectés à l'anneau principal à l'aide de 2 commutateurs réseau *RCP* chacun, et l'anneau secondaire 3 avec 1 commutateur réseau *RCP*. Les coûts de chemin pour chaque liaison dans un anneau sont supposés être identiques.

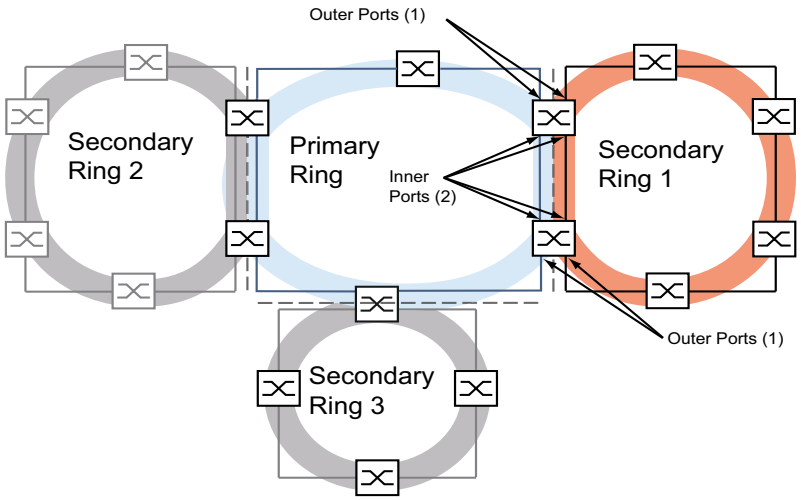


Figure 66 : Anneau principal avec 3 anneaux secondaires connectés à l'aide de RCP

Configuration de l'anneau principal

Les chapitres suivants décrivent le principe de la configuration et ne comprennent ainsi pas les étapes à effectuer.

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Lorsque vous procédez à une configuration, prenez des mesures pour prévenir la génération de boucles.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Pour spécifier le root bridge et le backup root bridge dans l'anneau principal, configurez leurs RSTP bridge priorities globales. Lorsque le root bridge et le backup root bridge sont à l'opposé l'un de l'autre dans l'anneau principal, vous obtenez un délai de reconfiguration optimal dans l'anneau principal. C'est la cas lorsque le backup root bridge a 2 chemins vers le root bridge dont le nombre d'équipements vers le root bridge diverge d'un maximum de 1.

Configurez les autres commutateurs réseau dans l'anneau principal situés entre le root bridge et le backup root bridge de manière à ce que les bridge priorities diminuent (c'est-à-dire augmentent numériquement) à mesure que leur distance par rapport au root bridge augmente.

La figure présente un exemple avec les détails RSTP de l'anneau principal. La topologie est réduite à l'anneau principal et à un anneau secondaire. Durant la configuration, la station d'administration réseau est connectée à l'anneau principal afin d'éviter les interruptions de communication avec les commutateurs réseau dans l'anneau secondaire.

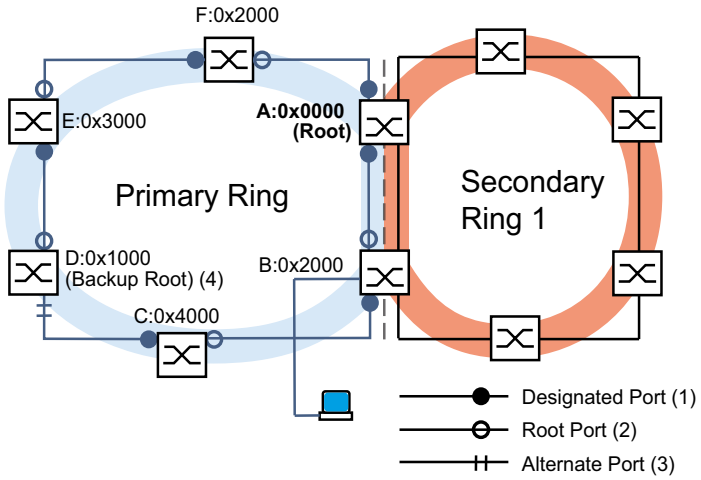


Figure 67 : Anneau principal avec un anneau secondaire connecté, avec détails pour l'anneau principal
A..F : identifiants de commutateurs réseau
0x0000..0x4000 : priorités en matière de commutateurs réseau dans l'anneau principal

Configuration de l'anneau secondaire

Pour spécifier le root bridge et le backup root bridge dans l'anneau secondaire, configurez la *Dual RSTP* bridge priority pour les commutateurs réseau *RCP*. Pour les autres commutateurs réseau dans l'anneau secondaire, configurez uniquement leur RSTP bridge priority globale. Lorsque le root bridge et le backup root bridge sont à l'opposé l'un de l'autre dans l'anneau secondaire, vous obtenez un délai de reconfiguration optimal dans l'anneau secondaire.

Configurez également les autres commutateurs réseau dans l'anneau secondaire de manière à ce que les bridge priorities diminuent (c'est-à-dire augmentent numériquement) à mesure que leur distance par rapport au root bridge augmente.

La figure présente un exemple avec les détails RSTP de l'anneau secondaire.

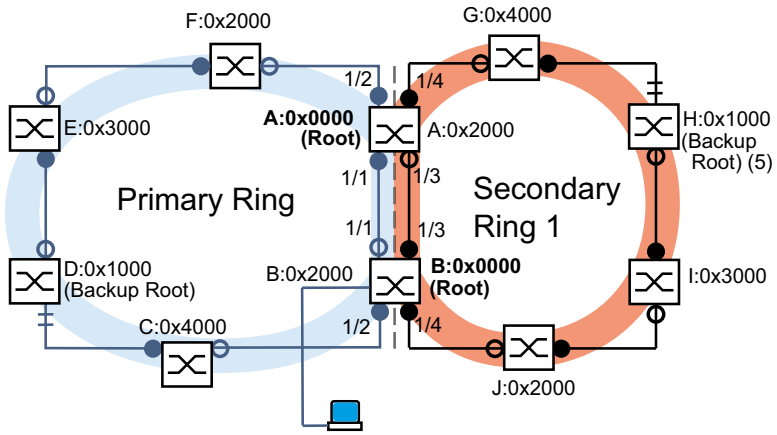


Figure 68 : Anneau principal avec un anneau secondaire connecté, avec détails pour l'anneau secondaire
A, B, G à J : identifiants de commutateurs réseau dans l'anneau secondaire
0x0000..0x4000 : bridge priorities
pour les commutateurs réseau A et B : Dual RSTP bridge priority
pour les commutateurs réseau G à J : RSTP bridge priority globale
5 : backup root bridge pour l'anneau secondaire

Les rôles root bridge dans l'anneau principal et dans l'anneau secondaire sont indépendants les uns des autres. Un commutateur réseau peut être la racine RSTP pour :
- Les deux anneaux
- Un anneau
- Aucun anneau

Utilisation de l'anneau secondaire uniquement avec RSTP.

Configuration du couplage des anneaux

Pour les commutateurs réseau *RCP*, définissez les ports intérieurs et extérieurs pour les anneaux principal et secondaire.

Tableau 44 : Ports d'anneau pour les commutateurs réseau RCP

Ports	RCP master (B)	RCP slave (A)
Anneau principal		
Port intérieur	1/1	1/1
Port extérieur	1/2	1/2
Anneau secondaire		
Port intérieur	1/3	1/3
Port extérieur	1/4	1/4

Ensuite, configurez le role pour chaque commutateur réseau *RCP*.

La figure présente un exemple.

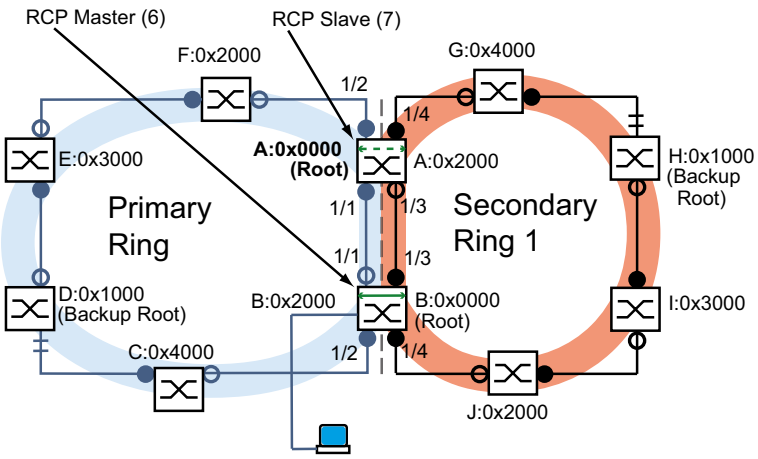


Figure 69 : Anneau principal avec un anneau secondaire connecté, avec numéros de ports et rôles RCP
6 : RCP master
7 : RCP slave

Les rôles root bridge et les rôles de couplage sont indépendants les uns des autres. Un commutateur réseau peut être *RCP* master et fonctionner en même temps que la racine RSTP pour :
- Les deux anneaux
- Un anneau
- Aucun anneau

Cela vaut aussi pour le *RCP* slave.

Ensuite, activez la fonction *RCP*.

13.13.3 Exemple d'application pour le couplage RCP avec Dual RSTP

Un hall de production contient plusieurs cellules de production. Les équipements dans une cellule de production sont connectés à une structure de réseau en ligne. Le réseau est connecté au réseau de niveau supérieur dans le hall de production. Le réseau du hall de production est interconnecté de manière redondante et fonctionne avec RSTP. Chaque équipement est du type MCSESM-E.

Vos exigences :
- Définir le réseau en ligne existant dans les cellules de production avec une redondance rapide des équipements.
- Connecter les cellules de production de manière redondante au réseau du hall de production.
- Reconfigurer le réseau du hall de production de manière à obtenir des délais de reconfiguration courts et déterministes.

Topologie de réseau existante, réduite à une cellule de production :

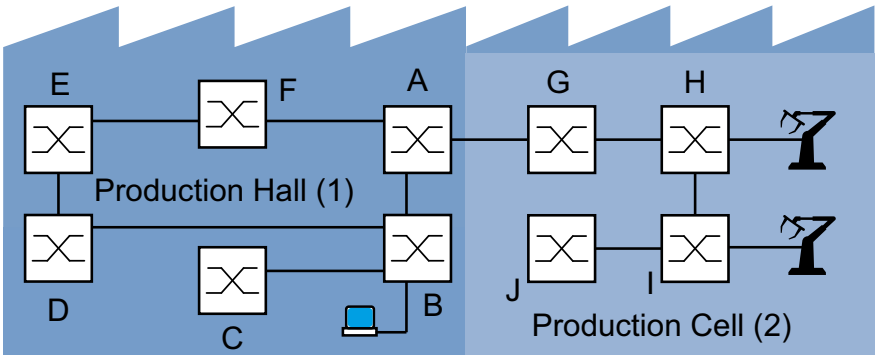


Figure 70 : Exemple de cellule de production dans un hall de production, topologie avant utilisation des fonctions RCP et Dual RSTP
1 : hall de production
2 : cellule de production

Topologie de réseau *Dual RSTP* souhaitée :

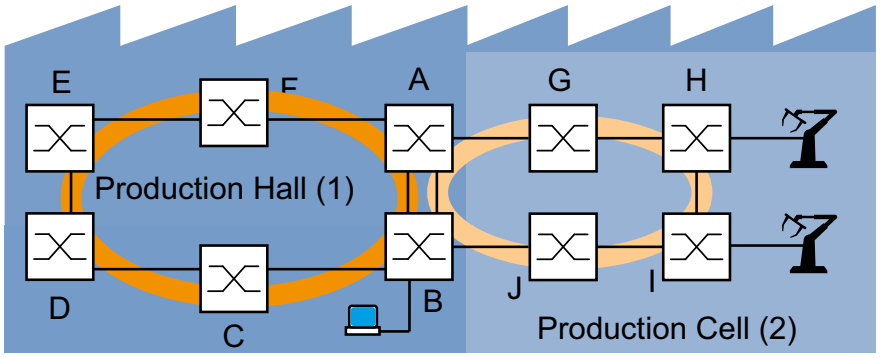


Figure 71 : Exemple de cellule de production dans un hall de production, topologie en cas d'utilisation des fonctions RCP et Dual RSTP
1 : hall de production
2 : cellule de production

Représentation schématique de la topologie de réseau *Dual RSTP* souhaitée :

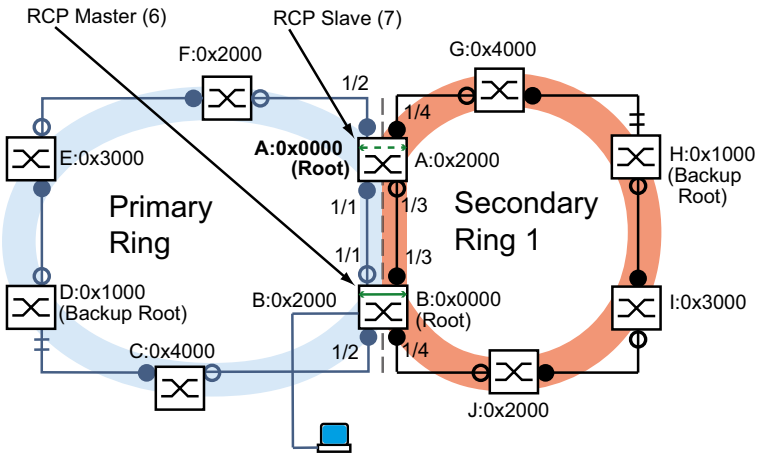


Figure 72 : Représentation schématique de la topologie de réseau Dual RSTP
6 : RCP master
7 : RCP slave

Le tableau suivant montre qu'un nombre réduit de paramètres est suffisant pour configurer la nouvelle topologie. Vous saisissez uniquement les paramètres *Dual RSTP* sur les équipements A et B.

Tableau 45 : Valeurs pour la configuration des commutateurs réseau de l'exemple Dual RSTP

Paramètre	A	B	C	D	E	F	G	H	I	J
Réglages RSTP										
Bridge priority (hex.)[1]	0x0000	0x2000	0x4000	0x1000	0x3000	0x2000	0x4000	0x1000	0x3000	0x2000
Réglages Dual RSTP										
Bridge priority (hex.)[a]	0x2000	0x0000	-	-	-	-	-	-	-	-
Réglages RCP										
Anneau principal, port intérieur	1/1	1/1	-	-	-	-	-	-	-	-
Anneau principal, port extérieur	1/2	1/2	-	-	-	-	-	-	-	-
Anneau secondaire, port intérieur	1/3	1/3	-	-	-	-	-	-	-	-
Anneau secondaire, port extérieur	1/4	1/4	-	-	-	-	-	-	-	-
Rôle de couplage	Slave	Master	-	-	-	-	-	-	-	-

1. Pour les priorités en matière de commutateurs réseau en notation hexadécimale et décimale, voir tableau 46.

Tableau 46 : Priorités possibles en matière de commutateurs réseau en notation hexadécimale et décimale

Bridge priority								
Hexadécimal	0x0000	0x1000	0x2000	0x3000	0x4000	0x5000	0x6000	0x7000
Décimal	0	4096	8192	12288	16384	20480	24576	28672

Hexadécimal	0x8000	0x9000	0xA000	0xB000	0xC000	0xD000	0xE000	0xF000
Décimal	32768	36864	40960	45056	49152	53248	57344	61440

Conditions nécessaires à la poursuite de la configuration :

- La liaison pour l'interconnexion existante entre les commutateurs réseau B et D est inactive dans l'ancienne topologie de l'anneau secondaire. Pour cela, vous pouvez par exemple désactiver manuellement les ports correspondants sur les commutateurs réseau B et D ou déconnecter la liaison.
- Les liaisons entre les commutateurs réseau C et D et entre les commutateurs réseau J et B sont désactivées. Pour cela, vous pouvez par exemple désactiver manuellement les ports correspondants sur les commutateurs réseau avant de connecter les liaisons.
- Les liaisons pour l'anneau secondaire entre les commutateurs réseau A et B sont désactivées.
- RSTP est activé sur chaque équipement et les paramètres sont dans l'état à la livraison.
- Votre station d'administration réseau est connectée à l'anneau principal.

- Vous avez ouvert l'interface utilisateur graphique ou l'interface de ligne de commande pour les équipements A et B.
- Vous avez accès aux interfaces utilisateur des équipements C à J.

⚠ AVERTISSEMENT

RISQUE DE BOUCLE

- Configurez chaque équipement de la configuration *RCP* et *Dual RSTP* individuellement. Avant de raccorder les lignes redondantes, terminez la configuration des autres équipements de la configuration de l'anneau.
- Configurez une temporisation dans la configuration de couplage *RCP* plus longue que la durée d'interruption la plus longue envisageable pour l'instance la plus rapide du protocole de redondance.
- Dans une topologie avec 2 commutateurs de couplage, configurez les rôles de couplage des deux équipements uniquement en tant que `master`, `slave` ou `auto`.
- Couplez les instances principale et secondaire uniquement au moyen de 1 commutateur *RCP* (pour une topologie à 1 commutateur *RCP*) ou au moyen de 2 commutateurs *RCP* (pour une topologie à 2 commutateurs *RCP*). Maintenez les ports de l'instance principale séparés des ports de chaque instance secondaire.
- Activez le réglage *Admin edge port* sur un port uniquement dans les cas où un équipement terminal est connecté au port.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Configuration des paramètres RSTP globaux des commutateurs réseau RCP

Sur la base des spécifications des tâches dans tableau 45, vous avez besoin des RSTP bridge priorities pour le commutateur réseau A et le commutateur réseau B. Le tableau suivant contient un résumé de ces valeurs.

Tableau 47 : Priorités en matière de commutateurs réseauRSTP pour les commutateurs réseau A et B

Paramètre RSTP	A	B
Bridge priority (hex.)	0x0000	0x2000
Bridge priority (déc.)	0	8192

Commentaire : Les instructions suivantes décrivent la configuration des commutateurs réseau *RCP* (A et B) en détails ; celle des autres commutateurs réseau (C à J) est fournie uniquement sous forme abrégée.

Configurez l'équipement A. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Dans le cadre *Bridge configuration*, sélectionnez la valeur `0` dans la liste déroulante *Priority*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`spanning-tree mst priority 0 0`	Définissez la RSTP bridge priority de l'instance MST `0` sur la valeur `0`. L'instance MST `0` est l'instance MST globale ou l'instance par défaut.

Configurez l'équipement B. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Dans le cadre *Bridge configuration*, sélectionnez la valeur `8192` dans la liste déroulante *Priority*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`spanning-tree mst priority 0 8192`	Définissez la RSTP bridge priority de l'instance MST globale sur la valeur `8192`.

Configuration des paramètres RSTP globaux des autres commutateurs réseau

Configurez maintenant les autres commutateurs réseau. Sur la base des spécifications des tâches, vous avez besoin des RSTP bridge priorities. Le tableau suivant contient un résumé de ces valeurs.

Tableau 48 : Priorités en matière de commutateurs réseau RSTP pour les commutateurs réseau C à J

Paramètre RSTP	C	D	E	F	G	H	I	J
Bridge priority (hex.)	0x4000	0x1000	0x3000	0x2000	0x4000	0x1000	0x3000	0x2000
Bridge priority (déc.)	16384	4096	12288	8192	16384	4096	12288	8192

Exécutez les étapes suivantes :

- ☐ Définissez la RSTP bridge priority de l'équipement C sur `16384 (0x4000)` et activez le réglage.
- ☐ Définissez la RSTP bridge priority de l'équipement D sur `4096 (0x1000)` et activez le réglage.
- ☐ Définissez la RSTP bridge priority de l'équipement E sur `12288 (0x3000)` et activez le réglage.
- ☐ Définissez la RSTP bridge priority de l'équipement F sur `8192 (0x2000)` et activez le réglage.
- ☐ Définissez la RSTP bridge priority de l'équipement G sur `16384 (0x4000)` et activez le réglage.

- ☐ Définissez la RSTP bridge priority de l'équipement H sur `4096 (0x1000)` et activez le réglage.
- ☐ Définissez la RSTP bridge priority de l'équipement I sur `12288 (0x3000)` et activez le réglage.
- ☐ Définissez la RSTP bridge priority de l'équipement J sur `8192 (0x2000)` et activez le réglage.

Configuration des paramètres Dual RSTP des commutateurs réseau RCP

Sur la base des spécifications des tâches, vous avez besoin de paramètres *Dual RSTP* spécifiques pour les commutateurs réseau A et B. Il s'agit des *Dual RSTP* bridge priorities, des ports d'anneau et des rôles de couplage. Les tableaux suivants contiennent un résumé de ces valeurs.

Tableau 49 : Paramètres Dual RSTP pour les commutateurs réseau A et B

Paramètre Dual RSTP	A	B
Dual RSTP bridge priority (hex.)	`0x2000`	`0x0000`
Dual RSTP bridge priority (déc.)	`8192`	`0`

Tableau 50 : Paramètres RCP pour les commutateurs réseau A et B

Paramètre Dual RSTP	A	B
Anneau principal, port intérieur	`1/1`	`1/1`
Anneau principal, port extérieur	`1/2`	`1/2`
Anneau secondaire, port intérieur	`1/3`	`1/3`
Anneau secondaire, port extérieur	`1/4`	`1/4`
Rôle de couplage	`Slave`	`Master`

Configurez l'équipement A. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > FuseNet > RCP*.
- ☐ Dans le cadre *Primary ring/network*, sélectionnez la valeur `1/1` dans la liste déroulante *Inner port*.
- ☐ Dans le cadre *Primary ring/network*, sélectionnez la valeur `1/2` dans la liste déroulante *Outer port*.
- ☐ Dans le cadre *Secondary ring/network*, sélectionnez la valeur `1/3` dans la liste déroulante *Inner port*.
- ☐ Dans le cadre *Secondary ring/network*, sélectionnez la valeur `1/4` dans la liste déroulante *Outer port*.
- ☐ Dans le cadre *Coupler configuration*, sélectionnez la valeur `slave` dans la liste déroulante *Role*.
- ☐ Pour activer la fonction, sélectionnez le bouton radio *On* dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.
- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*.
- ☐ Dans le cadre *Bridge configuration*, sélectionnez la valeur `8192` dans la liste déroulante *Priority*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`spanning-tree drstp mst priority 0 8192`	Définissez la RSTP bridge priority de l'instance *Dual RSTP* sur la valeur `8192`.
`redundant-coupling port primary inner 1/1`	Sélectionnez le port *1/1* en tant que port intérieur pour l'anneau principal *RCP*.
`redundant-coupling port primary outer 1/2`	Sélectionnez le port *1/2* en tant que port extérieur pour l'anneau principal *RCP*.
`redundant-coupling port secondary inner 1/3`	Sélectionnez le port *1/3* en tant que port intérieur pour l'anneau secondaire *RCP*.
`redundant-coupling port secondary outer 1/4`	Sélectionnez le port *1/4* en tant que port extérieur pour l'anneau secondaire *RCP*.
`redundant-coupling role slave`	Configurez cet équipement en tant que *RCP* slave.
`exit`	Basculez sur le mode Privileged EXEC.

Configurez l'équipement B. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > FuseNet > RCP*.
- ☐ Dans le cadre *Primary ring/network*, sélectionnez la valeur `1/1` dans la liste déroulante *Inner port*.
- ☐ Dans le cadre *Primary ring/network*, sélectionnez la valeur `1/2` dans la liste déroulante *Outer port*.
- ☐ Dans le cadre *Secondary ring/network*, sélectionnez la valeur `1/3` dans la liste déroulante *Inner port*.
- ☐ Dans le cadre *Secondary ring/network*, sélectionnez la valeur `1/4` dans la liste déroulante *Outer port*.
- ☐ Dans le cadre *Coupler configuration*, sélectionnez la valeur *`master`* dans la liste déroulante *Role*.
- ☐ Pour activer la fonction, sélectionnez le bouton radio *On* dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.
- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*.
- ☐ Dans le cadre *Bridge configuration*, sélectionnez la valeur `0` dans la liste déroulante *Priority*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`spanning-tree drstp mst priority 0 0`	Définissez la RSTP bridge priority de l'instance *Dual RSTP* sur la valeur `0`.
`redundant-coupling port primary inner 1/1`	Sélectionnez le port *1/1* en tant que port intérieur pour l'anneau principal *RCP*.
`redundant-coupling port primary outer 1/2`	Sélectionnez le port *1/2* en tant que port extérieur pour l'anneau principal *RCP*.
`redundant-coupling port secondary inner 1/3`	Sélectionnez le port *1/3* en tant que port intérieur pour l'anneau secondaire *RCP*.
`redundant-coupling port secondary outer 1/4`	Sélectionnez le port *1/4* en tant que port extérieur pour l'anneau secondaire *RCP*.
`redundant-coupling role master`	Configurez cet équipement en tant que *RCP* master.
`exit`	Basculez sur le mode Privileged EXEC.

Contrôle de la configuration

Activez les nouvelles connexions redondantes :
- Liaison des ports intérieurs pour l'anneau secondaire entre l'équipement A, port *1/3* et l'équipement B, port *1/3*.
- Bouclage de l'anneau secondaire entre les équipements G et H.
- Bouclage de l'anneau principal entre les équipements C et D.

Comparez les rôles de commutateur réseau actuels dans l'anneau principal avec les rôles de commutateur réseau requis :

Le commutateur réseau A devrait être le root bridge.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*.
- ☐ Dans le cadre *Topology information*, vérifiez la case à cocher *Bridge is root*.

```
show spanning-tree global

Spanning Tree Information:
--------------------------
Spanning Tree Mode.....................RSTP
Spanning Tree Trap Mode.................enabled
Bridge is root.........................true
...
```

Comparez les 4 ports que vous avez configurés en tant que ports intérieurs et extérieurs dans les anneaux principal et secondaire avec les spécifications dans tableau 45.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > FuseNet > RCP*.
- ☐ Dans les cadres *Primary ring/network* et *Secondary ring/network*, vérifiez les ports affichés.

```
show redundant-coupling global

Redundant coupling protocol global settings
-------------------------------------------
RCP global state.......................enabled
RCP device configured role.............slave
RCP inner primary interface............1/1
RCP outer primary interface............1/2
RCP inner secondary interface..........1/3
RCP outer secondary interface..........1/4
RCP timeout............................45 milliseconds
```

Comparez les rôles de commutateur réseau actuels dans l'anneau secondaire avec les rôles de commutateur réseau requis. Le commutateur réseau B sera le root bridge.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*.
- ☐ Dans le cadre *Topology information*, vérifiez la case à cocher *Bridge is root*.

```
show spanning-tree drstp
Dual Spanning Tree Information:
-------------------------------
Spanning Tree Mode.....................RSTP
Spanning Tree Trap Mode.....................enabled
Bridge is root.............................true
...
```

Comparez les rôles de port actuels pour les commutateurs réseau dans l'anneau principal avec les rôles de port requis :

- Pour les ports du commutateur réseau D menant au commutateur réseau C :
  Rôle `alternate`
- Pour les autres ports des commutateurs réseau menant vers le root bridge A :
  Rôle `root`
- Pour les autres ports des commutateurs réseau menant vers le backup root bridge D :
  Rôle `designated`

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*.
- ☐ Dans la colonne *Port role*, vérifiez la valeur `alternate`, `root` or `designated` comme mentionné ci-dessus.

```
show spanning-tree mst port 0 1/<port>
```

Comparez les rôles de port actuels pour les commutateurs réseau dans l'anneau secondaire avec les rôles de port requis :

- Pour les ports du commutateur réseau H menant au commutateur réseau G :
  Rôle `alternate`
- Pour les autres ports des commutateurs réseau menant vers le root bridge B :
  Rôle `root`
- Pour les autres ports des commutateurs réseau menant vers le backup root bridge H :
  Rôle `designated`

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*.
- ☐ Dans la colonne *Port role*, vérifiez la valeur `alternate`, `root` or `designated` comme mentionné ci-dessus.

```
show spanning-tree mst port 0 1/<port>
```

Si la fonction *RCP* ou *Spanning Tree* est désactivée, l'équipement désactive automatiquement la fonction *Dual RSTP*.

