Modicon

Commutateur MCSESM, MCSESM-E, MCSESP avec fonctionnalité d'administration Manual de GUI

QGH59087.02

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

Remarques relatives à l'interface utilisateur graphique

L'équipement prend en charge les systèmes d'exploitation suivants :
- Windows 10
- Linux

L'interface utilisateur graphique de l'équipement est divisée comme suit :
- Zone de navigation
- Zone de boîte de dialogue
- Boutons

Zone de navigation

La zone de navigation est située sur le côté gauche de l'interface utilisateur graphique.

La zone de navigation contient les éléments suivants :
- Barre d'outils
- Filtre
- Menu

Vous avez la possibilité de réduire l'ensemble de la zone de navigation, par exemple lorsque vous affichez l'interface utilisateur graphique sur de petits écrans. Pour réduire ou développer la zone, cliquez sur la petite flèche située dans la partie supérieure de la zone de navigation.

Barre d'outils

La barre d'outils située dans la partie supérieure de la zone de navigation contient plusieurs boutons.
- Lorsque vous placez le pointeur de souris au-dessus d'un bouton, une infobulle affiche des informations supplémentaires.
- Lorsque la connexion aux équipements est perdue, la barre d'outils apparaît grisée.

L'équipement réactualise automatiquement les informations de la barre d'outils toutes les 5 secondes.

Pour recharger la barre d'outils manuellement, cliquez sur le bouton.

Lorsque vous placez le pointeur de souris au-dessus d'un bouton, une infobulle affiche les informations suivantes :
- *User:*
  Nom de l'utilisateur connecté
- *Device name:*
  Nom de l'équipement

Cliquez sur ce bouton pour ouvrir la boîte de dialogue *Device Security > User Management*.

Lorsque vous placez le pointeur de souris au-dessus d'un bouton, une infobulle affiche un aperçu de la boîte de dialogue *Diagnostics > System > Configuration Check*.

Cliquez sur ce bouton pour ouvrir la boîte de dialogue *Diagnostics > System > Configuration Check*.

Cliquez sur ce bouton pour déconnecter l'utilisateur actuel et afficher la boîte de dialogue de connexion.

Si le profil de configuration dans la mémoire volatile (*RAM*) et le profil de configuration « Selected » (Sélectionné) dans la mémoire non-volatile (*NVM*) sont différents, l'équipement affiche la boîte de dialogue *Warning*.

- Pour sauvegarder les modifications de façon permanente, cliquez sur le bouton *Yes* dans la boîte de dialogue *Warning*.
- Pour annuler les modifications, cliquez sur le bouton *No* dans la boîte de dialogue *Warning*.

Affiche le temps restant en secondes avant que l'équipement ne déconnecte automatiquement un utilisateur inactif.

Cliquez sur ce bouton pour ouvrir la boîte de dialogue *Device Security > Management Access > Web*. Celle-ci vous permet de spécifier le délai d'attente.

Lorsque le profil de configuration stocké dans la mémoire volatile (*RAM*) diffère du profil de configuration sélectionné (« Selected ») dans la mémoire non volatile (*NVM*), ce bouton est visible. Sinon, ce bouton est masqué.

Cliquez sur ce bouton pour ouvrir la boîte de dialogue *Basic Settings > Load/Save*.

Cliquez avec le bouton droit de la souris pour sauvegarder les réglages actuels dans la mémoire non volatile (*NVM*).

Lorsque vous placez le pointeur de souris au-dessus d'un bouton, une infobulle affiche les informations suivantes :

- *Device Status:* Cette section affiche un aperçu du cadre *Device status* de la boîte de dialogue *Basic Settings > System*. Cette section affiche l'alarme actuellement active et dont la survenue a été enregistrée en premier.
- *Security Status:* Cette section affiche un aperçu du cadre *Security status* de la boîte de dialogue *Basic Settings > System*. Cette section affiche l'alarme actuellement active et dont la survenue a été enregistrée en premier.
- *Boot Parameter:* Lorsque vous sauvegardez définitivement les modifications apportées aux réglages et qu'au moins un paramètre de démarrage diffère du profil de configuration utilisé lors du dernier redémarrage, une remarque apparaît dans cette section.
  Les réglages suivants entraînent la modification des paramètres de redémarrage :
  - Boîte de dialogue *Basic Settings > External Memory*, paramètre *Software auto update*
  - Boîte de dialogue *Basic Settings > External Memory*, paramètre *Config priority*
  - Boîte de dialogue *Device Security > Management Access > Server*, onglet *SNMP*, paramètre *UDP port*
  - Boîte de dialogue *Diagnostics > System > Selftest*, paramètre *RAM test*
  - Boîte de dialogue *Diagnostics > System > Selftest*, paramètre *SysMon1 is available*
  - Boîte de dialogue *Diagnostics > System > Selftest*, paramètre *Load default config on error*

Cliquez sur ce bouton pour ouvrir la boîte de dialogue *Diagnostics > Status Configuration > Device Status*.

Filtre

Le filtre vous permet de réduire le nombre d'options de menu apparaissant dans le menu. Lorsque vous utilisez le filtre, le menu affiche uniquement les options de menu correspondant à la chaîne de recherche saisie dans le champ de filtre.

Menu

Le menu affiche les options de menu.

Vous pouvez filtrer les options de menu. Voir la section « Filtre ».

Pour afficher la boîte de dialogue correspondante dans la zone de boîte de dialogue, cliquez sur l'option de menu souhaitée. Lorsque l'élément de menu sélectionné est un nœud contenant plusieurs sous-options, ce nœud se développe ou se réduit lorsque vous cliquez dessus. La zone de boîte de dialogue continue d'afficher la de dialogue précédemment affichée.

Vous avez la possibilité de réduire ou de développer tous les nœuds du menu simultanément. Lorsque vous cliquez avec le bouton droit de la souris dans le menu, un menu contextuel affiche les entrées suivantes :

- *Expand*
  Développe simultanément tous les nœuds du menu. Le menu affiche les options de menu de l'ensemble des niveaux.
- *Collapse*
  Réduit simultanément tous les nœuds du menu. Le menu affiche les options de menu du niveau principal.

Zone de boîte de dialogue

La zone de boîte de dialogue est située sur la droite de l'interface utilisateur graphique. Lorsque vous cliquez sur une option de menu dans la zone de navigation, la zone de boîte de dialogue affiche la boîte de dialogue correspondante.

Actualisation de l'affichage

Lorsqu'une boîte de dialogue reste ouverte de manière prolongée, les valeurs associées à l'équipement auront probablement subi des modifications depuis l'ouverture de la boîte de dialogue.

☐ Pour actualiser l'affichage de la boîte de dialogue, cliquez sur le bouton . Les informations non sauvegardées de la boîte de dialogue seront perdues.

Sauvegarde des réglages

La sauvegarde transfère les réglages modifiés vers la mémoire volatile (*RAM*) de l'équipement. Exécutez l'étape suivante :

☐ Cliquez sur le bouton .

Pour conserver les réglages modifiés même après le redémarrage de l'équipement, exécutez les étapes suivantes :

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

☐ Dans la table, mettez le profil de configuration souhaité en surbrillance.

☐ Lorsque la case est non cochée dans la colonne *Selected*, cliquez sur le bouton , puis sur l'option *Select*.

☐ Cliquez sur le bouton puis sur l'élément *Save*.

Commentaire : Des modifications non intentionnelles apportées aux réglages peuvent mettre fin à la connexion entre votre PC et l'équipement. Pour que l'équipement reste accessible, activez la fonction *Undo configuration modifications* dans la boîte de dialogue *Basic Settings > Load/Save* avant de modifier tout réglage. Lorsque cette fonction est utilisée, l'équipement vérifie constamment s'il peut toujours être joint par l'adresse IP de votre PC. Lorsque la connexion est perdue, l'équipement charge le profil de configuration enregistré dans la mémoire non volatile (*NVM*) après le laps de temps spécifié. L'équipement peut alors être à nouveau joint.

Utilisation des tables

Les boîtes de dialogue affichent de nombreux réglages sous forme de table.

Lorsque vous modifiez une cellule de table, la cellule de table affiche une coche rouge dans le coin supérieur gauche. La coche rouge indique que vos modifications n'ont pas encore été transférées vers la mémoire volatile (*RAM*) de l'équipement.

Vous avez la possibilité de personnaliser l'apparence des tables de manière à l'adapter à vos besoins. Lorsque vous placez le pointeur de souris au-dessus d'un en-tête de colonne, une liste déroulante apparaît dans l'en-tête de colonne. Lorsque vous cliquez sur ce bouton, la liste déroulante affiche les entrées suivantes :

▶ Tri dans l'ordre croissant
Trie les entrées de la table dans l'ordre croissant en se basant sur les entrées de la colonne sélectionnée.
Les entrées de table triées sont signalées par une flèche apparaissant dans l'en-tête de colonne.

- Tri dans l'ordre décroissant
  Trie les entrées de la table dans l'ordre décroissant en se basant sur les entrées de la colonne sélectionnée.
  Les entrées de table triées sont signalées par une flèche apparaissant dans l'en-tête de colonne.
- Colonnes
  Affiche ou masque les colonnes.
  Les colonnes masquées sont signalées par une case non cochée dans la liste déroulante.
- Filtres
  La table affiche uniquement les entrées dont le contenu correspond aux critères de filtres spécifiés de la colonne sélectionnée.
  Les entrées de table filtrées sont signalées par un en-tête de colonne apparaissant en surbrillance.

Vous avez la possibilité de sélectionner plusieurs entrées de table simultanément et de leur appliquer par la suite une action. Cette option s'avère très utile lorsque vous supprimez simultanément plusieurs entrées de table.

- Sélectionnez plusieurs entrées de table successives :
  - ☐ Cliquez sur la première entrée de table souhaitée afin de la mettre en surbrillance.
  - ☐ Maintenez appuyée la touche <MAJ>.
  - ☐ Cliquez sur la dernière entrée de table pour mettre en surbrillance toutes les entrées de table souhaitées.
- Sélectionnez plusieurs entrées de table individuelles :
  - ☐ Cliquez sur la première entrée de table souhaitée afin de la mettre en surbrillance.
  - ☐ Maintenez appuyée la touche <CTRL>.
  - ☐ Cliquez sur la prochaine entrée de table souhaitée afin de la mettre en surbrillance. Répétez l'opération jusqu'à ce que toutes les entrées de table souhaitées soient mises en surbrillance.

Boutons

Cette section contient la description des boutons par défaut. Les boutons spécifiques aux boîtes de dialogue sont décrits dans la rubrique d'aide de la boîte de dialogue correspondante.

Transfère les modifications apportées à la mémoire volatile (*RAM*) de l'équipement et les applique à l'équipement. Pour sauvegarder les modifications dans la mémoire non-volatile, procédez comme suit :

- ☐ Ouvrez la boîte de dialogue *Basic Settings > Load/Save*.
- ☐ Dans la table, mettez le profil de configuration souhaité en surbrillance.
- ☐ Lorsque la case est `non cochée` dans la colonne *Selected*, cliquez sur le bouton  , puis sur l'option *Select*.
- ☐ Cliquez sur le bouton  pour sauvegarder vos modifications actuelles.

Actualise les champs avec les valeurs sauvegardées dans la mémoire volatile (*RAM*) de l'équipement.

Transfère les réglages de la mémoire volatile (*RAM*) vers le profil de configuration désigné comme sélectionné (« Selected ») dans la mémoire non volatile (*NVM*).

Lorsque la case est cochée dans la colonne *Backup config when saving* dans la boîte de dialogue *Basic Settings > External Memory*, l'équipement génère une copie du profil de configuration dans la mémoire externe.

Affiche un sous-menu contenant les options de menu correspondant à la boîte de dialogue correspondante.

Ouvre la boîte de dialogue *Wizard*.

Ajoute une nouvelle entrée de table.

Supprime l'entrée de table mise en surbrillance.

Ouvre l'aide en ligne.

1 Basic Settings

Le menu contient les boîtes de dialogue suivantes :

- System
- Network
- Out of Band over USB
- Software
- Load/Save
- External Memory
- Port
- Power over Ethernet (MCSESP)
- Restart

1.1 System

[Basic Settings > System]

Dans cette boîte de dialogue, vous surveillez les états de fonctionnement individuels.

Device status

Les champs dans ce cadre affichent l'état de l'équipement et vous informent des alarmes émises. Lorsqu'une alarme est en cours, le cadre est mis en surbrillance.

Vous spécifiez les paramètres surveillés par l'équipement dans la boîte de dialogue *Diagnostics* > Status Configuration > *Device Status*.

Commentaire : Si vous raccordez un seul bloc d'alimentation pour alimenter en tension un équipement avec un bloc d'alimentation redondant, cet équipement émet une alarme. Pour éviter cette alarme, désactivez la surveillance des blocs d'alimentation manquants dans la boîte de dialogue *Diagnostics > Status Configuration > Device Status*.

Alarm counter

Affiche le nombre d'alarmes actuellement en cours.

Lorsqu'il existe au moins une alarme en cours, l'icône est visible.

Lorsque vous positionnez le pointeur de la souris sur l'icône, une infobulle affiche la cause des alarmes en cours et l'heure à laquelle l'équipement a déclenché l'alarme.

Si un paramètre surveillé diffère de l'état souhaité, l'équipement déclenche une alarme. La boîte de dialogue *Diagnostics > Status Configuration > Device Status*, onglet *Status*, affiche une vue d'ensemble des alarmes.

Security status

Les champs dans ce cadre affichent l'état de sécurité et vous informent des alarmes émises. Lorsqu'une alarme est en cours, le cadre est mis en surbrillance.

Vous spécifiez les paramètres surveillés par l'équipement dans la boîte de dialogue *Diagnostics* > Status Configuration > *Security Status*.

Alarm counter

Affiche le nombre d'alarmes actuellement en cours.

Lorsqu'il existe au moins une alarme en cours, l'icône est visible.

Lorsque vous positionnez le pointeur de la souris sur l'icône, une infobulle affiche la cause des alarmes en cours et l'heure à laquelle l'équipement a déclenché l'alarme.

Si un paramètre surveillé diffère de l'état souhaité, l'équipement déclenche une alarme. La boîte de dialogue *Diagnostics > Status Configuration > Security Status*, onglet *Status*, affiche une vue d'ensemble des alarmes.

Signal contact status

Les champs dans ce cadre affichent l'état du contact sec et vous informent des alarmes émises. Lorsqu'une alarme est en cours, le cadre est mis en surbrillance.

Vous spécifiez les paramètres surveillés par l'équipement dans la boîte de dialogue *Diagnostics* > Status Configuration > *Signal Contact > Signal Contact 1*/*Signal Contact 2*.

Alarm counter

Affiche le nombre d'alarmes actuellement en cours.

Lorsqu'il existe au moins une alarme en cours, l'icône est visible.

Lorsque vous positionnez le pointeur de la souris sur l'icône, une infobulle affiche la cause des alarmes en cours et l'heure à laquelle l'équipement a déclenché l'alarme.

Si un paramètre surveillé diffère de l'état souhaité, l'équipement déclenche une alarme. La boîte de dialogue *Diagnostics > Status Configuration > Signal Contact > Signal Contact 1*/*Signal Contact 2*, onglet *Status*, affiche une vue d'ensemble des alarmes.

System data

Les champs dans ce cadre affichent des données de fonctionnement et des informations sur l'emplacement de l'équipement.

System name

Spécifie le nom sous lequel l'équipement est connu dans le réseau.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères
  Les caractères suivants sont autorisés :
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`
  - `<nom de l'équipement>-<adresse MAC>` (réglage par défaut)

Lors de la création de certificats HTTPS X.509, l'application qui génère le certificat utilise la valeur spécifiée comme nom de domaine et nom commun.

Les fonctions suivantes utilisent la valeur spécifiée comme nom d'hôte ou FQDN (Fully Qualified Domain Name). Pour des raisons de compatibilité, il est recommandé de n'utiliser que des lettres minuscules, car tous les systèmes ne comparent pas la casse dans le FQDN. Vérifiez que ce nom est unique dans tout le réseau.

- Client DHCP
- *Syslog*
- *IEC61850-MMS*

Location

Spécifie l'emplacement de l'équipement.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

Contact person

Spécifie le contact pour cet équipement.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

Device type

Affiche le nom de produit de l'équipement.

Power supply 1
Power supply 2

Affiche l'état du bloc d'alimentation sur le raccordement d'alimentation en tension pertinent

Valeurs possibles :

- *present*
- *defective*

- *not installed*
- *unknown*

Uptime

Affiche le temps écoulé depuis le dernier redémarrage de cet équipement.

Valeurs possibles :

- Durée au format `jour(s), ...h ...m ...s`

Temperature [°C]

Affiche la température actuelle dans l'équipement en °C.

Vous activez la surveillance des seuils de température dans la boîte de dialogue *Diagnostics > Status Configuration > Device Status*.

Upper temp. limit [°C]

Spécifie le seuil de température supérieur en °C.

Valeurs possibles :

- `-99..99` (entier)
  Si la température dans cet équipement excède cette valeur, l'équipement génère une alarme.

Lower temp. limit [°C]

Spécifie le seuil de température inférieur en °C.

Valeurs possibles :

- `-99..99` (entier)
  Si la température dans cet équipement chute en deçà de cette valeur, l'équipement génère une alarme.

LED status

Ce cadre affiche les états des LED d'état de l'équipement au moment de la dernière mise à jour. Le manuel d'utilisation « Installation » contient des informations détaillées sur les LED d'état de l'équipement.

Paramètres	Couleur	Signification
Status	●	Aucune alarme relative à l'état de l'équipement n'est en cours. L'état de l'équipement est OK.
	●	Au moins une alarme d'état de l'équipement est en cours. Voir le cadre *Device status* ci-dessus.
Power	●	Variante de l'équipement avec 2 blocs d'alimentation : Une seule tension d'alimentation est activée.
	●	Variante de l'équipement avec 1 bloc d'alimentation : La tension d'alimentation est activée. Variante de l'équipement avec 2 blocs d'alimentation : Les deux tensions d'alimentation sont activées.

Paramètres	Couleur	Signification
EAM	●	Aucune mémoire externe n'est connectée.
	●	La mémoire externe est connectée, mais elle n'est pas opérationnelle.
	●	La mémoire externe est connectée et opérationnelle.

Port status

Ce cadre affiche une vue simplifiée des ports de l'équipement au moment de la dernière mise à jour.

Les icônes illustrent l'état des ports individuels. Dans certaines situations, les icônes suivantes interfèrent entre elles. Lorsque vous positionnez le pointeur de la souris sur l'icône du port concerné, une infobulle affiche des informations détaillées sur l'état du port.

Paramètres	État	Signification
`<Numéro de port>`		Le port est désactivé. Le port n'envoie ni ne reçoit aucune donnée.
		Le port est désactivé. Le câble est connecté. Lien activé.
		Le port est activé. Aucun câble de données n'est connecté ou aucune liaison n'est activée.
		Le port est activé. Le câble est connecté. La liaison est ok. Lien activé. Mode full duplex
		Le mode half duplex est activé. Vérifiez les réglages dans la boîte de dialogue *Basic Settings > Ports*, onglet *Configuration*.
		Le port est dans un état de blocage dû à une fonction de redondance.
		Le port fonctionne en tant qu'interface de routeur.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

1.2 Network

[Basic Settings > Network]

Le menu contient les boîtes de dialogue suivantes :
- Global
- IPv4
- IPv6

1.2.1 Global

[Basic Settings > Network > Global]

Cette boîte de dialogue vous permet de spécifier les réglages du VLAN et de Ethernet Switch Configurator requis pour accéder à l'administration de l'équipement par le biais du réseau.

Management interface

Ce cadre vous permet de spécifier le VLAN dans lequel l'administration de l'équipement est accessible.

VLAN ID

Spécifie le VLAN dans lequel l'administration de l'équipement est accessible via le réseau. L'administration de l'équipement est accessible via des ports qui sont membres de ce VLAN.

Valeurs possibles :

- `1..4042` (réglage par défaut : `1`)
  La condition préalable est que le VLAN soit déjà configuré. Voir la boîte de dialogue *Switching > VLAN > Configuration*.

Lorsque vous cliquez sur le bouton ☑ après avoir modifié la valeur, la fenêtre *Information* s'ouvre. Sélectionnez le port via lequel vous vous connecterez à l'équipement à l'avenir. Après avoir cliqué sur le bouton *Ok*, les nouveaux réglages du VLAN d'administration sont affectés au port.

- Le port est alors un membre du VLAN et transmet les paquets de données sans tag de VLAN (non taggés). Voir la boîte de dialogue *Switching > VLAN > Configuration*.
- L'équipement affecte au port le VLAN-ID de port du VLAN d'administration de l'équipement. Voir la boîte de dialogue *Switching > VLAN > Port*.

Après un court délai, l'équipement est accessible via le nouveau port dans le nouveau VLAN d'administration.

MAC address

Affiche l'adresse MAC de l'équipement. L'administration de l'équipement est accessible via le réseau à l'aide de l'adresse MAC.

Ethernet Switch Configurator protocol v1/v2

Ce cadre vous permet de spécifier les réglages de l'accès à l'équipement à l'aide du protocole Ethernet Switch Configurator.

Sur un PC, le logiciel Ethernet Switch Configurator affiche les équipements Schneider Electric accessibles dans le réseau pour lequel la fonction Ethernet Switch Configurator est activée. Vous pouvez accéder à ces équipements même si les paramètres IP qui leur sont affectés sont invalides ou inexistants. Le logiciel Ethernet Switch Configurator vous permet d'affecter ou de modifier les paramètres IP dans l'équipement.

Commentaire : Avec le logiciel Ethernet Switch Configurator, vous n'accédez à l'équipement que par le biais de ports qui sont membres du même VLAN que l'administration de l'équipement. Vous spécifiez à quel VLAN un port donné est affecté dans la boîte de dialogue *Switching > VLAN > Configuration*.

Operation

Active/désactive la fonction Ethernet Switch Configurator dans l'équipement.

Valeurs possibles :

- `On` (réglage par défaut)
  Ethernet Switch Configurator est activé.
  Vous pouvez utiliser le logiciel Ethernet Switch Configurator pour accéder à l'équipement depuis votre PC.
- `Off`
  Ethernet Switch Configurator est désactivé.

Access

Active/désactive l'accès en écriture à l'équipement à l'aide de Ethernet Switch Configurator.

Valeurs possibles :

- `readWrite` (réglage par défaut)
  Le logiciel Ethernet Switch Configurator a accès en écriture à l'équipement.
  Avec ce réglage, vous pouvez modifier les paramètres IP de l'équipement.
- `readOnly`
  Le logiciel Ethernet Switch Configurator a accès en lecture seule à l'équipement.
  Avec ce réglage, vous pouvez afficher les paramètres IP de l'équipement.

Recommandation : modifiez le réglage sur la valeur `readOnly` uniquement après avoir mis l'équipement en service.

Signal

Active/désactive le clignotement des LED du port et assure la fonction du même nom dans le logiciel Ethernet Switch Configurator. La fonction vous permet d'identifier l'équipement dans le champ.

Valeurs possibles :

- `case cochée`
  Le clignotement des LED du port est activé.
  Les LED du port clignotent jusqu'à ce que vous désactiviez la fonction de nouveau.
- `case non cochée` (réglage par défaut)
  Le clignotement des LED du port est désactivé.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

1.2.2 IPv4

[Basic Settings > Network > IPv4]

Cette boîte de dialogue vous permet de spécifier les réglages IPv4 requis pour accéder à l'administration de l'équipement par le biais du réseau.

Management interface

IP address assignment

Spécifie la source depuis laquelle l'administration de l'équipement reçoit ses paramètres IP.

Valeurs possibles :

- `Local`
  L'équipement utilise les paramètres IP de la mémoire interne. Pour cela, vous spécifiez les réglages dans le cadre *IP parameter*.
- `BOOTP`
  L'équipement reçoit ses paramètres IP d'un serveur BOOTP ou DHCP.
  Le serveur évalue l'adresse MAC de l'équipement, puis affecte les paramètres IP.
- `DHCP` (réglage par défaut)
  L'équipement reçoit ses paramètres IP d'un serveur DHCP.
  Le serveur évalue l'adresse MAC, le nom DHCP ou d'autres paramètres de l'équipement, puis affecte les paramètres IP.
  Lorsque le serveur fournit également les adresses des serveurs DNS, l'équipement affiche ces adresses dans la boîte de dialogue *Advanced > DNS > Cache > Current*.

Commentaire : En l'absence de réponse du serveur BOOTP ou DHCP, l'équipement définit l'adresse IP sur `0.0.0.0` et tente une nouvelle fois d'obtenir une adresse IP valide.

BOOTP/DHCP

Client ID

Affiche l'ID de client DHCP que l'équipement envoie au serveur BOOTP ou DHCP. Si le serveur est configuré en conséquence, il réserve une adresse IP à cet ID de client DHCP. Ainsi, l'équipement reçoit la même adresse IP du serveur chaque fois qu'il la demande.

L'ID de client DHCP que l'équipement envoie est le nom de l'équipement spécifié dans le champ *System name* de la boîte de dialogue *Basic Settings > System*.

DHCP option 66/67/4/42

Active/désactive la fonction *DHCP option 66/67/4/42* dans l'équipement.

Valeurs possibles :

- *On* (réglage par défaut)
  La fonction *DHCP option 66/67/4/42* est activée.
  L'équipement charge le profil de configuration et reçoit les informations sur le serveur de temps à l'aide des options DHCP suivantes :
  - `Option 66: TFTP server name`
    `Option 67: Boot file name`
    L'équipement importe et charge automatiquement le profil de configuration du serveur DHCP dans la mémoire volatile (*RAM*) via TFTP. L'équipement utilise les réglages du profil de configuration importé dans `running-config`.
  - `Option 4: Time Server`
    `Option 42: Network Time Protocol Servers`
    L'équipement reçoit les informations sur le serveur de temps du serveur DHCP.
- *Off*
  La fonction *DHCP option 66/67/4/42* est désactivée.
  - L'équipement ne charge pas de profil de configuration à l'aide des options DHCP 66/67.
  - Le périphérique ne reçoit pas d'informations sur le serveur de temps à l'aide des options DHCP 4/42.

IP parameter

Ce cadre vous permet d'affecter les paramètres IP manuellement. Si vous avez sélectionné le bouton radio `Local` dans le cadre *Management interface*, liste d'options *IP address assignment*, ces champs peuvent être modifiés.

IP address

Spécifie l'adresse IP via laquelle l'administration de l'équipement est accessible par le biais du réseau.

Valeurs possibles :

- Adresse IPv4 valide

Netmask

Spécifie le masque réseau.

Valeurs possibles :

- Masque réseau IPv4 valide

Gateway address

Spécifie l'adresse IP d'un routeur via lequel l'équipement accède à d'autres équipements en dehors de son propre réseau.

Valeurs possibles :

- Adresse IPv4 valide

Remaining lease time

Lease time [s]

Affiche le temps restant en secondes pendant lequel l'adresse IP attribuée à l'agent d'administration de l'équipement par le serveur DHCP est encore valide.

Pour mettre à jour l'affichage, cliquez sur le bouton  .

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

1.2.3 IPv6

[Basic Settings > Network > IPv6]

Cette boîte de dialogue vous permet de spécifier les réglages IPv6 requis pour accéder à l'administration de l'équipement par le biais du réseau .