Vérifiez l'état de la fonction *Dual RSTP*.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*. Dans le cadre *Operation*, le bouton radio *Off* est sélectionné.

```
show redundant-coupling status

Redundant coupling protocol status
------------------------------------------
RCP global state.........................forwarding
RCP device actual role...................disabled
Redundancy state availability............redNotAvailable
Primary ring protocol....................NONE
Secondary ring protocol..................NONE
```

Fin de la configuration

Pour les équipements A à J, sauvegardez les réglages dans la mémoire non volatile. Suivez les instructions de la section « Sauvegarde d'un profil de configuration » à la page 103.

14 Diagnostic de fonctionnement

L'équipement fournit les outils de diagnostic suivants :
- Envoi de traps SNMP
- Surveillance de l'état de l'équipement
- Signalisation out-of-band à l'aide du contact sec
- Affichage de l'état des ports
- Compteur d'événements au niveau des ports
- Détection de la non-concordance des modes duplex
- Auto-Disable
- Affichage de l'état SFP
- Découverte de la topologie
- Détection des conflits d'adresses IP
- Détection des boucles
- Protection contre les boucles de réseau de couche 2
- Rapports
- Observation du trafic de données sur un port (port mirroring)
- Syslog
- Log des événements
- Gestion des causes et des actions pendant l'auto-test

14.1 Envoi de traps SNMP

L'équipement signale immédiatement des événements inhabituels se produisant pendant le fonctionnement normal de la station d'administration réseau. Pour ce faire, des messages appelés traps SNMP sont utilisés pour contourner la procédure de scrutation (la scrutation consiste à interroger les stations de données à intervalles réguliers). Les traps SNMP vous permettent de réagir rapidement à des événements inhabituels.

Voici des exemples de ce type d'événements :
- Réinitialisation de matériel
- Modifications de la configuration
- Segmentation d'un port

L'équipement envoie des traps SNMP à différents hôtes afin d'accroître la sécurité de transmission des messages. Le message de trap SNMP non acquitté est composé d'un paquet contenant des informations relatives à un événement inhabituel.

L'équipement envoie des traps SNMP aux hôtes saisis dans le tableau de destinations de trap. L'équipement vous permet de configurer le tableau de destinations de trap avec la station d'administration réseau à l'aide du protocole SNMP.

14.1.1 Liste des traps SNMP

Le tableau suivant affiche les traps SNMP pouvant être envoyés par l'équipement.

Tableau 51 : Traps SNMP possibles

Nom du trap SNMP	Signification
authenticationFailure	Lorsqu'une station tente d'accéder à un agent sans autorisation, ce trap est envoyé.
coldStart	Envoyé après un redémarrage.
sa2DevMonSenseExtNvmRemoval	Lorsque la mémoire externe a été retirée, le trap est envoyé.
linkDown	Lorsque la connexion à un port est interrompue, ce trap est envoyé.
linkUp	Lorsque la connexion est établie avec un port, ce trap est envoyé.
sa2DevMonSensePSState	Lorsque l'état d'un bloc d'alimentation change, ce trap est envoyé.
sa2SigConStateChange	Lorsque l'état d'un contact sec change lors de la surveillance du fonctionnement, ce trap est envoyé.
newRoot	Lorsque l'agent émetteur devient la nouvelle racine du Spanning Tree, ce trap est envoyé.
topologyChange	Lorsque l'état du port passe de blocking à forwarding ou de forwarding à blocking, ce trap est envoyé.
alarmRisingThreshold	Lorsque que l'entrée RMON dépasse sa valeur limite supérieure, ce trap est envoyé.
alarmFallingThreshold	Lorsque que l'entrée RMON passe en dessous de sa valeur limite inférieure, ce trap est envoyé.
sa2AgentPortSecurityViolation	Lorsqu'une adresse MAC détectée sur ce port ne correspond pas aux réglages actuels du paramètre sa2AgentPortSecurityEntry, ce trap est envoyé.
sa2DiagSelftestActionTrap	Lorsqu'un auto-test relatif aux quatre catégories « task », « resource », « software », et « hardware » est effectué conformément aux réglages configurés, ce trap est envoyé.
sa2MrpReconfig	Lorsque la configuration de l'anneau MRP change, ce trap est envoyé.
sa2DiagIfaceUtilizationTrap	Lorsque la valeur de l'interface passe au-dessus ou en dessous de la valeur limite supérieure ou inférieure spécifiée, ce trap est envoyé.
sa2LogAuditStartNextSector	Lorsque la piste de vérification a terminé la vérification d'un secteur et commence la vérification d'un autre secteur, ce trap est envoyé.
sa2PtpSynchronizationChance	Lorsque l'état de la synchronisation PTP a été modifié, ce trap est envoyé.
sa2ConfigurationSavedTrap	Lorsque l'équipement a sauvegardé localement sa configuration avec succès, ce trap est envoyé.
sa2ConfigurationChangedTrap	Lorsque vous modifiez la configuration de l'équipement pour la première fois après une sauvegarde locale, ce trap est envoyé.
sa2PlatformStpInstanceLoopInconsistentStartTrap	Lorsque le port de cette instance STP passe à l'état « loop inconsistent », ce trap est envoyé.
sa2PlatformStpInstanceLoopInconsistentEndTrap	Lorsque le port de cette instance STP quitte l'état « loop inconsistent » en recevant un paquet BPDU, ce trap est envoyé.

14.1.2 Traps SNMP relatifs à l'activité de configuration

Une fois que vous sauvegardez une configuration dans la mémoire, l'équipement envoie un `sa2ConfigurationSavedTrap`. Ce trap SNMP contient à la fois les variables d'état correspondant à la mémoire non volatile (*NVM*) et à la mémoire externe (*ENVM*) indiquant si la configuration en cours d'exécution est synchronisée avec la mémoire non volatile ou avec la mémoire externe. Vous pouvez également déclencher ce trap SNMP en copiant un fichier de configuration sur l'équipement afin de remplacer la configuration active sauvegardée.

En outre, l'équipement envoie un `sa2ConfigurationChangedTrap` à chaque fois que vous modifiez la configuration locale afin d'indiquer une non-concordance entre la configuration en cours d'exécution et la configuration sauvegardée.

14.1.3 Réglage des traps SNMP

L'équipement vous permet d'envoyer un trap SNMP en réaction à des événements spécifiques. Créez au moins une destination de trap recevant les traps SNMP.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)*.
- ☐ Cliquez sur le bouton .
  La boîte de dialogue affiche la fenêtre *Create*.
- ☐ Dans le cadre *Name*, spécifiez le nom utilisé par l'équipement pour s'identifier en tant que source du trap SNMP.
- ☐ Dans le cadre *Address*, spécifiez l'adresse IP de la destination de trap à laquelle l'équipement envoie les traps SNMP.
- ☐ Dans la colonne *Active*, sélectionnez les entrées que l'équipement prend en compte lorsqu'il envoie des traps SNMP.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

Par exemple, dans les boîtes de dialogue suivantes, spécifiez quand l'équipement doit déclencher un trap SNMP :

- Boîte de dialogue *Basic Settings > Port*
- Boîte de dialogue *Basic Settings > Power over Ethernet > Global*
- Boîte de dialogue *Network Security > Port Security*
- Boîte de dialogue *Switching > L2-Redundancy > Link Aggregation*
- Boîte de dialogue *Diagnostics > Status Configuration > Device Status*
- Boîte de dialogue *Diagnostics > Status Configuration > Security Status*
- Boîte de dialogue *Diagnostics > Status Configuration > Signal Contact*
- Boîte de dialogue *Diagnostics > Status Configuration > MAC Notification*
- Boîte de dialogue *Diagnostics > System > IP Address Conflict Detection*
- Boîte de dialogue *Diagnostics > System > Selftest*
- Boîte de dialogue *Diagnostics > Ports > Port Monitor*
- Boîte de dialogue *Advanced > Digital IO Module*

14.1.4 Messages ICMP

L'équipement vous permet d'utiliser le protocole ICMP (Internet Control Message Protocol) pour les applications de diagnostic, par exemple ping et traceroute. L'équipement utilise également ICMP pour le time-to-live et le rejet des messages en renvoyant un message ICMP à l'équipement source du paquet.

Utilisez l'outil de diagnostic réseau ping pour tester le chemin d'accès vers un hôte particulier à travers un réseau IP. L'outil de diagnostic traceroute affiche les chemins d'accès et les délais de transit des paquets à travers un réseau.

14.2 Surveillance de l'état de l'équipement

L'état de l'équipement donne un aperçu de l'état général de l'équipement. De nombreux systèmes de visualisation de processus enregistrent l'état d'un équipement afin de représenter son état de fonctionnement sous forme de graphique.

L'équipement affiche son état actuel en indiquant la mention `error` ou `ok` dans le cadre *Device status*. L'équipement détermine cet état à partir des résultats de surveillance individuels.

L'équipement vous permet :
- d'utiliser la signalisation out-of-band à l'aide du contact sec
- de signaler l'état modifié d'un équipement en envoyant un trap SNMP
- de détecter l'état de l'équipement dans la boîte de dialogue *Basic Settings > System* de l'interface utilisateur graphique
- d'interroger l'état de l'équipement dans l'interface de ligne de commande

L'onglet *Global* de la boîte de dialogue *Diagnostics > Status Configuration > Device Status* vous permet de configurer l'équipement afin que celui-ci envoie un trap à la station d'administration réseau pour les événements suivants :
- Tension d'alimentation incorrecte
  - au moins l'une des 2 tensions d'alimentation ne fonctionne pas
  - la tension d'alimentation interne ne fonctionne pas
- Lorsque la température de fonctionnement de l'équipement est située en dehors des valeurs limites de la température définie par l'utilisateur
- Perte de redondance (en mode gestionnaire d'anneau)
- L'interruption des connexions de lien
  Configurez au moins un port pour cette fonction. Lorsque le lien est interrompu, dans la boîte de dialogue *Diagnostics > Status Configuration > Device Status*, spécifiez quels ports sont signalés par l'équipement dans la ligne *Propagate connection error* de l'onglet *Port*.
- La suppression de la mémoire externe.
  La configuration de la mémoire externe est désynchronisée avec la configuration de l'équipement.

Sélectionnez les entrées correspondantes pour décider quels événements sont inclus dans l'état de l'équipement.

Commentaire : En l'absence d'alimentation en tension redondante, le commutateur indique l'absence d'une tension d'alimentation. Pour désactiver ce message, alimentez la tension d'alimentation via les deux entrées ou ignorez la surveillance.

14.2.1 Événements pouvant faire l'objet d'une surveillance

Tableau 52 : Événements Device Status

Nom	Signification
Temperature	Surveille si la température passe au-dessus ou en dessous de la valeur spécifiée.
Ring redundancy	En présence d'une redondance d'anneau, activez cette fonction.
Connection errors	Activez cette fonction pour surveiller chaque événement de lien de port pour lequel la case *Propagate connection error* est cochée.

Tableau 52 : Événements Device Status (cont

Nom	Signification
External memory removal	Activez cette fonction pour surveiller la présence d'un équipement de stockage externe.
External memory not in sync	L'équipement surveille la synchronisation entre la configuration de l'équipement et la configuration sauvegardée dans la mémoire externe (*ENVM*).
Power supply	Activez cette fonction pour surveiller l'alimentation en tension.

14.2.2 Configuration de l'état de l'équipement

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Status Configuration > Device Status*, onglet *Global*.
- ☐ Cochez les cases correspondant aux paramètres à surveiller dans la colonne *Monitor*.
- ☐ Pour envoyer un trap SNMP sur la station d'administration réseau, activez la fonction *Send trap* dans le cadre *Traps*.
- ☐ Dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)*, créez au moins une destination de trap recevant les traps SNMP.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.
- ☐ Ouvrez la boîte de dialogue *Basic Settings > System*.
- ☐ Pour surveiller la température, en bas du cadre *System data*, spécifiez les valeurs limites de température.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`device-status trap`	Lorsque l'état de l'équipement change, envoyer un trap SNMP.
`device-status monitor envm-not-in-sync`	Surveille le profil de configuration de l'équipement et de la mémoire externe. Le champ *Device status* passe à `error` dans les situations suivantes : • Le profil de configuration existe uniquement dans l'équipement. • Le profil de configuration de l'équipement diffère du profil de configuration de la mémoire externe.
`device-status monitor envm-removal`	Surveille la mémoire externe active. Lorsque vous retirez la mémoire externe active de l'équipement, la mention indiquée dans le cadre *Device status* passe à `error`.

`device-status monitor power-supply 1`	Surveille le bloc d'alimentation `1`. Lorsque l'équipement détecte une erreur de l'alimentation en tension, la mention indiquée dans le cadre *Device status* passe à `error`.
`device-status monitor ring-redundancy`	Surveille la redondance d'anneau. Le champ *Device status* passe à `error` dans les situations suivantes : • La fonction de redondance est activée (perte de réserve de redondance). • L'équipement est un membre normal de l'anneau et détecte une erreur dans ses réglages.
`device-status monitor temperature`	Surveille la température de l'équipement. Lorsque la température est supérieure ou inférieure à la limite spécifiée, la mention `error` est indiquée dans le cadre *Device status*.

Pour activer la fonction de surveillance de lien actif sans connexion sur l'équipement, activez d'abord la fonction globale, puis activez les ports individuels.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Status Configuration > Device Status*, onglet *Global*.
- ☐ Cochez la case correspondant au paramètre *Connection errors* dans la colonne *Monitor*.
- ☐ Ouvrez la boîte de dialogue *Diagnostics > Status Configuration > Device Status*, onglet *Port*.
- ☐ Cochez la case correspondant au paramètre *Propagate connection error* dans la colonne des ports à surveiller.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`device-status monitor link-failure`	Surveille le lien des ports/interfaces. Lorsque le lien est interrompu sur un port ou une interface faisant l'objet d'une surveillance, la mention indiquée dans le cadre *Device status* passe à `error`.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`device-status link-alarm`	Surveille le lien du port/de l'interface. Lorsque le lien est interrompu sur un port ou une interface, la mention indiquée dans le cadre *Device status* passe à `error`.

Commentaire : Les commandes ci-dessus activent la surveillance et les traps pour les composants pris en charge. Lorsque vous souhaitez activer ou désactiver la surveillance pour certains composants individuels, vous trouverez la syntaxe appropriée dans le manuel de référence « Interface de ligne de commande » ou dans l'aide de la console de l'interface de ligne de commande. Pour afficher l'aide dans l'interface de ligne de commande, insérez un point d'interrogation `?` et appuyez sur la touche <Entrée>.

14.2.3 Affichage de l'état de l'équipement

Exécutez les étapes suivantes :

☐ Ouvrez la boîte de dialogue *Basic Settings > System*.

`show device-status all`	En mode EXEC Privilege : indique l'état de l'équipement et le réglage de détermination de l'état de l'équipement.

14.3 Security status ‹État de la sécurité›

Cette boîte de dialogue donne un aperçu de l'état de sécurité général de l'équipement. De nombreux processus vous aident à visualiser le système en enregistrant l'état de la sécurité de l'équipement et en le représentant sous forme de graphique. L'équipement affiche l'état général de la sécurité dans le cadre *Security status* de la boîte de dialogue *Basic Settings > System*.

Dans l'onglet *Global* de la boîte de dialogue *Diagnostics > Status Configuration > Security Status*, l'équipement affiche son état actuel à l'aide de la mention `error` ou `ok` dans le cadre *Security status*. L'équipement détermine cet état à partir des résultats de surveillance individuels.

L'équipement vous permet :
- d'utiliser la signalisation out-of-band à l'aide du contact sec
- de signaler l'état modifié de la sécurité en envoyant un trap SNMP
- de détecter l'état de la sécurité dans la boîte de dialogue *Basic Settings > System* de l'interface utilisateur graphique
- d'interroger l'état de la sécurité dans l'interface de ligne de commande

14.3.1 Événements pouvant faire l'objet d'une surveillance

Exécutez les étapes suivantes :
- ☐ Spécifiez les événements surveillés par l'équipement.
- ☐ Cochez la case du paramètre correspondant dans la colonne *Monitor*.

Tableau 53 : Événements Security Status

Nom	Signification
Password default settings unchanged	Après l'installation, modifiez les mots de passe pour augmenter la sécurité. Lorsque la case correspondante est cochée et que les mots de passe par défaut n'ont pas été modifiés, l'équipement affiche une alarme.
Min. password length < 8	Créez des mots de passe d'une longueur de plus de 8 caractères afin de maintenir un niveau de sécurité élevé. Lorsque la case correspondante est cochée, l'équipement surveille le réglage *Min. password length*.
Password policy settings deactivated	L'équipement surveille les réglages situés dans la boîte de dialogue *Device Security > User Management* relatifs aux stratégies de mot de passe.
User account password policy check deactivated	L'équipement surveille les réglages de la case à cocher *Policy check*. Lorsque la case *Policy check* est décochée, l'équipement envoie un trap SNMP.
Telnet server active	L'équipement surveille si vous activez la fonction *Telnet*.
HTTP server active	L'équipement surveille si vous activez la fonction *HTTP*.
SNMP unencrypted	L'équipement surveille si vous activez la fonction *SNMPv1* ou la fonction *SNMPv2*.
Access to system monitor with serial interface possible	L'équipement surveille l'état du moniteur du système.
Saving the configuration profile on the external memory possible	L'équipement surveille la possibilité de sauvegarder les configurations dans la mémoire non volatile externe.
Link interrupted on enabled device ports	L'équipement surveille l'état du lien des ports actifs.

Tableau 53 : Événements Security Status (cont

Nom	Signification
Access with Ethernet Switch Configurator possible	L'équipement surveille si vous activez la fonction d'accès en lecture/écriture à Ethernet Switch Configurator.
Load unencrypted config from external memory	L'équipement surveille les réglages de sécurité relatifs au chargement de la configuration depuis la mémoire non volatile externe.
IEC61850-MMS active	L'équipement surveille le réglage d'activation du protocole IEC 61850-MMS.
Modbus TCP active	L'équipement surveille le réglage d'activation du protocole Modbus TCP/IP.
Self-signed HTTPS certificate present	L'équipement surveille le serveur HTTPS pour les certificats numériques auto-créés.

14.3.2 Configuration de l'état de la sécurité

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Status Configuration > Security Status*, onglet *Global*.
- ☐ Cochez les cases correspondant aux paramètres à surveiller dans la colonne *Monitor*.
- ☐ Pour envoyer un trap SNMP sur la station d'administration réseau, activez la fonction *Send trap* dans le cadre *Traps*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.
- ☐ Dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)*, créez au moins une destination de trap recevant les traps SNMP.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`security-status monitor pwd-change`	Surveille le mot de passe pour les comptes d'utilisateurs `user` et `admin` créés localement. Lorsque le mot de passe pour les comptes `user` ou `admin` correspond au réglage par défaut, la mention indiquée dans le cadre *Security status* passe à *`error`*.
`security-status monitor pwd-min-length`	Surveille la valeur spécifiée dans la stratégie *Min. password length*. Lorsque la valeur de la stratégie *Min. password length* est inférieure à `8`, la mention indiquée dans le cadre *Security status* passe à *`error`*.
`security-status monitor pwd-policy-config`	Surveille les réglages de la stratégie de mot passe. Lorsque la valeur d'au moins l'une des stratégies suivantes est réglée sur `0`, la mention indiquée dans le cadre *Security status* passe à *`error`*. • *Upper-case characters (min.)* • *Lower-case characters (min.)* • *Digits (min.)* • *Special characters (min.)*

`security-status monitor pwd-policy-inactive`	Surveille les réglages de la stratégie de mot passe. Lorsque la valeur d'au moins l'une des stratégies suivantes est réglée sur `0`, la mention indiquée dans le cadre *Security status* passe à `error`.
`security-status monitor telnet-enabled`	Surveille le serveur Telnet. Lorsque vous activez le serveur Telnet, la mention indiquée dans le cadre *Security status* passe à `error`.
`security-status monitor http-enabled`	Surveille le serveur HTTP. Lorsque vous activez le serveur HTTP, la mention indiquée dans le cadre *Security status* passe à `error`.
`security-status monitor snmp-unsecure`	Surveille le serveur SNMP. Lorsqu'au moins l'une des conditions suivantes s'applique, la mention indiquée dans le cadre *Security status* passe à `error`. • La fonction *SNMPv1* est activée. • La fonction *SNMPv2* est activée. • Le chiffrement pour SNMPv3 est désactivé. Activez le chiffrement dans le champ *SNMP encryption type* de la boîte de dialogue *Device Security > User Management*.
`security-status monitor sysmon-enabled`	Pour surveiller l'activation de la fonction System Monitor dans l'équipement.
`security-status monitor extnvm-upd-enabled`	Pour surveiller l'activation de la mise à jour de la mémoire non volatile externe mémoire.
`security-status monitor iec61850-mms-enabled`	Surveille la fonction *IEC61850-MMS*. Lorsque vous activez la fonction *IEC61850-MMS*, la valeur indiquée dans le cadre *Security status* passe à `error`.
`security-status trap`	Lorsque l'état de l'équipement change, il envoie un trap SNMP.

Pour activer la fonction de surveillance de lien actif sans connexion sur l'équipement, activez d'abord la fonction globale, puis activez les ports individuels.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Status Configuration > Security Status*, onglet *Global*.
- ☐ Cochez la case correspondant au paramètre *Link interrupted on enabled device ports* dans la colonne *Monitor*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.
- ☐ Ouvrez la boîte de dialogue *Diagnostics > Status Configuration > Device Status*, onglet *Port*.
- ☐ Cochez la case correspondant au paramètre *Link interrupted on enabled device ports* dans la colonne des ports à surveiller.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.

`security-status monitor no-link-enabled`	Surveille le lien sur les ports actifs. Lorsque le lien est interrompu sur un port activé, la mention indiquée dans le cadre *Security status* passe à `error`.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`security-status monitor no-link`	Surveille le lien sur l'interface/le port `1`.

14.3.3 Affichage de l'état de la sécurité

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > System*.

`show security-status all`	En mode EXEC Privilege, indique l'état de la sécurité et le réglage de détermination de l'état de la sécurité.

14.4 Signalisation out-of-band

L'équipement utilise le contact sec pour contrôler les équipements externes et surveiller les fonctions de l'équipement. La surveillance des fonctions vous permet d'effectuer des diagnostics à distance.

L'équipement signale l'état de fonctionnement à l'aide d'une rupture du contact sec libre de potentiel (contact à relais, circuit fermé) pour le mode sélectionné. L'équipement surveille les fonctions suivantes :

- Tension d'alimentation incorrecte
  - au moins l'une des 2 tensions d'alimentation ne fonctionne pas
  - la tension d'alimentation interne ne fonctionne pas
- Lorsque la température de fonctionnement de l'équipement est située en dehors des valeurs limites de la température définie par l'utilisateur
- Événements relatifs à la redondance d'anneau
  Perte de redondance (en mode gestionnaire d'anneau)
  Avec le réglage par défaut, la surveillance de la redondance d'anneau est désactivée. L'équipement est un membre normal de l'anneau et détecte une erreur dans la configuration locale.
- L'interruption des connexions de lien
  Configurez au moins un port pour cette fonction. Dans le cadre *Propagate connection error*, spécifiez quels ports sont signalés par l'équipement pour une interruption de lien. Dans le réglage par défaut, la surveillance de lien est désactivée.
- La suppression de la mémoire externe.
  La configuration de la mémoire externe ne correspond pas à la configuration de l'équipement.

Sélectionnez les entrées correspondantes pour décider quels événements sont inclus dans l'état de l'équipement.

Commentaire : En l'absence d'alimentation en tension redondante, le commutateur indique l'absence d'une tension d'alimentation. Pour désactiver ce message, alimentez la tension d'alimentation via les deux entrées ou ignorez la surveillance.

14.4.1 Contrôle du contact sec

Avec le mode `Manual setting`, vous contrôlez ce contact sec à distance.

Options d'applications :

- Simulation d'une erreur détectée lors d'une surveillance d'erreur SPS
- Commande à distance d'un équipement utilisant SNMP (ex. : mise en marche d'une caméra)

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Status Configuration > Signal Contact*, onglet *Global*.
- ☐ Pour contrôler le contact sec manuellement, dans le cadre *Configuration*, sélectionnez l'élément `Manual setting` dans la liste déroulante *Mode*.
- ☐ Pour ouvrir le contact sec, sélectionnez le bouton radio `open` dans le cadre *Configuration*.
- ☐ Pour fermer le contact sec, sélectionnez le bouton radio `close` dans le cadre *Configuration*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`signal-contact 1 mode manual`	Sélectionner le mode de réglage manuel pour le contact sec `1`.
`signal-contact 1 state open`	Ouvrir le contact sec `1`.
`signal-contact 1 state closed`	Fermer le contact sec `1`.

14.4.2 Surveillance de l'état de l'équipement et de la sécurité

Dans le champ *Configuration*, spécifiez quels événements sont indiqués par le contact sec.

- *Device status*
  Lorsque ce réglage est utilisé, le contact sec indique l'état des paramètres surveillés dans la boîte de dialogue *Diagnostics > Status Configuration > Device Status*.
- *Security status*
  Lorsque ce réglage est utilisé, le contact sec indique l'état des paramètres surveillés dans la boîte de dialogue *Diagnostics > Status Configuration > Security Status*.
- *Device/Security status*
  Lorsque ce réglage est utilisé, le contact sec indique l'état des paramètres surveillés dans les boîtes de dialogue *Diagnostics > Status Configuration > Device Status* et *Diagnostics > Status Configuration > Security Status*.

Configuration de la surveillance du fonctionnement

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Status Configuration > Signal Contact*, onglet *Global*.
- ☐ Pour surveiller les fonctions de l'équipement à l'aide du contact sec, dans le cadre *Configuration*, spécifiez la valeur *Monitoring correct operation* dans le champ *Mode*.
- ☐ Cochez les cases correspondant aux paramètres à surveiller dans la colonne *Monitor*.
- ☐ Pour envoyer un trap SNMP sur la station d'administration réseau, activez la fonction *Send trap* dans le cadre *Traps*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.
- ☐ Dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)*, créez au moins une destination de trap recevant les traps SNMP.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.
- ☐ Vous pouvez spécifier les valeurs limite de surveillance de la température dans la boîte de dialogue *Basic Settings > System*.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`signal-contact 1 monitor temperature`	Surveille la température de l'équipement. Lorsque la température est inférieure ou supérieure aux valeurs limites, le contact sec s'ouvre.

`signal-contact 1 monitor ring-redundancy`	Surveille la redondance d'anneau. Le contact sec s'ouvre dans les situations suivantes : • La fonction de redondance est activée (perte de réserve de redondance). • L'équipement est un membre normal de l'anneau et détecte une erreur dans ses réglages.
`signal-contact 1 monitor link-failure`	Surveille le lien des ports/interfaces. Lorsque le lien est interrompu sur un port ou une interface faisant l'objet d'une surveillance, le contact sec s'ouvre.
`signal-contact 1 monitor envm-removal`	Surveille la mémoire externe active. Lorsque vous retirez la mémoire externe active de l'équipement, le contact sec s'ouvre.
`signal-contact 1 monitor envm-not-in-sync`	Surveille le profil de configuration de l'équipement et de la mémoire externe. Le contact sec s'ouvre dans les situations suivantes : • Le profil de configuration existe uniquement dans l'équipement. • Le profil de configuration de l'équipement diffère du profil de configuration de la mémoire externe.
`signal-contact 1 monitor power-supply 1`	Surveille le bloc d'alimentation `1`. Lorsque l'équipement détecte une erreur de l'alimentation en tension, le contact sec s'ouvre.
`signal-contact 1 monitor module-removal 1`	Surveille le module `1`. Lorsque vous retirez le module `1` de l'équipement, le contact sec s'ouvre.
`signal-contact 1 trap`	Active l'envoi d'un trap SNMP par l'équipement en cas de modification de l'état de la surveillance du fonctionnement.
`no signal-contact 1 trap`	Désactivation du trap SNMP

Pour activer la fonction de surveillance de lien actif sans connexion sur l'équipement, activez d'abord la fonction globale, puis activez les ports individuels.

Exécutez les étapes suivantes :

- ☐ Dans la colonne *Monitor*, activez la fonction *Link interrupted on enabled device ports*.
- ☐ Ouvrez la boîte de dialogue *Diagnostics > Status Configuration > Device Status*, onglet *Port*.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.

`signal-contact 1 monitor link-failure`	Surveille le lien des ports/interfaces. Lorsque le lien est interrompu sur un port ou une interface faisant l'objet d'une surveillance, le contact sec s'ouvre.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`signal-contact 1 link-alarm`	Surveille le lien du port/de l'interface. Lorsque le lien est interrompu sur un port ou une interface, le contact sec s'ouvre.

Événements pouvant faire l'objet d'une surveillance

Tableau 54 : Événements Device Status

Nom	Signification
Temperature	Lorsque la température passe au-dessus ou en dessous de la valeur spécifiée.
Ring redundancy	En présence d'une redondance d'anneau, activez cette fonction pour procéder à la surveillance.
Connection errors	Activez cette fonction pour surveiller chaque événement de lien de port pour lequel la case *Propagate connection error* est cochée.
External memory not in sync with NVM	L'équipement surveille la synchronisation entre la configuration de l'équipement et la configuration sauvegardée dans la mémoire externe (*ENVM*).
External memory removed	Activez cette fonction pour surveiller la présence d'un équipement de stockage externe.
Power supply	Activez cette fonction pour surveiller l'alimentation en tension.

Affichage de l'état du contact sec

L'équipement vous fournit des options supplémentaires pour afficher l'état du contact sec :
- Affichage dans l'interface utilisateur graphique
- Interrogation dans l'interface de ligne de commande

Exécutez les étapes suivantes :

☐ Ouvrez la boîte de dialogue *Basic Settings > System*.
Le cadre *Signal contact status* affiche l'état du contact sec et vous informe des alarmes survenues. Lorsqu'une alarme est en cours, le cadre est mis en surbrillance.

`show signal-contact 1 all`	Affiche les réglages de contact sec pour le contact sec spécifié.

14.5 Affichage de l'état des ports

Pour visualiser l'état des ports, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > System*.

La boîte de dialogue affiche l'équipement avec la configuration actuelle. En outre, la boîte de dialogue indique l'état des ports individuels à l'aide d'une icône.

Les icônes suivantes représentent l'état des ports individuels. Dans certaines situations, ces icônes interfèrent l'une avec l'autre. Lorsque vous positionnez le pointeur de souris au-dessus de l'icône du port, une infobulle affiche une description détaillée de l'état du port.

Tableau 55 : Icônes identifiant l'état des ports

Critères	Icône
Bande passante du port	10 Mbit/s Port activé, connexion ok, mode full duplex 100 Mbit/s Port activé, connexion ok, mode full duplex 1000 Mbit/s Port activé, connexion ok, mode full duplex
Mode opérationnel	Mode half duplex activé Voir la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*, case à cocher *Automatic configuration*, champ *Manual configuration* et *Manual cable crossing (Auto. conf. off)*. Auto-négociation activée Voir la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*, case à cocher *Automatic configuration*. Le port est bloqué par une fonction de redondance.
AdminLink	Le port est désactivé, connexion ok Le port est désactivé, pas de connexion établie Voir la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*, case à cocher *Port on* et champ *Link/Current settings*.

14.6 Compteur d'événements de port

Le tableau des statistiques des ports permet aux administrateurs du réseau d'identifier de potentiels problèmes détectés sur le réseau.

Ce tableau affiche les contenus des différents compteurs d'événements. Les compteurs de paquets totalisent les événements envoyés et reçus. Dans la boîte de dialogue *Basic Settings > Restart*, vous pouvez réinitialiser les compteurs d'événements.

Tableau 56 : Exemples d'indices de points faibles

Compteur	Indice d'éventuel point faible
Fragments reçus	• Contrôleur défectueux de l'équipement connecté • Interférences électromagnétiques dans le support de transmission
Erreur CRC	• Contrôleur défectueux de l'équipement connecté • Interférences électromagnétiques dans le support de transmission • Composant inutilisable dans le réseau
Collisions	• Contrôleur défectueux de l'équipement connecté • Trop grande étendue du réseau/longueur excessive du câblage • Collision ou erreur détectée avec un paquet de données

Exécutez les étapes suivantes :

- ☐ Pour afficher le compteur d'événements, ouvrez la boîte de dialogue *Basic Settings > Port*, onglet *Statistics*.
- ☐ Pour réinitialiser les compteurs, dans la boîte de dialogue *Basic Settings > Restart*, cliquez sur le bouton *Clear port statistics*.

14.6.1 Détection de la non-concordance des modes duplex

Des problèmes surviennent lorsque 2 ports directement interconnectés présentent des modes non concordants. Ces problèmes sont difficiles à détecter. La détection et la signalisation automatiques ont pour avantage de permettre l'identification des modes duplex non concordants avant même que des problèmes ne surviennent.

Cette situation apparaît en raison d'une mauvaise configuration, par exemple en cas de désactivation de la configuration automatique sur le port à distance.

Un effet typique de la non-concordance se manifeste par l'enregistrement d'un grand nombre d'erreurs CRC détectées par l'équipement et la chute de la connexion à un niveau significativement plus bas que sa capacité normale lorsque le trafic bidirectionnel est élevé, alors que la connexion semble fonctionner avec un débit de données plus faible.

L'équipement vous permet de détecter cette situation et la signale à la station d'administration réseau. L'équipement analyse en outre les compteurs d'erreurs détectées du port en fonction des réglages du port.

Causes possibles des événements d'erreur de port

Le tableau suivant indique les modes opérationnels duplex pour les ports TX avec les événements d'erreur possibles. Les significations des termes utilisés dans le tableau sont les suivantes :

- Collisions
  Les collisions indiquent un fonctionnement normal en mode half duplex.
- Problème de duplex
  Modes duplex non concordants.
- IEM
  Interférences électromagnétiques.
- Extension du réseau
  L'extension du réseau est trop grande, ou le nombre de concentrateurs en cascade est trop élevé.
- Collisions, Late Collisions
  En mode full duplex, pas d'incrémentation du compteur de port pour les collisions ou les Late Collisions.
- Erreur CRC
  L'équipement analyse ces erreurs détectées comme modes duplex non concordants en mode full duplex manuel.

Tableau 57 : Analyse de non-concordance de mode duplex

N°	Configuration automatique	Mode duplex actuel	Événements d'erreur détectés (≥ 10 après lien « up »)	Modes duplex	Causes possibles
1	coché	Half duplex	Aucun	OK	
2	coché	Half duplex	Collisions	OK	
3	coché	Half duplex	Late Collisions	Problème duplex détecté	Problème duplex, EMI, extension du réseau
4	coché	Half duplex	Erreur CRC	OK	EMI
5	coché	Full duplex	Aucun	OK	
6	coché	Full duplex	Collisions	OK	EMI
7	coché	Full duplex	Late Collisions	OK	EMI
8	coché	Full duplex	Erreur CRC	OK	EMI
9	case non cochée	Half duplex	Aucun	OK	
10	case non cochée	Half duplex	Collisions	OK	
11	case non cochée	Half duplex	Late Collisions	Problème duplex détecté	Problème duplex, EMI, extension du réseau
12	case non cochée	Half duplex	Erreur CRC	OK	EMI
13	case non cochée	Full duplex	Aucun	OK	

Tableau 57 : Analyse de non-concordance de mode duplex (cont

N°	Configuration automatique	Mode duplex actuel	Événements d'erreur détectés (≥ 10 après lien « up »)	Modes duplex	Causes possibles
14	case non cochée	Full duplex	Collisions	OK	EMI
15	case non cochée	Full duplex	Late Collisions	OK	EMI
16	case non cochée	Full duplex	Erreur CRC	Problème duplex détecté	Problème de duplex, EMI

14.7 Auto-Disable

L'équipement peut désactiver un port pour différentes raisons pouvant être configurées. Chaque raison entraîne la désactivation du port. Pour annuler la désactivation du port, vous pouvez effacer manuellement la condition à l'origine de la désactivation du port ou spécifier un temporisateur pour réactiver automatiquement le port.

Lorsque la configuration indique qu'un port est activé, mais que l'équipement détecte une erreur ou une modification de la condition, le logiciel éteint ce port. En d'autres termes, le logiciel de l'équipement désactive le port en raison d'une erreur détectée ou d'une modification de la condition.

Lorsqu'un port est auto-désactivé, l'équipement éteint effectivement le port et le port bloque le trafic. La LED du port clignote en vert trois fois par période et identifie la raison de la désactivation du port. En outre, l'équipement crée une entrée de fichier log qui répertorie les causes de la désactivation. Lorsque vous réactivez le port après écoulement d'un délai d'attente à l'aide de la fonction *Auto-Disable*, l'équipement génère une entrée de log.

La fonction *Auto-Disable* offre une fonction de récupération qui active automatiquement un port auto-désactivé après écoulement d'un délai défini par l'utilisateur. Lorsque cette fonction active un port, l'équipement envoie un trap SNMP avec le numéro de port, mais sans indiquer de valeur pour le paramètre *Reason*.

La fonction *Auto-Disable* permet de remplir les finalités suivantes :
- Elle assiste l'administrateur du réseau lors de l'analyse des ports.
- Elle réduit les risques d'instabilité du réseau due à ce port.

La fonction *Auto-Disable* est disponible pour les fonctions suivantes :
- *Link flap* (fonction *Port Monitor*)
- *CRC/Fragments* (fonction *Port Monitor*)
- Détection de Duplex Mismatch (fonction *Port Monitor*)
- *DHCP Snooping*
- *Dynamic ARP Inspection*
- *Spanning Tree*
- *Port Security*
- *Overload detection* (fonction *Port Monitor*)
- *Link speed/Duplex mode detection* (fonction *Port Monitor*)

L'exemple suivant montre comment configurer l'équipement pour que celui-ci désactive un port en raison de valeurs détectées situées en dehors des valeurs limites spécifiées dans l'onglet *CRC/Fragments* de la boîte de dialogue *Diagnostics > Ports > Port Monitor* avant de réactiver automatiquement le port désactivé.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Ports > Port Monitor*, onglet *CRC/Fragments*.
- ☐ Vérifiez que les valeurs limites spécifiées dans le tableau correspondent à vos préférences pour le port `1/1`.
- ☐ Ouvrez la boîte de dialogue *Diagnostics > Ports > Port Monitor*, onglet *Global*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Pour permettre à l'équipement de désactiver le port pour cause d'erreurs détectées, cochez la case dans la colonne *CRC/Fragments on* pour le port `1/1`.

- Dans la colonne *Action*, vous pouvez choisir comment l'équipement réagit aux erreurs détectées. Dans cet exemple, l'équipement désactive le port `1/1` en raison de violations de valeurs limites, puis réactive automatiquement le port.
  - Pour permettre à l'équipement de désactiver et de réactiver automatiquement le port, sélectionnez la valeur `auto-disable` et configurez la fonction *Auto-Disable*. La valeur `auto-disable` fonctionne conjointement avec la fonction *Auto-Disable*.

  L'équipement peut également désactiver un port sans réactivation automatique.
  - Pour permettre à l'équipement de désactiver le port sans le réactiver, sélectionnez la valeur `disable port`.

    Pour réactiver manuellement un port désactivé, mettez le port en surbrillance.

    Cliquez sur le bouton ☰ puis sur l'élément *Reset*.
  - Lorsque vous configurez la fonction *Auto-Disable*, la valeur `disable port` réactive également le port automatiquement.
- Ouvrez la boîte de dialogue *Diagnostics > Ports > Port Monitor*, onglet *Auto-disable*.
- Pour permettre à l'équipement de réactiver le port une fois qu'il a été désactivé en raison de valeurs détectées situées en dehors des valeurs limites, cochez la case dans la colonne *CRC error*.
- Ouvrez la boîte de dialogue *Diagnostics > Ports > Port Monitor*, onglet *Port*.
- Réglez le temps de retard sur 120 s dans la colonne *Reset timer [s]* pour les ports que vous souhaitez activer.

Commentaire : L'élément *Reset* vous permet d'activer le port avant que le délai spécifié dans la colonne *Reset timer [s]* commence à s'écouler.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`port-monitor condition crc-fragments count 2000`	Réglage du compteur CRC/de fragments sur 2000 parties par million.
`port-monitor condition crc-fragments interval 15`	Définit l'intervalle de mesure sur 15 secondes pour la détection CRC/de fragments.
`auto-disable timer 120`	Indique le temps d'attente de `120` secondes après lequel la fonction *Auto-disable* réactive le port.
`exit`	Basculez sur le mode de configuration.
`auto-disable reason crc-error`	Activer la fonction d'auto-désactivation CRC.
`port-monitor condition crc-fragments mode`	Activer la condition CRC/Fragments pour déclencher une action.
`port-monitor operation`	Activez la fonction *Port Monitor*.

Lorsque l'équipement désactive un port en raison de valeurs détectées situées en dehors des valeurs limites, l'équipement vous permet d'utiliser les commandes suivantes pour réinitialiser manuellement le port désactivé.

Exécutez les étapes suivantes :

`enable`	Basculez sur le mode Privileged EXEC.

```
configure
```

Basculez sur le mode de configuration.

```
interface 1/1
```

Basculez sur le mode de configuration de l'interface `1/1`.

```
auto-disable reset
```

Vous permet d'activer le port avant que le temporisateur commence son compte à rebours.

14.8 Affichage de l'état SFP

L'affichage de l'état SFP vous permet de visualiser les connexions actuelles des transceivers SFP et leurs propriétés. Les propriétés comprennent :

- type de module
- numéro de série du module média
- température en ° C
- puissance de transmission en mW
- puissance de réception en mW

Exécutez l'étape suivante :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Ports > SFP*.

14.9 Découverte de la topologie

IEEE 802.1AB définit le protocole LLDP (Link Layer Discovery Protocol). Le protocole LLDP vous permet de détecter automatiquement la topologie du réseau LAN.

Les équipements avec LLDP activé :
- diffusent leurs propres informations de connexion et d'administration aux équipements voisins du LAN commun. Lorsque la fonction *LLDP* de l'équipement de réception est activée, l'analyse des équipements est effectuée.
- reçoivent des informations de connexion et d'administration provenant d'équipements voisins du LAN commun à condition que la fonction LLDP soit également activée sur ces équipements adjacents.
- créent une base de données d'informations d'administration et des définitions d'objets afin de stocker des informations relatives aux équipements adjacents dont la fonction LLDP est activée.

En tant qu'élément principal, les informations de connexion contiennent un identifiant exact univoque pour l'équipement terminal de la connexion : MAC (Service Access Point). Celui-ci est composé d'un identifiant d'équipement univoque sur l'ensemble du réseau et d'un identifiant de port univoque pour cet équipement.
- Identifiant du châssis (son adresse MAC)
- Identifiant du port (son adresse MAC de port)
- Description du port
- Nom du système
- Description du système
- Fonctionnalités du système prises en charge
- Fonctionnalités du système actuellement activées
- ID d'interface de l'adresse d'administration
- VLAN-ID du port
- État de l'auto-négociation sur le port
- Support, réglage half/full duplex et réglage de vitesse de port
- Informations sur les VLAN installés dans l'équipement (VLAN-ID et noms des VLAN, que le port soit ou non un participant du VLAN).

Une station d'administration réseau peut appeler ces informations relatives à des équipements dont la fonction LLDP est activée. Grâce à ces informations, la station d'administration réseau est en mesure de représenter la topologie du réseau.

Les équipements non-LLDP bloquent généralement l'adresse MAC IEE LLDP Multicast spéciale utilisée pour l'échange d'informations. C'est pourquoi les équipements non-LLDP rejettent les paquets LLDP. Si vous positionnez un équipement non compatible avec LLDP entre 2 équipements compatibles avec LLDP, l'équipement non compatible avec LLDP interdit l'échange d'informations entre les 2 équipements compatibles avec LLDP.

La Management Information Base (MIB) d'un équipement compatible avec LLDP contient les informations LLDP dans la MIB lldp et dans la SA2-LLDP-EXT-HM-MIB privée et la SA2-LLDP-MIB.

14.9.1 Affichage des résultats de la découverte de topologie

Affichez la topologie du réseau. Pour ce faire, exécutez l'étape suivante :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > LLDP > Topology Discovery*, onglet *LLDP*.

Lorsque vous utilisez un port pour connecter plusieurs équipements, par exemple via un concentrateur, le tableau contient une ligne pour chaque équipement connecté.

L'activation de l'affichage des entrées FDB en bas du tableau vous permet d'afficher les équipements sans prise en charge active de LLDP dans le tableau. Dans ce cas, l'équipement inclut également les informations de sa base de données FDB (Forwarding Database).

Si vous connectez le port à des équipements dont la fonction de découverte de la topologie est activée, les équipements échangent les unités de données LLDP (LLDPDU) et le tableau de topologie affiche ces équipements voisins.

Lorsqu'un port connecte uniquement des équipements sans découverte de la topologie activée, le tableau contient une ligne pour ce port afin de représenter les équipements connectés. Cette ligne contient le nombre d'équipements connectés.

Le tableau d'adresses de la FDB contient les adresses MAC des équipements que le tableau de topologie masque à des fins de clarté.

14.9.2 LLDP-Med

LLDP-MED (LLDP for Media Endpoint Devices) est une extension du protocole LLDP intervenant entre les équipements terminaux. Les équipements terminaux incluent des équipements tels que les téléphones IP ou d'autres équipements ou serveurs de Voix sur IP (VoIP), et des équipements de réseau tels que des commutateurs. Cette extension permet spécifiquement la prise en charge des applications VoIP. LLDP-MED offre cette prise en charge à l'aide d'un ensemble supplémentaire de messages communs d'annonces Type Longueur Valeur (TLV) dédiés à la découverte des fonctionnalités, la stratégie de réseau, la fonction Power-over-Ethernet, la gestion de l'inventaire et les informations de localisation.

L'équipement prend en charge les messages suivants :

- TLV de fonctionnalités
  Permet aux équipements terminaux LLDP-MED de déterminer les fonctionnalités prises en charge par l'équipement connecté et celles que l'équipement a activées.
- TLV de stratégie de réseau
  Permet aux équipements de connectivité réseau d'annoncer les configurations de VLAN et les attributs associés pour l'application spécifique sur ce port. Par exemple, l'équipement notifie un téléphone du numéro de VLAN. Le téléphone se connecte à un commutateur, obtient son numéro de VLAN, puis démarre la communication avec le contrôle d'appel.

LLDP-MED offre les fonctions suivantes :

- Découverte de la stratégie de réseau, y compris le VLAN-ID, la priorité 802.1p et le DSCP (Diffserv code point)
- Localisation des équipements et découverte de la topologie basées sur les informations d'adresse MAC/de port au niveau du LAN
- Notification de détection de déplacement des équipements terminaux allant de l'équipement de connectivité réseau à l'application de gestion VoIP associée
- Identification étendue des équipements pour la gestion de l'inventaire
- Identification des fonctionnalités de connectivité réseau des équipements terminaux, par exemple, téléphone IP multi-port avec fonctionnalité intégrée de commutateur ou de pont
- Interactions de niveau application avec les éléments du protocole LLDP permettant le démarrage en temps voulu du protocole LLDP afin de prendre en charge la disponibilité rapide d'un service d'appel d'urgence
- Applicabilité de LLDP-MED aux environnements de LAN sans fil, prise en charge de la VoWLAN (Voice over Wireless Local Area Network)

14.10 Détection des boucles

Les boucles dans le réseau conduisent à des pannes de connexion ou à la perte de données. Cela vaut également pour les boucles temporaires. La détection automatique et la signalisation de cette situation vous permettent de la détecter plus rapidement et de la diagnostiquer plus facilement.

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Pour vous aider à éviter les boucles pendant la phase de configuration, configurez chaque équipement de l'anneau individuellement. Avant de raccorder les lignes redondantes, terminez la configuration des autres équipements de la configuration de l'anneau.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Une configuration incorrecte peut entraîner des boucles, par exemple, la désactivation du protocole Spanning Tree.

L'équipement vous permet de détecter les effets typiques généralement entraînés par les boucles et signale automatiquement cette situation à la station d'administration réseau. Vous avez ici la possibilité de spécifier l'ampleur des effets des boucles qui déclenche l'envoi d'un rapport par l'équipement.

L'envoi de trames BPDU par le port désigné et reçues soit sur un port différent du même équipement soit sur le même port dans un bref laps de temps représente un effet typique d'une boucle.

Pour vérifier si l'équipement a détecté une boucle, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*, onglet *CIST*.
- ☐ Vérifiez la valeur contenue dans les champs *Port state* et *Port role*. Lorsque le port *Port state* affiche la valeur `discarding` et que le champ *Port role* affiche la valeur `backup`, le port présente un état de boucle.
  ou
- ☐ Ouvrez la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*, onglet *Guards*.
- ☐ Vérifiez la valeur contenue dans la colonne *Loop state*. Lorsque le champ contient la valeur `true`, le port présente un état de boucle.

14.11 Protection contre les boucles de réseau de couche 2

L'équipement permet de se protéger contre les boucles de réseau de couche 2.

Une boucle de réseau peut provoquer un arrêt du réseau en raison d'une surcharge. Cela peut être dû à la duplication continue de paquets de données suite à une mauvaise configuration. La cause peut être, par exemple, un câble mal connecté ou un mauvais réglage de l'équipement.

Par exemple, une boucle de réseau de couche 2 peut se produire dans les cas suivants si aucun protocole de redondance n'est activé :
- Deux ports du même équipement sont directement interconnectés.
- Plus d'une connexion active est établie entre deux équipements.

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Pour éviter les boucles durant la phase de configuration, configurez chaque équipement du réseau de couche 2 individuellement. Avant de raccorder les lignes redondantes, terminez la configuration des autres équipements du réseau de couche 2.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

14.11.1 Exemple d'application

La figure présente des exemples de boucles de couche 2 possibles dans un réseau. La fonction *Loop Protection* est activée dans chaque équipement.

▶ **A** : *mode actif*
Les ports destinés à connecter des équipements terminaux fonctionnent en mode *active*. L'équipement évalue et envoie les paquets de *détection de boucle* sur ces ports.

- **P** : *mode passif*
  Les ports appartenant aux anneaux redondants fonctionnent en mode *passive*. L'équipement évalue uniquement les paquets de *détection de boucle* sur ces ports.
- **Boucle 1**..**Boucle 4**
  Boucles de réseau de couche 2 configurées involontairement.

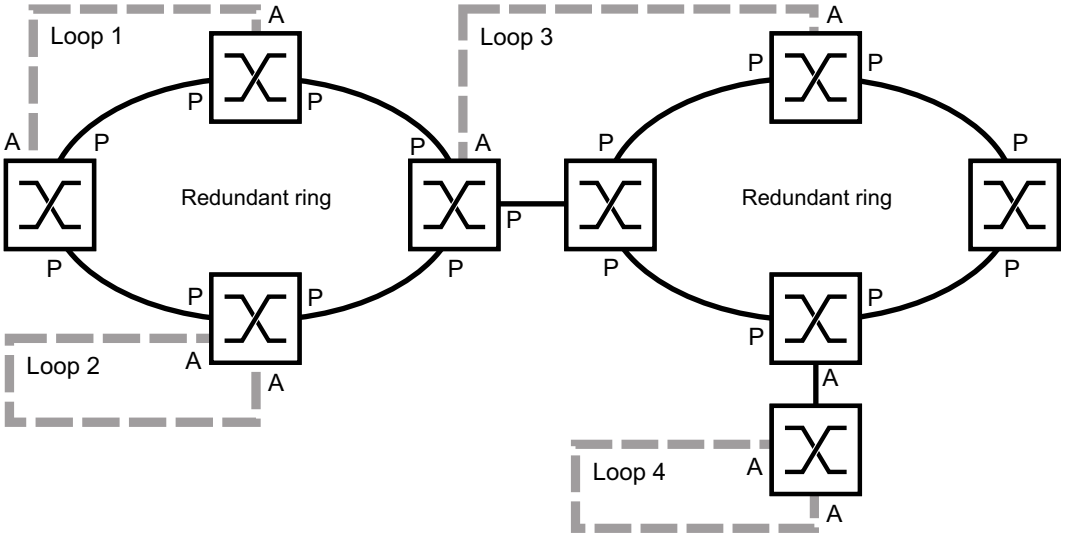


Figure 73 : Exemples de boucles de réseau de couche 2 involontaires

Affectation des réglages Loop Protection aux ports

Pour chaque port *actif* et chaque port *passif*, affectez les réglages de la fonction *Loop Protection*.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Loop Protection*.
- ☐ Dans le cadre *Global*, champ *Transmit interval*, ajustez la valeur, si nécessaire.
- ☐ Dans le cadre *Global*, champ *Receive threshold*, ajustez la valeur, si nécessaire.
- ☐ Dans la colonne *Mode*, spécifiez le comportement de la fonction *Loop Protection* sur le port :
  - `active` pour les ports qui sont destinés à connecter des équipements terminaux
  - `passive` pour les ports appartenant aux anneaux redondants
- ☐ Dans la colonne *Action*, spécifiez la valeur *all*.
  Lorsque l'équipement détecte une boucle de couche 2 sur ce port, il envoie un trap et désactive le port à l'aide de la fonction *Auto-Disable*. Si nécessaire, ajustez la valeur.
- ☐ Dans la colonne *Active*, cochez la case.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`loop-protection tx-interval 5`	Spécifiez l'intervalle de transmission, si nécessaire.
`loop-protection rx-threshold 1`	Spécifiez le seuil de réception, si nécessaire.
`interface 1/1`	Basculez sur le mode interface. Exemple : port *1/1*.

`loop-protection mode active`	Spécifiez le mode `active` pour les ports qui sont destinés à connecter des équipements terminaux.
`loop-protection mode passive`	Spécifiez le mode `passive` pour les ports appartenant aux anneaux redondants.
`loop-protection action all`	Spécifiez l'action que que l'équipement exécute lorsqu'il détecte une boucle de réseau de couche 2 sur ce port.
`loop-protection operation`	Activez la fonction *Loop Protection* sur le port.
`exit`	Basculez sur le mode de configuration.

Activation de la fonction Auto-Disable

Après avoir affecté les réglages *Loop Protection* aux ports, activez la fonction *Auto-Disable*.

Exécutez les étapes suivantes :

- ☐ Dans le cadre *Configuration*, cochez la case *Auto-disable*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`loop-protection auto-disable`	Activez la fonction *Auto-Disable*.

Activation de la fonction Loop Protection dans l'équipement

Une fois terminé, activez la fonction *Loop Protection* dans l'équipement.

Exécutez les étapes suivantes :

- ☐ Dans le cadre *Operation*, sélectionnez le bouton radio *On*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`loop-protection operation`	Activez la fonction *Loop Protection* dans l'équipement.

14.11.2 Recommandations pour les ports redondants

En fonction des réglages *Loop Protection*, l'équipement désactive les ports à l'aide de la fonction *Auto-Disable* lorsqu'il détecte une boucle de réseau de couche 2.

Si une fonction de redondance est active sur un port, n'activez pas le mode *active* sur ce port. Sinon, cela peut provoquer des interruptions de port sur les chemins réseau redondants Dans l'exemple ci-dessus, il s'agit des ports appartenant aux anneaux redondants.

Vérifiez qu'un chemin réseau redondant est disponible comme support de sauvegarde. L'équipement passe sur le chemin redondant en cas d'interruption du chemin primaire.

Les réglages suivants permettent d'éviter les interruptions de port sur les chemins réseau redondants :

- ☐ Désactivez la fonction *Loop Protection* sur les ports redondants.
  ou
- ☐ Activez le mode *passive* sut les ports redondants.