Operation

Operation

Active/désactive le protocole IPv6 dans l'équipement.

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.

Valeurs possibles :

- *On* (réglage par défaut)
  Le protocole IPv6 est activé.
- *Off*
  Le protocole IPv6 est désactivé.
  Si vous souhaitez que l'équipement fonctionne uniquement avec le protocole IPv4, désactivez le protocole IPv6 dans l'équipement.

Configuration

Dynamic IP address assignment

Spécifie la source depuis laquelle l'administration de l'équipement reçoit ses paramètres IPv6.

Valeurs possibles :

- *None*
  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 loopback, de lien local et *Multicast* comme adresses IPv6 statiques.
- *Auto* (réglage par défaut)
  L'équipement reçoit ses paramètres IPv6 de manière dynamique. L'équipement reçoit un maximum de 2 adresses IPv6.
  Le Router Advertisement Daemon (radvd) en est un exemple. Le radvd utilise les messages *Router Solicitation* et *Router Advertisement* pour configurer automatiquement une adresse IPv6. Les messages *Router Solicitation* et *Router Advertisement* sont décrits dans RFC 4861.
- *DHCPv6*
  L'équipement reçoit ses paramètres IPv6 d'un serveur DHCPv6.
- *All*
  Si le bouton radio *All* est sélectionné, l'équipement reçoit ses paramètres IPv6 au moyen de toutes les possibilités d'affectation dynamique et manuelle.

DHCP

Client ID

Affiche l'ID de client DHCPv6 que l'équipement envoie au serveur DHCPv6. Si le serveur est configuré en conséquence, il reçoit une adresse IPv6 pour cet ID de client DHCPv6.

L'adresse IPv6 reçue du serveur DHCPv6 a une *PrefixLength* de `128`. Selon RFC 8415, un serveur DHCPv6 ne peut actuellement pas être utilisé pour fournir des informations sur *Gateway address* ou *PrefixLength*.

L'équipement ne peut recevoir qu'une seule adresse IPv6 du serveur DHCPv6.

IP parameter

Gateway address

Spécifie l'adresse IPv6 d'un routeur par lequel l'équipement accède à d'autres équipements en dehors de son propre réseau.

Valeurs possibles :

- Adresse IPv6 valide (sauf adresses de loopback et *Multicast*)

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 la *Gateway address* définie manuellement.

Duplicate Address Detection

Dans ce champ, vous pouvez spécifier le nombre de messages *Neighbor Solicitation* consécutifs que l'équipement envoie pour la fonction *Duplicate Address Detection*. Cette fonction est utilisée pour déterminer l'unicité d'une adresse unicast IPv6 sur l'interface.

Number of neighbor solicitants

Spécifie le nombre de messages *Neighbor Solicitation* que l'équipement envoie pour la fonction *Duplicate Address Detection*.

Valeurs possibles :

- `0`
  La fonction est désactivée.
- `1..5` (réglage par défaut : `1`)

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).

Table

Cette table affiche une liste des adresses IPv6 configurées pour l'administration de l'équipement.

Prefix

Affiche le préfixe de l'adresse IPv6 dans un format compressé. Le préfixe indique les bits les plus à gauche d'une adresse IPv6, également connus comme la partie réseau de l'adresse.

PrefixLength

Affiche la longueur du préfixe de l'adresse IPv6.

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.

Valeurs possibles :

- `0..128`

IP address

Affiche l'adresse IPv6 complète dans un format compressé.

Le format compressé est automatiquement appliqué à chaque adresse IPv6, quelle que soit la source depuis laquelle l'administration de l'équipement reçoit ses paramètres IPv6.

Valeurs possibles :

- Adresse IPv6 valide
  Pour utiliser une adresse IPv6 dans une URL, utilisez la syntaxe URL suivante : `https://[<ipv6_address>]`.

Pour plus d'informations sur les règles de compression et les types d'adresses IPv6, consultez le manuel « Configuration ».

EUI option

Indique si la fonction *EUI option* est appliquée à l'adresse IPv6.

Lorsque vous cochez cette case, l'ID d'interface de l'adresse IPv6 est automatiquement configuré. 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`.

Valeurs possibles :

- `case cochée`
  La fonction *EUI option* est activée.
- `case non cochée` (réglage par défaut)
  La fonction *EUI option* est désactivée.

Origin

Spécifie de quelle manière l'équipement a reçu ses paramètres IPv6.

Valeurs possibles :

- *Autoconf*
  L'équipement a reçu l'adresse IPv6 de manière dynamique lorsque le bouton radio *Auto* est sélectionné.
- *Manual*
  L'équipement a reçu l'adresse IPv6 manuellement.
- *DHCP*
  L'équipement a reçu l'adresse IPv6 d'un serveur DHCPv6.
- *Linklayer*
  L'équipement configure automatiquement une adresse IPv6 de type lien local. L'adresse de lien local ne peut pas être modifiée.

Status

Affiche l'état actuel de l'adresse IPv6.

Valeurs possibles :

- *active*
  L'adresse IPv6 est activée.
- *notInService*
  L'adresse IPv6 est désactivée.
- *notReady*
  L'adresse IPv6 est spécifiée, mais n'est pas actuellement *active* car certains paramètres de configuration sont encore manquants.

Commentaire : Lorsque l'adresse IPv6 est spécifiée manuellement, vous pouvez changer manuellement entre les états *active* et *notInService*. Pour effectuer ce changement, sélectionnez dans la colonne *Status* l'état souhaité dans la liste déroulante relative à votre entrée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

1.3 Out of Band over USB

[Basic Settings > Out of Band over USB]

L'équipement s'accompagne d'une interface réseau USB qui vous permet d'accéder à l'administration de l'équipement out-of-band. En cas de charge in-band élevée sur les ports de commutation, vous pouvez également utiliser cette interface réseau USB pour accéder à l'administration de l'équipement.

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

Lorsque vous accédez à l'administration de l'équipement, les limitations suivantes s'appliquent :
- La station d'administration réseau est directement connectée au port USB.
- L'interface réseau USB ne prend pas en charge les fonctions suivantes :
  - Paquets dotés de tags prioritaires
  - Paquets incluant un tag *VLAN*
  - *DHCP L2 Relay*
  - *LLDP*
  - *DiffServ*
  - *ACL*
  - *Industrial Protocols*

Dans cette boîte de dialogue, l'équipement vous permet de modifier les paramètres IP et de désactiver l'interface réseau USB, le cas échéant.

Operation

Operation

Active/désactive l'interface réseau USB.

Valeurs possibles :
- `On` (réglage par défaut)
  L'équipement vous permet d'accéder à l'administration de l'équipement par le biais de l'interface réseau USB.
- `Off`
  L'équipement interdit l'accès à l'administration de l'équipement par le biais de l'interface réseau USB.

Management interface

Device MAC address

Affiche l'adresse MAC de l'interface réseau USB.

Host MAC address

Affiche l'adresse MAC de la station d'administration réseau connectée.

IP parameter

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

IP address

Spécifie l'adresse IP de l'administration de l'équipement pour l'accès par le biais de l'interface réseau USB.

Valeurs possibles :

▶ Adresse IPv4 valide
(réglage par défaut : `91.0.0.100`)
L'équipement affecte cette adresse IP incrémentée de 1 à la station d'administration réseau connectée à l'équipement.
Exemple : `91.0.0.100` pour l'interface réseau USB, `91.0.0.101` pour la station d'administration réseau.

Netmask

Spécifie le masque réseau.

Valeurs possibles :

▶ Masque réseau IPv4 valide
(réglage par défaut : `255.255.255.0`)

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

1.4 Software

[Basic Settings > Software]

Cette boîte de dialogue vous permet de mettre à jour le logiciel de l'équipement et d'afficher des informations sur le logiciel de l'équipement.

Vous avez aussi la possibilité de restaurer une sauvegarde du logiciel enregistré sur l'équipement.

Commentaire : Avant de mettre à jour le logiciel de l'équipement, suivez les instructions propres à la version dans le fichier texte `Lisezmoi`.

Version

Stored version

Affiche le numéro de version et la date de création du logiciel de l'équipement sauvegardés dans la mémoire flash. L'équipement charge le logiciel de l'équipement lors du redémarrage suivant.

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.

Backup version

Affiche le numéro de version et la date de création du logiciel de l'équipement enregistré en tant que sauvegarde dans la mémoire flash. L'équipement a copié ce logiciel dans la mémoire de sauvegarde lors de la dernière mise à jour du logiciel ou après que vous avez cliqué sur le bouton *Restore*.

Restore

Restaure le logiciel de l'équipement enregistré en tant que sauvegarde. Durant ce processus, l'équipement modifie la *Stored version* et la *Backup version* du logiciel de l'équipement.

Lors du redémarrage, l'équipement charge la *Stored version*.

Bootcode

Affiche le numéro de version et la date de création du code de démarrage.

Software update

Alternativement, lorsque le fichier image se trouve dans la mémoire externe, l'équipement vous permet de mettre à jour le logiciel en effectuant un clic droit dans la table.

URL

Spécifie le chemin et le nom du fichier image avec lequel vous mettez à jour le logiciel de l'équipement.

L'équipement vous offre les options suivantes pour mettre à jour le logiciel :

- Mise à jour du logiciel à partir du PC
  Lorsque le fichier se trouve sur votre PC ou sur un lecteur réseau, effectuez un glisser-déposer du fichier dans la zone  . Vous pouvez également cliquer sur la zone pour sélectionner le fichier.
- Mise à jour du logiciel depuis un serveur FTP
  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 fichier>`
- Mise à jour du logiciel depuis un serveur TFTP
  Lorsque le fichier se trouve sur un serveur TFTP, spécifiez l'URL du fichier au format suivant :
  `tftp://<adresse IP>/<chemin d'accès>/<nom fichier>`
- Mise à jour du logiciel depuis un serveur SCP ou SFTP
  Lorsque le fichier se trouve sur un serveur SCP ou SFTP, spécifiez l'URL du fichier dans l'un des formats suivants :
  - `scp://` ou `tftp://<adresse IP>/<chemin d'accès>/<nom 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>`

Start

Met à jour le logiciel de l'équipement.

L'équipement installe le fichier sélectionné dans la mémoire flash en remplaçant le logiciel de l'équipement précédemment sauvegardé. Lors du redémarrage, l'équipement charge le logiciel de l'équipement installé.

L'équipement copie le logiciel existant dans la mémoire de sauvegarde.

Pour rester connecté à l'équipement durant la mise à jour du logiciel, déplacez le pointeur de la souris de temps en temps. Sinon, spécifiez une valeur suffisamment élevée dans la boîte de dialogue *Device Security > Management Access > Web*, champ *Web interface session timeout [min]*, avant la mise à jour du logiciel.

Table

File location

Affiche l'emplacement de stockage du logiciel de l'équipement.

Valeurs possibles :

- *ram*
  Mémoire volatile de l'équipement

- *flash*
  Mémoire non-volatile (*NVM*) de l'équipement
- *usb*
  Mémoire USB externe (EAM)

Index

Affiche l'index du logiciel de l'équipement.

Pour le logiciel de l'équipement dans la mémoire flash, l'index a la signification suivante :

- 1
  Lors du redémarrage, l'équipement charge ce logiciel.
- 2
  L'équipement a copié ce logiciel dans la zone de sauvegarde lors de la dernière mise à jour du logiciel.

File name

Affiche le nom de fichier du logiciel interne à l'équipement.

Firmware

Affiche le numéro de version et la date de création du logiciel de l'équipement.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

1.5 Load/Save

[Basic Settings > Load/Save]

Cette boîte de dialogue vous permet de sauvegarder les réglages de l'équipement de manière permanente dans un profil de configuration.

L'équipement peut avoir plusieurs profils de configuration. Lorsque vous activez un autre profil de configuration, vous basculez sur d'autres réglages de l'équipement. Vous avez la possibilité d'exporter les profils de configuration sur votre PC ou sur un serveur. Vous pouvez aussi importer les profils de configuration depuis votre PC ou depuis un serveur sur l'équipement.

Dans le réglage par défaut, l'équipement sauvegarde les profils de configuration non chiffrés. Si vous saisissez un mot de passe dans le cadre *Configuration encryption*, l'équipement sauvegarde les profils de configuration actuels et futurs dans un format chiffré.

Des modifications non intentionnelles apportées aux réglages peuvent mettre fin à la connexion entre votre PC et l'équipement. Pour que l'équipement reste accessible, activez la fonction *Undo configuration modifications* avant de modifier un réglage quelconque. Si la connexion est perdue, l'équipement charge le profil de configuration sauvegardé dans la mémoire non-volatile (*NVM*) après la durée spécifiée.

External memory

Selected external memory

Affiche le type de la mémoire externe.

Valeurs possibles :

- *usb*
  Mémoire USB externe (EAM)

Status

Affiche l'état opérationnel de la mémoire externe.

Valeurs possibles :

- *notPresent*
  Aucune mémoire externe n'est connectée.
- *removed*
  Quelqu'un a retiré la mémoire externe de l'équipement en cours de fonctionnement.
- *ok*
  La mémoire externe est connectée et opérationnelle.
- *outOfMemory*
  L'espace mémoire est occupé dans la mémoire externe.
- *genericErr*
  L'équipement a détecté une erreur.

Configuration encryption

Active

Affiche si le chiffrement de la configuration est activé/désactivé dans l'équipement.

Valeurs possibles :

- `case cochée`
  Le chiffrement de la configuration est activé.
  Si le profil de configuration est chiffré et que le mot de passe correspond au mot de passe sauvegardé dans l'équipement, ce dernier charge un profil de configuration depuis la mémoire non-volatile (*NVM*).
- `case non cochée`
  Le chiffrement de la configuration est désactivé.
  Si le profil de configuration n'est pas chiffré, l'équipement charge un profil de configuration depuis la mémoire non-volatile (*NVM*) uniquement.

Lorsque, dans la boîte de dialogue *Basic Settings > External Memory*, la colonne *Config priority* a la valeur `first` et que le profil de configuration n'est pas chiffré, le cadre *Security status* dans la boîte de dialogue *Basic Settings > System* affiche une alarme.

Dans la boîte de dialogue *Diagnostics > Status Configuration > Security Status*, onglet *Global*, colonne *Monitor*, vous spécifiez si l'équipement surveille le paramètre *Load unencrypted config from external memory*.

Set password

Ouvre la fenêtre *Set password* qui vous permet de saisir le mot de passe requis pour le chiffrement du profil de configuration. Le chiffrement des profils de configuration rend l'accès non autorisé plus difficile. Pour ce faire, exécutez les étapes suivantes :

- ☐ Lorsque vous modifiez un mot de passe existant, saisissez le mot de passe existant dans le champ *Old password*. Pour afficher le mot de passe en texte clair au lieu de ***** (astérisques), cochez la case *Display content*.
- ☐ Dans le champ *New password*, saisissez le mot de passe.
  Pour afficher le mot de passe en texte clair au lieu de ***** (astérisques), cochez la case *Display content*.
- ☐ Cochez la case *Save configuration afterwards* pour utiliser le chiffrement aussi pour le profil de configuration Selected (Sélectionné) dans la mémoire non-volatile (*NVM*) et dans la mémoire externe.

Commentaire : Si un profil de configuration au maximum est sauvegardé dans la mémoire non-volatile (*NVM*) de l'équipement, utilisez uniquement cette fonction. Avant de créer des profils de configuration supplémentaires, déterminez si le chiffrement de configuration doit ou non être activé de manière permanente dans l'équipement. Sauvegardez les profils de configuration supplémentaires non chiffrés ou chiffrés avec le même mot de passe.

Si vous remplacez un équipement avec un profil de configuration chiffré, par exemple en raison d'un équipement non fonctionnel, exécutez les étapes suivantes :

- ☐ Redémarrez le nouvel équipement et affectez les paramètres IP.
- ☐ Ouvrez la boîte de dialogue *Basic Settings > Load/Save* sur le nouvel équipement.
- ☐ Chiffrez le profil de configuration sur le nouvel équipement. Voir ci-dessus. Saisissez le mot de passe que vous utilisiez pour l'équipement non fonctionnel.

- ☐ Installez la mémoire externe de l'équipement non fonctionnel dans le nouvel équipement.
- ☐ Redémarrez le nouvel équipement.
  Lorsque vous redémarrez l'équipement, ce dernier charge le profil de configuration avec les réglages de l'équipement non fonctionnel depuis la mémoire externe. L'équipement copie les réglages dans la mémoire volatile (`RAM`) et dans la mémoire non-volatile (`NVM`).

Delete

Ouvre la fenêtre *Delete* qui vous permet d'annuler le chiffrement de la configuration sur l'équipement. Pour annuler le chiffrement de la configuration, exécutez les étapes suivantes :

- ☐ Dans le champ *Old password*, saisissez le mot de passe existant.
  Pour afficher le mot de passe en texte clair au lieu de ***** (astérisques), cochez la case *Display content*.
- ☐ Cochez la case *Save configuration afterwards* pour supprimer le chiffrement aussi pour le profil de configuration Selected (Sélectionné) dans la mémoire non-volatile (`NVM`) et dans la mémoire externe.

Commentaire : Si vous conservez des profils de configuration chiffrés supplémentaires dans la mémoire, l'équipement vous permet d'éviter d'activer ou de désigner ces profils de configuration en tant que « Selected ».

Information

NVM in sync with running config

Affiche si le profil de configuration dans la mémoire volatile (`RAM`) et le profil de configuration « Selected » (Sélectionné) dans la mémoire non-volatile (`NVM`) sont identiques.

Valeurs possibles :

- ▶ `case cochée`
  Les profils de configuration sont identiques.
- ▶ `case non cochée`
  Les profils de configuration sont différents.

External memory in sync with NVM

Affiche si le profil de configuration « Selected » (Sélectionné) dans la mémoire externe et le profil de configuration « Selected » (Sélectionné) dans la mémoire non-volatile (`NVM`) sont identiques.

Valeurs possibles :

- ▶ `case cochée`
  Les profils de configuration sont identiques.
- ▶ `case non cochée`
  Les profils de configuration sont différents.
  Causes possibles :
  - Aucune mémoire externe n'est connectée à l'équipement.
  - Dans la boîte de dialogue *Basic Settings > External Memory*, la fonction *Backup config when saving* est désactivée.

Backup config on a remote server when saving

Operation

Active/désactive la fonction *Backup config on a remote server when saving*.

Valeurs possibles :

- *Enabled*
  La fonction *Backup config on a remote server when saving* est activée.
  Lorsque vous sauvegardez le profil de configuration dans la mémoire non-volatile (*NVM*), l'équipement sauvegarde automatiquement le profil de configuration sur le serveur distant spécifié dans le champ *URL*.
- *Disabled* (réglage par défaut)
  La fonction *Backup config on a remote server when saving* est désactivée.

URL

Spécifie le chemin et le nom de fichier du profil de configuration sauvegardé sur le serveur distant.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..128 caractères
  Exemple : `tftp://192.9.200.1/cfg/config.xml`
  L'équipement prend en charge les caractères génériques suivants :
  - `%d`
    Date système au format `YYYY-mm-dd`
  - `%t`
    Heure système au format `HH_MM_SS`
  - `%i`
    Adresse IP de l'équipement
  - `%m`
    Adresse MAC de l'équipement au format `AA-BB-CC-DD-EE-FF`
  - `%p`
    Nom de produit de l'équipement

Set credentials

Ouvre la fenêtre *Credentials* qui vous permet de saisir les identifiants de connexion requis pour vous authentifier sur le serveur distant. Pour ce faire, exécutez les étapes suivantes :

- ☐ Dans le champ *User name*, saisissez le nom d'utilisateur.
  Pour afficher le nom d'utilisateur en texte clair au lieu de ***** (astérisques), cochez la case *Display content*.
  Valeurs possibles :
  - Chaîne de 1..32 caractères ASCII alphanumériques
- ☐ Dans le champ *Password*, saisissez le mot de passe.
  Pour afficher le mot de passe en texte clair au lieu de ***** (astérisques), cochez la case *Display content*.
  Valeurs possibles :
  - Chaîne de 6..64 caractères ASCII alphanumériques
    Les caractères suivants sont autorisés :

```
a..z
A..Z
0..9
!#$%&'()*+,-./:;<=>?@[\\]^_`{}~
```

Undo configuration modifications

Operation

Active/désactive la fonction *Undo configuration modifications*. Lorsque cette fonction est utilisée, l'équipement vérifie constamment s'il peut toujours être joint par l'adresse IP de votre PC. Si la connexion est perdue, après un délai spécifié, l'équipement charge le profil de configuration « Selected » (Sélectionné) depuis la mémoire non-volatile (*NVM*). L'équipement peut alors être à nouveau joint.

Valeurs possibles :

- *On*
  La fonction est activée.
  - Vous spécifiez la durée entre l'interruption de la connexion et le chargement du profil de configuration dans le champ *Timeout [s] to recover after connection loss*.
  - Lorsque la mémoire non-volatile (*NVM*) contient plusieurs profils de configuration, l'équipement charge le profil de configuration avec la désignation « Selected » (Sélectionné).
- *Off* (réglage par défaut)
  La fonction est désactivée.
  Désactive de nouveau la fonction avant que vous ne fermiez l'interface utilisateur graphique. Vous contribuez ainsi à éviter que l'équipement ne restaure le profil de configuration avec la désignation « Selected ».

Commentaire : Avant d'activer la fonction, sauvegardez les réglages dans le profil de configuration. Les modifications actuelles, qui sont sauvegardées temporairement, sont ainsi conservées dans l'équipement.

Timeout [s] to recover after connection loss

Spécifie la durée en secondes après laquelle l'équipement charge le profil de configuration « Selected » (Sélectionné) depuis la mémoire non-volatile (*NVM*) si la connexion est perdue.

Valeurs possibles :

- `30..600` (réglage par défaut : `600`)

Spécifiez une valeur suffisamment élevée. Tenez compte de la durée pendant laquelle vous affichez les boîtes de dialogue de l'interface utilisateur graphique sans les modifier ni les mettre à jour.

Watchdog IP address

Affiche l'adresse IP du PC sur lequel vous avez activé la fonction.

Valeurs possibles :

- Adresse IPv4 (réglage par défaut : `0.0.0.0`)

Table

Storage type

Affiche l'emplacement de stockage du profil de configuration.

Valeurs possibles :

- *RAM* (mémoire volatile de l'équipement)
  Dans la mémoire volatile, l'équipement sauvegarde les réglages pour le fonctionnement courant.
- *NVM* (mémoire non-volatile de l'équipement)
  Lors de l'application de la fonction *Undo configuration modifications* ou lors d'un redémarrage, l'équipement charge le profil de configuration « Selected » depuis la mémoire non-volatile.
  La mémoire non-volatile fournit un espace pour plusieurs profils de configuration, en fonction du nombre de réglages sauvegardés dans le profil de configuration. L'équipement gère au maximum 20 profils de configuration dans la mémoire non-volatile.
  Vous pouvez charger un profil de configuration dans la mémoire volatile (*RAM*). Pour ce faire, exécutez les étapes suivantes :
  - ☐ Dans la table, mettez le profil de configuration en surbrillance.
  - ☐ Cliquez sur le bouton puis sur l'élément *Activate*.
- *ENVM* (mémoire externe)
  Dans la mémoire externe, l'équipement enregistre une copie de sauvegarde du profil de configuration « Selected ».
  La condition préalable est que vous cochiez, dans la boîte de dialogue *Basic Settings > External Memory* la case à cocher *Backup config when saving*.

Profile name

Affiche le nom du profil de configuration.

Valeurs possibles :

- `running-config`
  Nom du profil de configuration dans la mémoire volatile (*RAM*).
- `config`
  Nom du profil de configuration du réglage d'usine dans la mémoire non-volatile (*NVM*).
- Nom défini par l'utilisateur
  L'équipement vous permet de sauvegarder un profil de configuration avec un nom spécifié par l'utilisateur en mettant en surbrillance un profil de configuration existant dans la table et en cliquant sur le bouton , puis sur l'élément *Save as...*.

Pour exporter le profil de configuration sous forme de fichier XML sur votre PC, cliquez sur le lien. Sélectionnez ensuite l'emplacement de stockage et spécifiez le nom du fichier.

Pour sauvegarder le fichier sur un serveur distant, cliquez sur le bouton , puis sur l'élément *Export...*.

Modification date (UTC)

Affiche l'heure (UTC) à laquelle l'utilisateur a sauvegardé le profil de configuration pour la dernière fois.

Selected

Affiche si le profil de configuration a la désignation « Selected ».

Pour désigner un autre profil de configuration en tant que « Selected », vous mettez en surbrillance dans la table le profil de configuration souhaité et vous cliquez sur le bouton , puis sur l'élément *Activate*.

Valeurs possibles :

- `case cochée`
  Le profil de configuration a la désignation « Selected ».
  - Lors de l'application de la fonction *Undo configuration modifications* ou durant un redémarrage, l'équipement charge le profil de configuration dans la mémoire volatile (`RAM`).
  - Lorsque vous cliquez sur le bouton , l'équipement enregistre les réglages sauvegardés provisoirement dans ce profil de configuration.
- `case non cochée`
  Un autre profil de configuration a la désignation « Selected ».

Encrypted

Affiche si le profil de configuration est chiffré.

Valeurs possibles :

- `case cochée`
  Le profil de configuration est chiffré.
- `case non cochée`
  Le profil de configuration n'est pas chiffré.

Vous activez/désactivez le chiffrement du profil de configuration dans le cadre *Configuration encryption*.

Encryption verified

Affiche si le mot de passe du profil de configuration chiffré correspond au mot de passe sauvegardé dans l'équipement.

Valeurs possibles :

- `case cochée`
  Les mots de passe correspondent. L'équipement peut déchiffrer le profil de configuration.
- `case non cochée`
  Les mots de passe sont différents. L'équipement ne peut pas déchiffrer le profil de configuration.

Software version

Affiche le numéro de version du logiciel exécuté par l'équipement lors de la sauvegarde du profil de configuration.

Fingerprint

Affiche le total de contrôle sauvegardé dans le profil de configuration.

Lors de l'enregistrement des réglages, l'équipement calcule le total de contrôle et l'insère dans le profil de configuration.

Fingerprint verified

Affiche si le total de contrôle sauvegardé dans le profil de configuration est valide.

L'équipement calcule le total de contrôle du profil de configuration marqué en tant que « Selected » et le compare au total de contrôle sauvegardé dans ce profil de configuration.

Valeurs possibles :

- `case cochée`
  Les totaux de contrôle calculé et sauvegardé correspondent.
  Les réglages sauvegardés sont cohérents.
- `case non cochée`
  Pour le profil de configuration marqué comme « Selected », ce qui suit s'applique :
  Les totaux de contrôle calculé et sauvegardé sont différents.
  Le profil de configuration contient des réglages modifiés.
  Causes possibles :
  – Le fichier est endommagé.
  – Le système de fichiers dans la mémoire externe est incohérent.
  – Un utilisateur a exporté le profil de configuration et modifié le fichier XML en dehors de l'équipement.
  Pour les autres profils de configuration, l'équipement n'a pas calculé le total de contrôle.