La fonction *Loop Protection* et la fonction *Spanning Tree* s'influencent mutuellement. En exécutant les étapes suivantes, vous pouvez éviter un comportement inattendu de l'équipement :

- ☐ Désactivez la fonction *Spanning Tree* sur le port sur lequel vous voulez activer la fonction *Loop Protection*. Voir la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*, colonne *STP active*.
- ☐ Désactivez la fonction *Spanning Tree* sur le port connecté de chaque équipement connecté. Voir la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree*.

14.12 Utilisation de la fonction Email Notification

L'équipement vous permet d'informer les utilisateurs par e-mail des événements qui se sont produits. La condition préalable est qu'un serveur de messagerie soit disponible sur le réseau sur lequel l'équipement transfère les e-mails.

Pour configurer l'équipement afin qu'il envoie des e-mails, exécutez les étapes décrites dans les chapitres suivants :

- ☐ Spécifier l'adresse de l'expéditeur
- ☐ Spécifier les événements déclencheurs
- ☐ Spécifier les destinataires
- ☐ Spécifier le serveur de messagerie
- ☐ Activer/désactiver la fonction Email Notification
- ☐ Envoyer un e-mail de test

14.12.1 Spécifier l'adresse de l'expéditeur

L'adresse de l'expéditeur est l'adresse e-mail qui indique quel équipement a envoyé l'e-mail. Dans l'équipement, le réglage par défaut est .

Modifiez la valeur prédéfinie. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Email Notification > Global*.
- ☐ Dans le cadre *Sender*, changez la valeur dans le champ *Address*.
  Ajoutez une adresse e-mail valide.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`logging email from-addr <user@doma.in>`	Modifie l'adresse de l'expéditeur.

14.12.2 Spécifier les événements déclencheurs

L'équipement fait la distinction entre les degrés de gravité suivants :

Tableau 58 : Signification des degrés de gravité des événements

Gravité	Signification
`emergency`	Équipement non opérationnel
`alert`	Intervention immédiate de l'utilisateur requise
`critical`	État critique
`error`	État d'erreur
`warning`	Avertissement

Tableau 58 : Signification des degrés de gravité des événements (cont

Gravité	Signification
notice	État normal significatif
informational	Message à titre informatif
debug	Message de débogage

Vous avez la possibilité de spécifier les événements dont l'équipement vous informe. Pour cela, attribuez le degré de gravité minimum souhaité aux niveaux de notification de l'équipement.

L'équipement informe les destinataires comme suit :

- *Notification immediate*
  Lorsqu'un événement de la gravité attribuée ou d'une gravité supérieure se produit, l'équipement envoie immédiatement un e-mail.
- *Notification periodic*
  - Lorsqu'un événement de la gravité attribuée ou d'une gravité supérieure se produit, l'équipement enregistre l'événement dans une mémoire tampon.
  - L'équipement envoie un e-mail contenant le fichier log périodiquement ou si la mémoire tampon est pleine.
  - Lorsqu'un événement d'une gravité moindre se produit, l'équipement ne consigne pas cet événement.

Exécutez les étapes suivantes :

☐ Ouvrez la boîte de dialogue *Diagnostics > Email Notification > Global*.

Dans le cadre *Notification immediate*, vous spécifiez les réglages des e-mails que l'équipement envoie immédiatement.

☐ Dans le champ *Severity*, vous spécifiez le degré de gravité minimum.
☐ Dans le champ *Subject*, vous spécifiez l'objet de l'e-mail.

Dans le cadre *Notification periodic*, vous spécifiez les réglages des e-mails que l'équipement envoie périodiquement.

☐ Dans le champ *Severity*, vous spécifiez le degré de gravité minimum.
☐ Dans le champ *Subject*, vous spécifiez l'objet de l'e-mail.

☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`logging email severity immediate <level>`	Spécifie le degré de gravité minimum des événements pour lesquels l'équipement envoie immédiatement un e-mail.
`logging email severity periodic <level>`	Spécifie le degré de gravité minimum des événements pour lesquels l'équipement envoie périodiquement un e-mail.
`logging email subject add <immediate | periodic> TEXT`	Crée une ligne d'objet avec le contenu `TEXT`.

14.12.3 Modifier l'intervalle d'envoi

L'équipement vous permet de spécifier à quel intervalle il envoie des e-mails contenant le fichier log. Le réglage par défaut est de `30` minutes.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Email Notification > Global*.

Dans le cadre *Notification periodic*, vous spécifiez les réglages des e-mails que l'équipement envoie périodiquement.

- ☐ Changez la valeur dans le champ *Sending interval [min]* pour modifier l'intervalle.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`logging email duration <30..1440>`	Spécifie l'intervalle selon lequel l'équipement envoie des e-mails contenant le fichier log.

14.12.4 Spécifier les destinataires

L'équipement vous permet de spécifier jusqu'à 10 destinataires.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Email Notification > Recipients*.
- ☐ Pour ajouter une entrée de tableau, cliquez sur le bouton .
- ☐ Dans la colonne *Notification type*, spécifiez si l'équipement envoie les e-mails à ce destinataire immédiatement ou périodiquement.
- ☐ Dans la colonne *Address*, spécifiez l'adresse e-mail du destinataire.
- ☐ Dans la colonne *Active*, cochez la case.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`logging email to-addr add <1..10> addr <user@doma.in> msgtype <immediately | periodically>`	Spécifie le destinataire avec l'adresse e-mail `user@doma.in`. L'équipement gère les réglages dans la mémoire `1..10`.

14.12.5 Spécifier le serveur de messagerie

L'équipement prend en charge les connexions chiffrées et non chiffrées au serveur de messagerie.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Email Notification > Mail Server*.
- ☐ Pour ajouter une entrée de tableau, cliquez sur le bouton .
- ☐ Dans la colonne *IP address*, spécifiez l'adresse IP ou le nom DNS du serveur.
- ☐ Dans la colonne *Encryption*, spécifiez le protocole qui chiffre la connexion entre l'équipement et le serveur de messagerie.
- ☐ Lorsque le serveur de messagerie utilise un port autre que le port connu, spécifiez le port TCP dans la colonne *Destination TCP port*.

Lorsque le serveur de messagerie demande une authentification :

- ☐ Dans les colonnes *User name* et *Password*, spécifiez les identifiants du compte que l'équipement utilise pour s'authentifier sur le serveur de messagerie.
- ☐ Dans la colonne *Description*, saisissez un nom évocateur pour le serveur de messagerie.
- ☐ Dans la colonne *Active*, cochez la case.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`logging email mail-server add <1..5> addr <IP ADDRESS> [security <none|tlsv1>] [username <USER NAME>] [password <PASSWORD>] [port <1..65535>]`	Spécifie le serveur de messagerie avec l'adresse IP `IP ADDRESS`. L'équipement gère les réglages dans la mémoire `1..5`.

14.12.6 Activer/désactiver la fonction Email Notification

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Email Notification > Global*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`logging email operation`	Active l'envoi d'e-mails.
`no logging email operation`	Désactive l'envoi d'e-mails.

14.12.7 Envoyer un e-mail de test

L'équipement vous permet de vérifier les réglages en envoyant un e-mail de test.

Prérequis :
- Les réglages d'email sont complètement spécifiés.
- La fonction *Email Notification* est activée.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Email Notification > Mail Server*.
- ☐ Cliquez sur le bouton ☰ puis sur l'élément *Connection test*.
  La boîte de dialogue affiche la fenêtre *Connection test*.
- ☐ Dans la liste déroulante *Recipient*, sélectionnez les destinataires auxquels l'équipement envoie l'e-mail de test.
- ☐ Dans le champ *Message text*, spécifiez le texte de l'e-mail de test.
- ☐ Cliquez sur le bouton *Ok* pour envoyer l'e-mail de test.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`logging email test msgtype <urgent|non-urgent> TEXT`	Envoie un e-mail avec le contenu `TEXT` aux destinataires.

Si aucun message d'erreur détectée ne s'affiche et que les destinataires reçoivent l'e-mail, les réglages de l'équipement sont corrects.

14.13 Rapports

La section suivante répertorie les rapports et boutons disponibles pour les diagnostics :

- Fichier log système
  Le fichier log est un fichier HTML dans lequel l'équipement enregistre des événements internes.
- Piste de vérification
  Consigne les commandes réussies et les commentaires des utilisateurs. Le fichier contient également la consignation des requêtes SNMP.
- Consignation permanente
  Lorsque la mémoire externe est présente, l'équipement sauvegarde les entrées de log dans un fichier stocké dans la mémoire externe. Ces fichiers sont disponibles après la mise hors tension. Il est possible de configurer la taille maximale, le nombre maximum de fichiers pouvant être conservés et le degré de gravité des événements consignés. Après avoir obtenu la taille maximale définie par l'utilisateur ou le nombre maximum de fichiers pouvant être conservés, l'équipement archive les entrées et crée un nouveau fichier. L'équipement supprime le fichier le plus ancien et renomme les autres fichiers de manière à conserver le nombre de fichiers configuré. Pour examiner ces fichiers, utilisez l'interface de ligne de commande ou copiez-les sur un serveur externe pour consultation ultérieure.
- *Download support information*
  Ce bouton vous permet de télécharger les informations système au format d'archive.

En cas de travaux d'entretien, ces rapports fournissent au technicien les informations nécessaires.

14.13.1 Réglages globaux

L'utilisation de cette boîte de dialogue vous permet d'activer ou de désactiver l'emplacement vers lequel l'équipement envoie les rapports, par exemple, vers une console, un serveur Syslog ou une connexion à l'interface de ligne de commande. Vous pouvez également définir le degré de gravité à partir duquel l'équipement signale les événements dans les rapports.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Report > Global*.
- ☐ Pour envoyer un rapport à la console, spécifiez le degré de gravité souhaité dans le champ *Severity* du cadre *Console logging*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Console logging*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

L'équipement met en mémoire tampon les événements consignés dans 2 zones de mémoire séparées de manière à ce que l'équipement conserve les entrées du log dédiées aux événements urgents. Spécifiez le degré de gravité minimum pour les événements que l'équipement consigne dans la zone de mémoire tampon présentant un degré de priorité supérieur.

Exécutez les étapes suivantes :

- ☐ Pour envoyer les événements à la mémoire tampon, spécifiez le degré de gravité souhaité dans le champ *Severity* du cadre *Buffered logging*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

Lorsque vous activez la consignation des requêtes SNMP, l'équipement consigne les requêtes en tant qu'événements dans le serveur Syslog. La fonction *Log SNMP get request* permet de consigner les requêtes d'informations de la configuration de l'équipement. La fonction *Log SNMP set request* permet de consigner les événements de configuration de l'équipement. Spécifiez le degré de gravité minimum pour les événements consignés par l'équipement dans le serveur Syslog.

Exécutez les étapes suivantes :

- ☐ Activez la fonction *Log SNMP get request* pour l'équipement afin d'envoyer les requêtes de lecture SNMP en tant qu'événements au serveur Syslog.
  Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *SNMP logging*.
- ☐ Activez la fonction *Log SNMP set request* pour l'équipement afin d'envoyer les requêtes d'écriture SNMP en tant qu'événements au serveur Syslog.
  Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *SNMP logging*.
- ☐ Choisissez le degré de gravité souhaité pour les requêtes get et set.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

Lorsque la fonction est activée, l'équipement consigne dans la piste de vérification les modifications de la configuration effectuées à l'aide de l'interface de ligne de commande. Cette fonction est basée sur la norme technique IEEE 1686 relative aux dispositifs électroniques intelligents des sous-stations.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Report > Global*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *CLI logging*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

L'équipement vous permet de sauvegarder les informations système suivantes dans un fichier ZIP stocké sur votre PC :

- `audittrail.html`
- `defaultconfig.xml`
- `script`
- `runningconfig.xml`
- `supportinfo.html`
- `systeminfo.html`
- `systemlog.html`

L'équipement crée le nom du fichier de l'archive ZIP automatiquement au format `<Adresse_IP>_<nom_système>.zip`.

Exécutez les étapes suivantes :

- ☐ Cliquez sur le bouton ☰ puis sur l'élément *Download support information*.
- ☐ Sélectionnez le répertoire dans lequel vous voulez sauvegarder les informations de prise en charge.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

14.13.2 Syslog

L'équipement vous permet d'envoyer des messages relatifs aux événements internes de l'équipement à un ou plusieurs serveurs Syslog (jusqu'à 8). En outre, vous pouvez également ajouter au serveur Syslog les requêtes SNMP envoyées à l'équipement en tant qu'événements.

Commentaire : Pour afficher les événements consignés, ouvrez la boîte de dialogue *Diagnostics > Report > Audit Trail* ou la boîte de dialogue *Diagnostics > Report > System Log*.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Syslog*.
- ☐ Pour ajouter une entrée de tableau, cliquez sur le bouton .
- ☐ Dans la colonne *IP address*, saisissez l'adresse IP ou *Hostname* du serveur Syslog. Vous pouvez spécifier une adresse IPv4 ou IPv6 valide pour le serveur Syslog.
- ☐ Dans la colonne *Destination UDP port*, spécifiez le port TCP ou UDP sur lequel le serveur Syslog s'attend à recevoir les entrées du log.
- ☐ Dans la colonne *Min. severity*, spécifiez le degré de gravité minimum qu'un événement requiert pour que l'équipement envoie une entrée de log au serveur Syslog.
- ☐ Cochez la case dans la colonne *Active*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

Dans le cadre *SNMP logging*, configurez les réglages suivants relatifs aux requêtes de lecture et d'écriture SNMP :

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Report > Global*.
- ☐ Activez la fonction *Log SNMP get request* pour l'équipement afin d'envoyer les requêtes de lecture SNMP en tant qu'événements au serveur Syslog.
  Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *SNMP logging*.
- ☐ Activez la fonction *Log SNMP set request* pour l'équipement afin d'envoyer les requêtes d'écriture SNMP en tant qu'événements au serveur Syslog.
  Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *SNMP logging*.
- ☐ Choisissez le degré de gravité souhaité pour les requêtes get et set.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`logging host add 1 addr 10.0.1.159 severity 3`	Ajoute un nouveau destinataire à la liste de serveurs Syslog. La valeur `3` spécifie le degré de gravité de l'événement que l'équipement consigne. La valeur `3` signifie `error`.
`logging host add 2 addr 2001::1 severity 4`	Ajoutez un nouveau destinataire IPv6 à la liste de serveurs Syslog. La valeur `4` signifie `warning`.
`logging syslog operation`	Activer la fonction *Syslog*.
`exit`	Basculez sur le mode Privileged EXEC.

```
show logging host                          Afficher les réglages d'hôte du serveur Syslog.
No.    Server IP      Port   Max. Severity   Type        Status
-----  -------------- -----  --------------  ----------  -------
1      10.0.1.159     514    error           systemlog   active
2      2001::1        514    warning         systemlog   active
configure                                  Basculez sur le mode de configuration.
logging snmp-requests get operation        Consigne les requêtes SNMP GET
logging snmp-requests get severity 5       La valeur 5 spécifie le degré de gravité de l'événement que l'équipement consigne en cas de requêtes SNMP GET. La valeur 5 signifie notice.
logging snmp-requests set operation        Consigne les requêtes SNMP SET.
logging snmp-requests set severity 5       La valeur 5 spécifie le degré de gravité de l'événement que l'équipement consigne en cas de requêtes SNMP SET. La valeur 5 signifie notice.
exit                                       Basculez sur le mode Privileged EXEC.
show logging snmp                          Afficher les réglages de la consignation des requêtes SNMP.
Log SNMP GET requests              : enabled
Log SNMP GET severity              : notice
Log SNMP SET requests              : enabled
Log SNMP SET severity              : notice
```

14.13.3 Log système

L'équipement vous permet de consulter un fichier log des événements système. Le tableau de la boîte de dialogue *Diagnostics > Report > System Log* répertorie les événements consignés.

Exécutez les étapes suivantes :

- ☐ Pour mettre à jour le contenu du log, cliquez sur le bouton .
- ☐ Pour archiver le contenu du log en tant que fichier html, cliquez sur le bouton , puis sur l'élément *Reset*.
- ☐ Pour supprimer le contenu du log, cliquez sur le bouton , puis sur l'élément *Reset*.
- ☐ Pour rechercher un mot-clé dans le contenu du log, utilisez la fonction de recherche de votre navigateur Web.

Commentaire : Vous avez la possibilité d'envoyer également les événements consignés à un ou plusieurs serveurs Syslog.

14.13.4 Syslog sur TLS

Le protocole TLS (Transport Layer Security) est un protocole cryptographique conçu pour assurer la sécurité des communications sur un réseau informatique. L'objectif principal du protocole TLS est d'assurer la confidentialité et l'intégrité des données entre deux applications informatiques en communication.

Après avoir initié une connexion avec un serveur Syslog à l'aide d'un handshake TLS, l'équipement valide le certificat reçu du serveur. À cette fin, vous transférez le certificat PEM d'un serveur distant ou de la mémoire externe sur l'équipement. Vérifiez que l'adresse IP ou le nom DNS configuré du serveur correspond aux informations fournies dans le certificat. Vous trouverez ces informations dans les champs Common Name ou Subject Alternative Name du certificat.

L'équipement envoie les messages Syslog chiffrés TLS sur le port TCP spécifié dans la colonne *Destination UDP port*.

Commentaire : Spécifiez l'adresse IP ou le nom DNS du serveur pour qu'il corresponde à l'adresse IP ou au nom DNS fourni dans le certificat du serveur. Les valeurs sont indiquées dans les champs Common Name ou the Subject Alternative Name du certificat.

Exemple

L'exemple donné décrit la configuration de la fonction *Syslog*. En suivant ces étapes, l'équipement vous permet d'envoyer les messages Syslog chiffrés TLS sur le port TCP spécifié dans la colonne *Destination UDP port*.

Les messages Syslog envoyés d'un équipement à un serveur Syslog peuvent passer par des réseaux non sécurisés. Pour configurer un serveur Syslog sur TLS, transférez le certificat de l'autorité de certification (CA) sur l'équipement.

Commentaire : Afin que les changements prennent effet après le chargement d'un nouveau certificat, redémarrez la fonction *Syslog*.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Syslog*.
- ☐ Pour établir une connexion avec les serveurs Syslog, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

L'équipement valide le certificat reçu. L'équipement authentifie également le serveur et commence à envoyer des messages Syslog.

- ☐ Transférez le certificat PEM du serveur distant ou de la mémoire externe sur l'équipement.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`logging host add 1 addr 192.168.3.215`	Ajoutez l'index `1` au serveur Syslog avec l'adresse IPv4`192.168.3.215`.
`logging host add 2 addr 2001::1`	Ajoutez l'index `2` au serveur Syslog avec l'adresse IPv6`2001::1`..
`logging host modify 1 port 6512 type systemlog`	Spécification du numéro de port `6512` et consignation des événements dans le log système.

`logging host modify 1 transport tls`	Spécifiez le type de transmission comme `tls`.
`logging host modify 1 severity informational`	Spécification du type d'événement à consigner dans le log système comme `informational`.
`exit`	Basculez sur le mode Privileged EXEC.
`copy syslogcacert evmm`	Copiez les certificats CA de la mémoire externe vers l'équipement.
`show logging host`	Afficher les réglages d'hôte du serveur Syslog.

14.13.5 Piste de vérification

La boîte de dialogue *Diagnostics > Report > Audit Trail* contient les informations système et les modifications de la configuration de l'équipement effectuées à l'aide de l'interface de ligne de commande et du protocole SNMP. Lorsque la configuration de l'équipement subit des modifications, la boîte de dialogue affiche Qui a effectué ces modifications, Quand et ce sur Quoi elles portent.

La boîte de dialogue *Diagnostics > Syslog* vous permet de spécifier jusqu'à 8 serveurs Syslog auxquels l'équipement envoie des pistes de vérification.

La liste suivante contient les événements consignés dans le log :
- Les modifications apportées aux paramètres de la configuration
- Les commandes utilisant l'interface de ligne de commande (à l'exception des commandes `show`)
- La commande `logging audit-trail <string>` utilisant l'interface de ligne de commande qui consigne le commentaire
- Les modifications automatiques apportées à l'heure système
- Les événements de chien de garde
- Le verrouillage d'un utilisateur après plusieurs échecs de tentative de connexion
- La connexion de l'utilisateur, soit localement soit à distance, à l'aide de l'interface de ligne de commande
- Déconnexion manuelle, initiée par l'utilisateur
- Déconnexion après un délai d'inactivité de l'interface de ligne de commande défini par l'utilisateur
- Opération de transfert de fichiers, y compris les mises à jour des firmwares
- Modifications de la configuration à l'aide de Ethernet Switch Configurator
- Configuration automatique ou mises à jour des firmwares à l'aide de la mémoire externe
- Accès bloqué à l'administration de l'équipement en raison d'une connexion invalide
- Redémarrage
- Ouverture et fermeture de SNMP via des tunnels HTTPS
- Panne de l'alimentation en tension

14.14 Analyse du réseau à l'aide de TCPdump

Tcpdump est un utilitaire UNIX renifleur de paquets utilisé par les administrateurs du réseau pour renifler et analyser le trafic d'un réseau. Le recours au reniflage du trafic sur un réseau se justifie notamment par la nécessité de vérifier la connectivité entre les hôtes ou d'analyser le trafic traversant le réseau.

L'utilisation de TCPDump sur l'équipement offre la possibilité de décoder ou de capturer les paquets reçus et transmis par l'UC d'administration. Cette fonction est disponible à l'aide de la commande `debug`. Reportez-vous au manuel de référence « Interface de ligne de commande » pour obtenir de plus amples informations sur la fonction TCPDump.

14.15 Surveillance des données du trafic

L'équipement vous permet de transmettre à un port cible les paquets de données transitant à travers l'équipement. Sur ce port, vous pouvez surveiller et évaluer les paquets de données.

L'équipement fournit les options suivantes :
- Port Mirroring

14.15.1 Port Mirroring

La fonction *Port Mirroring* vous permet de copier les paquets de données des ports physiques sources vers un port physique cible.

Vous pouvez surveiller le trafic de données sur les ports sources dans les sens d'émission et de réception à l'aide d'un outil d'administration connecté au port cible, par exemple une sonde RMON. La fonction n'affecte pas le trafic de données au niveau des ports sources.

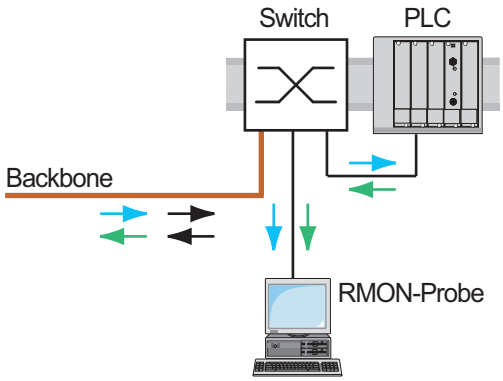


Figure 74 : Exemple

Sur le port cible, l'équipement transmet uniquement les paquets de données copiés à partir des ports sources.

Avant d'activer la fonction *Port Mirroring*, cochez la case *Allow management* pour accéder à l'administration de l'équipement via le port cible. L'équipement permet aux utilisateurs d'avoir accès à l'administration de l'équipement via le port cible sans interrompre la session *Port Mirroring* active.

Commentaire : L'équipement duplique les multicasts, broadcasts et unicasts inconnus sur le port cible.

Les réglages du VLAN sur le port cible restent inchangés. La condition préalable à l'accès à l'équipement via le port cible est que le port cible soit un membre du VLAN d'administration de l'équipement.

Activation de la fonction Port Mirroring.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > Ports > Port Mirroring*.
- ☐ Spécifiez les ports sources.
  Cochez la case située dans la colonne *Enabled* pour les ports concernés.
- ☐ Indiquez le port cible.
  Dans le cadre *Destination port*, sélectionnez le port souhaité dans la liste déroulante *Primary port*.
  La liste déroulante affiche uniquement les ports disponibles. Les ports déjà spécifiés en tant que ports sources sont indisponibles.
- ☐ Si nécessaire, spécifiez un deuxième port cible.
  Dans le cadre *Destination port*, sélectionnez le port souhaité dans la liste déroulante *Secondary port*.
  La condition préalable est que vous ayez déjà spécifié le port cible primaire.
- ☐ Pour accéder à l'administration de l'équipement via le port cible :
  Dans le cadre *Destination port*, cochez la case *Allow management*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

Pour désactiver la fonction *Port Mirroring* et restaurer les réglages par défaut, cliquez sur le bouton , puis sur l'option *Reset config*.

14.16 Auto-test

L'équipement contrôle ses actifs pendant le démarrage, et occasionnellement après le démarrage. L'équipement vérifie la disponibilité ou la cessation des tâches système et l'espace mémoire disponible. En outre, l'équipement vérifie la fonctionnalité des applications et la présence de toute dégradation matérielle au niveau des puces.

Lorsque l'équipement détecte une perte d'intégrité, l'équipement réagit à la dégradation en exécutant une action définie par l'utilisateur. Les catégories suivantes sont disponibles pour la configuration.

- `task`
  Action à exécuter en cas d'échec d'une tâche.
- `resource`
  Action à exécuter en cas de ressources insuffisantes.
- `software`
  Action à exécuter en cas de perte d'intégrité logicielle ; par exemple, somme de contrôle de segment de code ou violations d'accès.
- `hardware`
  Action à exécuter en cas de dégradation matérielle.

Configurez chaque catégorie afin qu'une action soit exécutée lorsque l'équipement détecte une perte d'intégrité. Les actions suivantes sont disponibles pour la configuration.

- `log only`
  Cette action écrit un message sur le fichier de consignation.
- `send trap`
  Envoie un trap SNMP à la destination de trap.
- `reboot`
  Lorsque la fonction est activée, une erreur détectée dans la catégorie concernée entraînera le redémarrage de l'équipement.

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Diagnostics > System > Selftest*.
- ☐ Dans la colonne *Action*, spécifiez l'action à exécuter pour une cause donnée.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`selftest action task log-only`	Pour envoyer un message au log des événements lorsqu'une tâche échoue.
`selftest action resource send-trap`	En cas de ressources insuffisantes, envoyer un trap SNMP.
`selftest action software send-trap`	Lorsque l'intégrité logicielle a été perdue, envoyer un trap SNMP.
`selftest action hardware reboot`	Pour redémarrer l'équipement en cas de dégradation matérielle.

La désactivation de ces fonctions vous permet de réduire le temps requis pour redémarrer l'équipement après un démarrage à froid. Vous trouverez ces options dans le cadre *Configuration* de la boîte de dialogue *Diagnostics > System > Selftest*.

- *RAM test*
  Active/désactive la fonction *RAM test* pendant un démarrage à froid.
- *SysMon1 is available*
  Active/désactive la fonction de Moniteur du système pendant un démarrage à froid.
- *Load default config on error*
  Active/désactive le chargement de la configuration de l'équipement par défaut lorsqu'aucune configuration lisible n'est disponible pendant un redémarrage.

Les réglages suivants bloquent votre accès à l'équipement de manière permanente lorsque l'équipement ne détecte aucun profil de configuration lisible pendant un redémarrage.

- La case *SysMon1 is available* est décochée.
- La case *Load default config on error* est décochée.

C'est par exemple le cas lorsque le mot de passe du profil de configuration que vous chargez diffère du mot de passe défini dans l'équipement. Pour débloquer à nouveau l'équipement, contactez votre revendeur.

Exécutez les étapes suivantes :

`selftest ramtest`	Activer l'auto-test RAM lors d'un redémarrage à froid.
`no selftest ramtest`	Désactiver la fonction « test ram ».
`selftest system-monitor`	Activer la fonction « SysMon1 ».
`no selftest system-monitor`	Désactiver la fonction « SysMon1 ».
`show selftest action`	Afficher l'état des actions à exécuter en cas de dégradation de l'équipement.
`show selftest settings`	Afficher les réglages pour les fonctions « test ram » et « SysMon » en cas de démarrage à froid.

14.17 Test des câbles en cuivre

Utilisez cette fonctionnalité pour tester les câbles en cuivre raccordés à une interface, afin de détecter un court-circuit ou un circuit ouvert. Le test interrompt le flux de trafic, lorsqu'il est en cours, sur ce port.