L'équipement vérifie le total de contrôle correctement uniquement si le profil de configuration a été sauvegardé au préalable comme suit :

- sur un équipement identique
- avec la même version logicielle que celle exécutée par l'équipement

Commentaire : Cette fonction identifie les modifications apportées aux réglages dans le profil de configuration. La fonction n'offre aucune protection contre l'utilisation de l'équipement avec des réglages modifiés.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Supprime le profil de configuration mis en surbrillance dans la table de la mémoire non-volatile (*NVM*) ou de la mémoire externe.

Si le profil de configuration a la désignation « Selected », l'équipement vous empêche de supprimer le profil de configuration.

Save as..

Copie le profil de configuration mis en surbrillance dans la table et le sauvegarde avec un nom spécifié par l'utilisateur dans la mémoire non-volatile (*NVM*). L'équipement désigne le nouveau profil de configuration en tant que « Selected ».

Commentaire : Avant de créer des profils de configuration supplémentaires, déterminez si le chiffrement de configuration doit ou non être activé de manière permanente dans l'équipement. Sauvegardez les profils de configuration supplémentaires non chiffrés ou chiffrés avec le même mot de passe.

Si, dans la boîte de dialogue *Basic Settings > External Memory*, la case dans la colonne *Backup config when saving* est cochée, l'équipement désigne le profil de configuration portant le même nom dans la mémoire externe en tant que « Selected ».

Activate

Charge les réglages du profil de configuration mis en surbrillance dans la table dans la mémoire volatile (*RAM*).

- L'équipement interrompt la connexion à l'interface utilisateur graphique. Pour accéder à nouveau à l'administration de l'équipement, exécutez les étapes suivantes :
  - Rechargez l'interface utilisateur graphique.
  - Connectez-vous de nouveau.
- L'équipement utilise immédiatement les réglages du profil de configuration à la volée.

Activez la fonction *Undo configuration modifications* avant d'activer un autre profil de configuration. Si la connexion est perdue par la suite, l'équipement charge le dernier profil de configuration avec la désignation « Selected » (Sélectionné) depuis la mémoire non-volatile (*NVM*). L'équipement est de nouveau accessible.

Si le chiffrement de la configuration est désactivé, l'équipement charge un profil de configuration non chiffré. Si le profil de configuration est activé et que le mot de passe correspond au mot de passe sauvegardé dans l'équipement, ce dernier charge un profil de configuration chiffré.

Lorsque vous activez un profil de configuration plus ancien, l'équipement reprend les réglages des fonctions contenues dans cette version du logiciel. L'équipement définit les nouvelles fonctions sur leurs valeurs par défaut.

Select

Désigne le profil de configuration mis en surbrillance dans la table en tant que « Selected ». Dans la colonne *Selected*, la case est alors cochée.

Lors de l'application de la fonction *Undo configuration modifications* ou durant un redémarrage, l'équipement charge les réglages de ce profil de configuration dans la mémoire volatile (*RAM*).

- Si le chiffrement de la configuration dans l'équipement est désactivé, désignez uniquement un profil de configuration non chiffré en tant que « Selected ».
- Si le chiffrement de la configuration dans l'équipement est activé et que le mot de passe du profil de configuration correspond au mot de passe sauvegardé dans l'équipement, désignez uniquement un profil de configuration chiffré en tant que « Selected ».

Sinon, l'équipement ne pourra pas charger et chiffrer les réglages dans le profil de configuration lors de son redémarrage suivant. Dans ce cas, vous spécifiez, dans la boîte de dialogue *Diagnostics > System > Selftest*, si l'équipement démarre avec les réglages par défaut ou bien s'il interrompt le redémarrage et s'arrête.

Commentaire : Vous ne marquez que les profils de configuration sauvegardés dans la mémoire non-volatile (*NVM*).

Si, dans la boîte de dialogue *Basic Settings > External Memory*, la case dans la colonne *Backup config when saving* est cochée, l'équipement désigne le profil de configuration portant le même nom dans la mémoire externe en tant que « Selected ».

Import...

Ouvre la fenêtre *Import...* pour importer un profil de configuration.

La condition préalable est que vous ayez exporté le profil de configuration à l'aide du bouton *Export...* ou via le lien dans la colonne *Profile name*.

- ☐ Dans la liste déroulante *Select source*, sélectionnez 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.
- ☐ Lorsque *PC/URL* est sélectionné ci-dessus, vous spécifiez dans le cadre *Import profile from PC/URL* le fichier du profil de configuration à importer.
  - – Importation depuis le PC
    Lorsque le fichier se trouve sur votre PC ou sur un lecteur réseau, effectuez un glisser-déposer du fichier dans la zone  . Vous pouvez également cliquer sur la zone pour sélectionner le fichier.
  - – Importation depuis un serveur FTP
    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 fichier>`
  - – Importation depuis un serveur TFTP
    Lorsque le fichier se trouve sur un serveur TFTP, spécifiez l'URL du fichier au format suivant :
    `tftp://<adresse IP>/<chemin d'accès>/<nom fichier>`
  - – Importation depuis un serveur SCP ou SFTP
    Lorsque le fichier se trouve sur un serveur SCP ou SFTP, spécifiez l'URL du fichier dans l'un des formats suivants :
    `scp://` ou `tftp://<adresse IP>/<chemin d'accès>/<nom 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>`

- ☐ Lorsque *External memory* est sélectionné ci-dessus, vous spécifiez dans le cadre *Import profile from external memory* le fichier du profil de configuration à importer.
  Dans la liste déroulante *Profile name* sélectionnez le nom du profil de configuration à importer.
- ☐ Dans le cadre *Destination*, vous spécifiez où l'équipement sauvegarde le profil de configuration importé.
  Dans le champ *Profile name*, vous spécifiez le nom sous lequel l'équipement sauvegarde le profil de configuration.
  Dans le champ *Storage type*, vous spécifiez l'emplacement de stockage pour le profil de configuration. La condition préalable est que vous sélectionniez, dans la liste déroulante *Select source*, l'élément *PC/URL*.
  - ▶ *RAM*
    L'équipement sauvegarde le profil de configuration dans la mémoire volatile (*RAM*) de l'équipement. Le profil de configuration `running-config` est remplacé, l'équipement utilise immédiatement les réglages du profil de configuration importé. L'équipement interrompt la connexion à l'interface utilisateur graphique. Rechargez l'interface utilisateur graphique. Connectez-vous de nouveau.
  - ▶ *NVM*
    L'équipement sauvegarde le profil de configuration dans la mémoire non-volatile (*NVM*) de l'équipement.

Lorsque vous importez un profil, l'équipement reprend les réglages comme suit :

- Si le profil de configuration a été exporté sur le même équipement ou sur un équipement doté de fonctionnalités identiques et de même type :
  L'équipement reprend la totalité des réglages.
- Si le profil de configuration a été exporté sur un autre équipement :
  L'équipement reprend les réglages qu'il peut interpréter sur la base de ses fonctionnalités matérielles et logicielles.
  L'équipement reprend les réglages restants dans le profil de configuration `running-config`.

Concernant le chiffrement du profil de configuration, consultez aussi le texte d'aide du cadre *Configuration encryption*. L'équipement importe un profil de configuration dans les conditions suivantes :

- Le chiffrement de la configuration de l'équipement est désactivé. Le profil de configuration n'est pas chiffré.
- Le chiffrement de la configuration de l'équipement est activé. Le profil de configuration est chiffré avec le même mot de passe que celui utilisé actuellement par l'équipement.

Export...

Exporte le profil de configuration mis en surbrillance dans la table et le sauvegarde sous forme de fichier XML sur un serveur distant.

Pour sauvegarder le fichier sur votre PC, cliquez sur le lien dans la colonne *Profile name* pour sélectionner l'emplacement de stockage et spécifier le nom du fichier.

L'équipement dispose des options suivantes pour exporter un profil de configuration :

- ▶ Exporter vers un serveur FTP
  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 fichier>`

- Exporter vers un serveur TFTP
  Pour sauvegarder le fichier sur un serveur TFTP, spécifiez l'URL pour le fichier au format suivant :
  `tftp://<adresse IP>/<chemin d'accès>/<nom fichier>`
- Exporter vers un serveur SCP ou SFTP
  Pour sauvegarder le fichier sur un serveur SCP ou SFTP, spécifiez l'URL pour le fichier dans l'un des formats suivants :
  - `scp://` ou `tftp://<adresse IP>/<chemin d'accès>/<nom 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.
  - `scp://` ou `sftp://<utilisateur>:<mot de passe>@<adresse IP>/<chemin>/<nom du fichier>`

Load running-config as script

Importe un fichier de script qui modifie le profil de configuration `running config` actuel.

L'équipement dispose des options suivantes pour importer un fichier de script :

- Importation depuis le PC
  Lorsque le fichier se trouve sur votre PC ou sur un lecteur réseau, effectuez un glisser-déposer du fichier dans la zone  . Vous pouvez également cliquer sur la zone pour sélectionner le fichier.
- Importation depuis un serveur FTP
  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 fichier>`
- Importation depuis un serveur TFTP
  Lorsque le fichier se trouve sur un serveur TFTP, spécifiez l'URL du fichier au format suivant :
  `tftp://<adresse IP>/<chemin d'accès>/<nom fichier>`
- Importation depuis un serveur SCP ou SFTP
  Lorsque le fichier se trouve sur un serveur SCP ou SFTP, spécifiez l'URL du fichier dans l'un des formats suivants :
  `scp://` ou `tftp://<adresse IP>/<chemin d'accès>/<nom fichier>`

Commentaire : L'équipement applique les fichiers de script en plus des réglages actuels. Vérifiez que le fichier de script ne contient pas de parties qui entrent en conflit avec les réglages actuels.

Save running-config as script

Sauvegarde le profil de configuration `running config` sous forme de fichier de script sur le PC local. Cela vous permet de sauvegarder vos réglages actuels de l'équipement ou de les utiliser sur différents équipements.

Back to factory...

Rétablit les valeurs par défaut des réglages de l'équipement.

- L'équipement supprime les profils de configuration sauvegardés de la mémoire volatile (*RAM*) et de la mémoire non-volatile (*NVM*).
- L'équipement supprime le certificat HTTPS utilisé par le serveur Web dans l'équipement.
- L'équipement supprime la clé RSA (clé hôte) utilisée par le serveur SSH dans l'équipement.
- Lorsqu'une mémoire externe est connectée, l'équipement supprime les profils de configuration sauvegardés dans la mémoire externe.
- Après un bref délai, l'équipement redémarre et charge les valeurs par défaut.

Back to default

Supprime les réglages de fonctionnement (`running config`) actuels de la mémoire volatile (*`RAM`*).

1.6 External Memory

[Basic Settings > External Memory]

Cette boîte de dialogue vous permet d'activer les fonctions que l'équipement exécute automatiquement en combinaison avec la mémoire externe. La boîte de dialogue affiche également l'état de fonctionnement et les caractéristiques d'identification de la mémoire externe.

Table

Type

Affiche le type de la mémoire externe.

Valeurs possibles :

- *usb*
  Mémoire USB externe (EAM)

Status

Affiche l'état opérationnel de la mémoire externe.

Valeurs possibles :

- *notPresent*
  Aucune mémoire externe n'est connectée.
- *removed*
  Quelqu'un a retiré la mémoire externe de l'équipement en cours de fonctionnement.
- *ok*
  La mémoire externe est connectée et opérationnelle.
- *outOfMemory*
  L'espace mémoire est occupé dans la mémoire externe.
- *genericErr*
  L'équipement a détecté une erreur.

Writable

Affiche si l'équipement dispose d'un accès en écriture à la mémoire externe.

Valeurs possibles :

- case cochée
  L'équipement a un accès en écriture à la mémoire externe.
- case non cochée
  L'équipement a un accès en lecture seule à la mémoire externe. La protection en écriture est peut-être activée dans la mémoire externe.

Software auto update

Active/désactive la mise à jour automatique du logiciel de l'équipement lors du redémarrage.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La mise à jour automatique du logiciel de l'équipement durant le redémarrage est activée.
  L'équipement met à jour son logiciel lorsque les fichiers suivants se trouvent dans la mémoire externe :
  - le fichier image du logiciel de l'équipement
  - un fichier texte `startup.txt` avec le contenu `autoUpdate=<nom_fichier_image>.bin`.
- `case non cochée`
  La mise à jour automatique du logiciel de l'équipement durant le redémarrage est désactivée.

SSH key auto upload

Active/désactive le chargement de la clé RSA depuis une mémoire externe lors du redémarrage.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  Le chargement de la clé RSA est activé.
  Durant un redémarrage, l'équipement charge la clé RSA depuis la mémoire externe lorsque les fichiers suivants se trouvent dans la mémoire externe :
  - fichier clé SSH RSA
  - un fichier texte `startup.txt` avec le contenu `autoUpdateRSA=<nom_fichier_clé_SSH_RSA>`

  L'équipement affiche des messages sur la console système de l'interface série.
- `case non cochée`
  Le chargement de la clé RSA est désactivé.

Commentaire : Lors du chargement de la clé RSA depuis la mémoire externe (*ENVM*), l'équipement écrase les clés existantes dans la mémoire non-volatile (*NVM*).

Config priority

Spécifie la mémoire depuis laquelle l'équipement charge le profil de configuration lors du redémarrage.

Valeurs possibles :

- `disable`
  L'équipement charge le profil de configuration depuis la mémoire non-volatile (*NVM*).
- `first`
  L'équipement charge le profil de configuration depuis la mémoire externe.
  Lorsque l'équipement ne trouve pas un profil de configuration dans la mémoire externe, il charge le profil de configuration depuis la mémoire non-volatile (*NVM*).

Commentaire : Lorsqu'il charge le profil de configuration depuis la mémoire externe (*ENVM*), l'équipement écrase les réglages du profil de configuration Selected (Sélectionné) dans la mémoire non-volatile (*NVM*).

Lorsque la colonne *Config priority* a la valeur `first` et que le profil de configuration n'est pas chiffré, le cadre *Security status* dans la boîte de dialogue *Basic Settings > System* affiche une alarme.

Dans la boîte de dialogue *Diagnostics > Status Configuration > Security Status*, onglet *Global*, colonne *Monitor*, vous spécifiez si l'équipement surveille le paramètre *Load unencrypted config from external memory*.

Backup config when saving

Active/désactive la création d'une copie du profil de configuration dans la mémoire externe.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La création d'une copie est activée. Lorsque vous cliquez, dans la boîte de dialogue *Basic Settings > Load/Save*, sur le bouton *Save*, l'équipement génère une copie du profil de configuration dans la mémoire externe.
- `case non cochée`
  La création d'une copie est désactivée. L'équipement ne génère pas de copie du profil de configuration.

Manufacturer ID

Affiche le nom du constructeur de la mémoire.

Revision

Affiche le numéro de révision spécifié par le constructeur de la mémoire.

Version

Affiche le numéro de version spécifié par le constructeur de la mémoire.

Name

Affiche le nom de produit spécifié par le constructeur de la mémoire.

Serial number

Affiche le numéro de série spécifié par le constructeur de la mémoire.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

1.7 Port

[Basic Settings > Port]

Cette boîte de dialogue vous permet de spécifier les réglages pour les ports individuels. La boîte de dialogue affiche aussi le mode de fonctionnement, l'état de connexion, le débit et le mode duplex pour chaque port.

La boîte de dialogue contient les onglets suivants :
- [Configuration]
- [Statistics]
- [Utilization]

[Configuration]

Table

Port

Affiche le numéro de port.

Name

Nom du port.

Valeurs possibles :
- Chaîne de 0..64 caractères ASCII alphanumériques
  Les caractères suivants sont autorisés :
  - `<space>`
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`

Port on

Active/désactive le port.

Valeurs possibles :
- `case cochée` (réglage par défaut)
  Le port est activé.
- `case non cochée`
  Le port est désactivé. Le port n'envoie ni ne reçoit aucune donnée.

State

Affiche si le port est actuellement physiquement activé ou désactivé.

Valeurs possibles :

- `case cochée`
  Le port est physiquement activé.
- `case non cochée`
  Le port est physiquement désactivé.
  Si la fonction *Port on* est active, la fonction *Auto-Disable* a désactivé le port.
  Vous spécifiez les réglages de la fonction *Auto-Disable* dans la boîte de dialogue *Diagnostics* > Ports > *Auto-Disable*.

Power state (port off)

Spécifie si le port est physiquement activé ou désactivé lorsque vous désactivez le port via la fonction *Port on*.

Valeurs possibles :

- `case cochée`
  Le port reste physiquement activé. Un équipement connecté reçoit un lien actif.
- `case non cochée` (réglage par défaut)
  Le port est physiquement désactivé.

Auto power down

Spécifie comment le port se comporte lorsqu'aucun câble n'est connecté.

Valeurs possibles :

- *no-power-save* (réglage par défaut)
  Le port reste activé.
- *auto-power-down*
  Le port bascule en mode économie d'énergie.
- *unsupported*
  Le port ne prend pas en charge cette fonction et reste activé.

Automatic configuration

Active/désactive la sélection automatique du mode de fonctionnement pour le port.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La sélection automatique du mode de fonctionnement est activée.
  Le port négocie le mode de fonctionnement indépendamment à l'aide de l'auto-négociation et détecte automatiquement les équipements connectés au port TP (Auto Cable Crossing). Ce réglage est prioritaire sur le réglage manuel du port.
  Plusieurs secondes s'écoulent jusqu'à ce que le port ait défini le mode de fonctionnement.
- `case non cochée`
  La sélection automatique du mode de fonctionnement est désactivée.
  Le port fonctionne avec les valeurs que vous spécifiez dans la colonne *Manual configuration* et dans la colonne *Manual cable crossing (Auto. conf. off)*.
- Affichage grisé
  Aucune sélection automatique du mode de fonctionnement.

Manual configuration

Spécifie le mode de fonctionnement des ports lorsque la fonction *Automatic configuration* est désactivée.

Valeurs possibles :

- `10 Mbit/s HDX`
  Connexion half duplex
- `10 Mbit/s FDX`
  Connexion full duplex
- `100 Mbit/s HDX`
  Connexion half duplex
- `100 Mbit/s FDX`
  Connexion full duplex
- `1000 Mbit/s FDX`
  Connexion full duplex
- `2500 Mbit/s FDX`
  Connexion full duplex

Commentaire : Les modes opérationnels du port actuellement disponibles dépendent de la configuration de l'équipement.

Link/Current settings

Affiche le mode de fonctionnement actuellement utilisé par le port.

Valeurs possibles :

- `-`
  Aucun câble connecté, aucune liaison.
- `10 Mbit/s HDX`
  Connexion half duplex
- `10 Mbit/s FDX`
  Connexion full duplex
- `100 Mbit/s HDX`
  Connexion half duplex
- `100 Mbit/s FDX`
  Connexion full duplex
- `1000 Mbit/s FDX`
  Connexion full duplex
- `2500 Mbit/s FDX`
  Connexion full duplex

Commentaire : Les modes opérationnels du port actuellement disponibles dépendent de la configuration de l'équipement.

Manual cable crossing (Auto. conf. off)

Spécifie les équipements connectés à un port TP.

La condition préalable est que la fonction *Automatic configuration* soit désactivée.

Valeurs possibles :

- *mdi*
  L'équipement intervertit les paires de lignes d'émission et de réception sur le port.

- `mdix` (réglage par défaut sur les ports TP)
  L'équipement prévient l'inversion des paires de lignes d'émission et de réception sur le port.
- `auto-mdix`
  L'équipement détecte les paires de lignes d'émission et de réception de l'équipement connecté et s'adapte automatiquement.
  Exemple : lorsque vous connectez un équipement terminal à l'aide d'un câble croisé, l'équipement réinitialise automatiquement le port de `mdix` sur `mdi`.
- `unsupported` (non pris en charge) (réglage par défaut sur les ports optiques ou les TP-SFP ports)
  Le port ne prend pas en charge cette fonction.

Flow control

Active/désactive le contrôle de flux sur le port.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  Le contrôle de flux sur le port est activé.
  L'envoi et l'évaluation des paquets de pause (fonctionnement full duplex) ou les collisions (fonctionnement half duplex) sont activés sur le port.
  - ☐ Pour activer le contrôle de flux dans l'équipement, activez aussi la fonction *Flow control* dans la boîte de dialogue *Switching > Global*.
  - ☐ Activez le contrôle de flux aussi sur le port de l'équipement connecté à ce port.

  Sur un port uplink, l'activation du contrôle de flux peut provoquer des interruptions d'envoi indésirables dans le segment de réseau de niveau supérieur (« wandering backpressure »).
- `case non cochée`
  Le contrôle de flux du port est désactivé.

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.

Send trap (Link up/down)

Active/désactive l'envoi de traps SNMP lorsque l'équipement détecte un changement dans l'état up/down du lien pour ce port.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'envoi de traps SNMP est activé.
  Lorsque l'équipement détecte un changement d'état up/down du lien, il envoie un trap SNMP.
- `case non cochée`
  L'envoi de traps SNMP est désactivé.

Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

MTU

Spécifie la taille maximale admissible des paquets Ethernet sur le port en octets.

Valeurs possibles :

- `1518..9720` (réglage par défaut : `1518`)
  Avec le réglage `1518`, le port transmet les paquets Ethernet jusqu'à la taille suivante :
  - 1518 octets sans tag de VLAN
    (1514 octets + 4 octets CRC)
  - 1522 octets avec tag de VLAN
    (1518 octets + 4 octets CRC)

Ce réglage vous permet d'augmenter la taille maximale admissible des paquets Ethernet que ce port peut recevoir ou transmettre.

La liste suivante contient les applications possibles :

- Lorsque vous utilisez l'équipement dans le réseau de transfert avec double taggage VLAN, vous pouvez avoir besoin d'une *MTU* supérieure à 4 octets.

Sur d'autres interfaces, vous spécifiez la taille maximale admissible pour les paquets Ethernet comme suit :

- Interfaces *Link Aggregation*
  Boîte de dialogue *Switching > L2-Redundancy > Link Aggregation*, colonne *MTU*

Signal

Active/désactive le clignotement de la LED du port. La fonction vous permet d'identifier le port dans le champ.

Valeurs possibles :

- `case cochée`
  Le clignotement de la LED du port est activé.
  La LED du port clignote jusqu'à ce que vous désactiviez la fonction de nouveau.
- `case non cochée` (réglage par défaut)
  Le clignotement de la LED du port est désactivé.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Clear port statistics

Remet le compteur des statistiques du port à `0`.

[Statistics]

Cet onglet affiche la vue d'ensemble suivante pour chaque port :

- Nombre de paquets de données/octets reçus dans l'équipement
  - *Received packets*
  - *Received octets*
  - *Received unicast packets*
  - *Received multicast packets*
  - *Received broadcast packets*
- Nombre de paquets de données/octets envoyés depuis l'équipement
  - *Transmitted packets*
  - *Transmitted octets*
  - *Transmitted unicast packets*
  - *Transmitted multicast packets*
  - *Transmitted broadcast packets*
- Nombre d'erreurs détectées par l'équipement
  - *Received fragments*
  - *Detected CRC errors*
  - *Detected collisions*
- Nombre de paquets de données par catégorie de taille reçus dans l'équipement
  - *Packets 64 bytes*
  - *Packets 65 to 127 bytes*
  - *Packets 128 to 255 bytes*
  - *Packets 256 to 511 bytes*
  - *Packets 512 to 1023 bytes*
  - *Packets 1024 to 1518 bytes*
- Nombre de paquets de données rejetés par l'équipement
  - *Received discards*
  - *Transmitted discards*

Pour trier la table selon un critère spécifique, cliquez sur l'en-tête de la ligne correspondante.

Par exemple, pour trier la table en fonction du nombre d'octets reçus par ordre croissant, cliquez une fois sur l'en-tête de la colonne *Received octets*. Pour le trier dans l'ordre décroissant, cliquez de nouveau sur l'en-tête.

Pour remettre le compteur des statistiques du port dans la table à `0`, exécutez les étapes suivantes :

- ☐ Dans la boîte de dialogue *Basic Settings > Port*, cliquez sur le bouton ☰, puis sur l'élément *Clear port statistics*.
  ou
- ☐ Dans la boîte de dialogue *Basic Settings > Restart*, cliquez sur le bouton *Clear port statistics*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Clear port statistics

Remet le compteur des statistiques du port à `0`.

[Utilization]

Cet onglet affiche l'utilisation (charge du réseau) des ports individuels.

Table

Port

Affiche le numéro de port.

Utilization [%]

Affiche l'utilisation actuelle en pourcentage par rapport à l'intervalle de temps spécifié dans la colonne *Control interval [s]*.

L'utilisation est le rapport entre la quantité de données reçues et la quantité de données maximale possible pour le débit actuellement configuré.

Lower threshold [%]

Spécifie un seuil inférieur pour l'utilisation. Si l'utilisation du port chute en deçà de cette valeur, la colonne *Alarm* affiche une alarme.

Valeurs possibles :

- `0.00..100.00` (réglage par défaut : `0.00`)

La valeur `0` désactive le seuil inférieur.

Upper threshold [%]

Spécifie un seuil supérieur pour l'utilisation. Si l'utilisation du port va au-delà de cette valeur, la colonne *Alarm* affiche une alarme.

Valeurs possibles :

- `0.00..100.00` (réglage par défaut : `0.00`)

La valeur `0` désactive le seuil supérieur.

Control interval [s]

Spécifie l'intervalle en secondes.

Valeurs possibles :

- `1..3600` (réglage par défaut : `30`)

Alarm

Affiche l'état de l'alarme d'utilisation.

Valeurs possibles :

- `case cochée`
  L'utilisation du port est inférieure à la valeur spécifiée dans la colonne *Lower threshold [%]* ou supérieure à la valeur spécifiée dans la colonne *Upper threshold [%]*. L'équipement envoie un trap SNMP.
- `case non cochée`
  L'utilisation du port est supérieure à la valeur spécifiée dans la colonne *Lower threshold [%]* et inférieure à la valeur spécifiée dans la colonne *Upper threshold [%]*.
  Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Clear port statistics

Remet le compteur des statistiques du port à `0`.

1.8 Power over Ethernet (MCSESP)

[Basic Settings > Power over Ethernet]

Avec Power-over-Ethernet (PoE), l'équipement de source d'alimentation (PSE, Power Sourcing Equipement) fournit du courant aux dispositifs alimentés (PD, Powered Devices), tels que les téléphones IP, via le câble à paire torsadée.

Le code produit et l'étiquetage spécifique à PoE sur le boîtier de l'équipement PSE indiquent si votre dispositif prend en charge *Power over Ethernet*. Les ports PoE du dispositif prennent en charge Power-over-Ethernet conformément à la norme IEEE 802.3at.

Le système fournit un budget de puissance maximum interne pour les ports. Les ports prévoient une réserve de puissance en fonction de la classe détectée pour un dispositif alimenté connecté. La puissance réelle fournie est égale ou inférieure à la puissance réservée.

Vous gérez la puissance de sortie avec le paramètre *Priority*. Lorsque la somme de la puissance requise par les dispositifs connectés dépasse la puissance disponible, le dispositif coupe l'alimentation fournie aux ports en fonction de la priorité configurée. Le dispositif coupe l'alimentation des ports en commençant par les ports configurés avec une faible priorité. Lorsque plusieurs ports ont une faible priorité, le dispositif coupe l'alimentation en commençant par les ports ayant le numéro le plus élevé.