Le tableau présente l'état et les longueurs de chaque paire individuelle. L'équipement renvoie un résultat avec la signification suivante :

- normal : indique que le câble fonctionne correctement.
- ouvert : indique une interruption dans le câble.
- court-circuit : indique un court-circuit dans le câble.
- non testé : indique un câble non testé.
- Inconnu : câble non branché.

15 Fonctions avancées de l'équipement

15.1 Utilisation de l'équipement en tant que serveur DHCP

Un serveur DHCP (« Dynamic Host Configuration Protocol ») attribue aux clients les adresses IP, les, Gateways, et autres définitions de réseau telles les paramètres DNS et NTP.

Les opérations DHCP sont composées de 4 phases de base : découverte IP, offre IP, requête IP et acquittement IP. Utilisez l'acronyme DORA, signifiant Découverte, Offre, Requête et Acquittement, pour vous aider à mémoriser ces phases. Le serveur reçoit les données du client sur le port UDP 67 et transmet les données au client sur le port UDP 68.

Le serveur DHCP fournit un pool d'adresses IP ou « pool », à l'aide duquel il attribue des adresses IP aux clients. Le pool est constitué d'une liste d'entrées. Une entrée permet de définir une adresse IP donnée ou une plage d'adresses IP.

L'équipement vous permet d'activer le serveur DHCP globalement et par interface.

15.1.1 Adresses IP attribuées par port ou par VLAN

Le serveur DHCP attribue une adresse IP statique ou une plage d'adresses IP dynamiques à un client connecté à un port ou un VLAN. L'équipement vous permet de créer des entrées pour un port ou un VLAN. Lorsque vous créez une entrée pour attribuer une adresse IP à un VLAN, l'entrée de port est grisée. Lorsque vous créez une entrée pour attribuer une adresse IP à un port, l'entrée de VLAN est grisée.

L'attribution statique signifie que le serveur DHCP attribue la même adresse IP à un client spécifique. Le serveur DHCP identifie le client à l'aide d'un ID matériel unique. Une entrée d'adresse statique contient une adresse IP et l'applique à un port ou un VLAN sur lequel le serveur reçoit une requête de la part d'un client spécifique. Pour l'attribution statique, créez une entrée de pool pour les ports ou un port spécifique, saisissez l'adresse IP et laissez la colonne *Last IP address* vide. Spécifiez un ID matériel avec lequel le serveur DHCP peut identifier le client de manière univoque. Cet ID est soit une adresse MAC, un ID client, un ID distant, ou un ID circuit. Lorsqu'un client contacte le serveur avec l'ID matériel configuré, le serveur DHCP attribue l'adresse IP statique.

L'équipement vous permet également d'attribuer une plage d'adresses IP aux ports ou aux VLAN à partir desquels le serveur DHCP attribue une adresse IP libre issue d'un pool. Pour ajouter un pool dynamique aux ports ou aux VLAN, spécifiez les première et dernière adresses IP pour la plage d'adresses IP en laissant les colonnes *MAC address*, *Client ID*, *Remote ID* et *Circuit ID* vides. La création de plusieurs entrées de pool vous permet de disposer de plages d'adresses IP contenant des blancs.

15.1.2 Exemple d'adresse IP statique de serveur DHCP

Dans cet exemple, configurez l'équipement pour attribuer une adresse IP statique à un port. L'équipement identifie les clients à l'aide de l'identification matérielle univoque. L'ID matériel dans ce cas est l'adresse MAC du client `00:24:E8:D6:50:51`. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Advanced > DHCP Server > Pool*.
- ☐ Pour ajouter une entrée de tableau, cliquez sur le bouton  .
- ☐ Dans la colonne *IP address*, spécifiez la valeur `192.168.23.42`.
- ☐ Dans la colonne *Port*, spécifiez la valeur `1/1`.
- ☐ Dans la colonne *MAC address*, spécifiez la valeur `00:24:E8:D6:50:51`.
- ☐ Pour attribuer une adresse IP au client de manière permanente, dans la colonne *Lease time [s]*, spécifiez la valeur `4294967295`.
- ☐ Cochez la case dans la colonne *Active*.
- ☐ Ouvrez la boîte de dialogue *Advanced > DHCP Server > Global*.
- ☐ Pour le port `1/1`, cochez la case dans la colonne *DHCP server active*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`dhcp-server pool add 1 static 192.168.23.42`	Création d'une entrée avec l'index `1` et ajout de l'adresse IP `192.168.23.42` au pool statique.
`dhcp-server pool modify 1 mode interface 1/1`	Attribuer l'adresse statique de l'index `1` à l'interface `1/1`.
`dhcp-server pool modify 1 mode mac 00:24:E8:D6:50:51`	Attribuer l'adresse IP de l'index `1` à l'équipement dont l'adresse MAC est `00:24:E8:D6:50:51`.
`dhcp-server pool mode 1`	Activer l'entrée de pool de l'index `1`.
`dhcp-server pool modify 1 leasetime infinite`	Modifier l'entrée correspondant à l'index `1` pour attribuer l'adresse IP au client de manière permanente.
`dhcp-server operation`	Activer le serveur DHCP de manière globale.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`dhcp-server operation`	Activer/désactiver la fonction *DHCP Server* sur ce port.

15.1.3 Exemple de plage d'adresses IP dynamiques de serveur DHCP

L'équipement vous permet de créer des plages d'adresses IP dynamiques. Laissez les champs *MAC address*, *Client ID*, *Remote ID* et *Circuit ID* vides. Pour créer des plages d'adresses IP dynamiques contenant des blancs entre les plages, ajoutez plusieurs entrées au tableau. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Advanced > DHCP Server > Pool*.
- ☐ Pour ajouter une entrée de tableau, cliquez sur le bouton .
- ☐ Dans la colonne *IP address*, spécifiez la valeur `192.168.23.92`. Il s'agit de la première adresse IP de la plage.
- ☐ Dans la colonne *Last IP address*, spécifiez la valeur `192.168.23.142`. Il s'agit de la dernière adresse IP de la plage.

Dans la colonne *Lease time [s]*, le réglage par défaut est de 60 jours.

- ☐ Dans la colonne *Port*, spécifiez la valeur `1/2`.
- ☐ Cochez la case dans la colonne *Active*.
- ☐ Ouvrez la boîte de dialogue *Advanced > DHCP Server > Global*.
- ☐ Pour le port `1/2`, cochez la case dans la colonne *DHCP server active*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton .

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142`	Ajouter un pool dynamique avec une plage d'adresses IP comprises entre `192.168.23.92` et `192.168.23.142`.
`dhcp-server pool modify 2 leasetime {seconds | infinite}`	Saisie du Lease Time en secondes ou pour une durée infinie.
`dhcp-server pool add 3 dynamic 192.198.23.172 192.168.23.180`	Ajouter un pool dynamique avec une plage d'adresses IP comprises entre `192.168.23.172` et `192.168.23.180`.
`dhcp-server pool modify 3 leasetime {seconds | infinite}`	Saisie du Lease Time en secondes ou pour une durée infinie.
`dhcp-server pool mode 2`	Activer l'entrée de pool de l'index `2`.
`dhcp-server pool mode 3`	Activer l'entrée de pool de l'index `3`.
`dhcp-server operation`	Activer le serveur DHCP de manière globale.
`interface 2/1`	Basculez sur le mode de configuration de l'interface `2/1`.
`dhcp-server operation`	Activer/désactiver la fonction *DHCP Server* sur ce port.

15.2 Relais DHCP L2

La façade avant de l'équipement présente le message de danger suivant :

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL

Ne modifiez pas les positions des câbles si DHCP Option 82 est activé. Vérifiez le manuel d'utilisation avant l'entretien.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Un administrateur du réseau utilise l'*agent de relais* DHCP de couche 2 pour ajouter les informations client DHCP. Ces informations sont requises par les *agents de relais* de couche 3 et les serveurs DHCP pour affecter une adresse et une configuration à un client.

Lorsqu'un serveur et un client DHCP sont dans le même sous-réseau IP, ils échangent directement des réponses et des demandes d'adresses IP. Cependant, le fait de disposer d'un serveur DHCP sur chaque sous-réseau est onéreux et souvent peu pratique. Une solution à la présence d'un serveur DHCP dans chaque sous-réseau consiste à utiliser les équipements de réseau pour relayer les paquets entre un client DHCP et un serveur DHCP situés dans un sous-réseau différent.

Un *agent de relais* de couche 3 est généralement un routeur qui possède des interfaces IP à la fois dans les sous-réseaux client et serveur et qui achemine le trafic entre eux. Cependant, dans les réseaux commutés de couche 2, il y a un ou plusieurs équipements de réseau, des commutateurs par exemple, entre le client et l'*agent de relais* de couche 3 ou le serveur DHCP. Dans ce cas, cet équipement fournit un *agent de relais* de couche 2 pour ajouter les informations dont l'*agent de relais* de couche 3 et le serveur DHCP ont besoin pour jouer leur rôle dans l'attribution des adresses et des configurations.

La liste suivante contient les réglages par défaut pour cette fonction :
- Réglage global :
  - Réglage actif : désactiver
- Réglages d'interface :
  - Réglage actif : désactiver
  - Port de confiance : désactiver
- Réglages VLAN :
  - Réglage actif : désactiver
  - *ID circuit* : activer
  - Type de l'*ID distant* : mac
  - *ID distant* : vierge

Pour le protocole DHCPv6, un *agent de relais* est utilisé pour ajouter des options d'*agent de relais* aux paquets DHCPv6 échangés entre un client et un serveur DHCPv6. Le Lightweight DHCPv6 Relay Agent (LDRA) est décrit dans RFC 6221.

Le LDRA traite 2 types de messages :
- Le premier type de message est le message *Relay-Forward* qui contient des informations uniques sur le client.
- Le deuxième type de message est le message *Relay-Reply* que le serveur DHCPv6 envoie à l'*agent de relais*. L'*agent de relais* valide ensuite le message pour inclure les informations encapsulées dans le message initial *Relay-Forward* et, s'il est valide, envoie le paquet au client.

Le message *Relay-Forward* contient l'information *Interface-ID*, également connue en tant que *Option 18*. Cette option fournit des informations qui identifient l'interface sur laquelle la requête du client a été envoyée. L'équipement rejette les paquets DHCPv6 qui ne contiennent pas l'information *Option 18*.

15.2.1 ID circuit et distants

Dans un environnement IPv4, avant de transférer la requête d'un client au serveur DHCP, l'équipement ajoute l'*ID circuit* et l'*ID distant* dans le champ *Option 82* du paquet de requêtes DHCP.
- L'*ID circuit* enregistre sur quel port l'équipement a reçu la requête du client.
- L'*ID distant* contient l'adresse MAC, l'adresse IP, le nom du système ou une chaîne de caractères définie par l'utilisateur. En l'utilisant, les équipements participants identifient l'*agent de relais* qui a reçu la requête du client.

L'équipement et les autres *agents de relais* utilisent ces informations pour rediriger la réponse de l'*agent relais* DHCP vers le client d'origine. Le serveur DHCP est en mesure d'analyser ces données, par exemple pour attribuer au client une adresse IP provenant d'un pool d'adresses spécifique.

De plus, le paquet de relais du serveur DHCP contient l'*ID circuit* et l'*ID distant*. Avant de transférer la réponse au client, l'équipement supprime les informations dans le champ *Option 82*.

15.2.2 Configuration du relais DHCP L2

La boîte de dialogue *Advanced > DHCP L2 Relay > Configuration* vous permet d'activer la fonction sur les ports actifs et sur les réseaux locaux virtuels. Dans le cadre *Operation*, sélectionnez le bouton radio *On*. Puis cliquez sur le bouton .

L'équipement transfère les paquets DHCPv4 avec les informations *Option 82*et les paquets DHCPv6 avec les informations *Option 18* sur les ports pour lesquels la case de la colonne *DHCP L2 Relay* et de la colonne *Trusted port* est cochée. Généralement, il s'agit de ports dans le réseau du serveur DHCP.

Pour les ports sur lesquels les clients DHCP sont connectés, vous activez la fonction *DHCP L2 Relay*, mais vous laissez la case *Trusted port* décochée. Sur ces ports, l'équipement ignore les paquets DHCPv4 avec les informations *Option 82*et les paquets DHCPv6 avec les informations *Option 18*.

Un exemple de configuration pour la fonction de relais DHCPv4 L2 est présenté ci-dessous. Les étapes de configuration de la fonction de relais DHCPv6 L2 sont analogues, à l'exception des entrées *Circuit ID* et *Remote ID* qui ne peuvent être spécifiées que pour *Option 82*.

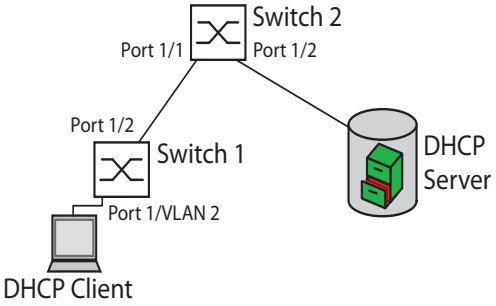


Figure 75 : Exemple de réseau DHCP de couche 2

Exécutez les étapes suivantes sur le commutateur 1 :

- ☐ Ouvrez la boîte de dialogue *Advanced > DHCP L2 Relay > Configuration*, onglet *Interface*.
- ☐ Pour le port `1/1`, spécifiez les réglages comme suit :
  - Cochez la case dans la colonne *Active*.
- ☐ Pour le port `1/2`, spécifiez les réglages comme suit :
  - Cochez la case dans la colonne *Active*.
  - Cochez la case dans la colonne *Trusted port*.
- ☐ Ouvrez la boîte de dialogue *Advanced > DHCP L2 Relay > Configuration*, onglet *VLAN ID*.
- ☐ Spécifiez les réglages de VLAN 2 comme suit :
  - Cochez la case dans la colonne *Active*.
  - Cochez la case dans la colonne *Circuit ID*.
  - Pour utiliser l'adresse IP de l'équipement comme *ID distant*, dans la colonne *Remote ID type*, spécifiez la valeur `ip`.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

Exécutez les étapes suivantes sur le commutateur 2 :

- ☐ Ouvrez la boîte de dialogue *Advanced > DHCP L2 Relay > Configuration*, onglet *Interface*.
- ☐ Pour les ports `1/1` et `1/2`, spécifiez les réglages comme suit :
  - Cochez la case dans la colonne *Active*.
  - Cochez la case dans la colonne *Trusted port*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

Vérifiez que VLAN 2 est présent. Puis, exécutez les étapes suivantes sur le commutateur 1 :
☐ Configurez VLAN 2 et spécifiez le port `1/1` comme membre de VLAN 2.

`enable`	Basculez sur le mode Privileged EXEC.
`vlan database`	Passer en mode de configuration VLAN.
`dhcp-l2relay circuit-id 2`	Activez l'ID circuit et DHCP Option 82 sur VLAN `2`.
`dhcp-l2relay remote-id ip 2`	Indiquez l'adresse IP de l'équipement comme ID distant sur VLAN `2`.

`dhcp-l2relay mode 2`	Activez la fonction *DHCP L2 Relay* sur VLAN `2`.
`exit`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`dhcp-l2relay mode`	Activez la fonction *DHCP L2 Relay* sur le port.
`exit`	Basculez sur le mode de configuration.
`interface 1/2`	Basculez sur le mode de configuration de l'interface `1/2`.
`dhcp-l2relay trust`	Spécifiez le port en tant que *Trusted port*.
`dhcp-l2relay mode`	Activez la fonction *DHCP L2 Relay* sur le port.
`exit`	Basculez sur le mode de configuration.
`dhcp-l2relay mode`	Activez la fonction *DHCP L2 Relay* dans l'équipement.

Exécutez les étapes suivantes sur le commutateur 2 :

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`dhcp-l2relay trust`	Spécifiez le port en tant que *Trusted port*.
`dhcp-l2relay mode`	Activez la fonction *DHCP L2 Relay* sur le port.
`exit`	Basculez sur le mode de configuration.
`interface 1/2`	Basculez sur le mode de configuration de l'interface `1/2`.
`dhcp-l2relay trust`	Spécifiez le port en tant que *Trusted port*.
`dhcp-l2relay mode`	Activez la fonction *DHCP L2 Relay* sur le port.
`exit`	Basculez sur le mode de configuration.
`dhcp-l2relay mode`	Activez la fonction *DHCP L2 Relay* dans l'équipement.

15.3 Utilisation de l'équipement en tant que client DNS

Le DNS (Domain Name System ou système de noms de domaine) interroge les serveurs DNS pour résoudre les noms d'hôtes et les adresses IP des équipements de réseau. À l'instar d'un annuaire téléphonique, le client DNS convertit les noms des equipements en adresses IP. Lorsque le client DNS reçoit une requête de résolution d'un nouveau nom, il interroge d'abord sa base de données statique interne, puis les serveurs DNS assignés pour obtenir les informations. Le client DNS enregistre les informations demandées dans un cache pour les requêtes futures.

L'équipement vous permet de configurer le client DNS à partir du serveur DHCP en utilisant le VLAN d'administration de l'équipement. L'équipement vous permet également d'attribuer des noms d'hôtes aux adresses IP de manière statique.

Le client DNS offre les fonctions utilisateur suivantes :
- liste de serveurs DNS, pouvant contenir 4 adresses IP de serveurs de noms de domaine
- mappage statique de noms d'hôtes et d'adresses IP, pouvant contenir 64 hôtes statiques configurables
- cache d'hôte, pouvant contenir 128 entrées

15.3.1 Exemple de configuration d'un serveur DNS

Nommez le client DNS et configurez-le pour qu'il interroge un serveur DNS afin de résoudre les noms d'hôtes. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Advanced > DNS > Client > Static*.
- ☐ Dans le cadre *Configuration*, champ *Configuration source*, spécifiez la valeur `user`.
- ☐ Dans le cadre *Configuration*, champ *Domain name*, spécifiez la valeur `device1`.
- ☐ Pour ajouter une entrée de tableau, cliquez sur le bouton  .
- ☐ Dans la colonne *Address*, spécifiez la valeur `192.168.3.5` comme adresse IPv4 du serveur DNS. Vous pouvez également spécifier une adresse IPv6 valide comme adresse IP du serveur DNS.
- ☐ Cochez la case dans la colonne *Active*.
- ☐ Ouvrez la boîte de dialogue *Advanced > DNS > Client > Global*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`dns client source user`	Spécification que l'utilisateur configure manuellement les réglages du client DNS.
`dns client domain-name devicel`	Spécification de la chaîne `device1` comme nom de domaine unique pour l'équipement.
`dns client servers add 1 ip 192.168.3.5`	Pour ajouter un serveur de noms DNS avec une adresseIPv4 de `192.168.3.5` comme index `1`.
`dns client servers add 2 ip 2001::1`	Ajoutez un serveur DNS avec une adresse IPv6 de `2001::1` comme index `2`.
`dns client adminstate`	Active la fonction *DNS Client* globalement.

Configurez le client DNS pour mapper les hôtes statiques avec les adresses IP. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Advanced > DNS > Client > Static Hosts*.
- ☐ Pour ajouter une entrée de tableau, cliquez sur le bouton  .
- ☐ Dans la colonne *Name*, saisissez la valeur `example.com`.
  Il s'agit du nom d'un équipement du réseau.
- ☐ Dans la colonne *IP address*, spécifiez la valeur `192.168.3.9`.
- ☐ Cochez la case dans la colonne *Active*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`dns client host add 1 name example.com ip 192.168.3.9`	Ajoutez `example.com` comme hôte statique avec une adresse IP de`192.168.3.9`.
`dns client adminstate`	Active la fonction *DNS Client* globalement.

15.4 GARP

Le protocole *GARP* (Generic Attribute Registration Protocol) est défini par l'IEEE afin de fournir un cadre générique permettant aux commutateurs d'enregistrer et de désenregistrer les valeurs d'attribut telles que les identifiants VLAN et l'appartenance à un groupe Multicast.

Lorsqu'un attribut d'un participant est enregistré ou désenregistré selon la fonction *GARP*, le participant est modifié selon des règles spécifiques. Les participants constituent un ensemble d'équipements terminaux et d'équipements de réseau accessibles. L'ensemble défini de participants à un moment donné, y compris leurs attributs, représente l'arbre d'accessibilité du sous-réseau de la topologies du réseau. L'équipement transfère les trames de données uniquement aux équipements terminaux enregistrés. L'enregistrement des équipements terminaux permet d'empêcher les tentatives d'envoi de données à des équipements terminaux inaccessibles.

15.4.1 Configurer GMRP

Le protocole *GMRP* (GARP Multicast Registration Protocol) est un protocole *GARP* (Generic Attribute Registration Protocol) qui fournit un mécanisme permettant aux équipements de réseau et aux équipements terminaux d'enregistrer dynamiquement l'appartenance à un groupe. L'équipement enregistre les informations d'appartenance à un groupe avec les équipements liés au même segment LAN. La fonction *GARP* permet également à l'équipement de disséminer les informations à travers les équipements du réseau prenant en charge les services de filtrage étendu.

Commentaire : Avant d'activer la fonction *GMRP*, assurez-vous que la fonction *MMRP* est désactivée.

L'exemple suivant décrit la configuration de la fonction *GMRP*. L'équipement offre une fonction d'inondation multicast contrainte sur un port sélectionné. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching* > *GARP* > *GMRP*.
- ☐ Pour activer la fonction de Multicast Flooding contrainte sur un port, cochez la case dans la colonne *GMRP active*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`garp gmrp operation`	Activation de la fonction *GMRP* sur le port.
`exit`	Basculez sur le mode de configuration.
`garp gmrp operation`	Activation de la fonction *GMRP* globalement.

15.4.2 Configuration de GVRP

Utilisez la fonction *GVRP* pour permettre à l'équipement d'échanger les informations de configuration de VLAN avec d'autres équipements *GVRP*. Il est ainsi possible de réduire le trafic Broadcast inutile et le trafic Unicast inconnu. En outre, la fonction *GVRP* permet de créer dynamiquement et de gérer les VLAN sur les équipements connectés via les ports trunk 802.1Q.

L'exemple suivant décrit la configuration de la fonction *GVRP*. L'équipement vous permet d'échanger les informations de configuration de VLAN avec d'autres équipements *GVRP*. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching* > *GARP* > *GVRP*.
- ☐ Pour échanger les informations de configuration de VLAN avec d'autres équipements *GVRP*, cochez la case dans la colonne *GVRP active* pour le port concerné.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 3/1`	Basculez sur le mode de configuration de l'interface `3/1`.
`garp gvrp operation`	Activation de la fonction *GVRP* sur le port.
`exit`	Basculez sur le mode de configuration.
`garp gvrp operation`	Activation de la fonction *GVRP* globalement.

15.5 MRP-IEEE

L'amendement IEEE 802.1ak de la norme technique IEEE 802.1Q a introduit le protocole MRP (Multiple Registration Protocol) pour remplacer le protocole *GARP* (Generic Attribute Registration Protocol). L'IEEE a également modifié et remplacé les applications *GARP*, le protocole *GARP* (*GMRP* Multicast Registration Protocol) et le protocole *GARP* (*GVRP* VLAN Registration Protocol) par le protocole *MMRP* (Multiple MAC Registration Protocol) et le protocole *MVRP* (Multiple VLAN Registration Protocol).

Pour confiner le trafic aux zones requises d'un réseau, les applications MRP distribuent des valeurs d'attributs aux équipements compatibles MRP à travers un LAN. Les applications MRP enregistrent et désenregistrent les appartenances à un groupe Multicast et les identifiants VLAN.

Commentaire : Le protocole MRP (Multiple Registration Protocol) requiert un réseau sans boucle. Pour contribuer à prévenir les boucles sur votre réseau, utilisez un protocole de réseau tel que le Media Redundancy Protocol, le Spanning Tree Protocol, ou le Rapid Spanning Tree Protocol avec MRP.

15.5.1 Fonctionnement du protocole MRP

Chaque participant contient un composant d'application et un composant MAD (MRP Attribute Declaration). Le composant d'application est responsable de la formation de valeurs d'attributs, ainsi que de leur enregistrement et désenregistrement. Le composant MAD génère des messages MRP pour la transmission et traite les messages envoyés par d'autres participants. Le composant MAD encode et transmet les attributs aux autres participants en unités de données MRP (MRPDU). Dans le commutateur, un composant MAP (MRP Attribute Propagation) distribue les attributs aux ports participants.

Un participant existe pour chaque application MRP et chaque port LAN. Par exemple, une application de participant existe sur un équipement terminal et une autre application existe sur un port de commutation. La machine d'état du composant d'application enregistre l'attribut et le port pour chaque déclaration de participant MRP sur un équipement terminal ou un commutateur. Toute modification de la variable de la machine d'état du composant d'application déclenche la transmission des MRPDU afin de communiquer la déclaration ou le retrait.

Pour établir une instance *MMRP*, un équipement terminal envoie d'abord un message Join empty (JoinMt) avec les attributs appropriés. Le commutateur diffuse ensuite le message JoinMt par inondation vers les ports participants et les commutateurs voisins. Les commutateurs voisins diffusent le message par inondation vers leur port participant, etc., établissant ainsi une voie d'accès pour le trafic du groupe.

15.5.2 Temporisateurs MRP

Les réglages par défaut du temporisateur contribuent à prévenir les déclarations et retraits d'attributs inutiles. Les réglages du temporisateur permettent aux participants de recevoir et de traiter les messages MRP avant l'expiration du temporisateur Leave ou LeaveAll.

Lorsque vous reconfigurez les temporisateurs, maintenez les relations suivantes :
- Pour permettre le ré-enregistrement après un événement Leave ou LeaveAll bien qu'un message ait été perdu, réglez la valeur de temporisation Leave comme suit : ≥ (2x JoinTime) + 60 in 1/100 s
- Pour réduire le volume du trafic supplémentaire généré à la suite d'un événement LeaveAll, spécifiez une valeur de temporisateur LeaveAll supérieure à la valeur LeaveTime.

La liste suivante contient différents événements MRP transmis par l'équipement :
- Join - Détermine l'intervalle pour la prochaine transmission de message Join
- Leave - Détermine la durée pendant laquelle un commutateur patiente à l'état Leave avant de passer à l'état de retrait
- LeaveAll - Détermine la fréquence à laquelle le commutateur génère des messages LeaveAll

Une fois expiré, le temporisateur Periodic initie un message Join de requête MRP que le commutateur envoie aux participants du LAN. Les commutateurs utilisent ce message pour contribuer à prévenir les retraits inutiles.

15.5.3 MMRP

Lorsqu'un équipement reçoit du trafic Broadcast, Multicast ou du trafic inconnu sur un port, l'équipement le diffuse par inondation vers les autres ports. Ce processus entraîne une utilisation superflue de bande passante sur le LAN.

Le protocole *MMRP* (Multiple MAC Registration Protocol) vous permet de contrôler la diffusion de trafic par inondation en distribuant une déclaration d'attribut aux participants d'un LAN. Les valeurs d'attribut que le composant MAD encode et transmet sur le LAN dans des messages MRP sont des informations d'exigences de service de groupe (« Group service requirement ») et des adresses MAC 48 bits.

Le commutateur enregistre les attributs dans une base de données de filtrage en tant qu'entrées d'enregistrement d'adresse MAC. Le processus de transmission utilise uniquement les entrées de la base de données de filtrage pour transmettre les données à travers les ports nécessaires pour accéder aux LAN des membres du groupe.

Les commutateurs facilitent les mécanismes de distribution aux groupes basés sur le concept de groupe d'hôte ouvert (« Open Host Group »), recevant les paquets sur les ports actifs et transmettant uniquement vers les ports associés aux membres du groupe. Tous les participants *MMRP* devant transmettre des paquets à un ou plusieurs groupes particuliers effectuent ainsi une demande d'appartenance au groupe. Les utilisateurs de service MAC envoient des paquets à un groupe particulier depuis n'importe quel emplacement sur le LAN. Un groupe reçoit ces paquets sur les LAN associés aux participants *MMRP* enregistrés. *MMRP* et les entrées d'enregistrement d'adresse MAC limitent ainsi les paquets aux segments requis d'un réseau sans boucle.

Afin de maintenir l'état d'enregistrement et de désenregistrement et de recevoir le trafic, un port déclare son intérêt de manière périodique. Chaque équipement présent sur un LAN dont la fonction *MMRP* est activée gère une base de données de filtrage et transmet aux participants répertoriés le trafic associé aux adresses MAC du groupe.

Exemple d'utilisation de MMRP

Dans cet exemple, l'hôte A a l'intention d'écouter le trafic destiné au groupe G1. Le commutateur A traite la requête Join du protocole *MMRP* envoyé à l'hôte A et envoie la requête aux deux commutateurs voisins. Les équipements présents sur le LAN détectent alors l'existence d'un hôte intéressé par la réception du trafic destiné au groupe G1. Lorsque l'hôte B commence à transmettre les données destinées au groupe G1, les données sont acheminées vers le chemin des enregistrements et l'hôte A les reçoit.

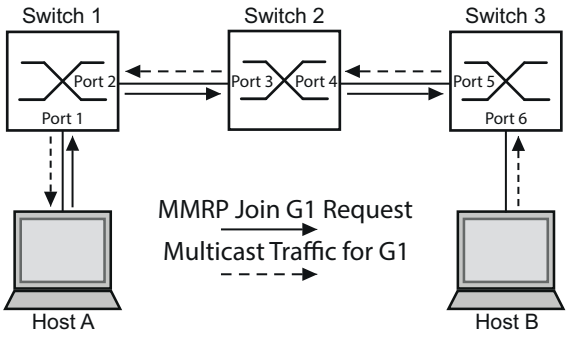


Figure 76 : Réseau MMRP pour enregistrement d'adresses MAC

Activez la fonction *MMRP* sur les commutateurs. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching* > *MRP-IEEE* > *MMRP*, onglet *Configuration*.
- ☐ Pour activer le port `1` et le port `2` comme participants *MMRP*, cochez la case dans la colonne *MMRP* du port `1` et du port `2` sur le commutateur 1.
- ☐ Pour activer le port `3` et le port `4` comme participants *MMRP*, cochez la case dans la colonne *MMRP* du port `3` et du port `4` sur le commutateur 2.
- ☐ Pour activer le port `5` et le port `6` comme participants *MMRP*, cochez la case dans la colonne *MMRP* du port `5` et du port `6` sur le commutateur 3.
- ☐ Pour envoyer des événements périodiques autorisant l'équipement à maintenir l'enregistrement du groupe d'adresses MAC, activez *Periodic state machine*. Sélectionnez le bouton radio `On` dans le cadre *Configuration*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ☑.

Pour activer les ports *MMRP* sur le commutateur 1, utilisez les commandes suivantes. En remplaçant les interfaces appropriées dans les commandes, activez les fonctions *MMRP* et les ports sur les commutateurs 2 et 3.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface `1/1`.
`mrp-ieee mmrp operation`	Activation de la fonction *MMRP* sur le port.
`interface 1/2`	Basculez sur le mode de configuration de l'interface `1/2`.
`mrp-ieee mmrp operation`	Activation de la fonction *MMRP* sur le port.
`exit`	Basculez sur le mode de configuration.
`mrp-ieee mrp periodic-state-machine`	Activation de la fonction *Periodic state machine* globalement.
`mrp-ieee mmrp operation`	Activation de la fonction *MMRP* globalement.

15.5.4 MVRP

Le protocole *MVRP* (Multiple VLAN Registration Protocol) est une application MRP qui fournit un enregistrement de VLAN dynamique et des services de retrait sur un LAN.

La fonction *MVRP* fournit un mécanisme de maintenance pour les entrées d'enregistrement de VLAN dynamique et pour la transmission des informations sur d'autres équipements. Ces informations permettent aux équipements compatibles *MVRP* d'établir et de mettre à jour leurs informations d'appartenance au VLAN. Lorsque les membres sont présents sur un VLAN, les informations indiquent les ports à travers lesquels le commutateur transmet le trafic pour joindre ces membres.

La finalité principale de la fonction *MVRP* est de permettre aux commutateurs de découvrir certaines informations de VLAN sans que vous ayez à les configurer manuellement. La découverte de ces informations permet aux commutateurs de surmonter les limitations de consommation de bande passante et de temps de convergence dans les réseaux VLAN de grande taille.

Exemple d'utilisation de MVRP

Configurez un réseau composé de commutateurs compatibles avec MVRP (1 - 4) reliés dans une topologie en anneau avec les groupes d'équipements terminaux, A1, A2, B1 et B2 dans 2 VLAN différents, A et B. Avec STP activé sur les commutateurs, les ports reliant le commutateur 1 au commutateur 4 présentent un état de rejet, contribuant ainsi à prévenir une condition de boucle.

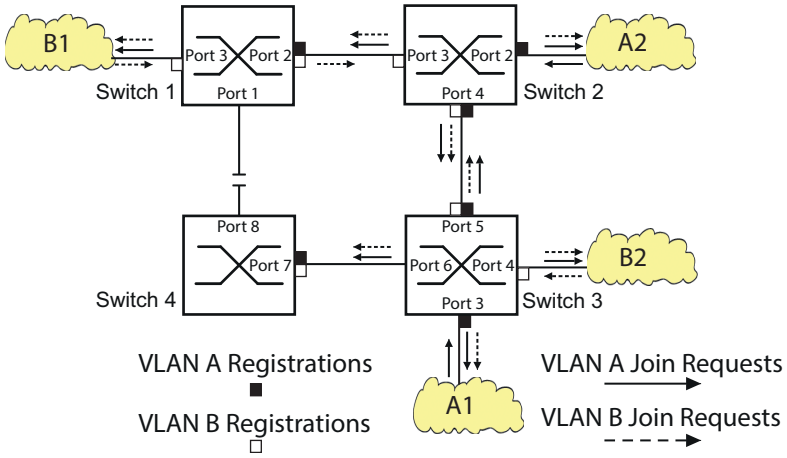


Figure 77 : Exemple de réseau MVRP pour l'enregistrement de VLAN

Dans l'exemple de réseau MVRP, les LAN envoient d'abord une requête Join aux commutateurs. Le commutateur saisit l'enregistrement de VLAN dans la base de données de transfert pour les ports recevant les trames.

Le commutateur propage ensuite la requête aux autres ports, puis envoie la requête aux LAN et commutateurs voisins. Ce processus se poursuit jusqu'à ce que les commutateurs aient enregistré les VLAN dans la base de données de transfert du port de réception.

Activez MVRP sur les commutateurs. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > MRP-IEEE > MVRP*, onglet *Configuration*.
- ☐ Pour activer les ports 1 à 3 comme participants *MVRP*, cochez la case dans la colonne *MVRP* pour les ports 1 à 3 sur le commutateur 1.
- ☐ Pour activer les ports 2 à 4 comme participants *MVRP*, cochez la case dans la colonne *MVRP* pour les ports 2 à 4 sur le commutateur 2.

- ☐ Pour activer les ports 3 à 6 comme participants *MVRP*, cochez la case dans la colonne *MVRP* pour les ports 3 à 6 sur le commutateur 3.
- ☐ Pour activer le port 7 et le port 8 comme participants *MVRP*, cochez la case dans la colonne *MVRP* du port 7 et du port 8 sur le commutateur 4.
- ☐ Pour maintenir l'enregistrement des VLAN, activez *Periodic state machine*. Sélectionnez le bouton radio *On* dans le cadre *Configuration*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio *On* dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✔.

Pour activer les ports *MVRP* sur le commutateur 1, utilisez les commandes suivantes. En remplaçant les interfaces appropriées dans les commandes, activez les fonctions *MVRP* et les ports sur les commutateurs 2, 3 et 4.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`interface 1/1`	Basculez sur le mode de configuration de l'interface 1/1.
`mrp-ieee mvrp operation`	Activation de la fonction *MVRP* sur le port.
`interface 1/2`	Basculez sur le mode de configuration de l'interface 1/2.
`mrp-ieee mvrp operation`	Activation de la fonction *MVRP* sur le port.
`exit`	Basculez sur le mode de configuration.
`mrp-ieee mvrp periodic-state-machine`	Activation de la fonction *Periodic state machine* globalement.
`mrp-ieee mvrp operation`	Activation de la fonction *MVRP* globalement.

16 Protocoles industriels

16.1 IEC 61850/MMS

Le protocole IEC 61850/MMS est un protocole industriel standardisé par l'International Electrotechnical Commission (IEC). Le protocole est utilisé dans l'automatisation des sous-stations, par exemple dans les systèmes de contrôle des fournisseurs d'énergie.

Ce protocole orienté paquet est basé sur le protocole de transport TCP/IP et utilise la norme MMS (Manufacturing Messaging Specification) pour la communication client-serveur. Il est orienté objet et définit un langage de configuration standardisé qui comprend entre autres les fonctions destinées aux systèmes SCADA, aux dispositifs électroniques intelligents (IED) et aux technologies de contrôle réseau.

La partie 6 de la norme technique IEC 61850 définit le langage de configuration SCL (Substation Configuration Language). Le langage SCL décrit les propriétés de l'équipement et la structure du système sous une forme pouvant faire l'objet d'un traitement automatique. Les propriétés de l'équipement décrites avec SCL sont sauvegardées dans le fichier ICD de l'équipement.

16.1.1 Modèle de commutateur réseau pour IEC 61850

Le rapport technique IEC 61850 90-4 spécifie un modèle de commutateur réseau. Le modèle de commutateur réseau représente les fonctions d'un commutateur en tant qu'objets d'un dispositif électronique intelligent (IED). Un client MMS (par exemple, le logiciel de salle de contrôle) utilise ces objets pour surveiller et configurer l'équipement.

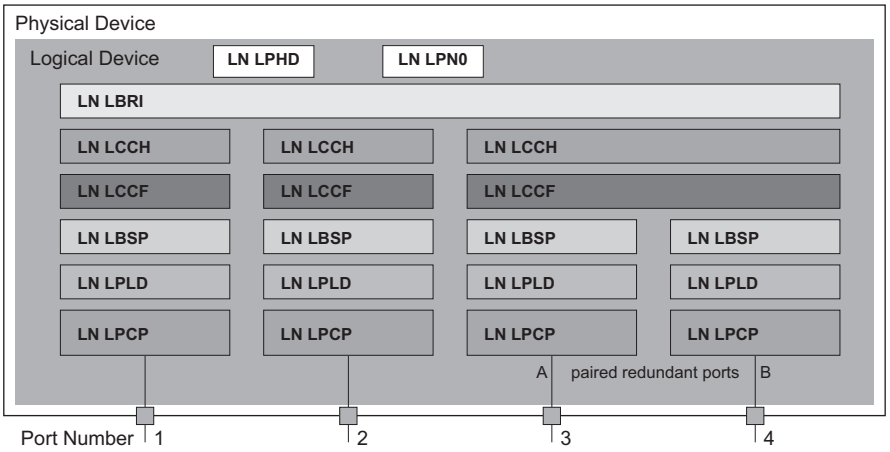


Figure 78 : Modèle de commutateur réseau basé sur le rapport technique IEC 61850 90-4

Tableau 59 : Classes de modèle de commutateur réseau basées sur TR IEC61850 90-4

Classe	Désignation
LN LLN0	Nœud logique Zero de l'IED du Bridge : Définit les propriétés logiques de l'équipement.
LN LPHD	Nœud logique Physical Device de l'IED du Bridge : Définit les propriétés physiques de l'équipement.
LN LBRI	Nœud logique Bridge : Représente les réglages généraux des fonctions de commutateur réseau de l'équipement.
LN LCCH	Nœud logique Communication Channel : Définit le Communication Channel logique composé d'un ou plusieurs ports physiques de l'équipement.
LN LCCF	Nœud logique Channel Communication Filtering : Définit les réglages VLAN et Multicast pour le Communication Channel de niveau supérieur.
LN LBSP	Nœud logique Port Spanning Tree Protocol : Définit les états Spanning Tree et les réglages pour le port physique correspondant de l'équipement.
LN LPLD	Nœud logique Port Layer Discovery : Définit les états LLDR et les réglages pour le port physique correspondant de l'équipement.
LN LPCP	Nœud logique Physical Communication Port : Représente le port physique correspondant de l'équipement.

16.1.2 Intégration à un système de contrôle

Préparation de l'équipement

Exécutez les étapes suivantes :

- ☐ Vérifiez qu'une adresse IP a été affectée à l'équipement.
- ☐ Ouvrez la boîte de dialogue *Advanced > Industrial Protocols > IEC61850-MMS*.
- ☐ Pour démarrer le serveur MMS, sélectionnez le bouton radio *On* dans le cadre *Operation* et cliquez sur le bouton ☑.
  Un client est alors capable de se connecter à l'équipement et de lire et surveiller les objets définis dans le modèle de commutateur réseau.

Le protocole IEC61850/MMS ne prévoit aucun mécanisme d'authentification. Si l'accès en écriture est activé pour le protocole IEC 61850/MMS, chaque client pouvant accéder à l'équipement en utilisant TCP/IP est capable de modifier les réglages de l'équipement. Cela peut entraîner une configuration incorrecte de l'équipement et des problèmes possibles sur le réseau.

ATTENTION
RISQUE D'ACCÈS NON AUTORISÉ À L'ÉQUIPEMENT Activez uniquement l'accès en écriture si vous avez pris des mesures supplémentaires (par exemple, installation d'un pare-feu, d'un VPN, etc.) pour limiter les risques d'accès non autorisé. **Le non-respect de ces instructions peut entraîner des endommagements de l'équipement.**

☐ Pour permettre au client MMS de modifier les réglages, cochez la case *Write access* et cliquez sur le bouton ✓.

Configuration hors ligne

L'équipement vous permet de télécharger le fichier ICD à l'aide de l'interface utilisateur graphique. Ce fichier contient les propriétés de l'équipement décrites avec SCL et vous permet de configurer la sous-station sans devoir vous connecter directement à l'équipement.

☐ Ouvrez la boîte de dialogue *Advanced > Industrial Protocols > IEC61850-MMS*.

☐ Pour sauvegarder le fichier ICD sur votre PC, cliquez sur le bouton ☰, puis sur l'élément *Download*.

Surveillance de l'équipement

Le serveur IEC61850/MMS intégré à l'équipement vous permet de surveiller plusieurs états de l'équipement à l'aide du bloc de contrôle de rapport (RCB). Jusqu'à 5 clients MMS peuvent s'enregistrer simultanément pour un bloc de contrôle de rapport.

L'équipement vous permet de surveiller les états suivants :

Tableau 60 : États de l'équipement pouvant être surveillés à l'aide d'IEC 61850/MMS

Classe	Objet RCB	Désignation
`LN LPHD`	`TmpAlm`	L'état change lorsque la température mesurée dans l'équipement passe au-dessus ou en dessous des valeurs limites de température définies.
	`PhyHealth`	L'état change lorsque l'état de l'objet RCB `LPHD.TmpAlm` change.
`LN LPHD`	`TmpAlm`	L'état change lorsque la température mesurée dans l'équipement passe au-dessus ou en dessous des valeurs limites de température définies.
	`PwrSupAlm`	L'état change lorsque l'un des blocs d'alimentation redondants tombe en panne ou se remet à fonctionner.
	`PhyHealth`	L'état change lorsque l'état de l'objet RCB `LPHD.PwrSupAlm` ou `LPHD.TmpAlm` change.

Tableau 60 : États de l'équipement pouvant être surveillés à l'aide d'IEC 61850/MMS (cont

Classe	Objet RCB	Désignation
LN LBRI	RstpRoot	L'état change lorsque l'équipement joue le rôle de commutateur racine ou abandonne ce rôle.
	RstpTopoCnt	L'état change lorsque la topologie change en raison d'un changement affectant le commutateur racine.
LN LCCH	ChLiv	L'état change lorsque l'état du lien du port physique change.
LN LPCP	PhyHealth	L'état change lorsque l'état du lien du port physique change.

16.2 Modbus TCP

Modbus TCP est un protocole de communication de la couche application permettant la communication client/serveur entre le client et les équipements connectés dans les réseaux Ethernet TCP/IP.

La fonction *Modbus TCP* vous permet d'installer l'équipement dans les réseaux utilisant déjà le protocole *Modbus TCP* et de récupérer les informations sauvegardées dans les registres de l'équipement.

16.2.1 Mode client/serveur de Modbus TCP/IP

L'équipement prend en charge le modèle client/serveur de Modbus TCP/IP. Dans cette constellation, cet équipement fonctionne en tant que serveur et répond aux requêtes d'un client portant sur les informations sauvegardées dans les registres.

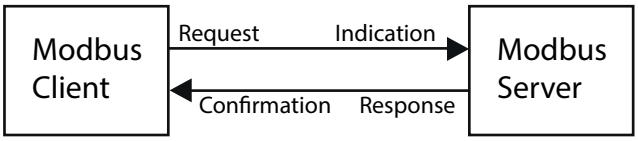


Figure 79 : Mode client/serveur de Modbus TCP/IP

Le modèle client/serveur utilise quatre types de messages pour échanger des données entre le client et le serveur :

- Modbus TCP/IP Request, le client crée une requête d'informations et envoie celles-ci au serveur.
- Modbus TCP/IP Indication, le serveur reçoit une requête indiquant qu'un client requiert des informations.
- Modbus TCP/IP Response, lorsque les informations requises sont disponibles, le serveur envoie une réponse contenant les informations requises. Lorsque les informations requises sont indisponibles, le serveur envoie une réponse d'exception pour informer le client de l'erreur détectée pendant le traitement. La réponse d'exception contient un code d'exception indiquant la cause de l'erreur détectée.
- Modbus TCP/IP Confirmation, le client reçoit une réponse contenant les informations requises de la part du serveur.

16.2.2 Fonctions prises en charge et topographie mémoire

L'équipement prend en charge les fonctions correspondant aux codes publics `0x03` (`Read Holding Registers`) et `0x05` (`Write Single Coil`). Les codes vous permettent de lire les informations sauvegardées dans les registres telles que les informations système, par exemple le nom du système, l'emplacement du système, la version logicielle, l'adresse IP, l'adresse MAC. Les codes vous permettent également de lire les informations des ports et les statistiques des ports. Le code `0x05` vous permet de réinitialiser les compteurs de port individuellement ou globalement.

La liste suivante contient les définitions des valeurs saisies dans la colonne `Format` :

- Bitmap : un groupe de 32 bits chiffré dans l'ordre d'octets big-endian et sauvegardé dans 2 registres. Les systèmes big-endian sauvegardent l'octet le plus significatif d'un mot dans l'adresse la plus basse et l'octet le moins significatif dans l'adresse la plus élevée.
- F1: 16-bit unsigned integer

- F2: Enumeration - power supply alarm
  - 0 = power supply good
  - 1 = power supply failure detected
- F3: Enumeration - OFF/ON
  - 0 = Off
  - 1 = On
- F4: Enumeration - port type
  - 0 = Giga - Gigabit Interface Converter (GBIC)
  - 1 = Copper - Twisted Pair (TP)
  - 2 = Fiber - 10 Mb/s
  - 3 = Fiber - 100 Mb/s
  - 4 = Giga - 10/100/1000 Mb/s (triple speed)
  - 5 = Giga - Copper 1000 Mb/s TP
  - 6 = Giga - Small Form-factor Pluggable (SFP)
- F9: 32-bit unsigned long
- Chaîne : octets sauvegardés en séquence, 2 octets par registre.

Codes Modbus TCP/IP

Le tableau ci-dessous répertorie les adresses permettant au client de réinitialiser les compteurs de port et de récupérer des informations spécifiques dans les registres de l'équipement.

Informations sur le port

Tableau 61 : Informations sur le port

Adresse	Qté	Désignation	Min	Max	Étape	Unité	Format
0400	1	Port 1 Type	0	6	1	-	F4
0401	1	Port 2 Type	0	6	1	-	F4
		...					
043F	1	Port 64 Type	0	6	1	-	F4
0440	1	Port 1 Link Status	0	1	1	-	F1
0441	1	Port 2 Link Status	0	1	1	-	F1
		...					
047F	1	Port 64 Link Status	0	1	1	-	F1
0480	1	Port 1 STP State	0	1	1	-	F1
0481	1	Port 2 STP State	0	1	1	-	F1
		...					
04BF	1	Port 64 STP State	0	1	1	-	F1
04C0	1	Port 1 Activity	0	1	1	-	F1
04C1	1	Port 2 Activity	0	1	1	-	F1
		...					
04FF	1	Port 64 Activity	0	1	1	-	F1
0500	1	Port 1 Counter Reset	0	1	1	-	F1
0501	1	Port 2 Counter Reset	0	1	1	-	F1
		...					
053F	1	Port 64 Counter Reset	0	1	1	-	F1

Statistiques du port

Tableau 62 : Statistiques du port

Adresse	Qté	Désignation	Min	Max	Étape	Unité	Format
0800	1	Port1 - Number of bytes received	0	4294967295	1	-	F9
0802	1	Port1 - Number of bytes sent	0	4294967295	1	-	F9
0804	1	Port1 - Number of frames received	0	4294967295	1	-	F9
0806	1	Port1 - Number of frames sent	0	4294967295	1	-	F9
0808	1	Port1 - Total bytes received	0	4294967295	1	-	F9
080A	1	Port1 - Total frames received	0	4294967295	1	-	F9
080C	1	Port1 - Number of broadcast frames received	0	4294967295	1	-	F9
080E	1	Port1 - Number of multicast frames received	0	4294967295	1	-	F9
0810	1	Port1 - Number of frames with CRC error	0	4294967295	1	-	F9
0812	1	Port1 - Number of oversized frames received	0	4294967295	1	-	F9
0814	1	Port1 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
0816	1	Port1 - Number of jabber frames received	0	4294967295	1	-	F9
0818	1	Port1 - Number of collisions occurred	0	4294967295	1	-	F9
081A	1	Port1 - Number of late collisions occurred	0	4294967295	1	-	F9
081C	1	Port1 - Number of 64-byte frames rcvd/sent	0	4294967295	1	-	F9
081E	1	Port1 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
0820	1	Port1 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
0822	1	Port1 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
0824	1	Port1 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
0826	1	Port1 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
0828	1	Port1 - Number of Mac Error Packets	0	4294967295	1	-	F9
082A	1	Port1 - Number of dropped received packets	0	4294967295	1	-	F9
082C	1	Port1 - Number of multicast frames sent	0	4294967295	1	-	F9
082E	1	Port1 - Number of broadcast frames sent	0	4294967295	1	-	F9
0830	1	Port1 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9
		...					
147E	1	Port64 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9

16.2.3 Exemple de configuration

Dans cet exemple, vous configurez l'équipement de manière à ce qu'il réponde aux requêtes des clients. La condition préalable à cette configuration est que l'équipement client soit configuré avec une adresse IP comprise dans la plage donnée. La fonction *Write access* reste désactivée dans cette exemple. Lorsque vous activez la fonction *Write access*, l'équipement vous permet de réinitialiser uniquement les compteurs de port. Dans la configuration par défaut, les fonctions *Modbus TCP* et *Write access* sont désactivées.

Le protocole *Modbus TCP* ne fournit aucun mécanisme d'authentification. Si l'accès en écriture est activé pour *Modbus TCP*, chaque client pouvant accéder à l'équipement en utilisant TCP/IP est capable de modifier les réglages de l'équipement. Cela peut entraîner une configuration incorrecte de l'équipement et des problèmes possibles sur le réseau.

ATTENTION
RISQUE D'ACCÈS NON AUTORISÉ À L'ÉQUIPEMENT Activez uniquement l'accès en écriture si vous avez pris des mesures supplémentaires (par exemple, installation d'un pare-feu, d'un VPN, etc.) pour limiter les risques d'accès non autorisé. **Le non-respect de ces instructions peut entraîner des endommagements de l'équipement.**

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > IP Access Restriction*.
- ☐ Ajoutez une entrée de tableau. Pour ce faire, cliquez sur le bouton  .
- ☐ Spécifiez la plage d'adresses IP dans la ligne où la colonne *Index* a la valeur `2`. Pour ce faire, saisissez les valeurs suivantes :
  - Dans la colonne *Address* : `10.17.1.0`
  - Dans la colonne *Netmask* : `255.255.255.248`
- ☐ Vérifiez que la case dans la colonne *Modbus TCP* est cochée.
- ☐ Activez la plage d'adresses IP. Pour ce faire, cochez la case dans la colonne *Active*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .
- ☐ Ouvrez la boîte de dialogue *Diagnostics > Status Configuration > Security Status*, onglet *Global*.
- ☐ Vérifiez que la case relative au paramètre *Modbus TCP active* est cochée.
- ☐ Ouvrez la boîte de dialogue *Advanced > Industrial Protocols > Modbus TCP*.
- ☐ Le port d'écoute *Modbus TCP* par défaut est le port `502`. Cependant, lorsque vous souhaitez écouter sur un autre port TCP, saisissez la valeur du port d'écoute dans le champ *TCP port*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton  .

Lorsque vous activez la fonction *Modbus TCP*, la fonction *Security Status* détecte l'activation et affiche une alarme dans le cadre *Security status* de la boîte de dialogue *Basic Settings > System*.

`enable`	Basculez sur le mode Privileged EXEC.
`network management access add 2`	Crée l'entrée pour la plage d'adresses du réseau. Numéro du prochain index disponible dans cet exemple : `2`.
`network management access modify 2 ip 10.17.1.0`	Spécifie l'adresse IP.
`network management access modify 2 mask 29`	Spécifie le masque réseau.
`network management access modify 2 modbus-tcp enable`	Indique que l'équipement permet au protocole *Modbus TCP* d'avoir accès à l'administration de l'équipement.
`network management access operation`	Active la restriction de l'accès IP.
`configure`	Basculez sur le mode de configuration.
`security-status monitor modbus-tcp-enabled`	Indique que l'équipement surveille l'activation du serveur *Modbus TCP*.
`modbus-tcp operation`	Active le serveur *Modbus TCP*.
`modbus-tcp port <1..65535>`	Spécifier le port TCP pour la communication *Modbus TCP* (facultatif). La valeur par défaut est le port `502`.
`show modbus-tcp`	Afficher les réglages du serveur *Modbus TCP*.

```
Modbus TCP/IP server settings
-------------------------
Modbus TCP/IP server operation.............enabled
Write-access...............................disabled
Listening port.............................502
Max number of sessions.....................5
Active sessions............................0
```

`show security-status monitor`	Afficher les réglages de l'état de la sécurité.

```
Device Security Settings
Monitor
---------------------------------
Password default settings unchanged..........monitored
...
Write access using Ethernet Switch Configurator is possible....monitored
Loading unencrypted configuration from ENVM...monitored
IEC 61850 MMS is enabled.....................monitored
Modbus TCP/IP server active..................monitored
```

`show security-status event`	Afficher les événements relatifs à l'état de la sécurité qui se sont produits.

```
Time stamp             Event                       Info
--------------------   ----------------------    ------
2014-01-01 01:00:39   password-change(10)          -
.................................................
2014-01-01 01:00:39   ext-nvm-load-unsecure(21)    -
2014-01-01 23:47:40   modbus-tcp-enabled(23)       -
```

```
show network management access rules 1
```

Afficher les règles de l'accès restreint à l'administration pour l'index 1.

```
Restricted management access settings
-------------------------------------
Index.....................................1
IP Address................................10.17.1.0
Prefix Length.............................29
HTTP......................................yes
SNMP......................................yes
Telnet....................................yes
SSH.......................................yes
HTTPS.....................................yes
IEC61850-MMS..............................yes
Modbus TCP/IP.............................yes
Active....................................[x]
```

16.3 EtherNet/IP

EtherNet/IP est un protocole industriel standardisé accepté dans le monde entier. Il est géré par l'Open DeviceNet Vendor Association (ODVA). Ce protocole repose sur les protocoles de transport Ethernet standard largement répandus TCP/IP et UDP/IP. *EtherNet/IP* est pris en charge par les principaux fabricants, fournissant ainsi une large base permettant une communication efficace des données dans le domaine industriel.