Le menu contient les boîtes de dialogue suivantes :
- PoE Global
- PoE Port

1.8.1 PoE Global

[Basic Settings > Power over Ethernet > Global]

En fonction des réglages spécifiés dans cette boîte de dialogue, le dispositif alimente les équipements de l'utilisateur final. Si la puissance consommée atteint le seuil défini par l'utilisateur, l'équipement envoie un trap SNMP.

Operation

Operation

Active/désactive la fonction *Power over Ethernet*.

Valeurs possibles :

- `On` (réglage par défaut)
  La fonction *Power over Ethernet* est activée.
- `Off`
  La fonction *Power over Ethernet* est désactivée.

Configuration

Send trap

Active/désactive l'envoi de traps SNMP.

Si la puissance consommée dépasse le seuil défini par l'utilisateur, l'équipement envoie un trap SNMP.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'équipement envoie des traps SNMP.
- `case non cochée`
  L'équipement n'envoie pas de traps SNMP.

Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

Threshold [%]

Spécifie la valeur seuil de la puissance consommée en pourcentage.

Si la puissance de sortie dépasse ce seuil, l'équipement mesure la puissance de sortie totale et envoie un trap SNMP.

Valeurs possibles :

- `0..99` (réglage par défaut : `90`)

System power

Budget [W]

Affiche la somme de la puissance disponible pour le budget global.

Reserved [W]

Affiche la puissance globale réservée. L'équipement prévoit une réserve de puissance en fonction des classes détectées pour les dispositifs alimentés connectés. La puissance réservée est égale ou inférieure à la puissance réelle fournie.

Delivered [W]

Affiche la puissance réelle fournie aux modules en watts.

Delivered [mA]

Affiche le courant réel fourni aux modules en milliampères.

Table

Module

Module du dispositif auquel se rapportent les entrées de la table.

Configured power budget [W]

Spécifie la puissance des modules pour la distribution aux ports.

Valeurs possibles :

- `0..n` (réglage par défaut : n)
  Ici, `n` correspond à la valeur de la colonne *Max. power budget [W]*.

Max. power budget [W]

Affiche la puissance maximale disponible pour ce module.

Reserved power [W]

Affiche la puissance réservée pour le module en fonction des classes détectées pour les dispositifs alimentés connectés.

Delivered power [W]

Affiche la puissance réelle en watts fournie aux dispositifs alimentés connectés à ce port.

Delivered current [mA]

Affiche le courant réel en milliampères fourni aux dispositifs alimentés connectés à ce port.

Power source

Affiche l'équipement de source d'alimentation du dispositif.

Valeurs possibles :

- *internal*
  Source d'alimentation interne
- *external*
  Source d'alimentation externe

Threshold [%]

Spécifie la valeur seuil de la puissance consommée par le module en pourcentage. Si la puissance de sortie dépasse ce seuil, l'équipement mesure la puissance de sortie totale et envoie un trap SNMP.

Valeurs possibles :

- `0..99` (réglage par défaut : `90`)

Send trap

Active/désactive l'envoi de traps SNMP si le dispositif détecte que la valeur seuil de la puissance consommée est dépassée.

Valeurs possibles :

- `case cochée`
  L'envoi de traps SNMP est activé.
  Si la puissance consommée dépasse le seuil défini par l'utilisateur, l'équipement envoie un trap SNMP.
- `case non cochée` (réglage par défaut)
  L'envoi de traps SNMP est désactivé.

Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

1.8.2 PoE Port

[Basic Settings > Power over Ethernet > Port]

Lorsque la puissance consommée est supérieure à la puissance pouvant être fournie, l'équipement coupe l'alimentation des dispositifs alimentés (PD) en fonction des niveaux de priorité et des numéros de port. Lorsque les PD connectés nécessitent plus d'énergie que celle fournie par l'équipement, ce dernier désactive la fonction *Power over Ethernet* sur les ports. L'équipement désactive d'abord la fonction *Power over Ethernet* sur les ports ayant la priorité la plus basse. Lorsque plusieurs ports ont la même priorité, l'équipement désactive d'abord la fonction *Power over Ethernet* sur les ports ayant le numéro de port le plus élevé. L'équipement coupe également l'alimentation des dispositifs alimentés (PD) pendant un délai spécifié.

Table

Port

Affiche le numéro de port.

PoE enable

Active/désactive l'alimentation PoE fournie au port.

Lorsque la fonction est activée ou désactivée, l'équipement consigne un événement dans le fichier log (System Log).

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'alimentation PoE du port est activée.
- `case non cochée`
  L'alimentation PoE du port est désactivée.

Fast startup

Active/désactive la fonction de démarrage rapide de Power-over-Ethernet sur le port.

La condition préalable est que la case dans la colonne *PoE enable* soit cochée.

Valeurs possibles :

- `case cochée`
  La fonction de démarrage rapide est activée. L'équipement alimente les dispositifs alimentés (PD) immédiatement après la mise sous tension de l'équipement.
- `case non cochée` (réglage par défaut)
  La fonction de démarrage rapide est désactivée. L'équipement alimente les dispositifs alimentés (PD) après avoir chargé sa propre configuration.

Priority

Spécifie la priorité du port.

Pour éviter les surcharges de courant, l'équipement désactive d'abord les ports à faible priorité. Pour éviter que l'équipement ne désactive les ports alimentant des dispositifs essentiels, spécifiez une priorité élevée pour ces ports.

Valeurs possibles :

- *critical*
- *high*
- *low* (réglage par défaut)

Status

Affiche l'état du port de détection du dispositif alimenté (PD).

Valeurs possibles :

- *disabled*
  L'équipement est à l'état DISABLED et ne fournit pas de courant aux dispositifs alimentés.
- *deliveringPower*
  L'équipement a identifié la classe du PD connecté et se trouve à l'état POWER ON.
- *fault*
  L'équipement est à l'état TEST ERROR.
- *otherFault*
  L'équipement est à l'état IDLE.
- *searching*
  L'équiepement est dans un état autre que ceux énumérés.
- *test*
  L'équipement est en TEST MODE.

Detected class

Affiche la classe de puissance du dispositif alimenté connecté au port.

Valeurs possibles :

- *Class 0*
- *Class 1*
- *Class 2*
- *Class 3*
- *Class 4*

Class 0
Class 1
Class 2
Class 3
Class 4

Active/désactive le courant des classes 0 à 4 sur le port.

Valeurs possibles :

- case cochée (réglage par défaut)
- case non cochée

Consumption [W]

Affiche la puissance consommée actuelle du port en watts.

Valeurs possibles :

▶ `0,0..30,0`

Consumption [mA]

Affiche le courant fourni au port en milliampères.

Valeurs possibles :

▶ `0..600`

Power limit [W]

Spécifie la puissance de sortie maximale en watts du port.

Cette fonction vous permet de répartir le budget de puissance disponible entre les ports PoE selon les besoins.

Le port réserve, par exemple, une quantité fixe de 15,4 W (classe 0) pour un dispositif connecté ne fournissant pas de « classe de puissance », même si le dispositif requiert une puissance moindre. La puissance excédentaire ne peut être utilisée par aucun autre port.

En spécifiant la limite de puissance, vous réduisez la puissance réservée aux besoins réels du dispositif connecté. La puissance non utilisée est disponible sur les autres ports.

Si la puissance consommée exacte du dispositif alimenté connecté est inconnue, le dispositif affiche la valeur dans la colonne *Max. consumption [W]*. Vérifiez que la limite de puissance est supérieure à la valeur de la colonne *Max. consumption [W]*.

Si la puissance maximale observée est supérieure à la limite de puissance définie, le dispositif considère la limite de puissance comme non valide. Dans ce cas, le dispositif utilise la classe PoE pour le calcul.

Valeurs possibles :

▶ `0,0..30,0` (réglage par défaut : `0`)

Max. consumption [W]

Affiche la puissance maximale en watts que le dispositif a consommée jusqu'à présent.

Vous réinitialisez cette valeur lorsque vous désactivez le PoE sur le port ou que vous mettez fin à la connexion avec le dispositif connecté.

Name

Spécifie le nom du port.

Spécifiez le nom de votre choix.

Valeurs possibles :

- Chaîne de 0..32 caractères ASCII alphanumériques

Auto-shutdown power

Active/désactive la fonction *Auto-shutdown power* en fonction des réglages.

Valeurs possibles :

- `case cochée`
- `case non cochée` (réglage par défaut)

Disable power at [hh:mm]

Spécifie l'heure à laquelle l'équipement désactive l'alimentation du port lors de l'activation de la fonction *Auto-shutdown power*.

Valeurs possibles :

- `00:00..23:59` (réglage par défaut : `00:00`)

Re-enable power at [hh:mm]

Spécifie l'heure à laquelle l'équipement active l'alimentation du port lors de l'activation de la fonction *Auto-shutdown power*.

Valeurs possibles :

- `00:00..23:59` (réglage par défaut : `00:00`)

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

1.9 Restart

[Basic Settings > Restart]

Cette boîte de dialogue vous permet de redémarrer l'équipement, de réinitialiser les compteurs du port et les tables d'adresses ainsi que de supprimer les fichiers journaux.

Restart

Restart in

Affiche le délai restant jusqu'au redémarrage de l'équipement.

Pour mettre à jour l'affichage du délai restant, cliquez sur le bouton .

Cancel

Annule un redémarrage retardé.

Cold start...

Ouvre la boîte de dialogue *Restart* pour initier un redémarrage immédiat ou retardé de l'équipement.

Si le profil de configuration dans la mémoire volatile (*RAM*) et le profil de configuration « Selected » (Sélectionné) dans la mémoire non-volatile (*NVM*) sont différents, l'équipement affiche la boîte de dialogue *Warning*.

- Pour sauvegarder les modifications de façon permanente, cliquez sur le bouton *Yes* dans la boîte de dialogue *Warning*.
- Pour annuler les modifications, cliquez sur le bouton *No* dans la boîte de dialogue *Warning*.
- Dans le champ *Restart in*, vous spécifiez le délai pour le redémarrage retardé.
  Valeurs possibles :
  - `00:00:00..596:31:23` (réglage par défaut : `00:00:00`)

Une fois le délai écoulé, l'équipement redémarre et enchaîne les phases suivantes :

- Si vous activez la fonction dans la boîte de dialogue *Diagnostics > System > Selftest*, l'équipement exécute un test de RAM.
- L'équipement démarre le logiciel affiché dans le champ *Stored version* de la boîte de dialogue *Basic Settings > Software*.
- L'équipement charge les réglages du profil de configuration « Selected ». Voir la boîte de dialogue *Basic Settings > Load/Save*.

Commentaire : Lors du redémarrage, l'équipement ne transfère aucune donnée. Durant ce délai, l'équipement est inaccessible via l'interface utilisateur graphique ou tout autre système d'administration.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset MAC address table

Supprime de la table de transfert les adresses MAC avec, dans la boîte de dialogue *Switching > Filter for MAC Addresses*, la valeur `learned` dans la colonne *Status*.

Reset ARP table

Supprime les adresses configurées dynamiquement de la table ARP.

Voir la boîte de dialogue *Diagnostics > System > ARP*.

Clear port statistics

Remet le compteur des statistiques du port à `0`.

Voir la boîte de dialogue *Basic Settings > Port*, onglet *Statistics*.

Clear management access statistics

Remet les compteurs des statistiques sur l'accès à l'administration de l'équipement à `0`.

Voir la boîte de dialogue *Diagnostics > System > System Information*, table `Used Management Ports`.

Reset IGMP snooping data

Supprime les entrées IGMP Snooping et remet le compteur dans le cadre *Information* à `0`.

Voir la boîte de dialogue *Switching > IGMP Snooping > Global*.

Delete log file

Supprime les événements consignés dans le fichier log.

Voir la boîte de dialogue *Diagnostics > Report > System Log*.

Delete persistent log file

Efface les fichiers log de la mémoire externe.

Voir la boîte de dialogue *Diagnostics > Report > Persistent Logging*.

Clear email notification statistics

Remet les compteurs du cadre *Information* à `0`.

Voir la boîte de dialogue *Diagnostics > Email Notification > Global*.

2 Time

Le menu contient les boîtes de dialogue suivantes :
- Basic Settings
- SNTP
- PTP
- 802.1AS

2.1 Basic Settings

[Time > Basic Settings]

L'équipement est doté d'une horloge matérielle à batterie tampon. Cette horloge continue à donner l'heure exacte même en cas de panne de l'alimentation ou lorsque l'équipement est débranché. Une fois l'équipement démarré, vous avez accès à l'heure actuelle, par exemple pour les entrées du log.

L'horloge matérielle permet de couvrir un temps d'arrêt de l'alimentation en tension de 3 heures. Il convient pour cela que l'alimentation en tension de l'équipement ait été préalablement raccordée de manière continue pendant au moins 5 minutes.

Cette boîte de dialogue vous permet d'effectuer des réglages de l'heure indépendamment du protocole de synchronisation de l'heure spécifié.

La boîte de dialogue contient les onglets suivants :
- [Global]
- [Daylight saving time]

[Global]

Cet onglet vous permet de spécifier l'heure système et le fuseau horaire de l'équipement.

Configuration

System time (UTC)

Affiche la date et l'heure actuelles en se référant au temps universel coordonné (UTC).

Set time from PC

L'équipement utilise l'heure du PC en tant qu'heure système.

System time

Affiche la date et l'heure actuelles en référence à l'heure locale : *System time* = *System time (UTC)* + *Local offset [min]* + *Daylight saving time*

Time source

Affiche la source de temps à partir de laquelle l'équipement obtient les informations temporelles.

L'équipement sélectionne automatiquement la source de temps disponible la plus précise.

Valeurs possibles :

- *local*
  Horloge système de l'équipement.
- *sntp*
  Le client *SNTP* est activé et l'équipement est synchronisé par un serveur *SNTP*.
- *ptp*
  PTP est activé et l'horloge de l'équipement est synchronisée avec une horloge maîtresse *PTP*.

Local offset [min]

Spécifie la différence entre l'heure locale et *System time (UTC)* en minutes : *Local offset [min]* = *System time* − *System time (UTC)*

Valeurs possibles :

- -780..840 (réglage par défaut : 60)

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Daylight saving time]

Cet onglet vous permet d'activer la fonction d'heure d'été. Vous pouvez spécifier le début et la fin de l'heure d'été en utilisant un profil pré-défini, ou vous pouvez spécifier ces réglages individuellement. Pendant l'heure d'été, l'équipement avance l'heure locale d'1 heure.

Operation

Daylight saving time

Permet d'activer/de désactiver le mode *Daylight saving time*.

Valeurs possibles :

- *On*
  Le mode *Daylight saving time* est activé.
  L'équipement bascule automatiquement entre l'heure d'hiver et l'heure d'été.
- *Off* (réglage par défaut)
  Le mode *Daylight saving time* est désactivé.

Les heures auxquelles l'équipement bascule entre l'heure d'été et l'heure d'hiver sont spécifiées dans les cadres *Summertime begin* et *Summertime end*.

Profile...

Affiche la boîte de dialogue *Profile...*. Vous pouvez y sélectionnez un profil prédéfini pour le début et la fin de l'heure d'été. Ce profil écrase les réglages spécifiés dans les cadres *Summertime begin* et *Summertime end*.

Summertime begin

Dans les 3 premiers champs, vous pouvez spécifier le jour de début de l'heure d'été, et dans le dernier champ, l'heure.

Lorsque l'heure spécifiée dans le champ *System time* atteint la valeur saisie ici, l'équipement passe à l'heure d'été.

Week

Indique la semaine du mois actuel.

Valeurs possibles :

- *none* (réglage par défaut)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Day

Indique le jour de la semaine.

Valeurs possibles :

- *none* (réglage par défaut)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Month

Indique le mois.

Valeurs possibles :

- *none* (réglage par défaut)
- *January*
- *February*
- *March*
- *April*
- *May*

- *June*
- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

System time

Indique l'heure.

Valeurs possibles :

- <HH:MM> (réglage par défaut : 00:00)

Summertime end

Dans les 3 premiers champs, vous pouvez spécifier le jour de fin de l'heure d'été, et dans le dernier champ, l'heure.

Lorsque l'heure spécifiée dans le champ *System time* atteint la valeur saisie ici, l'équipement passe à l'heure d'hiver.

Week

Indique la semaine du mois actuel.

Valeurs possibles :

- *none* (réglage par défaut)
- *first*
- *second*
- *third*
- *fourth*
- *last*

Day

Indique le jour de la semaine.

Valeurs possibles :

- *none* (réglage par défaut)
- *Sunday*
- *Monday*
- *Tuesday*
- *Wednesday*
- *Thursday*
- *Friday*
- *Saturday*

Month

Indique le mois.

Valeurs possibles :
- *none* (réglage par défaut)
- *January*
- *February*
- *March*
- *April*
- *May*
- *June*
- *July*
- *August*
- *September*
- *October*
- *November*
- *December*

System time

Indique l'heure.

Valeurs possibles :
- <HH:MM> (réglage par défaut : 00:00)

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

2.2 SNTP

[Time > SNTP]

Le Simple Network Time Protocol (SNTP) est une procédure décrite dans RFC 4330 destinée à la synchronisation de l'heure dans le réseau.

L'équipement vous permet de synchroniser l'heure système de l'équipement en tant que client *SNTP*. En tant que serveur *SNTP*, l'équipement met les informations temporelles à la disposition d'autres équipements.

Le menu contient les boîtes de dialogue suivantes :
- SNTP Client
- SNTP Server

2.2.1 SNTP Client

[Time > SNTP > Client]

Cette boîte de dialogue vous permet d'effectuer des réglages avec lesquels l'équipement fonctionne en tant que client *SNTP*.

En tant que client *SNTP*, l'équipement obtient les informations temporelles à la fois de la part des serveurs *SNTP* et des serveurs *NTP*, et synchronise l'horloge locale avec l'heure du serveur de temps.

Operation

Operation

Active/désactive la fonction *SNTP Client* de l'équipement.

Valeurs possibles :

- `On`
  La fonction *SNTP Client* est activée.
  L'équipement fonctionne en tant que client *SNTP*.
- `Off` (réglage par défaut)
  La fonction *SNTP Client* est désactivée.

Configuration

Mode

Indique si l'équipement demande activement les informations temporelles à un serveur *SNTP* connu et configuré sur le réseau (mode Unicast) ou attend passivement de recevoir les informations temporelles de la part d'un serveur *SNTP* aléatoire (mode Broadcast).

Valeurs possibles :

- `unicast` (réglage par défaut)
  L'équipement récupère uniquement les informations temporelles provenant du serveur *SNTP* configuré. L'équipement envoie des requêtes Unicast au serveur *SNTP* et évalue ses réponses.
- `broadcast`
  L'équipement obtient les informations temporelles provenant uniquement d'un ou plusieurs serveurs *SNTP* ou *NTP*. L'équipement évalue les broadcasts ou multicasts provenant uniquement de ces serveurs.

Request interval [s]

Indique l'intervalle en secondes selon lequel l'équipement demande les informations temporelles au serveur *SNTP*.

Valeurs possibles :

- `5..3600` (réglage par défaut : `30`)

Broadcast recv timeout [s]

Indique le temps en secondes pendant lequel un client patiente en mode client broadcast avant de remplacer la valeur du champ `syncToRemoteServer` par `notSynchronized` lorsque le client ne reçoit pas de paquets broadcast.

Valeurs possibles :

- `128..2048` (réglage par défaut : `320`)

Disable client after successful sync

Active/désactive la désactivation du client *SNTP* une fois que l'équipement a synchronisé le temps avec succès.

Valeurs possibles :

- `case cochée`
  La désactivation du client *SNTP* est activée.
  L'équipement désactive le client *SNTP* après avoir synchronisé le temps avec succès.
- `case non cochée` (réglage par défaut)
  La désactivation du client *SNTP* est désactivée.
  Le client *SNTP* reste activé après avoir synchronisé le temps avec succès.

State

State

Affiche l'état du client *SNTP*.

Valeurs possibles :

- *disabled*
  Le client *SNTP* est désactivé.
- *notSynchronized*
  Le client *SNTP* n'est synchronisé avec aucun serveur *SNTP* ou *NTP*.
- *synchronizedToRemoteServer*
  Le client *SNTP* est synchronisé avec un serveur *SNTP* ou *NTP*.

Table

Dans la table, vous pouvez spécifier les réglages pour un maximum de 4 serveurs *SNTP*.

Index

Affiche l'index auquel l'entrée de table se réfère.

Valeurs possibles :

- `1..4`

l'équipement affecte automatiquement ce numéro.

Si vous supprimez une entrée de table, il reste un blanc dans la numérotation. Si vous créez une entrée de table, l'équipement remplit le 1er blanc.

Après le démarrage, l'équipement envoie des requêtes au serveur *SNTP* configuré dans la première entrée de la table. Lorsque le serveur ne répond pas, l'équipement envoie ses requêtes au serveur *SNTP* configuré dans l'entrée de table suivante.

Si aucun des serveurs *SNTP* configurés ne répond, le client *SNTP* interrompt sa synchronisation. L'équipement envoie des requêtes de manière cyclique à chaque serveur *SNTP* jusqu'à ce qu'un serveur lui fournisse une heure valide. L'équipement se synchronise avec ce serveur *SNTP* même si les autres serveurs sont à nouveau joignables ultérieurement.

Name

Indique le nom du serveur *SNTP*.

Valeurs possibles :

- Chaîne de 1..32 caractères ASCII alphanumériques

Address

Indique l'adresse IP du serveur *SNTP*.

Valeurs possibles :

- Adresse IPv4 valide (réglage par défaut : `0.0.0.0`)
- Adresse IPv6 valide
- Nom d'hôte

Destination UDP port

Indique le port UDP sur lequel le serveur *SNTP* s'attend à recevoir les informations temporelles.

Valeurs possibles :

- `1..65535` (réglage par défaut : `123`)
  Exception : le port `2222` est réservé à des fonctions internes.

Status

Affiche l'état de la connexion entre le client *SNTP* et le serveur *SNTP*.

Valeurs possibles :

- *`success`*
  L'équipement a correctement synchronisé l'heure avec le serveur *SNTP*.

- *badDateEncoded*
  Les informations temporelles reçues contiennent des erreurs de protocole - la synchronisation a échoué.
- *other*
  - La valeur 0.0.0.0 est saisie pour l'adresse IP du serveur *SNTP* - la synchronisation a échoué.
    ou
  - Le client *SNTP* utilise un serveur *SNTP* différent.
- *requestTimedOut*
  L'équipement n'a pas reçu de réponse de la part du serveur *SNTP* - la synchronisation a échoué.
- *serverKissOfDeath*
  Le serveur *SNTP* est surchargé. L'équipement est invité à se synchroniser avec un autre serveur *SNTP*. Lorsqu'aucun autre serveur *SNTP* n'est disponible et que le serveur demeure surchargé, l'équipement vérifie la disponibilité du serveur avec des intervalles plus longs que le réglage spécifié dans le champ *Request interval [s]*.
- *serverUnsychronized*
  Le serveur *SNTP* n'est synchronisé ni avec une source de l'heure locale ni avec une source de temps de référence externe - la synchronisation a échoué.
- *versionNotSupported*
  Les versions du protocole *SNTP* du client et du serveur sont incompatibles - la synchronisation a échoué.

Active

Active/désactive la connexion au serveur *SNTP*.

Valeurs possibles :

- case cochée
  La connexion au serveur *SNTP* est activée.
  Le client *SNTP* a accès au serveur *SNTP*.
- case non cochée (réglage par défaut)
  La connexion au serveur *SNTP* est désactivée.
  Le client *SNTP* n'a pas accès au serveur *SNTP*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

2.2.2 SNTP Server

[Time > SNTP > Server]

Cette boîte de dialogue vous permet d'effectuer des réglages avec lesquels l'équipement fonctionne en tant que serveur *SNTP*.

Le serveur *SNTP* fournit le temps universel coordonné (UTC) indépendamment des différences avec l'heure locale.

Si le réglage est approprié, le serveur *SNTP* fonctionne en mode Broadcast. En mode Broadcast, le serveur *SNTP* envoie automatiquement des messages broadcast ou multicast selon l'intervalle d'envoi de broadcast.

Operation

Operation

Active/désactive la fonction *SNTP Server* de l'équipement.

Valeurs possibles :

- *On*
  La fonction *SNTP Server* est activée.
  L'équipement fonctionne en tant que serveur *SNTP*.
- *Off* (réglage par défaut)
  La fonction *SNTP Server* est désactivée.

Notez le réglage dans la case à cocher *Disable server at local time source* du cadre *Configuration*.

Configuration

UDP port

Indique le numéro du port UDP sur lequel le serveur *SNTP* de l'équipement reçoit les requêtes provenant d'autres client.

Valeurs possibles :

- `1..65535` (réglage par défaut : `123`)
  Exception : le port `2222` est réservé à des fonctions internes.

Broadcast admin mode

Active/désactive le mode Broadcast.

- `case cochée`
  Le serveur *SNTP* répond aux requêtes provenant des clients *SNTP* en mode Unicast et envoie également des paquets *SNTP* en mode Broadcast en tant que broadcasts ou multicasts.
- `case non cochée` (réglage par défaut)
  Le serveur *SNTP* répond aux requêtes provenant des clients *SNTP* en mode Unicast.

Broadcast destination address

Indique l'adresse IP à laquelle le serveur *SNTP* de l'équipement envoie les paquets *SNTP* en mode Broadcast.

Valeurs possibles :

- Adresse IPv4 valide (réglage par défaut : `0.0.0.0`)

Les adresses broadcast et multicast sont autorisées.

Broadcast UDP port

Indique le numéro du port UDP sur lequel le serveur *SNTP* envoie les paquets *SNTP* en mode Broadcast.

Valeurs possibles :

- `1..65535` (réglage par défaut : `123`)
  Exception : le port `2222` est réservé à des fonctions internes.

Broadcast VLAN ID

Indique l'ID du VLAN auquel le serveur *SNTP* de l'équipement envoie les paquets *SNTP* en mode Broadcast.

Valeurs possibles :

- `0`
  Le serveur *SNTP* envoie les paquets *SNTP* au VLAN sur lequel l'accès à l'administration de l'équipement est possible. Voir la boîte de dialogue *Basic Settings > Network*.
- `1..4042` (réglage par défaut : `1`)

Broadcast send interval [s]

Indique l'intervalle de temps dans lequel le serveur *SNTP* de l'équipement envoie des paquets *SNTP* broadcast.

Valeurs possibles :

- `64..1024` (réglage par défaut : `128`)

Disable server at local time source

Active/désactive la désactivation du serveur *SNTP* lorsque l'équipement est synchronisé avec l'horloge locale.

Valeurs possibles :

- `case cochée`
  La désactivation du serveur *SNTP* est activée.
  Si l'équipement est synchronisé avec l'horloge locale, l'équipement désactive le serveur *SNTP*. Le serveur *SNTP* continue de répondre aux requêtes provenant des clients *SNTP*. Dans le paquet *SNTP*, le serveur *SNTP* informe les clients qu'il est synchronisé localement.
- `case non cochée` (réglage par défaut)
  La désactivation du serveur *SNTP* est désactivée.
  Si l'équipement est synchronisé avec l'horloge locale, le serveur *SNTP* reste activé.

State

State

Affiche l'état du serveur *SNTP*.

Valeurs possibles :

- *disabled*
  Le serveur *SNTP* est désactivé.
- *notSynchronized*
  Le serveur *SNTP* n'est synchronisé ni avec une source de l'heure locale ni avec une source de temps de référence externe.
- *syncToLocal*
  Le serveur *SNTP* est synchronisé avec l'horloge matérielle de l'équipement.
- *syncToRefclock*
  Le serveur *SNTP* est synchronisé avec une source de temps de référence externe, par exemple PTP.
- *syncToRemoteServer*
  Le serveur *SNTP* est synchronisé avec un serveur *SNTP* placé en amont de l'équipement au sein d'une cascade.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

2.3 PTP

[Time > PTP]

Le menu contient les boîtes de dialogue suivantes :

- PTP Global
- PTP Boundary Clock
- PTP Transparent Clock

2.3.1 PTP Global

[Time > PTP > Global]

Cette boîte de dialogue vous permet de spécifier les réglages de base du protocole *PTP*.

Le Precision Time Protocol (PTP) est une procédure décrite dans la norme IEEE 1588-2008 qui fournit une heure précise aux équipements du réseau. La méthode synchronise les horloges du réseau avec une précision de quelques 100 ns. Le protocole utilise la communication multicast, de sorte que la charge imposée au réseau par les messages de synchronisation *PTP* est négligeable.

Le PTP est bien plus précis que le SNTP. Si la fonction *SNTP* et la fonction *PTP* sont activées en même temps dans l'équipement, la fonction *PTP* est prioritaire.

Grâce à l'*algorithme de la meilleure horloge maîtresse*, les équipements du réseau déterminent l'équipement ayant l'heure la plus précise. Les équipements utilisent comme source de temps de référence l'équipement ayant l'heure la plus précise (*Grandmaster*). Les équipements participants se synchronisent alors avec cette source de temps de référence.

Si vous souhaitez distribuer l'heure PTP avec précision sur votre réseau, n'utilisez que des équipements avec un support hardware de PTP sur le trajet.

Le protocole fait la distinction entre les horloges suivantes :

- *Boundary Clock (BC)*
  Cette horloge possède un nombre quelconque de ports PTP et fonctionne à la fois comme maître *PTP* et comme esclave *PTP*. Dans son segment de réseau respectif, l'horloge fonctionne comme une horloge ordinaire.
  - En tant qu'esclave *PTP*, l'horloge se synchronise avec un maître *PTP* placé en amont de l'équipement au sein d'une cascade.
  - En tant que maître *PTP*, l'horloge transmet les informations temporelles via le réseau aux esclaves *PTP* placés en aval de l'équipement au sein d'une cascade.
- *Transparent Clock (TC)*
  Cette horloge possède un nombre quelconque de ports PTP. Contrairement à *Boundary Clock*, cette horloge corrige les informations temporelles avant de les transmettre, sans se synchroniser.

Operation IEEE1588/PTP

Operation IEEE1588/PTP

Active/désactive la fonction *PTP*.

La fonction *802.1AS* ou la fonction *PTP* peuvent être activées en même temps dans l'équipement.

Valeurs possibles :

- `On`
  La fonction *PTP* est activée.
  L'équipement synchronise son horloge avec PTP.
  Si la fonction *SNTP* et la fonction *PTP* sont activées en même temps dans l'équipement, la fonction *PTP* est prioritaire.
- `Off` (réglage par défaut)
  La fonction *PTP* est désactivée.
  L'équipement transmet les messages de synchronisation *PTP* sans apporter de correction sur chaque port.

Configuration IEEE1588/PTP

PTP mode

Spécifie la version et le mode PTP de l'horloge locale.

Valeurs possibles :

- *v2-transparent-clock* (réglage par défaut)
- *v2-boundary-clock*

Sync lower bound [ns]

Spécifie la valeur du seuil inférieur en nanosecondes pour la différence de chemin entre l'horloge locale et la source de temps de référence (*Grandmaster*). Si la différence de chemin mesurée est inférieure à cette valeur, l'horloge locale est considérée comme synchronisée.

Valeurs possibles :

- `0..999999999` (réglage par défaut : `30`)

Sync upper bound [ns]

Spécifie la valeur du seuil supérieur en nanosecondes pour la différence de chemin entre l'horloge locale et la source de temps de référence (*Grandmaster*). Si la différence de chemin mesurée est supérieure à cette valeur, l'horloge locale est considérée comme non synchronisée.

Valeurs possibles :

- `31..1000000000` (réglage par défaut : `5000`)

PTP management

Active/désactive la gestion PTP définie dans la norme PTP.

Valeurs possibles :

- `case cochée`
  La gestion PTP est activée.
- `case non cochée` (réglage par défaut)
  La gestion PTP est désactivée.

Status

Is synchronized

Affiche si l'horloge locale est synchronisée avec la source de temps de référence (*Grandmaster*).

Si la différence de chemin entre l'horloge locale et la source de temps de référence (*Grandmaster*) tombe en dessous du seuil inférieur de synchronisation, l'horloge locale est alors synchronisée. Ce statut est conservé jusqu'à ce que la différence de chemin dépasse une fois le seuil supérieur de synchronisation.

Vous spécifiez les seuils de synchronisation dans le cadre *Configuration IEEE1588/PTP*.

Max. offset absolute [ns]

Affiche la différence de temps maximale survenue (mesurée en nanosecondes) depuis que l'horloge locale a été synchronisée avec la source de temps de référence (*Grandmaster*).

PTP time

Affiche la date et l'heure de l'échelle de temps PTP lorsque l'horloge locale est synchronisée avec la source de temps de référence (*Grandmaster*). Format : `Mois Jour, Année hh:mm:ss AM/PM`

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

2.3.2 PTP Boundary Clock

[Time > PTP > Boundary Clock]

Ce menu vous permet de configurer le mode Boundary Clock pour l'horloge locale.

Le menu contient les boîtes de dialogue suivantes :
- PTP Boundary Clock Global
- PTP Boundary Clock Port

2.3.2.1 PTP Boundary Clock Global

[Time > PTP > Boundary Clock > Global]

Dans cette boîte de dialogue, vous saisissez les réglages généraux et communs à l'ensemble des ports du mode *Boundary Clock* pour l'horloge locale. La *Boundary Clock (BC)* fonctionne selon le protocole PTP version 2 (IEEE 1588-2008).

Les réglages sont effectifs lorsque l'horloge locale fonctionne comme *Boundary Clock (BC)*. Pour cela, vous devez sélectionner la valeur `v2-boundary-clock` dans le champ *PTP mode* de la boîte de dialogue *Time > PTP > Global*.

Operation IEEE1588/PTPv2 BC

Priority 1

Spécifie la *priorité 1* pour l'équipement.

Valeurs possibles :

- `0..255` (réglage par défaut : `128`)

L'*algorithme de la meilleure horloge maîtresse* évalue d'abord la *priorité 1* parmi les équipements participants afin de déterminer la source de temps de référence (*Grandmaster*).

Plus cette valeur est faible, plus il est probable que l'équipement devienne la source de temps de référence (*Grandmaster*). Voir le cadre *Grandmaster*.

Priority 2

Spécifie la *priorité 2* pour l'équipement.

Valeurs possibles :

- `0..255` (réglage par défaut : `128`)

Lorsque les critères précédemment évalués sont les mêmes pour plusieurs équipements, l'*algorithme de la meilleure horloge maîtresse* évalue la *priorité 2* des équipements participants.

Plus cette valeur est faible, plus il est probable que l'équipement devienne la source de temps de référence (*Grandmaster*). Voir le cadre *Grandmaster*.

Domain number

Affecte l'équipement à un domaine *PTP*.

Valeurs possibles :

- `0..255` (réglage par défaut : `0`)

L'équipement transmet les informations temporelles depuis et vers les équipements du même domaine uniquement.

Status IEEE1588/PTPv2 BC

Two step

Indique que l'horloge fonctionne en mode Two-Step.

Steps removed

Affiche le nombre de chemins de communication parcourus entre l'horloge locale de l'équipement et la source de temps de référence (*Grandmaster*).

Dans le cas d'un esclave *PTP*, la valeur `1` signifie que l'horloge est connectée à la source de temps de référence (*Grandmaster*) directement par 1 chemin de communication.

Offset to master [ns]

Affiche la différence mesurée (dérive) entre l'horloge locale et la source de temps de référence (*Grandmaster*) en nanosecondes. L'esclave *PTP* calcule la différence à partir des informations temporelles reçues.

En mode Two-Step, les informations temporelles se composent de 2 messages de synchronisation *PTP* qui sont envoyés cycliquement par le maître *PTP* :

- Le premier message de synchronisation (sync) contient une valeur estimative de l'heure exacte d'envoi du message.
- Le deuxième message de synchronisation (follow-up) contient l'heure exacte d'envoi du premier message.

L'esclave *PTP* utilise les deux messages de synchronisation *PTP* pour calculer la différence (dérive) avec le maître et corrige son horloge de cette différence. L'esclave *PTP* tient également compte de la valeur *Delay to master [ns]*.

Delay to master [ns]

Affiche le délai de transmission des messages de synchronisation *PTP* du maître *PTP* à l'esclave *PTP* en nanosecondes.

L'esclave *PTP* envoie un paquet « Demande de délai » au maître *PTP* et détermine ainsi l'heure exacte d'envoi du paquet. Lorsqu'il reçoit le paquet, le maître *PTP* génère un horodatage et le renvoie dans un paquet « Réponse de délai » à l'esclave *PTP*. L'esclave *PTP* utilise les deux paquets pour calculer le délai qu'il prend en compte à partir de la prochaine mesure de dérive.

La condition préalable est que la valeur du mécanisme de délai des ports esclaves soit spécifiée comme `e2e`.

Grandmaster

Ce cadre affiche les critères que l'*algorithme de la meilleure horloge maîtresse* utilise pour évaluer la source de temps de référence (*Grandmaster*).

L'algorithme évalue d'abord la *priorité 1* des équipements participants. L'équipement ayant la valeur la plus basse pour la *priorité 1* est désigné comme source de temps de référence (*Grandmaster*). Lorsque la valeur est la même pour plusieurs équipements, l'algorithme utilise le critère suivant ; lorsque cette valeur est également la même, l'algorithme utilise le critère qui suit celui-ci. Lorsque chaque valeur est la même pour plusieurs équipements, la valeur la plus basse du champ *Clock identity* décide quel équipement est désigné comme source de temps de référence (*Grandmaster*).

L'équipement vous permet d'influencer quel équipement du réseau est désigné comme source de temps de référence (*Grandmaster*). Pour ce faire, modifiez la valeur du champ *Priority 1* ou du champ *Priority 2* dans le cadre *Operation IEEE1588/PTPv2 BC*.

Priority 1

Affiche la *priorité 1* pour l'équipement qui est actuellement la source de temps de référence (*Grandmaster*).

Clock class

Affiche la classe de la source de temps de référence (*Grandmaster*). Paramètre pour l'*algorithme de la meilleure horloge maîtresse*.

Clock accuracy

Affiche la précision estimée de la source de temps de référence (*Grandmaster*). Paramètre pour l'*algorithme de la meilleure horloge maîtresse*.

Clock variance

Affiche l'écart de la source de temps de référence (*Grandmaster*), également désignée par l'attribut *Offset scaled log variance*. Paramètre pour l'*algorithme de la meilleure horloge maîtresse*.

Priority 2

Affiche la *priorité 2* pour l'équipement qui est actuellement la source de temps de référence (*Grandmaster*).

Local time properties

Time source

Spécifie la source de temps à partir de laquelle l'horloge locale obtient ses informations temporelles.

Valeurs possibles :

- `atomicClock`
- `gps`
- `terrestrialRadio`
- `ptp`

- *ntp*
- *handSet*
- *other*
- *internalOscillator* (réglage par défaut)

UTC offset [s]

Spécifie la différence entre l'échelle de temps *PTP* et l'UTC.

Voir la case à cocher *PTP timescale*.

Valeurs possibles :

- `-32768..32767`

Commentaire : Le réglage par défaut est la valeur valide à la date de création du logiciel de l'équipement. Vous trouverez de plus amples informations dans le « Bulletin C » du Service de la rotation terrestre et des systèmes de référence (IERS) : http://www.iers.org/IERS/EN/Publications/Bulletins/bulletins.html

UTC offset valid

Indique si la valeur spécifiée dans le champ *UTC offset [s]* est correcte.

Valeurs possibles :

- `case cochée`
- `case non cochée` (réglage par défaut)

Time traceable

Indique si l'équipement obtient l'heure à partir d'une référence UTC primaire, par exemple à partir d'un serveur NTP.

Valeurs possibles :

- `case cochée`
- `case non cochée`

Frequency traceable

Indique si l'équipement obtient la fréquence à partir d'une référence UTC primaire, par exemple à partir d'un serveur NTP.

Valeurs possibles :

- `case cochée`
- `case non cochée`

PTP timescale

Indique si l'équipement utilise l'échelle de temps PTP.

Valeurs possibles :

- `case cochée`
- `case non cochée`

Selon la norme IEEE 1588, l'échelle de temps PTP est le temps atomique international TAI démarré le 01.01.1970.

Contrairement à l'UTC, le TAI n'utilise pas de secondes intercalaires.

Depuis le 1er juillet 2020, l'heure TAI a 37 secondes d'avance sur l'heure UTC.

Identities

L'équipement affiche les identités sous forme de séquences d'octets en notation hexadécimale.

Les numéros d'identification (UUID) sont constitués comme suit :
- Le numéro d'identification de l'équipement est constitué de l'adresse MAC de l'équipement, avec les valeurs `ff` et `fe` ajoutées entre l'octet 3 et l'octet 4.
- L'UUID du port est constitué du numéro d'identification de l'équipement suivi d'un ID de port de 16 bits.

Clock identity

Affiche le numéro d'identification propre à l'équipement (UUID).

Parent port identity

Affiche le numéro d'identification du port (UUID) de l'équipement maître en amont.

Grandmaster identity

Affiche le numéro d'identification de l'équipement de la source de temps de référence (*Grandmaster*).

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

2.3.2.2 PTP Boundary Clock Port

[Time > PTP > Boundary Clock > Port]

Dans cette boîte de dialogue, vous spécifiez les réglages de la *Boundary Clock (BC)* sur chaque port individuel.

Les réglages sont effectifs lorsque l'horloge locale fonctionne comme *Boundary Clock (BC)*. Pour cela, vous devez sélectionner la valeur `v2-boundary-clock` dans le champ *PTP mode* de la boîte de dialogue *Time > PTP > Global*.

Table

Port

Affiche le numéro de port.

PTP enable

Active/désactive la transmission des messages de synchronisation *PTP* sur le port.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La transmission est activée. Le port transmet et reçoit des messages de synchronisation *PTP*.
- `case non cochée`
  La transmission est désactivée. Le port bloque les messages de synchronisation *PTP*.

PTP status

Affiche l'état actuel du port.

Valeurs possibles :

- *initializing*
  Phase d'initialisation
- *faulty*
  Mode défectueux : erreur dans le protocole PTP.
- *disabled*
  Le protocole PTP est désactivé sur le port.
- *listening*
  Le port de l'équipement attend des messages de synchronisation *PTP*.
- *pre-master*
  Mode pré-maître *PTP*
- *master*
  Mode maître *PTP*
- *passive*
  Mode passif *PTP*
- *uncalibrated*
  Mode non calibré *PTP*
- *slave*
  Mode esclave *PTP*

Sync interval

Spécifie l'intervalle en secondes auquel le port transmet les messages de synchronisation *PTP*.

Valeurs possibles :

- `0.25`
- `0.5`
- `1` (réglage par défaut)
- `2`

Delay mechanism

Spécifie le mécanisme avec lequel l'équipement mesure le délai de transmission des messages de synchronisation *PTP*.

Valeurs possibles :

- *`disabled`*
  La mesure du délai des messages de synchronisation *PTP* pour les équipements PTP connectés est désactivée.
- *`e2e`* (réglage par défaut)
  De bout en bout : en tant qu'esclave *PTP*, le port mesure le délai de transmission des messages de synchronisation *PTP* au maître *PTP*.
  L'équipement affiche la valeur mesurée dans la boîte de dialogue *Time > PTP > Boundary Clock >* Global.
- *`p2p`*
  Pair à pair : l'équipement mesure le délai des messages de synchronisation *PTP* pour les équipements PTP connectés, à condition que ces équipements prennent en charge le P2P.
  Ce mécanisme évite à l'équipement d'avoir à déterminer à nouveau le délai en cas de reconfiguration.

P2P delay

Affiche le délai pair à pair mesuré pour les messages de synchronisation *PTP*.

La condition préalable est que vous ayez sélectionné la valeur *`p2p`* dans la colonne *Delay mechanism*.

P2P delay interval [s]

Spécifie l'intervalle en secondes auquel le port mesure le délai pair à pair.

La condition préalable est que vous ayez spécifié la valeur *`p2p`* sur ce port et sur le port de l'équipement distant.

Valeurs possibles :

- `1` (réglage par défaut)
- `2`
- `4`
- `8`
- `16`
- `32`

Network protocol

Spécifie le protocole que le port utilise pour transmettre les messages de synchronisation *PTP*.

Valeurs possibles :

- *IEEE 802.3* (réglage par défaut)
- *UDP/IPv4*

Announce interval [s]

Spécifie l'intervalle en secondes auquel le port transmet des messages pour la découverte de la topologie PTP.

Attribuez la même valeur à chaque équipement d'un domaine *PTP*.

Valeurs possibles :

- 1
- 2 (réglage par défaut)
- 4
- 8
- 16

Announce timeout

Spécifie le nombre d'intervalles d'annonce.

Exemple :

Pour le réglage par défaut (*Announce interval [s]* = 2 et *Announce timeout* = 3), le délai d'attente est 3 × 2 s = 6 s.

Valeurs possibles :

- 2..10 (réglage par défaut : 3)
  Attribuez la même valeur à chaque équipement d'un domaine *PTP*.

E2E delay interval [s]

Affiche l'intervalle en secondes selon lequel le port mesure le délai de bout en bout :

- Lorsque le port fonctionne en tant que maître *PTP*, l'équipement attribue au port la valeur 8.
- Lorsque le port fonctionne en tant qu'esclave *PTP*, la valeur est spécifiée par le maître *PTP* connecté au port.

V1 hardware compatibility

Spécifie si le port ajuste la longueur des messages de synchronisation *PTP* lorsque vous avez défini la valeur *udpIpv4* dans la colonne *Network protocol*.

Il est possible que d'autres équipements du réseau s'attendent à ce que les messages de synchronisation *PTP* aient la même longueur que les messages PTPv1.

Valeurs possibles :

- *auto* (réglage par défaut)
  L'équipement détecte automatiquement si les autres équipements du réseau s'attendent à ce que les messages de synchronisation *PTP* aient la même longueur que les messages PTPv1. Dans ce cas, l'équipement augmente la longueur des messages de synchronisation *PTP* avant de les transmettre.

- *on*
  L'équipement augmente la longueur des messages de synchronisation *PTP* avant de les transmettre.
- *off*
  L'équipement transmet les messages de synchronisation *PTP* sans en modifier la longueur.

Asymmetry

Corrige la valeur du délai mesuré corrompu par des chemins de transmission asymétriques.

Valeurs possibles :

- `-2000000000..2000000000` (réglage par défaut : `0`)

La valeur représente la différence de délai en nanosecondes entre les chemins asymétriques.

Une valeur de délai mesurée de y ns correspond à une asymétrie de y × 2 ns.

La valeur est positive si le délai entre le maître *PTP* et l'esclave *PTP* est plus long que dans la direction opposée.

VLAN

Spécifie le VLAN-ID avec lequel l'équipement marque les messages de synchronisation *PTP* sur ce port.

Valeurs possibles :

- *none* (réglage par défaut)
  L'équipement transmet les messages de synchronisation *PTP* sans tag de VLAN.
- `0..4042`
  Vous spécifiez des VLAN que vous avez déjà configurés dans l'équipement à partir de la liste.

Vérifiez que le port est membre du VLAN.

Voir la boîte de dialogue *Switching > VLAN > Configuration*.

VLAN priority

Spécifie la priorité avec laquelle l'équipement transmet les messages de synchronisation *PTP* marqués d'un VLAN-ID (couche 2, IEEE 802.1D).

Valeurs possibles :

- `0..7` (réglage par défaut : `6`)

Si vous avez spécifié la valeur *none* dans la colonne *VLAN*, l'équipement ignore la priorité de VLAN.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

2.3.3 PTP Transparent Clock

[Time > PTP > Transparent Clock]

Ce menu vous permet de configurer le mode *Transparent Clock* pour l'horloge locale.

Le menu contient les boîtes de dialogue suivantes :
- PTP Transparent Clock Global
- PTP Transparent Clock Port

2.3.3.1 PTP Transparent Clock Global

[Time > PTP > Transparent Clock > Global]

Dans cette boîte de dialogue, vous saisissez les réglages généraux et communs à l'ensemble des ports du mode *Transparent Clock* pour l'horloge locale. La *Transparent Clock (TC)* fonctionne selon le protocole PTP version 2 (IEEE 1588-2008).

Les réglages sont effectifs lorsque l'horloge locale fonctionne comme *Transparent Clock (TC)*. Pour cela, vous devez sélectionner la valeur `v2-transparent-clock` dans le champ *PTP mode* de la boîte de dialogue *Time > PTP > Global*.

Operation IEEE1588/PTPv2 TC

Delay mechanism

Spécifie le mécanisme avec lequel l'équipement mesure le délai de transmission des messages de synchronisation *PTP*.

Valeurs possibles :

- `e2e` (réglage par défaut)
  En tant qu'esclave *PTP*, le port mesure le délai de transmission des messages de synchronisation *PTP* au maître *PTP*.
  L'équipement affiche la valeur mesurée dans la boîte de dialogue *Time > PTP > Transparent Clock > Global*.
- `p2p`
  L'équipement mesure le délai des messages de synchronisation *PTP* pour chaque équipement PTP connecté, à condition que l'équipement prenne en charge le P2P.
  Ce mécanisme évite à l'équipement d'avoir à déterminer à nouveau le délai en cas de reconfiguration.
  Si vous spécifiez cette valeur, la valeur `IEEE 802.3` est uniquement disponible dans le champ *Network protocol*.
- `e2e-optimized`
  Comme `e2e`, avec les caractéristiques particulières suivantes :
  - L'équipement transmet les demandes de délai des esclaves *PTP* uniquement au maître *PTP*, bien que ces demandes soient des messages multicast. L'équipement épargne ainsi aux autres équipements les demandes multicast inutiles.
  - Si la topologie maître/esclave change, l'équipement réapprend le port pour le maître *PTP* dès qu'il reçoit un message de synchronisation d'un autre maître *PTP*.
  - Si l'équipement ne connaît pas de maître *PTP*, il transmet des demandes de délai aux ports.
- `disabled`
  La mesure du délai est désactivée sur le port. L'équipement rejette les messages pour la mesure du délai.

Primary domain

Affecte l'équipement à un domaine *PTP*.

Valeurs possibles :

- `0..255` (réglage par défaut : `0`)

L'équipement transmet les informations temporelles depuis et vers les équipements du même domaine uniquement.

Network protocol

Spécifie le protocole que le port utilise pour transmettre les messages de synchronisation *PTP*.

Valeurs possibles :

- `ieee8023` (réglage par défaut)
- `udpIpv4`

Multi domain mode

Active/désactive la correction des messages de synchronisation *PTP* dans chaque domaine *PTP*.

Valeurs possibles :

- `case cochée`
  L'équipement corrige les messages de synchronisation *PTP* dans chaque domaine *PTP*.
- `case non cochée` (réglage par défaut)
  L'équipement corrige les messages de synchronisation *PTP* uniquement dans le domaine *PTP* primaire. Voir le champ *Primary domain*.

VLAN ID

Spécifie le VLAN-ID avec lequel l'équipement marque les messages de synchronisation *PTP* sur ce port.

Valeurs possibles :

- `none` (réglage par défaut)
  L'équipement transmet les messages de synchronisation *PTP* sans tag de VLAN.
- `0..4042`
  Vous spécifiez des VLAN que vous avez déjà configurés dans l'équipement à partir de la liste.

VLAN priority

Spécifie la priorité avec laquelle l'équipement transmet les messages de synchronisation *PTP* marqués d'un VLAN-ID (couche 2, IEEE 802.1D).

Valeurs possibles :

- `0..7` (réglage par défaut : `6`)

Si vous avez spécifié la valeur `none` dans le champ *VLAN ID*, l'équipement ignore la valeur spécifiée.

Local synchronization

Syntonize

Active/désactive la synchronisation de fréquence de la *Transparent Clock* avec le maître *PTP*.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La synchronisation de la fréquence est activée.
  L'équipement synchronise la fréquence.
- `case non cochée`
  La synchronisation de la fréquence est désactivée.
  La fréquence reste inchangée.

Synchronize local clock

Active/désactive la synchronisation de l'heure système locale.

Valeurs possibles :

- `case cochée`
  La synchronisation est activée.
  L'équipement synchronise l'heure système locale avec l'heure reçue via PTP. La condition préalable est que la case *Syntonize* soit cochée.
- `case non cochée` (réglage par défaut)
  La synchronisation est désactivée.
  L'heure système locale reste inchangée.

Current master

Affiche le numéro d'identification du port (UUID) de l'équipement maître en amont sur lequel l'équipement synchronise sa fréquence.

Si la valeur ne contient que des zéros, c'est parce que :

- La fonction *Syntonize* est désactivée.
  ou
- L'équipement ne trouve pas de maître *PTP*.

Offset to master [ns]

Affiche la différence mesurée (dérive) entre l'horloge locale et le maître *PTP* en nanosecondes. L'équipement calcule la différence à partir des informations temporelles reçues.

La condition préalable est que la fonction *Synchronize local clock* soit activée.

Delay to master [ns]

Affiche le délai de transmission des messages de synchronisation *PTP* du maître *PTP* à l'esclave *PTP* en nanosecondes.

Condition préalable :

- La fonction *Synchronize local clock* est activée.
- La valeur `e2e` est sélectionnée dans le champ *Delay mechanism*.

Status IEEE1588/PTPv2 TC

Clock identity

Affiche le numéro d'identification propre à l'équipement (UUID).

L'équipement affiche les identités sous forme de séquences d'octets en notation hexadécimale.

Le numéro d'identification de l'équipement est constitué de l'adresse MAC de l'équipement, avec les valeurs `ff` et `fe` ajoutées entre l'octet 3 et l'octet 4.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

2.3.3.2 PTP Transparent Clock Port

[Time > PTP > Transparent Clock > Port]

Dans cette boîte de dialogue, vous spécifiez les réglages de la *Transparent Clock (TC)* sur chaque port individuel.

Les réglages sont effectifs lorsque l'horloge locale fonctionne comme *Transparent Clock (TC)*. Pour cela, vous devez sélectionner la valeur `v2-transparent-clock` dans le champ *PTP mode* de la boîte de dialogue *Time > PTP > Global*.

Table

Port

Affiche le numéro de port.

PTP enable

Active/désactive la transmission des messages de synchronisation *PTP* sur le port.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La transmission est activée.
  Le port transmet et reçoit des messages de synchronisation *PTP*.
- `case non cochée`
  La transmission est désactivée.
  Le port bloque les messages de synchronisation *PTP*.