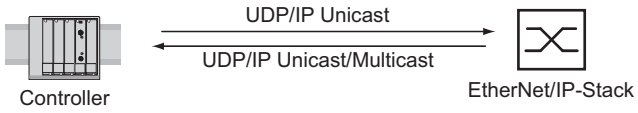


Figure 80 : Réseau EtherNet/IP

EtherNet/IP ajoute le protocole industriel CIP (Common Industrial Protocol) aux protocoles industriels Ethernet standard. *EtherNet/IP* implémente CIP au niveau des couches session et supérieures et adapte CIP à la technologie *EtherNet/IP* spécifique au niveau des couches transport et inférieures. En cas d'automatisation des applications, *EtherNet/IP* implémente CIP au niveau de la couche application. *EtherNet/IP* s'avère ainsi parfaitement adapté au secteur des techniques de commande industrielles.

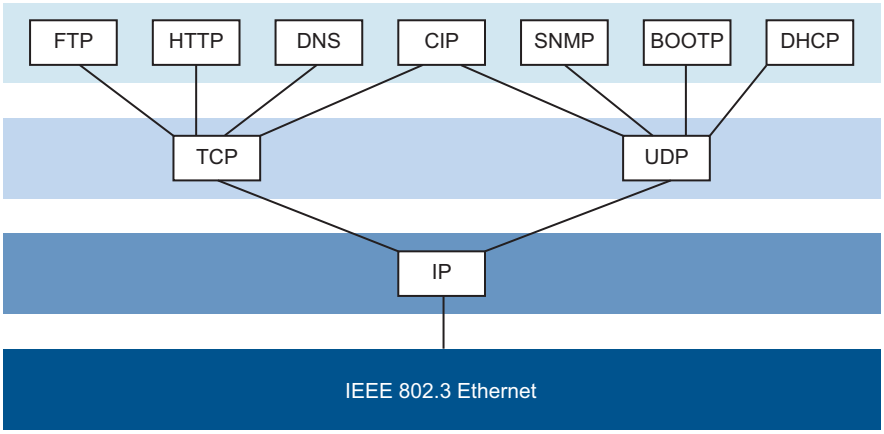


Figure 81 : IEEE802.3 EtherNet/IP

Pour des informations détaillées sur *EtherNet/IP*, voir le site Web ODVA à la page www.odva.org.

16.3.1 Intégration à un système de contrôle

Exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Switching > IGMP Snooping > Global*.
  Vérifiez que la fonction *IGMP Snooping* est activée.
- ☐ Ouvrez la boîte de dialogue *Advanced > Industrial Protocols > EtherNet/IP*.
  Vérifiez que la fonction *EtherNet/IP* est activée.
- ☐ Ouvrez la boîte de dialogue *Advanced > Industrial Protocols > EtherNet/IP*.
- ☐ Pour sauvegarder le fichier EDS en tant qu'archive ZIP sur votre PC, cliquez sur *Download*.
  L'archive ZIP contient le fichier de configuration *EtherNet/IP* et l'icône utilisés pour configurer le contrôleur à connecter à l'équipement.

16.3.2 Paramètres d'entité EtherNet/IP

Les paragraphes suivants permettent d'identifier les objets et opérations pris en charge par l'équipement.

Opérations prises en charge

Tableau 63 : Vue d'ensemble des requêtes EtherNet/IP prises en charge pour les instances des objets

Service Code	Identity Object	TCP/IP Interface Object	Ethernet Link Object	Switch Agent Object	Base Switch Object
0x01 Get Attribute All	All attributes	All attributes	All attributes	All attributes	All attributes
0x02 Set Attribute All	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA)	Settable attributes (0x6, 0x9)	–	–
0x0e Get Attribute Single	All attributes	All attributes	All attributes	All attributes	All attributes
0x10 Set Attribute Single	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA, 0x64)	Settable attributes (0x6, 0x9, 0x65, 0x67, 0x68, 0x69, 0x6C)	Settable attributes (0x5, 0x7)	–
0x05 Reset	Parameter (0x0, 0x1)	–	–	–	–
0x35 Save Configuration Vendor specific	–	–	–	Save switch configuration	–
0x36 Mac Filter Vendor specific	–	–	–	Add MAC filter STRUCT of: USINT VlanId ARRAY of: 6 USINT Mac DWORD PortMask	–

Identity Object

L'équipement prend en charge l'Identity Object (Class Code 0x01) du protocole *EtherNet/IP*. L'ID fabricant de Schneider Electric est 634. Schneider Electric utilise l'ID 44 (0x2C) pour indiquer le type de produit « Managed Ethernet Switch »

Tableau 64 : Attributs d'instance (seule l'instance 1 est disponible)

Id	Attribute	Access Rule	Data type	Description
0x1	Vendor ID	Get	UINT	Schneider Electric634
0x2	Device Type	Get	UINT	Managed Ethernet Switch 44 (0x2C) (0x2C)
0x3	Product Code	Get	UINT	Product Code: mapping is defined for every device type
0x4	Revision	Get	STRUCT of: USINT Major USINT Minor	Revision of the EtherNet/IP implementation, 2.1.
0x5	Status	Get	WORD	Support for the following Bit status only: 0: Owned (always 1) 2: Configured (always 1) 4: Extend Device Status 5: 0x3: No I/O connection established 6: 0x7: At least one I/O connection established, all in idle mode. 7:
0x6	Serial number	Get	UDINT	Serial number of the device (contains last 3 Bytes of MAC address).
0x7	Product name	Get	SHORT-STRING	Displayed as "Schneider Electric" + product family + product ID + software variant.

TCP/IP Interface Object

L'équipement prend uniquement en charge l'instance 1 du TCP/IP Interface Object (Class Code 0xF5) de *EtherNet/IP*.

En fonction de l'état de l'accès en écriture, l'équipement sauvegarde la configuration complète dans sa mémoire flash. La sauvegarde du fichier de configuration peut prendre jusqu'à 10 secondes. Si le processus d'enregistrement est interrompu, par exemple en raison d'une panne de l'alimentation en tension, le fonctionnement de l'équipement peut être impossible.

Commentaire : L'équipement répond à la modification de la configuration `Get Request` au moyen d'une `Response` bien que la configuration n'ait pas encore été entièrement sauvegardée.

Tableau 65 : Attributs de classe

Id	Attribute	Access Rule	Data type	Description
0x1	Revision	Get	UINT	Revision of this object: 3
0x2	Max Instance	Get	UINT	Maximum instance number: 1
0x3	Number of instance	Get	UINT	Number of object instances currently created: 1

Tableau 66 : Attributs d'instance 1

Id	Attribute	Access Rule	Data type	Description
0x1	Status	Get	DWORD	0: Interface Status (0=Interface not configured, 1=Interface contains valid config) 6: ACD status (default 0) 7: ACD fault (default 0)
0x2	Interface Capability flags	Get	DWORD	0: BOOTP Client 1: DNS Client 2: DHCP Client 3: DHCP-DNS Update 4: Configuration setable (within CIP) Other bits reserved (0) 7: ACD capable (0=not capable, 1=capable)
0x3	Config Control	Set/Get	DWORD	0: 1: 2: 3: 0x0=using stored config 0x1=using BOOTP 0x2=using DHCP 4: One device uses DNS for name lookup (always 0 because it is not supported) Other bits reserved (0)
0x4	Physical Link Object	Get	STRUCT of: UINT PathSize EPATH Path	Path to the Physical Link Object, always {0x20, 0xF6, 0x24, 0x01} describing instance 1 of the Ethernet Link Object.
0x5	Interface Configuration	Set/Get	STRUCT of: UDINT IpAddress UDINT Netmask UDINT GatewayAddress UDINT NameServer1 UDINT NameServer2 STRING DomainName	IP Stack Configuration (IP-Address, Netmask, Gateway, 2 Name servers (DNS, if supported) and the domain name).
0x6	Host Name	Set/Get	STRING	Host Name (for DHCP DNS Update)
0x7	Safety Network Number			Not supported
0x8	TTL Value	Get/Set	USINT	Time to live value for IP multicast packets Range 1..255 (default = 1)

Tableau 66 : Attributs d'instance 1 (cont

Id	Attribute	Access Rule	Data type	Description
0x9	Mcast Config	Get/Set	STRUCT of: USINT AllocControl USINT reserved UINT NumMcast UDINT McastStartAddr	Alloc Control = 0 Number of IP multicast addresses = 32 Multicast start address = 239.192.1.0
0xA	Selected Acd	Get/Set	BOOL	0=ACD disable 1=ACD enable (default)
0xB	Last Conflict Detected	Get	STRUCT of: USINT AcdActivity ARRAY of: 6 USINT RemoteMac ARRAY of: 28 USINT ArpPdu	ACD Diagnostic Parameters

Tableau 67 : Extensions Schneider Electric du TCP/IP Interface Object

Id	Attribute	Access Rule	Data type	Description
0x64	Cable Test	Set/Get	STRUCT of: USINT Interface USINT Status	Interface Status (1=Active, 2=Success, 3=Failure, 4=Uninitialized)
0x65	Cable Pair Size	Get	USINT	Size of the Cable Test Result STRUCT of: 2 Pair for 100BASE 4 Pair for 1000BASE

Tableau 67 : Extensions Schneider Electric du TCP/IP Interface Object (cont

Id	Attribute	Access Rule	Data type	Description

0x66	Cable Test Result	Get	STRUCT of:
			USINT Interface
			USINT CablePair
			USINT CableStatus
			USINT CableMinLength
			USINT CableMaxLength
			USINTCableFailureLocation
				100BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}
				1000BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair3, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair4, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}

Ethernet Link object

Les informations des deux tables font partie de l'Ethernet Link Object. Pour accéder à ces informations, utilisez les valeurs suivantes :

- Class(####)
- Instance(###)
- Attribute(#)

Par exemple, les valeurs *class*, *instance* et *attribute* pour accéder aux informations de l'alarme d'utilisation à l'aide d'un message explicite sont :
- Class = 0xF6
- Instance = 1
- Attribute = 6

Tableau 68 : Attributs d'instance et Schneider Electric extensions à l'Ethernet Link Object

Id	Attribute	Access Rule	Data type	Description
Attributs d'instance				
0x1	Interface Speed	Get	UDINT	Used interface speed in MBit/s (10, 100, 1000, …). 0 is used when the speed has not been determined or is invalid because of detected errors.
0x2	Interface Flags	Get	DWORD	Interface Status Flags: 0: Link State (0=No link, 1=Link) 1: Duplex mode (0=Half, 1=Full) 2: Auto-Negotiation Status 3: 0x0=Auto-Negotiation in progress 4: 0x1=Auto-Negotiation failed 0x2=Failed but speed detected 0x3=Auto-Negotiation success 0x4=No Auto-Negotiation 5: Manual configuration require reset (always 0 because it is not needed) 6: Hardware error
0x3	Physical Address	Get	ARRAY of: 6 USINT	MAC address of physical interface
0x4	Interface Counters	Get	STRUCT of: UDINT MibIICounter1 UDINT MibIICounter2 …	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors
0x5	Media Counters	Get	STRUCT of: UDINT EthernetMib Counter1 UDINT EthernetMib Counter2 …	Erreurs détectées : Alignment, FCS, single collision, multiple collision, SQE Test, deferred transmissions, late collisions, excessive collisions, MAC TX, carrier sense, frame too long, MAC RX

Tableau 68 : Attributs d'instance et Schneider Electric extensions à l'Ethernet Link Object (cont

Id	Attribute	Access Rule	Data type	Description
0x6	Interface Control	Get/Set	STRUCT of:	Control Bits:
			WORD ControlBits	0: Auto-negotiation enable/disable (0=disable, 1=enable)
				1: Duplex mode (0=Half, 1=Full), if Auto-negotiation disabled
			UINT ForcedInterface Speed	Interface speed in MBits/s: 10,100,…, if Auto-negotiation disabled
0x7	Interface type	Get	USINT	Type of interface: 0: Unknown interface type 1: The interface is internal 2: Twisted-pair 3: Optical fiber
0x8	Interface state	Get	USINT	Current state of the interface: 0: Unknown interface state 1: The interface is enabled 2: The interface is disabled 3: The interface is testing
0x9	Admin State	Set/Get	USINT	Administrative state: 1: Enable the interface 2: Disable the interface
0xA	Interface label	Get	SHORT-STRING	Human readable ID
Extensions Schneider Electric de l'Ethernet Link Object				
0x64	Ethernet Interface Index	Get	USINT	Interface/Port Index (ifIndex out of MIBII)
0x65	Port Control	Get/Set	DWORD	0: Link state (0=link down, 1=link up)
				1: Link admin state (0=disabled, 1=enabled)
				8: Access violation alarm (read-only)
				9: Utilization alarm (read-only)
0x66	Interface Utilization	Get	USINT	The existing Counter out of the private MIB hm2IDiagfaceUtilization is used. Utilization in percentage (Unit 1%=100, %/100). RX Interface Utilization.
0x67	Interface Utilization Alarm Upper Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmUpperThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Upper Limit.
0x68	Interface Utilization Alarm Lower Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Lower Limit.
0x69	Broadcast limit	Get/Set	USINT	Broadcast limiter Service (Egress BC-Frames limitation, 0=disabled), Frames/second

Tableau 68 : Attributs d'instance et Schneider Electric extensions à l'Ethernet Link Object (cont

Id	Attribute	Access Rule	Data type	Description
0x6A	Ethernet Interface Description	Get/Set	STRING	Interface/Port Description (from MIB II ifDescr), for example "Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX" or "unavailable", max. 64 Bytes.
0x6B	Port Monitor	Get/Set	DWORD	0: Link Flap (0=Off, 1=On)
				1: CRC/Fragment (0=Off, 1=On)
				2: Duplex Mismatch (0=Off, 1=On)
				3: Overload-Detection (0=Off, 1=On)
				4: Link-Speed/ Duplex Mode (0=Off, 1=On)
				5: Deactivate port action (0=Off, 1=On)
				6: Send trap action (0=Off, 1=On)
				7: Active Condition (displays which condition caused an action to occur) 00001_B: Link Flap 00010_B: CRC/Fragments 00100_B: Duplex Mismatch 01000_B: Overload-Detection 10000_B: Link-Speed/ Duplex mode
				8:
				9:
				10:
				11:
				12: Reserved (always 0)
				13: Reserved (always 0)
				14: Reserved (always 0)
				15: Reserved (always 0)
0x6C	Quick Connect	Get/Set	USINT	Quick Connect on the interface (0=Off, 1=On) If you enable Quick Connect, then the device sets the port speed to 100FD, disables Auto-Negotiation, and Spanning Tree on the interface.
0x6D	SFP Diagnostics	Get	STRUCT of:	
			STRING ModuleType	
			SHORT-STRING SerialNumber	
			USINT Connector	
			USINT Supported	
			DINT Temperature	in °C
			DINT TxPower	in mW
			DINT RxPower	in mW
			DINT RxPower	in dBm
			DINT TxPower	in dBm

Tableau 69 : Affectation des ports aux instances Ethernet Link Object

Ethernet Port	Ethernet Link Object Instance
CPU	1
1	2
2	3
3	4
4	5
…	…

Commentaire : Le nombre de ports dépend du type de matériel utilisé. L'Ethernet Link Object existe uniquement lorsque le port est connecté.

Switch Agent Object

L'équipement prend en charge le Ethernet Switch Agent Object spécifique à Schneider Electric (Class Code 0x95) pour la configuration de l'équipement et les paramètres d'information avec l'instance 1.

Tableau 70 : Attributs de classe

Id	Attribute	Access Rule	Data type	Description	
0x1	Switch Status	Get	DWORD	0:	Like the signal contact, the value indicates the Device Overall state (0=ok, 1=failed)
				1:	Device Security Status (0=ok, 1=failed)
				2:	Power Supply 1 (0=ok, 1=failed)
				3:	Power Supply 2 (0=ok, 1=failed or not existing)
				4:	Reserved
				5:	Reserved
				6:	Signal Contact 1 (0=closed, 1=open)
				7:	Signal Contact 2 (0=closed, 1=open or not existing)
				8:	Reserved
				9:	Temperature (0=ok, 1=failure)
				10:	Module removed (1=removed)
				11:	EAM removed (1=removed)
				12:	EAM-SD removed (1=removed)
				13:	Reserved
				14:	Reserved
				15:	Reserved
				16:	Reserved
				17:	Reserved
				18:	Reserved
				19:	Reserved
				20:	Reserved
				21:	Reserved
				22:	Reserved
				23:	MRP (0=disabled, 1=enabled)
				24:	Reserved
				25:	Reserved
				26:	RSTP (0=disabled, 1=enabled)
				27:	LAG (0=disabled, 1=enabled)
				28:	Reserved
				29:	Reserved
				30:	Reserved
				31:	Connection Error (1=failure)

Tableau 70 : Attributs de classe (cont

Id	Attribute	Access Rule	Data type	Description
0x2	Switch Temperature	Get	STRUCT of:	
			INT TemperatureF	in °F
			INT TemperatureC	in °C
0x3	Reserved	Get	UDINT	Reserved for future use (always 0)
0x4	Switch Max Ports	Get	UINT	Maximum number of Ethernet Switch Ports
0x5	Multicast Settings (IGMP Snooping)	Get/Set	WORD	0: IGMP Snooping (0=disabled, 1=enabled) 1: IGMP Querier (0=disabled, 1=enabled) 2: IGMP Querier Mode (read-only) (0=Non-Querier, 1=Querier) 3: 4: 5: 6: 7: IGMP Querier Packet Version Off=0 IGMP Querier disabled V1=1 V2=2 V3=3 8: 9: 10: Treatment of Unknown Multicasts: 0=Send To All Ports 2=Discard
0x6	Switch Existing Ports	Get	ARRAY of: DWORD	Bitmask of existing switch ports Per bit starting with Bit 0 (=Port 1) (0=Port not available, 1=Port existing) Array (bit mask) size is adjusted to the size of maximum number of switch ports (for max. 28 Ports 1 DWORD is used)
0x7	Switch Port Control	Get/Set	ARRAY of: DWORD	Bitmask Link Admin Status switch ports Per bit starting with Bit 0 (=Port 1) (0=Port enabled, 1=Port disabled) Array (bit mask) size is adjusted to the size of maximum number of Switch ports (for max. 28 Ports 1 DWORD is used)
0x8	Switch Ports Mapping	Get	ARRAY of: USINT	Instance number of the Ethernet-Link-Object Starting with Index 0 (=Port 1) All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N, maximum number of ports). When the entry is 0, the Ethernet Link Object for this port does not exist

Tableau 70 : Attributs de classe (cont

Id	Attribute	Access Rule	Data type	Description
0x9	Switch Action Status	Get	DWORD	Status of the last executed action (for example config save, software update, etc.)
				0: Flash Save Configuration In Progress/Flash Write In Progress
				1: Flash Save Configuration Failed/Flash Write Failed
				4: Configuration changed (configuration not in sync. between running configuration

L'Ethernet Switch Agent Object spécifique à Schneider Electric vous fournit le service supplémentaire spécifique au fournisseur correspondant au Service Code 0x35 permettant de sauvegarder la configuration du commutateur. Lorsque vous envoyez une requête depuis votre PC pour sauvegarder une configuration de l'équipement, l'équipement sauvegarde la configuration dans la mémoire flash puis envoie une réponse.

Base Switch object

Le Base Switch object fournit l'interface CIP de niveau application vers les informations d'état de base pour un commutateur Ethernet géré (révision 1).

Seule l'instance 1 du commutateur de base (Class Code 0x51) est disponible.

Tableau 71 : Attributs d'instance

Id	Attribute	Access Rule	Data type	Description
0x1	Device Up Time	Get	UDINT	Time since the device powered up
0x2	Total port count	Get	UDINT	Number of physical ports
0x3	System Firmware Version	Get	SHORT-STRING	Human readable representation of System Firmware Version
0x4	Power source	Get	WORD	Status of switch power source
0x5	Port Mask Size	Get	UINT	Number of DWORD in port array attributes
0x6	Existing ports	Get	ARRAY of:	Port Mask
			DWORD	
0x7	Global Port Admin State	Get	ARRAY of:	Port Admin Status
			DWORD	
0x8	Global Port link Status	Get	ARRAY of:	Port Link Status
			DWORD	
0x9	System Boot Loader Version	Get	SHORT-STRING	Readable System Firmware Version
0xA	Contact Status	Get	UDINT	Switch Contact Closure

Tableau 71 : Attributs d'instance (cont

Id	Attribute	Access Rule	Data type	Description
0xB	Aging Time	Get	UDINT	Range 10..1000000 · 1/10 seconds (default=300) 0=Learning off
0xC	Temperature C	Get	UINT	Switch temperature in degrees Celsius
0xD	Temperature F	Get	UINT	Switch temperature in degrees Fahrenheit

RSTP Bridge Object (MCSESM-E)

Le RSTP est un protocole Layer 2 qui permet d'utiliser une topologie Ethernet redondante (une topologie en anneau par exemple). Le RSTP est spécifié au chapitre 17 de la standardisation IEEE 802.1D-2004.

L'équipement prend en charge le pont RSTP spécifique à Schneider Electric (Class Code 64_H, 100) pour les paramètres de configuration et d'information du l'équipement.

L'équipement prend en charge 2 instances :
- L'instance 1 représente l'instance RSTP primaire du pont et
- l'instance 2 représente l'instance RSTP secondaire (Dual).

Pour plus d'informations sur ces paramètres et pour savoir comment les régler, veuillez consulter le manuel de référence « Interface utilisateur graphique ».

Tableau 72 : Schneider Electric RSTP Bridge Object

Id	Attribute	Access rule	Data type	Description
1	Bridge Identifier Priority	Set	UDINT	Range: 0 to 61,440 in steps of 4,096, default: 32,768 (refer to IEEE, 802.1D-2004, § 17.13.7)
2	Transmit Hold Count	Set	UINT	Range: 1 to 40, default: 10 (refer to IEEE 802.1D-2004, §17.13.12)
3	Force Protocol Version	Set	UINT	Default:2 (refer to IEEE 802.1D-2004, §17.13.4 and dot1dStpVersion in RFC 4318)
4	Bridge Hello Time	Set	UDINT	Range: 100 to 200, unit: centi-seconds (1/100 of a second), default: 200 (refer to IEEE 802.1D-2004, §17.13.6 and dot1dStpHoldTime in RFC 4188)
5	Bridge Forward Delay	Set	UDINT	Range: 400 to 3000, unit: centi-seconds, default: 2100 (refer to IEEE 802.1D-2004, §17.13.5 and dot1dStpForwardDelay in RFC 4188)
6	Bridge Max. Age	Set	UINT	Range: 600 to 4000, unit: centi-seconds, default: 4000 (refer to IEEE 802.1D-2004, §17.13.8 and dot1dStpBridgeMaxAge in RFC 4188)

Tableau 72 : Schneider Electric RSTP Bridge Object (cont

Id	Attribute	Access rule	Data type	Description
7	Time Since Topology Change	Get	UDINT	Unit: centi-seconds (refer to dot1dStpTimeSinceTopologyChange in RFC 4188)
8	Topology Change	Get	UDINT	Refer to dot1dStpTopChanges in RFC 4188
100	InnerPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance‘s inner port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance‘s inner port.
101	OuterPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance‘s outer port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance‘s outer port.

RSTP Port Object (MCSESM-E)

L'équipement prend en charge le port RSTP spécifique à Schneider Electric (Class Code 65_H, 101) pour les paramètres de configuration et d'information RSTP avec au moins une instance (instance 1).

L'instance 1 représente la CPU Ethernet Interface, l'instance 2 représente le 1er port physique, l'instance 3 le 2e port physique, etc.

Pour plus d'informations sur ces paramètres et pour savoir comment les régler, veuillez consulter le manuel de référence « Interface utilisateur graphique ».

Tableau 73 : Schneider Electric RSTP Port Object

Id	Attribute	Access rule	Data type	Description
1	Port Identifier Priority	Set	UDINT	Range: 0 to 240 in steps of 16, default: 128 (refer to IEEE, 802.1D-2004, § 17.13.10).
2	mcheck	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.19.13 and dot1dStpPortProtocolMigration in RFC 4318).
3	Port Path Cost	Set	UDINT	Range: 1 to 200,00,000, default:auto (0) (refer to IEEE 802.1D-2004, §17.13.11 and dot1dStpPortAdminPathCost in RFC 4318).
4	Port Admin Edge Port	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.13.1 and dot1dStpPortAdminEdgePort in RFC 4318).
5	Port Oper Edge Port	Get	BOOL	True (1), False (2) (refer to dot1dStpPortOperEdgePort in RFC 4318).
6	Port Admin PointToPoint	Set	UINT	forceTrue (0), forceFalse (1), auto (2) (refer to dot1dStpPortAdminPointToPoint in RFC 4318).

Tableau 73 : Schneider Electric RSTP Port Object (cont

Id	Attribute	Access rule	Data type	Description
7	Port Oper PointToPoint	Get	UINT	True (1), False (2) (refer to dot1dStpPortOperPointToPoint in RFC 4318).
8	Port Enable	Set	UINT	Enabled (1), Disabled (2) (Refer to dot1dStpPortEnable in RFC 4188).
9	Port State	Get	UINT	Disabled (1), Blocking (2), Listening (3), Learning (4), Forwarding (5), Broken (6) (refer to dot1dStpPortState in RFC 4188).
10	Port Role	Get	UNT	Unknown (0), Alternate/Backup (1), Root (2), Designated (3) (refer to dot1dStpTopChanges in RFC 4188).
100	DRSTP	Get	UINT	Schneider Electric-specific object. True (1), False (2).

Services, connexions et données I/O

L'équipement prend en charge les types et paramètres de connexion suivants.

Tableau 74 : Réglages pour l'intégration d'un nouveau module

Setting	I/O connection	Input only	Listen only
Comm Format:	Data - DINT	Data - DINT	Input Data - DINT - Run/Program
IP Address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	100	100	100
Input Size	32	32	32
Output Assembly Instance	150	152	153
Output Size	32	0	0
Configuration Assembly Instance	151	151	151
Data Size	10	10	10

Tableau 75 : Structure des données I/O de l'équipement

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
Device Status	Bitmask (see Switch Agent Attribute 0x1)	Input	DWORD
Link Status	Bitmask, 1 Bit per port (0=No link, 1=Link up)	Input	DWORD
Output Links Admin State applied	Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, for example for controller access port. (0=Port enabled, 1=Port disabled)	Input	DWORD
Utilization Alarm[2]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD

Tableau 75 : Structure des données I/O de l'équipement (cont

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
Access Violation Alarm[3]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Multicast Connections	Integer, number of connections	Input	DINT
TCP/IP Connections	Integer, number of connections	Input	DINT
Quick Connect Mask	Bitmask (1 Bit per port) (0=Quick Connect disabled, 1=Quick Connec enabled)	Input	DINT
Link Admin State	Bitmask, 1 Bit per port (0=Port enabled, 1=Port disabled)	Output	DWORD

1. La taille par défaut des masques de bits de port est de 32 bits (DWORD). Pour les équipements présentant plus de 28 ports, les masques de bits de port ont été étendus à n * DWORD.
2. Vous spécifiez les réglages de l'alarme d'utilisation dans la boîte de dialogue *Basic Settings > Port*, onglet *Utilization*. Le seuil supérieur est la limite à laquelle la condition de l'alarme est activée. Le seuil inférieur est la limite à laquelle la condition de l'alarme est désactivée.
3. La boîte de dialogue *Network Security > Port Security* permet de spécifier les réglages de l'alarme de violation d'accès. Le seuil supérieur est la limite à laquelle la condition de l'alarme est activée. Le seuil inférieur est la limite à laquelle la condition de l'alarme est désactivée.

Tableau 76 : Association des types de données aux tailles de bit

Type d'objet	Taille de bit
BOOL	1 bit
DINT	32 bit
DWORD	32 bit
SHORT-STRING	max. 32 bytes
STRING	max. 64 bytes
UDINT	32 bit
UINT	16 bit
USINT	8 bit
WORD	16 bit

A Préparation de l'environnement de configuration

A.1 Configuration d'un serveur DHCP/BOOTP

L'exemple suivant décrit la configuration d'un serveur DHCP à l'aide du logiciel haneWIN DHCP Server. Ce shareware est un produit de IT-Consulting Dr. Herbert Hanewinkel. Vous pouvez télécharger le logiciel depuis www.hanewin.net. Vous pouvez tester le logiciel pendant 30 jours calendaires à partir de la date de première installation, puis décider si vous souhaitez acheter une licence.