P2P delay interval [s]

Spécifie l'intervalle en secondes auquel le port mesure le délai pair à pair.

La condition préalable est que vous ayez spécifié la valeur `p2p` sur ce port et sur le port de l'équipement distant. Voir la liste d'options *Delay mechanism* dans la boîte de dialogue *Time > PTP > Transparent Clock > Global*.

Valeurs possibles :

- `1` (réglage par défaut)
- `2`
- `4`
- `8`
- `16`
- `32`

P2P delay

Affiche le délai pair à pair mesuré pour les messages de synchronisation *PTP*.

La condition préalable est que vous ayez sélectionné le bouton radio `p2p` dans la liste d'options *Delay mechanism*. Voir le champ *Delay mechanism* dans la boîte de dialogue *Time > PTP > Transparent Clock > Global*.

Asymmetry

Corrige la valeur du délai mesuré corrompu par des chemins de transmission asymétriques.

Valeurs possibles :

- `-2000000000..2000000000` (réglage par défaut : `0`)

La valeur représente la différence de délai en nanosecondes entre les chemins asymétriques.

Une valeur de délai mesurée de y ns correspond à une asymétrie de y × 2 ns.

La valeur est positive si le délai entre le maître *PTP* et l'esclave *PTP* est plus long que dans la direction opposée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

2.4 802.1AS

[Time > 802.1AS]

Le protocole *802.1AS* est une procédure décrite dans la norme IEEE 802.1AS-2011 qui définit comment synchroniser avec précision le temps entre les équipements du réseau. Lorsque vous utilisez le protocole *802.1AS* sur le réseau Ethernet, vous pouvez considérer le protocole comme un profil de la norme IEEE 1588-2008.

Grâce à l'*algorithme de la meilleure horloge maîtresse*, les équipements du réseau déterminent l'équipement ayant l'heure la plus précise. Les équipements utilisent comme source de temps de référence l'équipement ayant l'heure la plus précise (*Grandmaster*). Les équipements participants se synchronisent alors avec cette source de temps de référence.

Le protocole *802.1AS* comporte les spécifications suivantes :

- La fonction *802.1AS* ou bien la fonction *PTP* peut être activée dans l'équipement.
- Si la fonction *SNTP* et la fonction *802.1AS* sont activées en même temps dans l'équipement, la fonction *802.1AS* est prioritaire.
- La fonction *802.1AS* ne prend en charge qu'un seul domaine.

Le menu contient les boîtes de dialogue suivantes :

- 802.1AS Global
- 802.1AS Port
- 802.1AS Statistics

2.4.1 802.1AS Global

[Time > 802.1AS > Global]

Cette boîte de dialogue vous permet de spécifier les réglages de base du protocole *802.1AS*.

Operation

Operation

Active/désactive la fonction *802.1AS*.

Valeurs possibles :

- `On`
  La fonction *802.1AS* est activée.
  L'équipement synchronise son horloge en utilisant le protocole *802.1AS*.
  Pensez à activer le protocole *802.1AS* sur les différents ports.

- `Off` (réglage par défaut)
  La fonction *802.1AS* est désactivée.

Configuration

Priority 1

Spécifie la *priorité 1* pour l'équipement.

Valeurs possibles :

- `0..255` (réglage par défaut : `246`)

L'*algorithme de la meilleure horloge maîtresse* évalue d'abord la *priorité 1* parmi les équipements participants afin de déterminer la source de temps de référence (*Grandmaster*).

Plus cette valeur est faible, plus il est probable que l'équipement soit désigné comme source de temps de référence (*Grandmaster*).

Si vous spécifiez la valeur `255`, l'équipement n'est pas désigné comme source de temps de référence (*Grandmaster*). Voir le cadre *Grandmaster*.

Priority 2

Spécifie la *priorité 2* pour l'équipement.

Valeurs possibles :

- `0..255` (réglage par défaut : `248`)

Lorsque les critères précédemment évalués sont les mêmes pour plusieurs équipements, l'*algorithme de la meilleure horloge maîtresse* évalue la *priorité 2* des équipements participants.

Plus cette valeur est faible, plus il est probable que l'équipement soit désigné comme source de temps de référence (*Grandmaster*). Voir le cadre *Grandmaster*.

Sync lower bound [ns]

Spécifie la valeur seuil inférieure en nanosecondes pour la différence de temps mesurée entre l'horloge locale et la source de temps de référence (*Grandmaster*). Si la différence de temps mesurée est inférieure à cette valeur, l'horloge locale est considérée comme synchronisée.

Valeurs possibles :

- `0..999999999` (réglage par défaut : `30`)

Sync upper bound [ns]

Spécifie la valeur seuil supérieure en nanosecondes pour la différence de temps mesurée entre l'horloge locale et la source de temps de référence (*Grandmaster*). Si la différence de temps mesurée est supérieure à cette valeur, l'horloge locale est alors considérée comme non synchronisée.

Valeurs possibles :

- `31..1000000000` (réglage par défaut : `5000`)

UTC offset [s]

Affiche la différence entre l'échelle de temps *802.1AS* et l'UTC.

UTC offset valid

Indique si la valeur affichée dans le champ *UTC offset [s]* est correcte.

Valeurs possibles :

- `case cochée`
- `case non cochée`

Status

Offset to master [ns]

Affiche la différence mesurée (dérive) entre l'horloge locale et la source de temps de référence (*Grandmaster*) en nanosecondes. L'équipement calcule la différence à partir des informations temporelles reçues.

Max. offset absolute [ns]

Affiche la différence de temps maximale survenue (mesurée en nanosecondes) depuis que l'horloge locale a été synchronisée avec la source de temps de référence (*Grandmaster*).

Is synchronized

Affiche si l'horloge locale est synchronisée avec la source de temps de référence (*Grandmaster*).

Si la différence de temps mesurée entre l'horloge locale et la source de temps de référence (*Grandmaster*) tombe en dessous du seuil inférieur de synchronisation, l'horloge locale est alors synchronisée. Ce statut est conservé jusqu'à ce que la différence de temps mesurée dépasse le seuil supérieur de synchronisation.

Vous spécifiez les seuils de synchronisation dans le cadre *Configuration*.

Steps removed

Affiche le nombre de chemins de communication parcourus entre l'horloge locale de l'équipement et la source de temps de référence (*Grandmaster*).

Dans le cas d'un esclave *802.1AS*, la valeur `1` signifie que l'horloge est connectée à la source de temps de référence (*Grandmaster*) directement par 1 chemin de communication.

Clock identity

Affiche le numéro d'identification de l'horloge de l'équipement.

L'équipement affiche le numéro d'identification sous forme de séquences d'octets en notation hexadécimale.

Le numéro d'identification de l'équipement est constitué de l'adresse MAC de l'équipement, avec les valeurs `ff` et `fe` ajoutées entre l'octet 3 et l'octet 4.

Grandmaster

Ce cadre affiche les critères que l'*algorithme de la meilleure horloge maîtresse* utilise pour évaluer la source de temps de référence (*Grandmaster*).

L'algorithme évalue d'abord la *priorité 1* des équipements participants. L'équipement ayant la valeur la plus basse pour la *priorité 1* est désigné comme source de temps de référence (*Grandmaster*). Lorsque la valeur est la même pour plusieurs équipements, l'algorithme utilise le critère suivant ; lorsque cette valeur est également la même, l'algorithme utilise le critère qui suit celui-ci. Lorsque chaque valeur est la même pour plusieurs équipements, la valeur la plus basse du champ *Clock identity* décide quel équipement est désigné comme source de temps de référence (*Grandmaster*).

L'équipement vous permet d'influencer quel équipement du réseau est désigné comme source de temps de référence (*Grandmaster*). Pour ce faire, modifiez la valeur du champ *Priority 1* ou du champ *Priority 2* dans le cadre *Configuration*.

Priority 1

Affiche la *priorité 1* pour l'équipement qui est actuellement la source de temps de référence (*Grandmaster*).

Clock class

Affiche la classe de la source de temps de référence (*Grandmaster*). Paramètre pour l'*algorithme de la meilleure horloge maîtresse*.

Clock accuracy

Affiche la précision estimée de la source de temps de référence (*Grandmaster*). Paramètre pour l'*algorithme de la meilleure horloge maîtresse*.

Clock variance

Affiche l'écart de la source de temps de référence (*Grandmaster*), également désignée par l'attribut *Offset scaled log variance*. Paramètre pour l'*algorithme de la meilleure horloge maîtresse*.

Priority 2

Affiche la *priorité 2* pour l'équipement qui est actuellement la source de temps de référence (*Grandmaster*).

Clock identity

Affiche le numéro d'identification de l'équipement de la source de temps de référence (*Grandmaster*). L'équipement affiche le numéro d'identification sous forme de séquences d'octets en notation hexadécimale.

Parent

Clock identity

Affiche le numéro d'identification du port de l'équipement maître en amont. L'équipement affiche le numéro d'identification sous forme de séquences d'octets en notation hexadécimale.

Port

Affiche le numéro de port de l'équipement maître en amont.

Cumulative rate ratio [ppm]

Affiche la différence de fréquence mesurée de l'horloge locale en parties par million par rapport à la source de temps de référence (*Grandmaster*).

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

2.4.2 802.1AS Port

[Time > 802.1AS > Port]

Dans cette boîte de dialogue, vous spécifiez les réglages de la *802.1AS* sur chaque port individuel.

Table

Port

Affiche le numéro de port.

Active

Active/désactive le protocole *802.1AS* sur le port.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  Le protocole est activé sur le port.
  L'équipement synchronise son horloge sur le port à l'aide du protocole *802.1AS*.
- `case non cochée`
  Le protocole est désactivé sur le port.

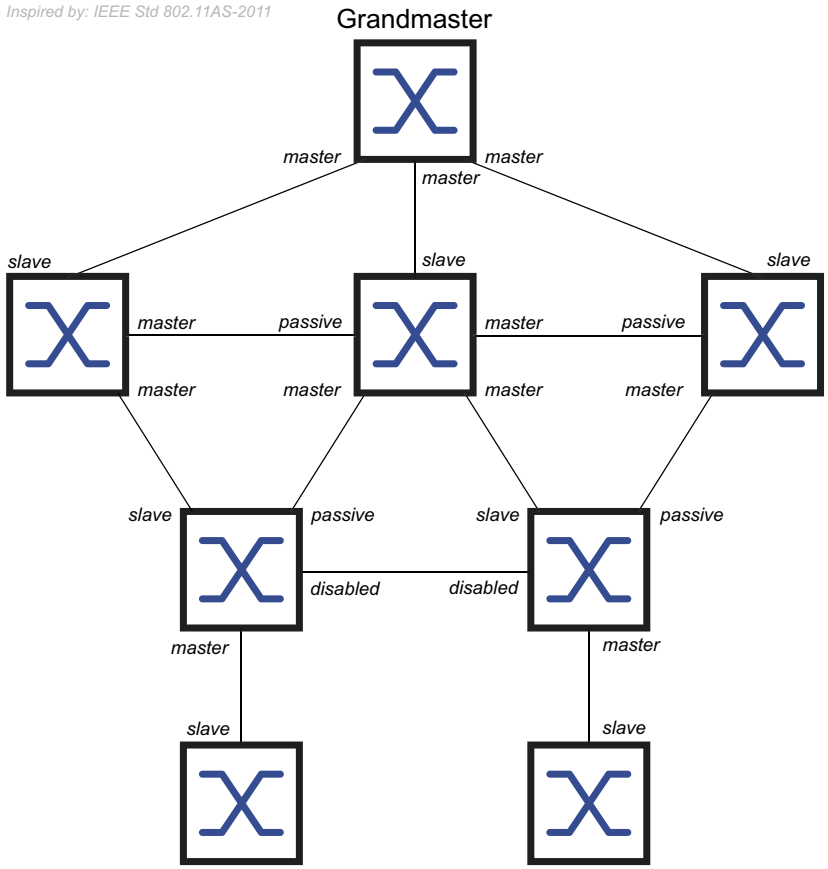
Role

Affiche le rôle actuel du port en prenant en compte le protocole *802.1AS*.

Valeurs possibles :

- *disabled*
  Le port fonctionne dans le rôle *Disabled Port*. Le port n'est pas compatible avec la norme *802.1AS*.
- *master*
  Le port fonctionne dans le rôle *Master Port*.

- `passive`
  Le port fonctionne dans le rôle *Passive Port*.
- `slave`
  Le port fonctionne dans le rôle *Slave Port*.



AS capable

Affiche si le protocole *802.1AS* est activé sur le port.

Valeurs possibles :

- `case cochée`
  Le protocole *802.1AS* est activé sur le port. Les conditions préalables sont :
  – Le port mesure un *Peer delay*, la case de la colonne *Measuring delay* est cochée.
  – La valeur de la colonne *Peer delay [ns]* est inférieure à la valeur de la colonne *Peer delay threshold [ns]*.
- `case non cochée`
  Le protocole *802.1AS* est désactivé sur le port.

Announce interval [s]

Spécifie l'intervalle en secondes auquel le port (dans le rôle *Master Port*) transmet les messages *Announce* pour la découverte de la topologie *802.1AS*.

Valeurs possibles :

- `1..2` (réglage par défaut : `1`)
  Attribuez la même valeur à chaque équipement d'un domaine *802.1AS*.
- `–`
  Le port ne transmet pas de messages *Announce*.

Announce timeout

Spécifie le nombre de *Announce interval [s]* pendant lesquels le port (dans le rôle *Slave Port*) attend les messages *Announce*.

Lorsque le nombre d'intervalles s'écoule sans réception d'un message *Announce*, l'équipement tente de trouver un nouveau chemin vers la source de temps de référence à l'aide de l'*algorithme de la meilleure horloge maîtresse*. Si l'équipement trouve une source de temps de référence (*Grandmaster*), il attribue le rôle *Slave Port* au port par lequel passe le nouveau chemin. Sinon, l'équipement devient la source de temps de référence (*Grandmaster*) et attribue le rôle *Master Port* à ses ports.

Exemple : dans le réglage par défaut (`Announce interval [s] = 1, Announce timeout = 3`), le délai d'attente est `3 × 1 s = 3 s`.

Valeurs possibles :

- `2..10` (réglage par défaut : `3`)
  Attribuez la même valeur à chaque port appartenant au même domaine *802.1AS*.

Sync interval [s]

Spécifie l'intervalle en secondes auquel le port (dans le rôle *Master Port*) transmet les messages *Sync* pour la synchronisation du temps.

Valeurs possibles :

- `0.125` (réglage par défaut)
- `0.250`
- `0.5`
- `1`
- `–`
  Le port ne transmet pas de messages *Sync*.

Sync timeout

Spécifie le nombre de *Sync interval [s]* pendant lesquels le port (dans le rôle *Slave Port*) attend les messages *Sync*.

Lorsque le nombre d'intervalles s'écoule sans réception d'un message *Sync*, l'équipement tente de trouver un nouveau chemin vers la source de temps de référence à l'aide de l'*algorithme de la meilleure horloge maîtresse*. Si l'équipement trouve une source de temps de référence (*Grandmaster*), il attribue le rôle *Slave Port* au port par lequel passe le nouveau chemin. Sinon, l'équipement devient la source de temps de référence (*Grandmaster*) et attribue le rôle *Master Port* à ses ports.

Exemple : dans le réglage par défaut (`Sync interval [s] = 0.125, Sync timeout = 3`), le délai d'attente est `3 × 0.125 s = 0.375 s`.

Valeurs possibles :

- `2..10` (réglage par défaut : `3`)
  Attribuez la même valeur à chaque port appartenant au même domaine *802.1AS*.

Peer delay interval [s]

Spécifie l'intervalle en secondes auquel le port (dans le rôle *Master Port*, *Passive Port* ou *Slave Port*) transmet un message *Peer delay request* pour mesurer le *Peer delay*.

Valeurs possibles :

- `1` (réglage par défaut)
- `2`
- `4`
- `8`
- `-`
  Le port ne transmet pas de messages *Peer delay request*.

Peer delay timeout

Spécifie le nombre de *Peer delay interval [s]* pendant lesquels le port (dans le rôle *Master Port*, *Passive Port* ou *Slave Port*) attend les messages *Delay response*.

Lorsque le nombre d'intervalles s'écoule sans réception d'un message *Delay response*, l'équipement attribue le rôle *Disabled Port* au port. Le port n'est plus compatible avec la norme *802.1AS*.

Valeurs possibles :

- `2..10` (réglage par défaut : `3`)

Peer delay threshold [ns]

Spécifie la valeur du seuil supérieur pour le *Peer delay* en nanosecondes. Si la valeur de la colonne *Peer delay [ns]* est supérieure à cette valeur, l'équipement attribue le rôle *Disabled Port* au port. Le port n'est plus compatible avec la norme *802.1AS*.

Valeurs possibles :

- `0..1000000000` (réglage par défaut : `10000`)

Measuring delay

Affiche si le port mesure un *Peer delay*.

Valeurs possibles :

- `case cochée`
  Le port mesure un *Peer delay*. Vous trouverez la valeur mesurée dans la colonne *Peer delay [ns]*.
- `case non cochée`
  Le port ne mesure pas de *Peer delay*.

Peer delay [ns]

Affiche la valeur mesurée du *Peer delay* en nanosecondes. La condition préalable est que la case dans la colonne *Measuring delay* soit cochée.

Neighbor rate ratio [ppm]

Affiche la différence de fréquence mesurée de l'horloge locale en parties par million par rapport à l'horloge de l'équipement adjacent.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

2.4.3 802.1AS Statistics

[Time > 802.1AS > Statistics]

Cette boîte de dialogue affiche les informations relatives au nombre de messages reçus, envoyés ou rejetés sur les ports. La boîte de dialogue affiche également des compteurs qui s'incrémentent chaque fois qu'un événement timeout se produit.

Table

Port

Affiche le numéro de port.

Received messages

Affiche les compteurs des messages reçus sur les ports :

Sync messages

Affiche le nombre de messages *Sync*.

Sync follow-up messages

Affiche le nombre de messages *Sync follow-up*.

Delay request messages

Affiche le nombre de messages *Peer delay request*.

Delay response messages

Affiche le nombre de messages *Peer delay response*.

Delay response follow-up messages

Affiche le nombre de messages *Peer delay response follow-up*.

Announce messages

Affiche le nombre de messages *Announce*.

Discarded messages

Affiche le nombre de messages *Sync* que l'équipement a rejeté sur ce port. L'équipement rejette un message *Sync*, par exemple, lorsque le port ne reçoit pas de message *Sync follow-up* pour un message *Sync* correspondant.

Sync timeout

Affiche le nombre de fois qu'un événement *Sync timeout* s'est produit sur le port. Voir la colonne *Sync timeout* dans la boîte de dialogue *Time > 802.1AS > Port*.

Announce timeout

Affiche le nombre de fois qu'un événement *Announce timeout* s'est produit sur ce port. Voir la colonne *Announce timeout* dans la boîte de dialogue *Time > 802.1AS > Port*.

Delay timeout

Affiche le nombre de fois qu'un événement *Peer delay timeout* s'est produit sur ce port. Voir la colonne *Peer delay timeout* dans la boîte de dialogue *Time > 802.1AS > Port*.

Transmitted messages

Affiche les compteurs des messages transmis sur les ports :

Sync messages

Affiche le nombre de messages *Sync*.

Sync follow-up messages

Affiche le nombre de messages *Sync follow-up*.

Delay request messages

Affiche le nombre de messages *Peer delay request*.

Delay response messages

Affiche le nombre de messages *Peer delay response*.

Delay response follow-up messages

Affiche le nombre de messages *Peer delay response follow-up*.

Announce messages

Affiche le nombre de messages *Announce*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

3 Device Security

Le menu contient les boîtes de dialogue suivantes :
- User Management
- Authentication List
- LDAP
- Management Access
- Pre-login Banner

3.1 User Management

[Device Security > User Management]

Lorsque les utilisateurs se connectent à l'aide de données de connexion valides, l'équipement leur permet d'accéder à l'administration de l'équipement.

Cette boîte de dialogue vous permet de gérer les utilisateurs de la gestion locale des utilisateurs. Vous pouvez également spécifier les réglages suivants ici :
- Les réglages de connexion
- Les réglages de sauvegarde des mots de passe
- Spécifier les stratégies de mots de passe valides

Vous pouvez spécifier les méthodes que l'équipement utilise pour l'authentification dans la boîte de dialogue *Device Security > Authentication List*.

Configuration

Ce cadre vous permet de spécifier les réglages relatifs à la connexion.

Login attempts

Indique le nombre de tentatives de connexion possibles lorsque l'utilisateur accède à l'administration de l'équipement à l'aide de l'interface utilisateur graphique et de l'interface de ligne de commande.

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.

Valeurs possibles :
- `0..5` (réglage par défaut : `0`)

Lorsque l'utilisateur effectue une tentative de connexion supplémentaire et échoue à nouveau, l'équipement verrouille l'accès de l'utilisateur.

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

La valeur `0` désactive le verrouillage. L'utilisateur dispose alors d'un nombre illimité de tentatives de connexion.

Login attempts period (min.)

Affiche le laps de temps qui s'écoule avant que l'équipement ne réinitialise le compteur dans le champ *Login attempts*.

Valeurs possibles :

- `0..60` (réglage par défaut : `0`)

Min. password length

L'équipement accepte le mot de passe si celui-ci contient au moins le nombre de caractères spécifié ici.

L'équipement vérifie le mot de passe en fonction de ce réglage, quel que soit le réglage de la case *Policy check*.

Valeurs possibles :

- `1..64` (réglage par défaut : `6`)

Password policy

Ce cadre vous permet de spécifier la stratégie relative aux mots de passe valides. L'équipement vérifie chaque nouveau mot de passe et chaque changement de mot de passe conformément à cette stratégie.

Les réglages affectent la colonne *Password*. Il convient pour cela que vous cochiez préalablement la case située dans la colonne *Policy check*.

Upper-case characters (min.)

L'équipement accepte le mot de passe si celui-ci contient au moins autant de lettres majuscules que spécifié ici.

Valeurs possibles :

- `0..16` (réglage par défaut : `1`)

La valeur `0` désactive ce réglage.

Lower-case characters (min.)

L'équipement accepte le mot de passe si celui-ci contient au moins autant de lettres minuscules que spécifié ici.

Valeurs possibles :

- `0..16` (réglage par défaut : `1`)

La valeur `0` désactive ce réglage.

Digits (min.)

L'équipement accepte le mot de passe si celui-ci contient au moins autant de chiffres que spécifié ici.

Valeurs possibles :

- `0..16` (réglage par défaut : `1`)

La valeur `0` désactive ce réglage.

Special characters (min.)

L'équipement accepte le mot de passe si celui-ci contient au moins autant de caractères spéciaux que spécifié ici.

Valeurs possibles :

- `0..16` (réglage par défaut : `1`)

La valeur `0` désactive ce réglage.

Table

Chaque utilisateur doit disposer d'un compte d'utilisateur activé pour bénéficier d'un accès à l'administration de l'équipement. La table vous permet de configurer et de gérer les comptes d'utilisateurs.

Pour modifier les réglages, cliquez sur le paramètre souhaité dans la table et modifiez la valeur.

User name

Affiche le nom du compte d'utilisateur.

Pour créer un nouveau compte d'utilisateur, cliquez sur le bouton  .

Active

Active/désactive le compte d'utilisateur.

Valeurs possibles :

- `case cochée`
  Le compte d'utilisateur est activé. L'équipement accepte la connexion d'un utilisateur associé à ce nom d'utilisateur.
- `case non cochée` (réglage par défaut)
  Le compte d'utilisateur est désactivé. L'équipement rejette la connexion d'un utilisateur associé à ce nom d'utilisateur.

Un compte d'utilisateur doté du rôle d'accès *`administrator`* est activé en permanence.

Password

Indique le nombre de tentatives de connexion possibles lorsque l'utilisateur accède à l'administration de l'équipement à l'aide de l'interface utilisateur graphique et de l'interface de ligne de commande.

Affiche ***** (astérisques) à la place du mot de passe avec lequel l'utilisateur se connecte. Pour modifier le mot de passe, cliquez sur le champ correspondant.

Lorsque vous spécifiez le mot de passe pour la première fois, l'équipement utilise le même mot de passe dans les colonnes *SNMP auth password* et *SNMP encryption password*.

- L'équipement vous permet de spécifier différents mots de passe dans les colonnes *SNMP auth password* et *SNMP encryption password*.
- Si vous changez le mot de passe dans la colonne actuelle, l'équipement change également les mots de passe des colonnes *SNMP auth password* et *SNMP encryption password*, mais seulement s'ils ne sont pas spécifiés individuellement auparavant.

Valeurs possibles :

- Chaîne de 6..64 caractères ASCII alphanumériques
  Les caractères suivants sont autorisés :
  - `a..z`
  - `A..Z`
  - `0..9`
  - `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

La longueur minimale du mot de passe est spécifiée dans le cadre *Configuration*. L'équipement fait la distinction entre les majuscules et les minuscules.

Lorsque la case de la colonne *Policy check* est cochée, l'équipement vérifie le mot de passe conformément à la stratégie spécifiée dans le cadre *Password policy*.

L'équipement vérifie constamment la longueur minimale du mot de passe, même lorsque la case de la colonne *Policy check* est `non cochée`.

Role

Indique le rôle d'utilisateur qui gère l'accès de l'utilisateur aux différentes fonctions de l'équipement.

Valeurs possibles :

- *unauthorized*
  L'utilisateur est bloqué, et l'équipement rejette la connexion de l'utilisateur.
  Affectez cette valeur pour verrouiller temporairement le compte d'utilisateur. Si l'équipement détecte une erreur lorsqu'un autre rôle est affecté, l'équipement affecte ce rôle au compte d'utilisateur.
- *guest* (réglage par défaut)
  L'utilisateur est autorisé à contrôler l'équipement.
- *auditor*
  L'utilisateur est autorisé à contrôler l'équipement et à sauvegarder le fichier log dans la boîte de dialogue *Diagnostics > Report > Audit Trail*.
- *operator*
  L'utilisateur est autorisé à contrôler l'équipement et à modifier les réglages – à l'exception des réglages de sécurité relatifs à l'accès à l'équipement.
- *administrator*
  L'utilisateur est autorisé à contrôler l'équipement et à modifier les réglages.

L'équipement affecte le type de service transmis dans la réponse d'un serveur RADIUS à un rôle d'utilisateur de la manière suivante :

- `Administrative-User`: *administrator*
- `Login-User`: *operator*
- `NAS-Prompt-User`: *guest*

User locked

Déverrouille le compte d'utilisateur.

Valeurs possibles :

- `case cochée`
  Le compte d'utilisateur est verrouillé. L'utilisateur ne dispose pas d'un accès à l'administration de l'équipement.
  Lorsque l'utilisateur échoue à se connecter un trop grand nombre de fois, l'équipement verrouille automatiquement l'utilisateur.
- `case non cochée` (grisé) (réglage par défaut)
  Le compte d'utilisateur est déverrouillé. L'utilisateur dispose d'un accès à l'administration de l'équipement.

Policy check

Active/désactive le contrôle du mot de passe.

Valeurs possibles :

- `case cochée`
  Le contrôle du mot de passe est activé.
  Lorsque vous définissez ou modifiez le mot de passe, l'équipement vérifie le mot de passe conformément à la stratégie spécifiée dans le cadre *Password policy*.
- `case non cochée` (réglage par défaut)
  Le contrôle du mot de passe est désactivé.

SNMP auth type

Indique le protocole d'authentification que l'équipement applique pour l'accès de l'utilisateur via SNMPv3.

Valeurs possibles :

- *hmacmd5* (valeur par défaut)
  Pour ce compte d'utilisateur, l'équipement utilise le protocole HMACMD5.
- *hmacsha*
  Pour ce compte d'utilisateur, l'équipement utilise le protocole HMACSHA.

SNMP auth password

Spécifie le mot de passe que l'équipement applique pour l'accès de l'utilisateur via SNMPv3.

Affiche ***** (astérisques) à la place du mot de passe avec lequel l'utilisateur se connecte. Pour modifier le mot de passe, cliquez sur le champ correspondant.

Par défaut, l'équipement utilise le même mot de passe que celui que vous spécifiez dans la colonne *Password*.

- Pour la colonne actuelle, l'équipement vous permet de spécifier un mot de passe différent de celui dans la colonne *Password*.
- Si vous changez le mot de passe dans la colonne *Password*, l'équipement change également le mot de passe pour la colonne actuelle, mais seulement s'il n'est pas spécifié individuellement.

Valeurs possibles :

- Chaîne de 6..64 caractères ASCII alphanumériques
  Les caractères suivants sont autorisés :
  - `a..z`
  - `A..Z`
  - `0..9`
  - `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

SNMP encryption type

Indique le protocole de chiffrement que l'équipement applique pour l'accès de l'utilisateur via SNMPv3.

Valeurs possibles :

- *none*
  Pas de chiffrement.
- *des* (valeur par défaut)
  Chiffrement DES
- *aesCfb128*
  Chiffrement AES128

SNMP encryption password

Spécifie le mot de passe que l'équipement applique pour chiffrer l'accès de l'utilisateur via SNMPv3.

Affiche ***** (astérisques) à la place du mot de passe avec lequel l'utilisateur se connecte. Pour modifier le mot de passe, cliquez sur le champ correspondant.

Par défaut, l'équipement utilise le même mot de passe que celui que vous spécifiez dans la colonne *Password*.

- Pour la colonne actuelle, l'équipement vous permet de spécifier un mot de passe différent de celui dans la colonne *Password*.
- Si vous changez le mot de passe dans la colonne *Password*, l'équipement change également le mot de passe pour la colonne actuelle, mais seulement s'il n'est pas spécifié individuellement.

Valeurs possibles :

- Chaîne de 6..64 caractères ASCII alphanumériques
  Les caractères suivants sont autorisés :
  - `a..z`
  - `A..Z`
  - `0..9`
  - `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée à la table.

- Spécifiez le nom du compte d'utilisateur dans le champ *User name*.
  Valeurs possibles :
  - Chaîne de 1..32 caractères ASCII alphanumériques

3.2 Authentication List

[Device Security > Authentication List]

Cette boîte de dialogue vous permet de gérer les listes d'authentification. Une liste d'authentification vous permet de spécifier quelle méthode l'équipement utilise pour l'authentification. Vous avez également la possibilité d'affecter des applications pré-définies aux listes d'authentification.

Lorsque les utilisateurs se connectent à l'aide de données de connexion valides, l'équipement leur permet d'accéder à l'administration de l'équipement. L'équipement authentifie les utilisateurs à l'aide des méthodes suivantes :
- Gestion des utilisateurs de l'équipement
- LDAP
- RADIUS

Avec le contrôle d'accès basé sur port conformément à la norme technique IEEE 802.1X, l'équipement permet aux équipements terminaux d'accéder au réseau lorsqu'ils se connectent avec des données de connexion valides. L'équipement authentifie les équipements terminaux à l'aide des méthodes suivantes :
- RADIUS
- IAS (Integrated Authentication Server)

Avec le réglage par défaut, les listes d'authentification suivantes sont disponibles :
- `defaultDot1x8021AuthList`
- `defaultLoginAuthList`
- `defaultV24AuthList`

Table

Commentaire : Si la table ne contient pas de liste, 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. Dans ce cas, l'équipement authentifie l'utilisateur à l'aide de la gestion locale des utilisateurs. Voir la boîte de dialogue *Device Security > User Management*.

Name

Affiche le nom de la liste.

Pour créer une nouvelle liste, cliquez sur le bouton  .

Valeurs possibles :

- Chaîne de 1..32 caractères ASCII alphanumériques

Policy 1
Policy 2
Policy 3
Policy 4
Policy 5

Indique la stratégie d'authentification que l'équipement utilise pour l'accès à l'aide de l'application spécifiée dans la colonne *Dedicated applications*.

L'équipement vous permet d'opter pour une solution de repli. Pour ce faire, spécifiez une autre stratégie dans chacun des champs dédiés à la stratégie. En cas d'échec de l'authentification à l'aide de la stratégie spécifiée, l'équipement utilise la stratégie suivante, selon l'ordre des valeurs saisies dans chaque stratégie.

Valeurs possibles :

- *local* (réglage par défaut)
  L'équipement authentifie les utilisateurs à l'aide de la gestion locale des utilisateurs. Voir la boîte de dialogue *Device Security > User Management*.
  Vous ne pouvez pas affecter cette valeur à la liste d'authentification `defaultDot1x8021Auth-List`.
- *radius*
  L'équipement authentifie les utilisateurs avec un serveur RADIUS intégré au réseau. Vous pouvez spécifier le serveur RADIUS dans la boîte de dialogue *Network Security > RADIUS > Authentication Server*.
- *reject*
  L'équipement accepte ou rejette l'authentification en fonction de la stratégie que vous essayez en premier. La liste suivante contient des scénarios d'authentification :
  - Lorsque la première stratégie figurant dans la liste d'authentification est *local* et que l'équipement accepte les identifiants de connexion de l'utilisateur, il connecte l'utilisateur sans tenter les autres stratégies.
  - Lorsque la première stratégie figurant dans la liste d'authentification est *local* et que l'équipement rejette les identifiants de connexion de l'utilisateur, il tente de connecter l'utilisateur à l'aide des autres stratégies dans l'ordre spécifié.
  - Lorsque la première stratégie de la liste d'authentification est *radius* ou *ldap* et que l'équipement rejette une connexion, la connexion est immédiatement rejetée sans tenter de connecter l'utilisateur à l'aide d'une autre stratégie.
    En l'absence de réponse de la part du serveur RADIUS ou LDAP, l'équipement tente d'authentifier l'utilisateur avec la stratégie suivante.
  - Lorsque la première stratégie figurant dans la liste d'authentification est *reject*, l'équipement rejette immédiatement la connexion de l'utilisateur sans tenter d'utiliser une autre stratégie.
  - Vérifiez que la liste d'authentification `defaultV24AuthList` contient au moins une stratégie différente de *reject*.
- *ias*
  L'équipement authentifie les équipements terminaux conformément à la norme technique 802.1X à l'aide du serveur IAS (Integrated Authentication Server). Le serveur IAS gère les données de connexion dans une base de données séparée. Voir la boîte de dialogue *Network Security > 802.1X Port Authentication > Integrated Authentication Server*.
  Vous pouvez uniquement affecter cette valeur à la liste d'authentification `default-Dot1x8021AuthList`.
- *ldap*
  L'équipement authentifie les utilisateurs à partir des données d'authentification et du rôle d'accès enregistrés dans un emplacement central. Vous spécifiez le serveur Active Directory utilisé par l'équipement dans la boîte de dialogue *Network Security > LDAP > Configuration*.

Dedicated applications

Affiche les applications dédiées. Lorsque les utilisateurs accèdent à l'équipement avec l'application concernée, l'équipement utilise les stratégies spécifiées pour l'authentification.

Pour affecter une autre application à la liste ou supprimer l'affectation, cliquez sur le bouton , puis sur l'élément *Allocate applications*. L'équipement vous permet d'affecter chaque application à une liste précise.

Active

Active/désactive la liste.

Valeurs possibles :

- `case cochée`
  La liste est activée. L'équipement utilise les stratégies de la liste lorsque les utilisateurs accèdent à l'équipement avec l'application concernée.
- `case non cochée` (réglage par défaut)
  La liste est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Allocate applications

Ouvre la fenêtre *Allocate applications*.

- Le champ de gauche affiche les applications qui peuvent être affectées à la liste mise en surbrillance.
- Le champ de droite affiche les applications qui sont affectées à la liste mise en surbrillance.
- Boutons :
  - Déplace toutes les entrées vers le champ de droite.
  - Déplace les entrées mises en surbrillance du champ de gauche vers le champ de droite.
  - Déplace les entrées mises en surbrillance du champ de droite vers le champ de gauche.
  - Déplace toutes les entrées vers le champ de gauche.

Commentaire : Lorsque vous déplacez l'entrée `WebInterface` vers le champ de gauche, la connexion à l'équipement est perdue une fois que vous appuyez sur le bouton *Ok*.

3.3 LDAP

[Device Security > LDAP]

Le Lightweight Directory Access Protocol (LDAP) permet d'authentifier et d'autoriser les utilisateurs en un point central du réseau. Un service d'annuaire largement utilisé et accessible via LDAP est Active Directory®.

L'équipement transmet les données de connexion de l'utilisateur au serveur d'authentification à l'aide du protocole LDAP. Le serveur d'authentification décide si les données de connexion sont valides et transmet les autorisations de l'utilisateur à l'équipement.

Une fois la connexion réussie, l'équipement sauvegarde temporairement les données de connexion dans le cache. Cela permet de gagner du temps quand les utilisateurs se connectent à nouveau. En effet, aucune opération complexe de recherche LDAP n'est nécessaire.

Le menu contient les boîtes de dialogue suivantes :
- LDAP Configuration
- LDAP Role Mapping

3.3.1 LDAP Configuration

[Device Security > LDAP > Configuration]

Cette boîte de dialogue vous permet de spécifier jusqu'à 4 serveurs d'authentification. Un serveur d'authentification authentifie et autorise les utilisateurs lorsque l'équipement transmet les données d'authentification au serveur.

L'équipement transmet les données de connexion au premier serveur d'authentification. Si ce serveur ne répond pas, l'équipement contacte le prochain serveur figurant dans la table.

Operation

Operation

Active/désactive le client *LDAP*.

Si, dans la boîte de dialogue *Device Security > Authentication List*, vous spécifiez la valeur `ldap` dans l'une des lignes *Policy 1* à *Policy 5*, l'équipement utilise le client *LDAP*. Au préalable, indiquez dans la boîte de dialogue *Device Security > LDAP > Role Mapping* au moins un mappage pour ce rôle *`administrator`*. Vous pourrez ainsi accéder à l'équipement en tant qu'administrateur après vous être connecté via LDAP.

Valeurs possibles :

- *`On`*
  Le client *LDAP* est activé.
- *`Off`* (réglage par défaut)
  Le client *LDAP* est désactivé.

Configuration

Client cache timeout [min]

Spécifie pendant combien de minutes, après une connexion réussie, les données de connexion d'un utilisateur restent valides. Lorsqu'un utilisateur se reconnecte dans ce délai, aucune opération complexe de recherche LDAP n'est nécessaire. La connexion se fait beaucoup plus rapidement.

Valeurs possibles :

- `1..1440` (réglage par défaut : `10`)

Bind user

Spécifie l'ID utilisateur sous la forme du « Distinguished Name » (DN) avec lequel l'équipement se connecte au serveur LDAP.

Cette information est nécessaire si le serveur LDAP exige un ID utilisateur sous la forme d'un « Distinguished Name » (DN) pour la connexion. Cette information n'est pas nécessaire dans les environnements Active Directory.

L'équipement se connecte au serveur LDAP avec l'ID utilisateur pour trouver le « Distinguished Name » (DN) des utilisateurs qui se connectent. L'équipement effectue la recherche en fonction des réglages dans les champs *Base DN* et *User name attribute*.

Valeurs possibles :

- Chaîne de 0..64 caractères ASCII alphanumériques

Bind user password

Spécifie le mot de passe que l'équipement utilise avec l'ID utilisateur spécifié dans le champ *Bind user* lors de la connexion au serveur LDAP.

Valeurs possibles :

- Chaîne de 0..64 caractères ASCII alphanumériques

Base DN

Spécifie le point de départ de la recherche dans l'arborescence du répertoire sous la forme du « Distinguished Name » (DN).

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

User name attribute

Spécifie l'attribut LDAP qui contient un nom d'utilisateur biunivoque. L'utilisateur utilise alors le nom d'utilisateur contenu dans cet attribut pour se connecter.

Souvent, les attributs LDAP `userPrincipalName`, `mail`, `sAMAccountName` et `uid` contiennent un nom d'utilisateur unique.

L'équipement ajoute la chaîne de caractères spécifiée dans le champ *Default domain* au nom d'utilisateur dans les conditions suivantes :

- Le nom d'utilisateur figurant dans l'attribut ne contient pas le caractère @.
- Un nom de domaine est spécifié dans le champ *Default domain*.

Valeurs possibles :

- Chaîne de 0..64 caractères ASCII alphanumériques
  (réglage par défaut : `userPrincipalName`)

Default domain

Spécifie la chaîne de caractères que l'équipement ajoute au nom d'utilisateur des utilisateurs qui se connectent si le nom d'utilisateur ne contient pas le caractère @.

Valeurs possibles :

- Chaîne de 0..64 caractères ASCII alphanumériques

CA certificate

URL

Indique le chemin et le nom de fichier du certificat.

L'équipement accepte les certificats présentant les propriétés suivantes :

- Format X.509
- Extension de fichier `.PEM`
- Codé en Base64, compris entre les mentions
  `-----BEGIN CERTIFICATE-----`
  et
  `-----END CERTIFICATE-----`

Pour des raisons de sécurité, nous recommandons de toujours utiliser un certificat signé par une autorité de certification.

L'équipement vous offre les options suivantes pour copier le certificat sur l'équipement :

- Importation depuis le PC
  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.
- Importation depuis un serveur FTP
  Lorsque le certificat est stocké sur un serveur FTP, spécifiez l'URL pour le fichier dans la forme suivante :
  `ftp://<utilisateur>:<mot de passe>@<adresse IP>:<port>/<chemin d'accès>/<nom fichier>`
- Importation depuis un serveur TFTP
  Lorsque le certificat est stocké sur un serveur TFTP, spécifiez l'URL pour le fichier dans la forme suivante :
  `tftp://<adresse IP>/<chemin d'accès>/<nom fichier>`
- Importation depuis un serveur SCP ou SFTP
  Lorsque le certificat est stocké sur un serveur SCP ou SFTP, spécifiez l'URL pour le fichier dans la forme suivante :
  - `scp://` ou `tftp://<adresse IP>/<chemin d'accès>/<nom 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>`

Start

Copie le certificat spécifié dans le champ *URL* sur l'équipement.

Table

Index

Affiche l'index auquel l'entrée de table se réfère.

Description

Spécifie la description.

Vous avez la possibilité de décrire ici le serveur d'authentification ou de noter des informations supplémentaires.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

Address

Spécifie l'adresse IP ou le nom DNS du serveur.

Valeurs possibles :

- Adresse IPv4 (réglage par défaut : `0.0.0.0`)
- Adresse IPv6
- Nom DNS au format `<domain>.<tld>` ou `<host>.<domain>.<tld>`
- `_ldap._tcp.<domain>.<tld>`
  À l'aide de ce nom DNS, l'équipement interroge la liste des serveurs LDAP (SRV Resource Record) à partir du serveur DNS.

Si, dans la ligne *Connection security*, une valeur autre que *none* est spécifiée et que le certificat ne contient que des noms DNS du serveur, utilisez un nom DNS. Activez la fonction *Client* dans la boîte de dialogue *Advanced > DNS > Client > Global*.

Destination TCP port

Spécifie le port TCP sur lequel le serveur s'attend à recevoir les requêtes.

Si vous avez spécifié la valeur `_ldap._tcp.domain.tld` dans la colonne *Address*, l'équipement ignore cette valeur.

Valeurs possibles :

- `0..65535` (réglage par défaut : `389`)
  Exception : le port `2222` est réservé à des fonctions internes.

Ports TCP fréquemment utilisés :

- `LDAP: 389`
- `LDAP over SSL: 636`
- `Active Directory Global Catalogue: 3268`
- `Active Directory Global Catalogue SSL: 3269`

Connection security

Spécifie le protocole qui chiffre la communication entre l'équipement et le serveur d'authentification.

Valeurs possibles :

- *none*
  Pas de chiffrement.
  L'équipement établit une connexion LDAP avec le serveur et transmet la communication, y compris les mots de passe, en texte clair.
- *ssl*
  Chiffrement avec SSL.
  L'équipement établit une connexion TLS avec le serveur et crée un tunnel pour la communication LDAP.
- *startTLS* (réglage par défaut)
  Chiffrement avec l'extension startTLS.
  L'équipement établit une connexion LDAP avec le serveur et chiffre la communication.

La condition préalable à la communication chiffrée est que l'équipement utilise l'heure correcte. Si le certificat ne contient que les noms DNS, vous devez spécifier le nom DNS du serveur dans la ligne *Address*. Activez la fonction *Client* dans la boîte de dialogue *Advanced > DNS > Client > Global*.

Si le certificat contient l'adresse IP du serveur dans le champ « Subject Alternative Name », l'équipement est en mesure de vérifier l'identité du serveur sans configuration DNS.

Server status

Affiche l'état de la connexion et l'authentification avec le serveur d'authentification.

Valeurs possibles :

- *ok*
  Le serveur est accessible.
  Si, dans la ligne *Connection security*, une valeur autre que *none* est spécifiée, l'équipement a vérifié le certificat du serveur.
- *unreachable*
  Le serveur est inaccessible.
- *other*
  L'équipement n'a pas encore établi de connexion avec le serveur.

Active

Active/désactive l'utilisation du serveur.

Valeurs possibles :

- `case cochée`
  L'équipement utilise le serveur
- `case non cochée` (réglage par défaut)
  L'équipement n'utilise pas le serveur.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Flush cache

Supprime les données de connexion en cache des utilisateurs qui se sont connectés avec succès.

3.3.2 LDAP Role Mapping

[Device Security > LDAP > Role Mapping]

Cette boîte de dialogue vous permet de créer jusqu'à 64 mappages pour attribuer un rôle aux utilisateurs.

Dans la table, vous spécifiez si l'équipement attribue un rôle à l'utilisateur en fonction d'un attribut avec une valeur spécifique ou en fonction de l'appartenance à un groupe.
- L'équipement recherche l'attribut et la valeur de l'attribut dans l'objet utilisateur.
- En évaluant le « Distinguished Name » (DN) contenu dans les attributs du membre, l'équipement vérifie l'appartenance au groupe.

Lorsqu'un utilisateur se connecte, l'équipement recherche les informations suivantes sur le serveur LDAP :
- Dans le projet utilisateur associé, l'équipement recherche les attributs spécifiés dans les mappages.
- Dans les objets groupe des groupes spécifiés dans les mappages, l'équipement recherche les attributs des membres.

Sur cette base, l'équipement vérifie tout mappage.
- L'objet utilisateur contient-il l'attribut requis ?
  ou
- L'utilisateur est-il membre du groupe ?

Si l'équipement ne trouve pas de correspondance, l'utilisateur n'a pas accès à l'équipement.

Si plusieurs mappages s'appliquent à un utilisateur, le réglage du champ *Matching policy* est déterminant. L'utilisateur obtient soit le rôle aux autorisations plus étendues, soit le premier rôle de la table qui s'applique.

Configuration

Matching policy

Spécifie quel rôle l'équipement applique si plusieurs mappages s'appliquent à un utilisateur.

Valeurs possibles :
- *highest* (réglage par défaut)
  L'équipement applique le rôle aux autorisations plus étendues.
- *first*
  L'équipement applique à l'utilisateur la règle qui a la valeur la plus faible dans la colonne *Index*.

Table

Index

Affiche l'index auquel l'entrée de table se réfère.

Role

Indique le rôle d'utilisateur qui gère l'accès de l'utilisateur aux différentes fonctions de l'équipement.

Valeurs possibles :

- *unauthorized*
  L'utilisateur est bloqué, et l'équipement rejette la connexion de l'utilisateur.
  Affectez cette valeur pour verrouiller temporairement le compte d'utilisateur. Si une erreur est détectée lorsqu'un autre rôle est affecté, l'équipement affecte ce rôle au compte d'utilisateur.
- *guest* (réglage par défaut)
  L'utilisateur est autorisé à contrôler l'équipement.
- *auditor*
  L'utilisateur est autorisé à contrôler l'équipement et à sauvegarder le fichier log dans la boîte de dialogue *Diagnostics > Report > Audit Trail*.
- *operator*
  L'utilisateur est autorisé à contrôler l'équipement et à modifier les réglages – à l'exception des réglages de sécurité relatifs à l'accès à l'équipement.
- *administrator*
  L'utilisateur est autorisé à contrôler l'équipement et à modifier les réglages.

Type

Spécifie si un groupe ou un attribut avec une valeur d'attribut est défini dans la colonne *Parameter*.

Valeurs possibles :

- *attribute* (réglage par défaut)
  La colonne *Parameter* contient un attribut avec une valeur d'attribut.
- *group*
  La colonne *Parameter* contient le « Distinguished Name » (DN) d'un groupe.

Parameter

Spécifie un groupe ou un attribut avec une valeur d'attribut en fonction du réglage de la colonne *Type*.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères
  L'équipement fait la distinction entre les majuscules et les minuscules.
  - Si la colonne *Type* indique la valeur *attribute*, vous spécifiez l'attribut sous la forme `Attribute_name=Attribute_value`.
    Exemple : `l=Germany`
  - Si la colonne *Type* indique la valeur *group*, vous spécifiez le « Distinguished Name » (DN) d'un groupe.
    Exemple : `CN=admin-users,OU=Groups,DC=example,DC=com`

Active

Active/désactive le mappage des rôles.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  Le mappage des rôles est activé.
- `case non cochée`
  Le mappage des rôles est désactivé.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée à la table.

- Spécifiez l'index dans le champ *Index*.
  Valeurs possibles :
  - `1..64`

3.4 Management Access

[Device Security > Management Access]

Le menu contient les boîtes de dialogue suivantes :

- Server
- IP Access Restriction
- Web
- Command Line Interface
- SNMPv1/v2 Community

3.4.1 Server

[Device Security > Management Access > Server]

Cette boîte de dialogue vous permet de définir les services de serveur qui permettront aux utilisateurs ou aux applications d'accéder à l'administration de l'équipement.

La boîte de dialogue contient les onglets suivants :
- [Information]
- [SNMP]
- [Telnet]
- [SSH]
- [HTTP]
- [HTTPS]

[Information]

Cet onglet affiche les services de serveur activés sous forme d'aperçu.

Table

SNMPv1

Indique si le service de serveur autorisant l'accès à l'équipement à l'aide de SNMP version 1 est activé ou désactivé. Voir l'onglet *SNMP*.

Valeurs possibles :

- `case cochée`
  Le service de serveur est activé.
- `case non cochée`
  Le service de serveur est désactivé.

SNMPv2

Indique si le service de serveur autorisant l'accès à l'équipement à l'aide de SNMP version 2 est activé ou désactivé. Voir l'onglet *SNMP*.

Valeurs possibles :

- `case cochée`
  Le service de serveur est activé.
- `case non cochée`
  Le service de serveur est désactivé.

SNMPv3

Indique si le service de serveur autorisant l'accès à l'équipement à l'aide de SNMP version 3 est activé ou désactivé. Voir l'onglet *SNMP*.

Valeurs possibles :

- `case cochée`
  Le service de serveur est activé.
- `case non cochée`
  Le service de serveur est désactivé.

Telnet server

Indique si le service de serveur autorisant l'accès à l'équipement à l'aide de Telnet est activé ou désactivé. Voir l'onglet *Telnet*.

Valeurs possibles :

- `case cochée`
  Le service de serveur est activé.
- `case non cochée`
  Le service de serveur est désactivé.

SSH server

Indique si le service de serveur autorisant l'accès à l'équipement à l'aide de Secure Shell est activé ou désactivé. Voir l'onglet *SSH*.

Valeurs possibles :

- `case cochée`
  Le service de serveur est activé.
- `case non cochée`
  Le service de serveur est désactivé.

HTTP server

Indique si le service de serveur autorisant l'accès à l'équipement à l'aide de l'interface graphique utilisateur via HTTP est activé ou désactivé. Voir l'onglet *HTTP*.

Valeurs possibles :

- `case cochée`
  Le service de serveur est activé.
- `case non cochée`
  Le service de serveur est désactivé.

HTTPS server

Indique si le service de serveur autorisant l'accès à l'équipement à l'aide de l'interface graphique utilisateur via HTTPS est activé ou désactivé. Voir l'onglet *HTTPS*.

Valeurs possibles :

- `case cochée`
  Le service de serveur est activé.
- `case non cochée`
  Le service de serveur est désactivé.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[SNMP]

Cet onglet vous permet de spécifier les réglages de l'agent SNMP de l'équipement et d'activer/désactiver l'accès à l'équipement avec différentes versions SNMP.

L'agent SNMP active l'accès à l'administration de l'équipement avec des applications basées sur SNMP.

Configuration

SNMPv1

Active/désactive l'accès à l'équipement avec SNMP version 1.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'accès est activé.
- `case non cochée`
  L'accès est désactivé.

Vous pouvez spécifier les noms de communauté dans la boîte de dialogue *Device Security > Management Access > SNMPv1/v2 Community*.

SNMPv2

Active/désactive l'accès à l'équipement avec SNMP version 2.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'accès est activé.
- `case non cochée`
  L'accès est désactivé.

Vous pouvez spécifier les noms de communauté dans la boîte de dialogue *Device Security > Management Access > SNMPv1/v2 Community*.

SNMPv3

Active/désactive l'accès à l'équipement avec SNMP version 3.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'accès est activé.
- `case non cochée`
  L'accès est désactivé.

Les systèmes d'administration de réseau tels que ConneXium Network Manager utilisent ce protocole pour communiquer avec l'équipement.

UDP port

Indique le numéro du port UDP sur lequel l'agent SNMP reçoit des requêtes de la part des clients.

Valeurs possibles :

- `1..65535` (réglage par défaut : `161`)
  Exception : le port `2222` est réservé à des fonctions internes.

Pour permettre à l'agent SNMP d'utiliser le nouveau port après une modification, procédez de la manière suivante :

- ☐ Cliquez sur le bouton ✔.
- ☐ Dans la boîte de dialogue *Basic Settings > Load/Save*, sélectionnez le profil de configuration actif.
- ☐ Cliquez sur le bouton 💾 pour sauvegarder les modifications actuelles.
- ☐ Redémarrez l'équipement.

SNMPover802

Active/désactive l'accès à l'équipement via SNMP à l'aide de IEEE-802.

Valeurs possibles :

- `case cochée`
  L'accès est activé.
- `case non cochée` (réglage par défaut)
  L'accès est désactivé.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Telnet]

Cet onglet vous permet d'activer/de désactiver le serveur Telnet dans l'équipement et de spécifier ses réglages.