Exécutez les étapes suivantes :

- ☐ Installez le serveur DHCP sur votre PC.
  Pour exécuter l'installation, suivez l'assistant d'installation.
- ☐ Lancez le programme *haneWIN DHCP Server*.

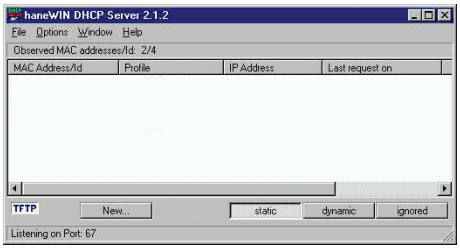


Figure 82 : Démarrez la fenêtre du programme haneWIN DHCP Server

Commentaire : Lorsque Windows est activé, l'installation comporte un service qui, dans la configuration de base, démarre automatiquement. Ce service est également actif bien que le programme lui-même n'ait pas été lancé. Une fois lancé, le service répond aux requêtes DHCP.

- ☐ Dans la barre de menus, cliquez sur les éléments *Options > Preferences* pour ouvrir la fenêtre des paramètres du programme.
- ☐ Sélectionnez l'onglet *DHCP*.
- ☐ Spécifiez les réglages affichés dans la figure.

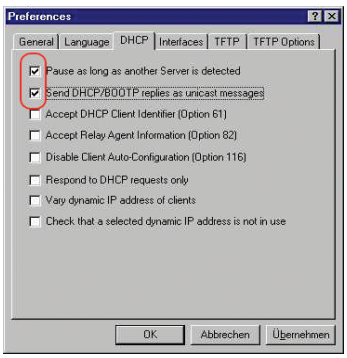


Figure 83 : Réglage DHCP

- ☐ Cliquez sur le bouton *OK*.
- ☐ Pour saisir les profils de configuration, cliquez sur les éléments *Options > Configuration Profiles* dans la barre de menus.

☐ Spécifiez le nom du nouveau profil de configuration.

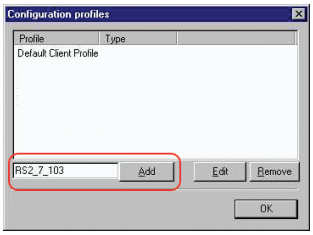


Figure 84 : Ajout des profils de configuration

☐ Cliquez sur le bouton *Add*.
☐ Spécifiez le masque réseau.

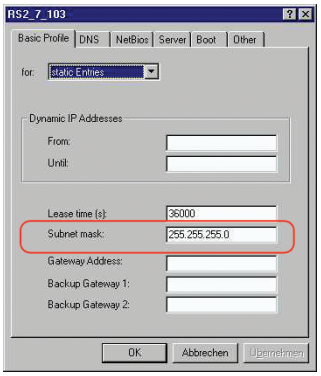


Figure 85 : Masque réseau dans le profil de configuration

☐ Cliquez sur le bouton *Apply*.
☐ Sélectionnez l'onglet *Boot*.
☐ Indiquez l'adresse IP de votre serveur tftp.
☐ Saisissez le chemin et le nom du fichier de configuration.

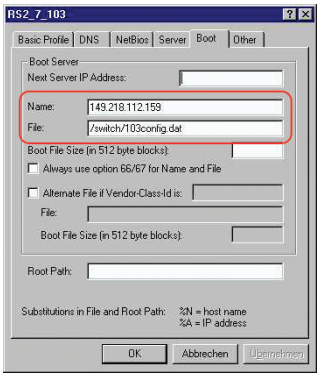


Figure 86 : Fichier de configuration sur le serveur tftp

☐ Cliquez sur le bouton *Apply*, puis sur le bouton *OK*.

☐ Ajoutez un profil pour chaque type d'équipement.
Lorsque les équipements du même type disposent de configurations différentes, ajoutez un profil pour chaque configuration.

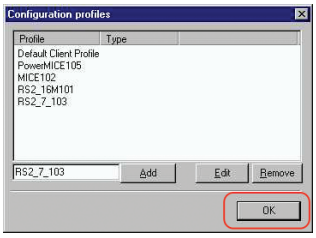


Figure 87 : Administration des profils de configuration

☐ Pour confirmer l'ajout des profils de configuration, cliquez sur le bouton *OK*.
☐ Pour saisir les adresses statiques, dans la fenêtre principale, cliquez sur le bouton *Static*.

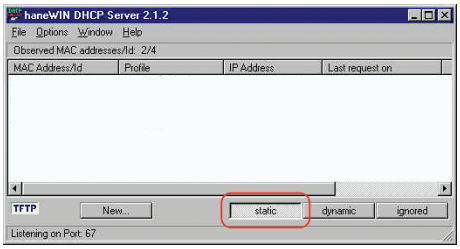


Figure 88 : Saisie d'adresses statiques

☐ Cliquez sur le bouton *Add*.

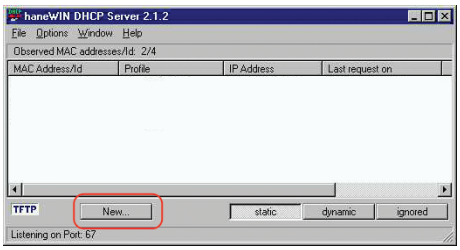


Figure 89 : Ajout des adresses statiques

☐ Saisissez l'adresse MAC de l'équipement.
☐ Saisissez l'adresse IP de l'équipement.

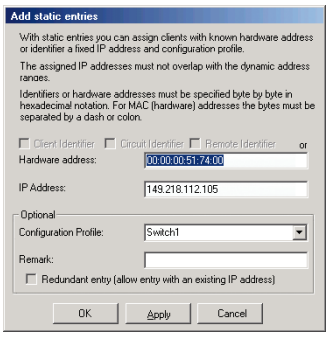


Figure 90 : Entrées des adresses statiques

☐ Sélectionnez le profil de configuration de l'équipement.

- ☐ Cliquez sur le bouton *Apply*, puis sur le bouton *OK*.
- ☐ Ajoutez une entrée pour chaque équipement devant recevoir ses paramètres du serveur DHCP.

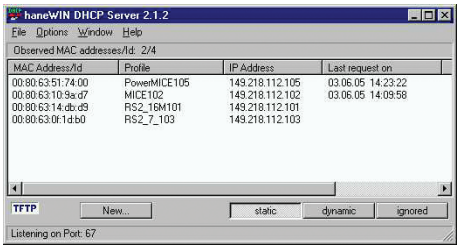


Figure 91 : Serveur DHCP avec entrées

A.2 Configuration d'un serveur DHCP avec l'option 82

L'exemple suivant décrit la configuration d'un serveur DHCP à l'aide du logiciel haneWIN DHCP Server. Ce shareware est un produit de IT-Consulting Dr. Herbert Hanewinkel. Vous pouvez télécharger le logiciel depuis www.hanewin.net. Vous pouvez tester le logiciel pendant 30 jours calendaires à partir de la date de première installation, puis décider si vous souhaitez acheter une licence.

Exécutez les étapes suivantes :

- ☐ Installez le serveur DHCP sur votre PC.
  Pour exécuter l'installation, suivez l'assistant d'installation.
- ☐ Lancez le programme *haneWIN DHCP Server*.

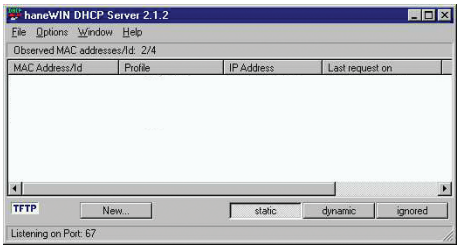


Figure 92 : Démarrez la fenêtre du programme haneWIN DHCP Server

Commentaire : Lorsque Windows est activé, l'installation comporte un service qui, dans la configuration de base, démarre automatiquement. Ce service est également actif bien que le programme lui-même n'ait pas été lancé. Une fois lancé, le service répond aux requêtes DHCP.

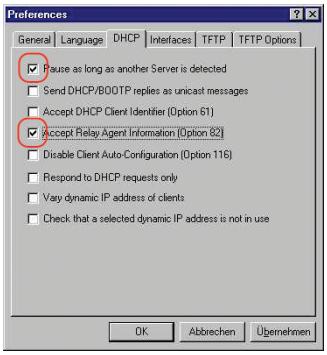


Figure 93 : Réglage DHCP

- ☐ Pour saisir les adresses statiques, cliquez sur le bouton *Add*.

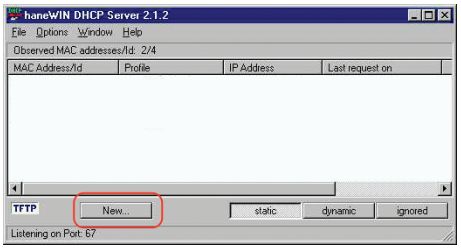


Figure 94 : Ajout des adresses statiques

- ☐ Cochez la case *Circuit Identifier*.
- ☐ Cochez la case *Remote Identifier*.

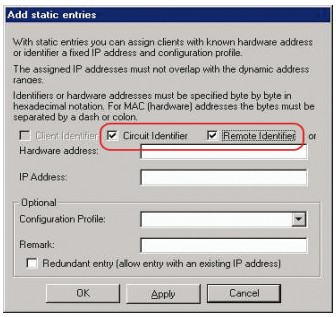


Figure 95 : Réglage par défaut pour l'attribution fixe d'adresses

- ☐ Dans le champ *Hardware address*, spécifiez les valeurs *Circuit Identifier* et *Remote Identifier* pour le commutateur et le port.
  Le serveur DHCP attribue l'adresse IP spécifiée dans le champ *IP address* à l'équipement que vous connectez au port spécifié dans le champ *Hardware address*.
  L'adresse matérielle présente le format suivant :
  `ciclvvvvssmmpprirlxxxxxxxxxxxx`
  - `ci`
    Sous-identifiant pour le type de l'ID circuit
  - `cl`
    Longueur de l'ID circuit.
  - Identifiant Schneider Electric :
    `01` lorsqu'un équipement Schneider Electric est connecté au port, sinon `00`.
  - `vvvv`
    VLAN-ID de la requête DHCP.
    Réglage par défaut : `0001` = VLAN 1
  - `ss`
    Prise de l'équipement sur laquelle est situé le module avec le port auquel l'équipement est

connecté. Spécifiez la valeur `00`.

- `mm`
  Module avec le port auquel l'équipement est connecté.
- `pp`
  Port auquel l'équipement est connecté.
- `ri`
  Sous-identifiant pour le type de l'ID distant
- `rl`
  Longueur de l'ID distant.
- `xxxxxxxxxxxx`
  ID distant de l'équipement (par exemple, adresse MAC) auquel l'équipement est connecté.

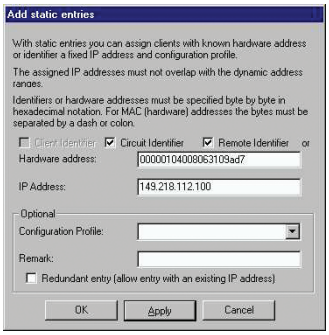


Figure 96 : Spécification des adresses

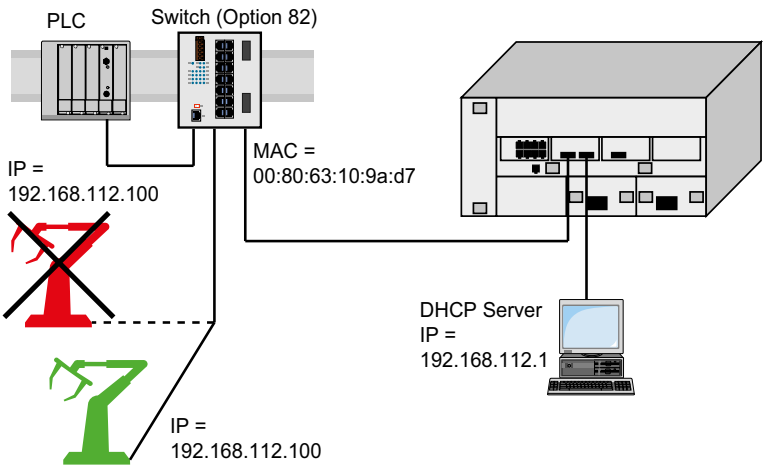


Figure 97 : Exemple d'utilisation de l'option 82

A.3 Préparation de l'accès via SSH

Vous pouvez vous connecter à l'équipement à l'aide du protocole SSH. Pour ce faire, exécutez les étapes suivantes :

- Génère une clé d'hôte dans l'équipement.
  ou
- Transfère votre propre clé sur l'équipement.
- Préparez l'accès à l'équipement dans le programme client SSH.

Commentaire : Avec le réglage par défaut, la clé existe déjà et l'accès à l'aide de SSH est activé.

A.3.1 Génération d'une clé d'hôte dans l'équipement

L'équipement vous permet de générer directement la clé dans l'équipement. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > Server*, onglet *SSH*.
- ☐ Pour désactiver le serveur SSH, sélectionnez le bouton radio `Off` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.
- ☐ Pour créer une clé RSA, dans le cadre *Signature*, cliquez sur le bouton *Create*.
- ☐ Pour activer le serveur SSH, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`ssh key rsa generate`	Générer une nouvelle clé RSA.

A.3.2 Chargement de votre propre clé sur l'équipement

OpenSSH offre aux administrateurs du réseau expérimentés la possibilité de générer leur propre clé. Pour générer la clé, saisissez la commande suivante sur votre PC :

```
ssh-keygen(.exe) -q -t rsa -f rsa.key -C '' -N ''
rsaparam -out rsaparam.pem 2048
```

L'équipement vous permet de transférer votre propre clé SSH sur l'équipement. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > Server*, onglet *SSH*.
- ☐ Pour désactiver le serveur SSH, sélectionnez le bouton radio `Off` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.
- ☐ Lorsque la clé d'hôte est stockée sur votre PC ou sur un lecteur réseau, glissez-déposez le fichier qui contient la clé dans la zone ⬆. Vous pouvez également cliquer sur la zone pour sélectionner le fichier.

- ☐ Cliquez sur le bouton *Start* dans le cadre *Key import* pour charger la clé sur l'équipement.
- ☐ Pour activer le serveur SSH, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

Exécutez les étapes suivantes :
- ☐ Copiez la clé auto-générée de votre PC vers la mémoire externe.
- ☐ Copiez la clé de la mémoire externe vers l'équipement.

`enable`	Basculez sur le mode Privileged EXEC.
`copy sshkey envm <file name>`	Charger votre propre clé sur l'équipement depuis la mémoire externe.

A.3.3 Préparation du programme client SSH

Le programme *PuTTY* vous permet d'accéder à l'équipement à l'aide du protocole SSH. Vous pouvez télécharger le logiciel depuis www.putty.org.

Exécutez les étapes suivantes :
- ☐ Lancez le programme en double-cliquant dessus.

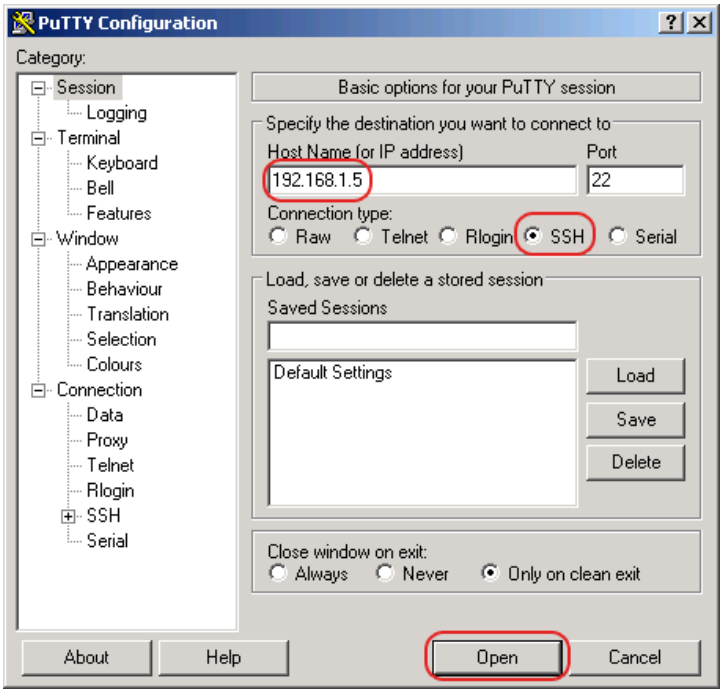


Figure 98 : Écran de saisie PuTTY

- ☐ Spécifiez l'adresse IP de votre équipement dans le champ *Host Name (or IP address)*. L'adresse IP (a.b.c.d) se compose de 4 nombres décimaux présentant des valeurs allant de `0` à `255`. Les 4 nombres décimaux sont séparés par des points.
- ☐ Pour sélectionner le type de connexion, sélectionnez le bouton radio *SSH* dans la liste d'options *Connection type*.
- ☐ Cliquez sur le bouton *Open* pour établir la liaison de données avec votre équipement.

Avant que la liaison de données soit établie, le programme *PuTTY* affiche un messages d'alarme de sécurité et vous permet de vérifier l'empreinte de la clé.

Figure 99 : Question de sécurité relative à l'empreinte

Avant que la liaison de données soit établie, le programme *PuTTY* affiche un messages d'alarme de sécurité et vous permet de vérifier l'empreinte de la clé.

- ☐ Vérifiez l'empreinte de la clé pour vous assurer que vous avez effectivement établi la liaison avec l'équipement souhaité.
- ☐ Lorsque l'empreinte correspond à votre clé, cliquez sur le bouton *Yes*.

Pour les administrateurs du réseau expérimentés, une autre manière d'accéder à votre équipement via un protocole SSH consiste à utiliser OpenSSH Suite. Pour établir la liaison de données, saisissez la commande suivante :

```
ssh admin@10.0.112.53
```

`admin` est le nom d'utilisateur.

`10.0.112.53` est l'adresse IP de votre équipement.

A.4 Certificat HTTPS

Votre navigateur Web établit la connexion à l'équipement à l'aide du protocole HTTPS. Il convient pour cela que la fonction *HTTPS server* soit préalablement activée dans l'onglet *HTTPS* de la boîte de dialogue *Device Security > Management Access > Server*.

Commentaire : Les logiciels tiers tels que les navigateurs Web valident des certificats basés sur des critères tels que la date d'expiration et les recommandations de paramètres cryptographiques actuelles. Les certificats périmés peuvent causer des problèmes dus à des informations non valides ou obsolètes. Exemple : un certificat expiré ou des recommandations cryptographiques changées. Pour résoudre les conflits de validation avec des logiciels tiers, transférez votre propre certificat mis à jour sur votre équipement ou regénérez le certificat avec le dernier firmware.

A.4.1 Gestion des certificats HTTPS

Un certificat standard selon la norme technique X.509/PEM (infrastructure à clés publiques) est requis pour le chiffrement. Avec le réglage par défaut, un certificat auto-généré est déjà présent dans l'équipement. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > Server*, onglet *HTTPS*.
- ☐ Pour créer un certificat X509/PEM, dans le cadre *Certificate*, cliquez sur le bouton *Create*.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.
- ☐ Redémarrez le serveur HTTPS pour activer la clé. Redémarrez le serveur à l'aide de l'interface de ligne de commande.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`https certificate generate`	Générer un certificat X.509/PEM https.
`no https server`	Désactiver la fonction *HTTPS*.
`https server`	Activer la fonction *HTTPS*.

☐ L'équipement vous permet de transférer un certificat X.509/PEM généré de façon externe sur l'équipement :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > Server*, onglet *HTTPS*.
- ☐ Lorsque le certificat est stocké sur votre PC ou sur un lecteur réseau, glissez-déposez le certificat dans la zone  . Vous pouvez également cliquer sur la zone pour sélectionner le certificat.
- ☐ Cliquez sur le bouton *Start* pour copier le certificat sur l'équipement.
- ☐ Sauvegardez les modifications temporairement. Pour ce faire, cliquez sur le bouton ✓.

`enable`	Basculez sur le mode Privileged EXEC.
`copy httpscert envm <file name>`	Copier le certificat HTTPS à partir de la mémoire externe non volatile.
`configure`	Basculez sur le mode de configuration.
`no https server`	Désactiver la fonction *HTTPS*.
`https server`	Activer la fonction *HTTPS*.

Commentaire : Pour activer le certificat une fois que vous l'avez créé ou transféré, redémarrez l'équipement ou le serveur HTTPS. Redémarrez le serveur HTTPS à l'aide de l'interface de ligne de commande.

A.4.2 Accès via HTTPS

Le réglage par défaut pour la liaison de données HTTPS est le port TCP `443`. Si vous modifiez le numéro du port HTTPS, redémarrez l'équipement ou le serveur HTTPS. La modification devient ainsi effective. Pour ce faire, exécutez les étapes suivantes :

- ☐ Ouvrez la boîte de dialogue *Device Security > Management Access > Server*, onglet *HTTPS*.
- ☐ Afin d'activer cette fonction, sélectionnez le bouton radio `On` dans le cadre *Operation*.
- ☐ Pour accéder à l'équipement via HTTPS, saisissez HTTPS au lieu de HTTP dans votre navigateur, puis saisissez l'adresse IP de l'équipement.

`enable`	Basculez sur le mode Privileged EXEC.
`configure`	Basculez sur le mode de configuration.
`https port 443`	Indique le numéro du port TCP sur lequel le serveur Web reçoit les requêtes HTTPS de la part des clients.
`https server`	Activer la fonction *HTTPS*.
`show https`	Indique l'état du serveur *HTTPS* et le numéro de port.

Lorsque vous modifiez le numéro du port HTTPS, désactivez le serveur HTTPS et réactivez-le afin de rendre la modification effective.

L'équipement utilise le protocole HTTPS et établit une nouvelle liaison de données. Lorsque vous vous déconnectez à la fin de la session, l'équipement met fin à la liaison de données.

B Annexe

B.1 Management Information Base (MIB)

La conception de la Management Information Base (MIB) repose une structure d'arborescence abstraite.

Les points d'embranchement sont les classes d'objet. Les « feuilles » de la MIB sont appelées « classes d'objet générique ».

Lorsqu'elles sont requises à des fins d'identification univoque, les classes d'objet générique sont instanciées. Cela signifie que la structure abstraite est reliée à la réalité en spécifiant le port ou l'adresse source.

Des valeurs (Integer, TimeTicks, Counter ou Octet String) sont attribuées à ces instances. Ces valeurs peuvent être lues et en partie modifiées. L'Object Description ou l'Object-ID (OID) désigne la classe d'objet. Le subidentifier (SID) est utilisé pour les instancier.

Exemple :

La classe d'objet générique `sa2PSState` (`OID` = `1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1`) est la description de l'information abstraite `état de l'alimentation en tension`. Cependant, il n'est pas possible de lire de valeur à l'aide de cette information, dans la mesure où le système ne sait pas quelle alimentation en tension est concernée.

L'indication du subidentifier `2` permet de relier cette information abstraite à la réalité (c'est-à-dire de l'instancier) et de l'identifier ainsi comme état de fonctionnement de l'alimentation en tension `2`. Une valeur est alors affectée à cette instance et peut être lue. L'instance `get 1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1` fournit la réponse `1`, ce qui signifie que l'alimentation en tension est opérationnelle.

Définition des termes de syntaxe utilisés :	
Integer	Nombre entier compris dans l'intervalle -2^{31} - $2^{31}-1$
Adresse IP	`xxx.xxx.xxx.xxx` (`xxx` = nombre entier compris dans l'intervalle `0..255`)
Adresse MAC	Nombre hexadécimal à 12 chiffres selon ISO/CEI 8802-3
Object Identifier	x.x.x.x… (par exemple 1.3.6.1.1.4.1.3833...)
Octet String	Chaîne de caractères ASCII
PSID	Identification de l'alimentation en tension (numéro du bloc d'alimentation)
TimeTicks	Chronomètre, temps écoulé = valeur numérique / 100 (en secondes) valeur numérique = nombre entier compris dans l'intervalle $0-2^{32}-1$
Timeout	Temps en centièmes de seconde temps = nombre entier compris dans l'intervalle $0-2^{32}-1$
Champ du type	Nombre hexadécimal à 4 chiffres selon ISO/CEI 8802-3
Compteur	Nombre entier ($0-2^{32}-1$), lorsque certains événements se produisent, la valeur est augmentée de `1`.

B.2 Liste des RFC

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 855	Telnet Option
RFC 951	BOOTP
RFC 1112	IGMPv1
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2236	IGMPv2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped IP Multicast
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2613	SMON
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 2863	The Interfaces Group MIB
RFC 2865	RADIUS Client
RFC 2866	RADIUS Accounting

RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 2869bis	RADIUS support for EAP
RFC 2933	IGMP MIB
RFC 3164	The BSD Syslog Protocol
RFC 3376	IGMPv3
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3580	802.1X RADIUS Usage Guidelines
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 3621	Power Ethernet MIB
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)
RFC 4188	Definitions of Managed Objects for Bridges
RFC 4251	SSH protocol architecture
RFC 4291	IPv6 Addressing Architecture
RFC 4252	SSH authentication protocol
RFC 4253	SSH transport layer protocol
RFC 4254	SSH connection protocol
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4318	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
RFC 4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
RFC 4836	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 4861	Neighbor Discovery for IPv6
RFC 5321	Simple Mail Transfer Protocol
RFC 6221	Leightweight DHCPv6 Relay Agent
RFC 8200	IPv6 Specification
RFC 8415	DHCPv6

B.3 Normes techniques IEEE de base

IEEE 802.1AB	Station and Media Access Control Connectivity Discovery
IEEE 802.1D	MAC Bridges (switching function)
IEEE 802.1Q	Virtual LANs (VLANs, MRP, Spanning Tree)
IEEE 802.1X	Port Authentication
IEEE 802.3	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control
IEEE 802.3af	Power over Ethernet

B.4 Normes techniques CEI de base

IEC 62439	High availability automation networks MRP – Media Redundancy Protocol based on a ring topology

B.5 Normes techniques ANSI de base

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

B.6 Caractéristiques techniques

16.3.3 Commutation

Taille du tableau d'adresses MAC (filtres statiques inclus)	16384
Nombre max. de filtres d'adresses MAC à configuration statique	100
Nombre max. de filtres d'adresses MAC pouvant être apprises via le IGMP Snooping	1024
Nombre max. d'entrées d'adresses MAC (MMRP)	64
Nombre de files d'attente prioritaires	8 files d'attente
Priorités réglables des ports	0..7
MTU (longueur max. admissible des paquets qu'un port peut recevoir ou transmettre)	9720 octets

16.3.4 VLAN

Plage de VLAN-ID	1..4042
Nombre de VLAN	au max. 128 simultanément par équipement au max. 128 simultanément par port

16.3.5 Listes de contrôle d'accès (ACL)

Nombre max. d'ACL	50
Nombre max. de règles par ACL	256
Nombre max. de règles par port	256
Nombre total de règles configurables	2048 (8 × 256)
Nombre max. d'affectations de VLAN	12
Nombre max. d'affectations de VLAN (sortie)	128
Nombre max. de règles d'entrée (Ingress)	514

B.7 Copyright des logiciels intégrés

Le produit contient entre autres des fichiers de logiciels open source développés par des tiers et mis sous licence open source.

Vous trouverez les termes de la licence dans l'interface utilisateur graphique de la boîte de dialogue *Help > Licenses*.

B.8 Abréviations utilisées

ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DUID	DHCP Unique Identifier
EUI	Extended Unique Identifier
FDB	Forwarding Database
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv6	Internet Protocol version 6
LDRA	Lightweight DHCPv6 Relay Agent
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MRP	Media Redundancy Protocol
NDP	Neighbor Discovery Protocol
NMS	Network Management System
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol

URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

C Index

R

S