Le serveur Telnet active l'accès à l'administration de l'équipement à distance à l'aide de l'interface de ligne de commande. Les connexions Telnet sont non chiffrées.

Operation

Telnet server

Active/désactive le serveur Telnet.

Valeurs possibles :

- Le serveur Telnet est activé.
  L'accès à l'administration de l'équipement est possible via l'interface de ligne de commande à l'aide d'une connexion Telnet non chiffrée.
- Le serveur Telnet est désactivé.

Commentaire : Lorsque le serveur *SSH* est désactivé et que vous désactivez également le serveur *Telnet*, l'accès à l'interface de ligne de commande n'est possible qu'à travers l'interface série de l'équipement.

Configuration

TCP port

Indique le numéro du port TCP sur lequel l'équipement reçoit des requêtes Telnet de la part des clients.

Valeurs possibles :

- `1..65535` (réglage par défaut : `23`)
  Exception : le port `2222` est réservé à des fonctions internes.

Le serveur redémarre automatiquement après un changement de port. Les connexions existantes restent en place.

Connections

Affiche le nombre de connexions Telnet actuellement établies avec l'équipement.

Connections (max.)

Indique le nombre maximum de connexions Telnet qui peuvent être établies simultanément avec l'équipement.

Valeurs possibles :

- `1..5` (réglage par défaut : `5`)

Session timeout [min]

Indique le délai d'attente en minutes. Lorsque l'équipement reste inactif pendant ce laps de temps, il met fin à la session pour l'utilisateur connecté.

Toute modification de la valeur prend effet à la prochaine connexion d'un utilisateur.

Valeurs possibles :

- `0`
  Désactive la fonction. La connexion reste établie en cas d'inactivité.
- `1..160` (réglage par défaut : `5`)

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[SSH]

Cet onglet vous permet d'activer/de désactiver le serveur SSH dans l'équipement et de spécifier ses réglages requis pour SSH. Le serveur fonctionne avec SSH version 2.

Le serveur SSH active l'accès à l'administration de l'équipement à distance à l'aide de l'interface de ligne de commande. Les connexion SSH sont chiffrées.

Le serveur SSH s'identifie auprès des clients à l'aide de sa clé publique RSA. Lors du premier établissement de la connexion, le programme client affiche l'empreinte de cette clé qui peut ainsi être consultée par l'utilisateur. L'empreinte contient une séquence de caractères codée en Base64 facile à vérifier. Lorsque vous rendez cette séquence de caractères disponible aux utilisateurs via un canal fiable, ils ont la possibilité de comparer les deux empreintes. Si les séquences de caractères correspondent, cela signifie que le client est connecté au bon serveur.

L'équipement vous permet de créer les clés privée et publique (clés d'hôte) requises pour RSA directement sur l'équipement. Vous avez également la possibilité de copier vos propres clés sur l'équipement au format PEM.

L'équipement vous offre en outre la possibilité de charger la clé RSA (clé d'hôte) depuis une mémoire externe lors du redémarrage. Dans la boîte de dialogue *Basic Settings > External Memory*, colonne *SSH key auto upload*.

Operation

SSH server

Active/désactive le serveur SSH.

Valeurs possibles :

- `On` (réglage par défaut)
  Le serveur SSH est activé.
  L'accès à l'administration de l'équipement est possible via l'interface de ligne de commande à l'aide d'une connexion SSH chiffrée.
  Vous ne pouvez démarrer le serveur qu'en présence d'une signature RSA dans l'équipement.
- `Off`
  Le serveur SSH est désactivé.
  Lorsque vous désactivez le serveur SSH, les connexions existantes restent établies. Cependant, l'équipement contribue à empêcher l'établissement de nouvelles connexions.

Commentaire : Lorsque le serveur *Telnet* est désactivé et que vous désactivez également le serveur *SSH*, l'accès à l'interface de ligne de commande n'est possible qu'à travers l'interface série de l'équipement.

Configuration

TCP port

Indique le numéro du port TCP sur lequel l'équipement reçoit des requêtes SSH de la part des clients.

Valeurs possibles :

- `1..65535` (réglage par défaut : `22`)
  Exception : le port `2222` est réservé à des fonctions internes.

Le serveur redémarre automatiquement après un changement de port. Les connexions existantes restent en place.

Sessions

Affiche le nombre de connexions SSH actuellement établies avec l'équipement.

Sessions (max.)

Indique le nombre maximum de connexions SSH avec l'équipement qui peuvent être établies simultanément.

Valeurs possibles :

- `1..5` (réglage par défaut : `5`)

Session timeout [min]

Indique le délai d'attente en minutes. Lorsque l'utilisateur connecté reste inactif pendant ce laps de temps, l'équipement met fin à la connexion.

Toute modification de la valeur prend effet à la prochaine connexion d'un utilisateur.

Valeurs possibles :

- `0`
  Désactive la fonction. La connexion reste établie en cas d'inactivité.
- `1..160` (réglage par défaut : `5`)

Fingerprint

L'empreinte est une chaîne de caractères facile à vérifier qui identifie de manière univoque la clé d'hôte du serveur SSH.

Une fois qu'une nouvelle clé d'hôte a été importée, l'équipement continue à afficher l'empreinte existante jusqu'au redémarrage du serveur.

Fingerprint type

Indique l'empreinte affichée par le champ *RSA fingerprint*.

Valeurs possibles :

- `md5`
  Le champ *RSA fingerprint* affiche l'empreinte sous forme de hachage MD5 hexadécimal.
- `sha256`
  Le champ *RSA fingerprint* affiche l'empreinte sous forme de hachage SHA256 codé en Base64.

RSA fingerprint

Affiche l'empreinte de la clé d'hôte publique du serveur SSH.

Après avoir modifié les réglages dans le champ *Fingerprint type*, cliquez sur le bouton , puis sur le bouton pour actualiser l'affichage.

Signature

RSA present

Indique si une clé d'hôte RSA est présente sur l'équipement.

Valeurs possibles :

- `case cochée`
  Une clé est présente.
- `case non cochée`
  Aucune clé n'est présente.

Create

Génère une clé d'hôte dans l'équipement. Il convient pour cela que le serveur *SSH* ait été préalablement désactivé.

Longueur de la clé créée :

- 2048 bits (RSA)

Pour que le serveur SSH utilise la clé d'hôte générée, réactivez le serveur SSH.

Vous avez également la possibilité de copier votre propre clé d'hôte sur l'équipement au format PEM. Voir le cadre *Key import*.

Delete

Supprime la clé d'hôte de l'équipement. Il convient pour cela que le SSH serveur ait été préalablement désactivé.

Oper status

Indique si l'équipement génère actuellement une clé d'hôte.

Il est possible qu'un autre utilisateur ait déclenché cette action.

Valeurs possibles :

- *rsa*
  L'équipement génère actuellement une clé d'hôte RSA.
- *none*
  L'équipement ne génère pas de clé d'hôte.

Key import

URL

Indique le chemin et le nom du fichier de votre propre clé d'hôte RSA.

L'équipement accepte la clé RSA lorsqu'elle présente la longueur de clé suivante :

- 2048 bit (RSA)

L'équipement vous offre les options suivantes pour copier la clé sur l'équipement :

- Importation depuis le PC
  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.
- Importation depuis un serveur FTP
  Lorsque la clé est stockée sur un serveur FTP, spécifiez l'URL pour le fichier dans la forme suivante :
  `ftp://utilisateur>:<mot de passe>@<adresse Ip>:<port>/<nom fichier>`
- Importation depuis un serveur TFTP
  Lorsque la clé est stockée sur un serveur TFTP, spécifiez l'URL pour le fichier dans la forme suivante :
  `tftp://<adresse IP>/<chemin d'accès>/<nom fichier>`
- Importation depuis un serveur SCP ou SFTP
  Lorsque la clé est stockée sur un serveur SCP ou SFTP, spécifiez l'URL pour le fichier dans la forme suivante :
  - `scp://` ou `tftp://<adresse IP>/<chemin d'accès>/<nom 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>`

Start

Copie la clé spécifiée dans le champ *URL* sur l'équipement.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[HTTP]

Cet onglet vous permet d'activer/de désactiver le protocole HTTP dans le serveur Web et de spécifier les réglages requis pour HTTP.

Le serveur Web fournit l'interface utilisateur graphique via une connexion HTTP non chiffrée. Pour des raisons de sécurité, désactivez le protocoles HTTP et utilisez le protocole HTTPS.

L'équipement prend en charge jusqu'à 10 connexions simultanées à l'aide des protocoles HTTP ou HTTPS.

Commentaire : Si vous modifiez les réglages dans cet onglet et cliquez sur le bouton ✓, l'équipement met fin à la session et déconnecte chaque connexion ouverte. Pour continuer à travailler avec l'interface utilisateur graphique, connectez-vous à nouveau.

Operation

HTTP server

Active/désactive le protocole *HTTP* pour le serveur Web.

Valeurs possibles :

- *On* (réglage par défaut)
  Le protocole *HTTP* est activé.
  L'accès à l'administration de l'équipement est possible via une connexion *HTTP* non chiffrée.
  Lorsque le protocole *HTTPS* est activé, l'équipement redirige automatiquement la requête de connexion *HTTP* vers une connexion *HTTPS* chiffrée.
- *Off*
  Le protocole *HTTP* est désactivé.
  Lorsque le protocole *HTTPS* est activé, l'accès à l'administration de l'équipement est possible via une connexion *HTTPS* chiffrée.

Commentaire : Lorsque les protocoles *HTTP* et *HTTPS* sont désactivés, vous pouvez activer le protocole *HTTP* à l'aide de la commande de l'interface de ligne de commande `http server` pour obtenir l'interface utilisateur graphique.

Configuration

TCP port

Indique le numéro du port TCP sur lequel le serveur Web reçoit les requêtes HTTP de la part des clients.

Valeurs possibles :

- `1..65535` (réglage par défaut : `80`)
  Exception : le port `2222` est réservé à des fonctions internes.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[HTTPS]

Cet onglet vous permet d'activer/de désactiver le protocole HTTPS dans le serveur Web et de spécifier les réglages requis pour HTTPS.

Le serveur Web fournit l'interface utilisateur graphique via une connexion HTTP chiffrée.

Un certificat numérique est requis pour le chiffrement de la connexion HTTP. L'équipement vous permet de créer ce certificat vous-même ou de charger un certificat existant sur l'équipement.

L'équipement prend en charge jusqu'à 10 connexions simultanées à l'aide des protocoles HTTP ou HTTPS.

Commentaire : Si vous modifiez les réglages dans cet onglet et cliquez sur le bouton , l'équipement met fin à la session et déconnecte chaque connexion ouverte. Pour continuer à travailler avec l'interface utilisateur graphique, connectez-vous à nouveau.

Operation

HTTPS server

Active/désactive le protocole *HTTPS* pour le serveur Web.

Valeurs possibles :

- *On* (réglage par défaut)
  Le protocole *HTTPS* est activé.
  L'accès à l'administration de l'équipement est possible via une connexion *HTTPS* chiffrée.
  En l'absence de certificat numérique, l'équipement génère un certificat numérique avant d'activer le protocole *HTTPS*.
- *Off*
  Le protocole *HTTPS* est désactivé.
  Lorsque le protocole *HTTP* est activé, l'accès à l'administration de l'équipement est possible via une connexion *HTTP* non chiffrée.

Commentaire : Lorsque les protocoles *HTTP* et *HTTPS* sont désactivés, vous pouvez activer le protocole *HTTPS* à l'aide de la commande de l'interface de ligne de commande `https server` pour obtenir l'interface utilisateur graphique.

Configuration

TCP port

Indique le numéro du port TCP sur lequel le serveur Web reçoit les requêtes HTTPS de la part des clients.

Valeurs possibles :

- `1..65535` (réglage par défaut : `443`)
  Exception : le port `2222` est réservé à des fonctions internes.

Fingerprint

L'empreinte est une séquence de nombres hexadécimaux qui identifie de manière univoque le certificat numérique du serveur HTTPS.

Une fois qu'un nouveau certificat numérique a été importé, l'équipement affiche l'empreinte actuelle jusqu'au redémarrage du serveur.

Fingerprint type

Indique l'empreinte affichée par le champ *Fingerprint*.

Valeurs possibles :

- *sha1*
  Le champ *Fingerprint* affiche l'empreinte SHA1 du certificat.
- *sha256*
  Le champ *Fingerprint* affiche l'empreinte SHA256 du certificat.

Fingerprint

La séquence de caractères du certificat numérique utilisé par le serveur.

Après avoir modifié les réglages dans le champ *Fingerprint type*, cliquez sur le bouton , puis sur le bouton pour actualiser l'affichage.

Certificate

Commentaire : Si l'équipement utilise un certificat qui n'est pas signé par une autorité de certification, le navigateur Web affiche un message pendant le chargement de l'interface utilisateur graphique. Pour continuer, ajoutez une règle d'exception pour le certificat dans le navigateur Web.

Present

Indique si le certificat numérique est présent sur l'équipement.

Valeurs possibles :

- `case cochée`
  Le certificat est présent.
- `case non cochée`
  Le certificat a été supprimé.

Create

Génère un certificat numérique dans l'équipement.

Jusqu'au redémarrage, le serveur Web utilise le certificat précédent.

Pour que le serveur utilise le certificat nouvellement généré, redémarrez le serveur Web. Le redémarrage du serveur Web n'est possible qu'à l'aide de l'interface de ligne de commande.

Vous avez également la possibilité de copier votre propre certificat sur l'équipement. Voir le cadre *Certificate import*.

Delete

Supprime le certificat numérique.

Jusqu'au redémarrage, le serveur Web utilise le certificat précédent.

Oper status

Indique si l'équipement génère ou supprime actuellement un certificat numérique.

Il est possible qu'un autre utilisateur ait déclenché cette action.

Valeurs possibles :

- *none*
  Actuellement, l'équipement ne génère pas ou ne supprime pas de certificat.
- *delete*
  L'équipement supprime actuellement un certificat.
- *generate*
  L'équipement génère actuellement un certificat.

Certificate import

URL

Indique le chemin et le nom de fichier du certificat.

L'équipement accepte les certificats présentant les propriétés suivantes :

- Format X.509
- Extension de fichier `.PEM`
- Codé en Base64, compris entre les mentions
  - `-----BEGIN PRIVATE KEY-----`
    et
    `-----END PRIVATE KEY-----`
    ainsi que
  - `-----BEGIN CERTIFICATE-----`
    et
    `-----END CERTIFICATE-----`
- Clé RSA d'une longueur de 2048 bits

L'équipement vous offre les options suivantes pour copier le certificat sur l'équipement :

- Importation depuis le PC
  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.
- Importation depuis un serveur FTP
  Lorsque le certificat est stocké sur un serveur FTP, spécifiez l'URL pour le fichier dans la forme suivante :
  `ftp://<utilisateur>:<mot de passe>@<adresse IP>:<port>/<chemin d'accès>/<nom fichier>`
- Importation depuis un serveur TFTP
  Lorsque le certificat est stocké sur un serveur TFTP, spécifiez l'URL pour le fichier dans la forme suivante :
  `tftp://<adresse IP>/<chemin d'accès>/<nom fichier>`
- Importation depuis un serveur SCP ou SFTP
  Lorsque le certificat est stocké sur un serveur SCP ou SFTP, spécifiez l'URL pour le fichier dans la forme suivante :
  - `scp://` ou `tftp://<adresse IP>/<chemin d'accès>/<nom 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>`

Start

Copie le certificat spécifié dans le champ *URL* sur l'équipement.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

3.4.2 IP Access Restriction

[Device Security > Management Access > IP Access Restriction]

Cette boîte de dialogue vous permet de restreindre l'accès à l'administration de l'équipement à des plages d'adresses IP spécifiques et à des applications basées sur IP sélectionnées.

- Lorsque la fonction est désactivée, l'accès à l'administration de l'équipement est possible depuis n'importe quelle adresse IP et à l'aide de toutes les applications.
- Lorsque la fonction est désactivée, l'accès est restreint. Vous ne disposez d'un accès à l'administration de l'équipement qu'aux conditions suivantes :
  - Au moins une entrée de la table est activée.
    et
  - Vous accédez à l'équipement avec une application autorisée depuis une plage d'adresses IP autorisées.

Operation

Commentaire : Avant d'activer cette fonction, vérifiez qu'au moins une entrée active de la table 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.

Operation

Active/désactive la fonction *IP Access Restriction*.

Valeurs possibles :

- `On`
  La fonction *IP Access Restriction* est activée.
  L'accès à l'administration de l'équipement est restreint.
- `Off` (réglage par défaut)
  La fonction *IP Access Restriction* est désactivée.

Table

Vous avez la possibilité de définir jusqu'à 16 entrées de table et de les activer séparément.

Index

Affiche l'index auquel l'entrée de table se réfère.

Si vous supprimez une entrée de table, il reste un blanc dans la numérotation. Si vous créez une entrée de table, l'équipement remplit le 1er blanc.

Valeurs possibles :

- `1..16`

Address

Indique l'adresse IP du réseau depuis lequel vous permettez l'accès à l'administration de l'équipement. Vous pouvez spécifier la plage du réseau dans la colonne *Netmask*.

Valeurs possibles :

- Adresse IPv4 valide (réglage par défaut : `0.0.0.0`)

Netmask

Indique la plage du réseau spécifiée dans la colonne *Address*.

Valeurs possibles :

- Masque réseau valide (réglage par défaut : `0.0.0.0`)

HTTP

Active/désactive l'accès via HTTP.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'accès est activé pour la plage d'adresses IP adjacente.
- `case non cochée`
  L'accès est désactivé.

HTTPS

Active/désactive l'accès via HTTPS.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'accès est activé pour la plage d'adresses IP adjacente.
- `case non cochée`
  L'accès est désactivé.

SNMP

Active/désactive l'accès via SNMP.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'accès est activé pour la plage d'adresses IP adjacente.
- `case non cochée`
  L'accès est désactivé.

Telnet

Active/désactive l'accès via Telnet.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'accès est activé pour la plage d'adresses IP adjacente.
- `case non cochée`
  L'accès est désactivé.

SSH

Active/désactive l'accès via SSH.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'accès est activé pour la plage d'adresses IP adjacente.
- `case non cochée`
  L'accès est désactivé.

IEC61850-MMS

Active/désactive l'accès au serveur MMS.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'accès est activé pour la plage d'adresses IP adjacente.
- `case non cochée`
  L'accès est désactivé.

Modbus TCP

Active/désactive l'accès au serveur *Modbus TCP*.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'accès est activé pour la plage d'adresses IP adjacente.
- `case non cochée`
  L'accès est désactivé.

EtherNet/IP

Active/désactive l'accès au serveur *EtherNet/IP*.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'accès est activé pour la plage d'adresses IP adjacente.
- `case non cochée`
  L'accès est désactivé.

Active

Active ou désactive l'entrée de table.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'entrée de table est activée. L'équipement restreint l'accès à l'administration de l'équipement à la plage d'adresses IP adjacente et aux applications basées sur IP sélectionnées.
- `case non cochée`
  L'entrée de table est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

3.4.3 Web

[Device Security > Management Access > Web]

Cette boîte de dialogue vous permet de spécifier les réglages de l'interface utilisateur graphique.

Configuration

Web interface session timeout [min]

Indique le délai d'attente en minutes. Lorsque l'équipement reste inactif pendant ce laps de temps, il met fin à la session pour l'utilisateur connecté.

Valeurs possibles :

- `0..160` (réglage par défaut : `5`)

La valeur `0` désactive la fonction et l'utilisateur reste connecté lorsqu'il est inactif.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

3.4.4 Command Line Interface

[Device Security > Management Access > CLI]

Cette boîte de dialogue vous permet de spécifier les réglages de l'interface de ligne de commande. Vous trouverez des informations détaillées relatives à l'interface de ligne de commande dans le manuel de référence « Interface de ligne de commande ».

La boîte de dialogue contient les onglets suivants :
- [Global]
- [Login banner]

[Global]

Cet onglet vous permet de modifier l'invite de l'interface de ligne de commande et de spécifier la fermeture automatique des sessions via l'interface série en cas d'inactivité.

L'équipement dispose des interfaces série suivantes.
- Interface USB-C

Configuration

Login prompt

Indique la chaîne de caractères que l'équipement affiche dans l'interface de ligne de commande au début de chaque ligne de commande.

Valeurs possibles :
- Chaîne de caractères ASCII alphanumériques de 0..128 caractères (`0x20..0x7E`) y compris les espaces
  Caractères génériques
  - `%d` date
  - `%i` adresse IP
  - `%m` adresse MAC
  - `%p` nom du produit
  - `%t` heure

  Réglage par défaut : `(MCSESM-E)`

Les modifications apportées à ce réglage sont immédiatement effectives dans la session d'interface de ligne de commande active.

Serial interface timeout [min]

Indique le laps de temps en minutes après lequel l'équipement ferme automatiquement la session d'un utilisateur inactif connecté dans l'interface de ligne de commande via l'interface de série.

Valeurs possibles :
- `0..160` (réglage par défaut : `5`)
  La valeur `0` désactive la fonction et l'utilisateur reste connecté lorsqu'il est inactif.

Toute modification de la valeur prend effet à la prochaine connexion d'un utilisateur.

Pour le serveur *Telnet* et le serveur *SSH*, vous pouvez spécifier le délai d'attente dans la boîte de dialogue *Device Security > Management Access > Server*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Login banner]

Dans cet onglet, vous remplacez l'écran de démarrage de l'interface de ligne de commande avec votre propre texte.

Dans le réglage par défaut, l'écran de démarrage affiche des informations relatives à l'équipement, comme la version logicielle et les réglages de l'équipement. La fonction de cet onglet vous permet de désactiver ces informations et de les remplacer par un texte individuel que vous saisissez.

Pour afficher votre propre texte dans l'interface de ligne de commande et dans l'interface utilisateur graphique avant de vous connecter, utilisez la boîte de dialogue *Device Security > Pre-login Banner*.

Operation

Operation

Active/désactive la fonction *Login banner*.

Valeurs possibles :

- `On`
  La fonction *Login banner* est activée.
  Lorsque les utilisateurs se connectent à l'aide de l'interface de ligne de commande, l'équipement affiche les informations textuelles spécifiées dans le champ *Banner text*.
- `Off` (réglage par défaut)
  La fonction *Login banner* est désactivée.
  L'écran de démarrage affiche les informations relatives à l'équipement. Les informations textuelles saisies dans le champ *Banner text* sont conservées.

Banner text

Banner text

Indique la chaîne de caractères que l'équipement affiche dans l'interface de ligne de commande au début de chaque session.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..1024 caractères (`0x20..0x7E`) y compris les espaces

- `<Tabulation>`
- `<Saut de ligne>`

Remaining characters

Affiche le nombre de caractères restants dans le champ *Banner text* pour les informations textuelles.

Valeurs possibles :

- `1024..0`

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

3.4.5 SNMPv1/v2 Community

[Device Security > Management Access > SNMPv1/v2 Community]

Cette boîte de dialogue vous permet de spécifier le nom de communauté pour les applications SNMPv1/v2.

Les applications envoient des requêtes via SNMPv1/v2 avec un nom de communauté dans l'en-tête du paquet de données SNMP. En fonction du nom de communauté, l'application obtient une autorisation en lecture ou une autorisation en lecture et en écriture pour l'équipement.

Vous activez l'accès à l'équipement via SNMPv1/v2 dans la boîte de dialogue *Device Security* > Management Access > *Server*.

Table

Community

Affiche l'autorisation pour les applications SNMPv1/v2 sur l'équipement :

- `Write`
  Pour les requêtes présentant un nom de communauté saisi, l'application reçoit une autorisation en lecture et en écriture pour l'équipement.
- `Read`
  Pour les requêtes présentant un nom de communauté saisi, l'application reçoit une autorisation en lecture pour l'équipement.

Name

Indique le nom de communauté pour l'autorisation adjacente.

Valeurs possibles :

- Chaîne de 0..32 caractères ASCII alphanumériques
  `admin` (réglage par défaut pour autorisations en lecture et en écriture)
  `user` (réglage par défaut pour autorisations en lecture)

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

3.5 Pre-login Banner

[Device Security > Pre-login Banner]

Cette boîte de dialogue vous permet d'afficher un texte d'accueil ou d'information destiné aux utilisateurs avant qu'ils ne se connectent.

Les utilisateurs voient ce texte apparaître dans la boîte de dialogue de connexion de l'interface graphique utilisateur et de l'interface de ligne de commande. Les utilisateurs se connectant avec SSH voient apparaître ce texte - indépendamment du client utilisé - avant ou pendant la connexion.

Pour afficher uniquement le texte dans l'interface de ligne de commande, utilisez les réglages de la boîte de dialogue *Device Security > Management Access > CLI*.

Operation

Operation

Active/désactive la fonction *Pre-login Banner*.

À l'aide de la fonction *Pre-login Banner*, l'équipement affiche un texte d'accueil et d'information dans la boîte de dialogue de l'interface utilisateur graphique et de l'interface de ligne de commande.

Valeurs possibles :

- *On*
  La fonction *Pre-login Banner* est activée.
  L'équipement affiche le texte spécifié dans le champ *Banner text* de la boîte de dialogue de connexion.
- *Off* (réglage par défaut)
  La fonction *Pre-login Banner* est désactivée.
  L'équipement n'affiche pas de texte dans la boîte de dialogue de connexion. Lorsque vous saisissez un texte dans le champ *Banner text*, ce texte est sauvegardé dans l'équipement.

Banner text

Banner text

Indique le texte d'information que l'équipement affiche dans la boîte de dialogue de l'interface utilisateur graphique et de l'interface de ligne de commande.

Valeurs possibles :

- Chaîne de 0..512 caractères ASCII alphanumériques (`0x20..0x7E`) y compris les espaces
- `<Tabulation>`
- `<Saut de ligne>`

Remaining characters

Affiche le nombre de caractères restants dans le champ *Banner text*.

Valeurs possibles :

- 512..0

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4 Network Security

Le menu contient les boîtes de dialogue suivantes :

- Network Security Overview
- Port Security
- 802.1X Port Authentication
- RADIUS
- DoS
- DHCP Snooping
- IP Source Guard
- Dynamic ARP Inspection
- ACL

4.1 Network Security Overview

[Network Security > Overview]

Cette boîte de dialogue affiche les règles de sécurité du réseau utilisées pour l'équipement.

Paramètre

Port/VLAN

Indique si l'équipement affiche des règles basées sur VLAN et/ou des règles basées sur port.

Valeurs possibles :

- `All` (réglage par défaut)
  L'équipement affiche les règles basées sur VLAN et les règles basées sur port que vous avez spécifiées.
- `Port: <Numéro de port>`
  L'équipement affiche les règles basées sur port pour un port spécifique. Cette sélection est disponible lorsque vous avez spécifié une ou plusieurs règles pour ce port.
- `VLAN: <VLAN-ID>`
  L'équipement affiche les règles basées sur VLAN pour un VLAN spécifique. Cette sélection est disponible lorsque vous avez spécifié une ou plusieurs règles pour ce VLAN.

ACL

Affiche les règles *ACL* dans l'aperçu.

La boîte de dialogue *Network Security > ACL* vous permet de modifier les règles *ACL*.

All

Permet de cocher les cases adjacentes. L'équipement affiche les règles associées dans l'aperçu.

None

Permet de décocher les cases adjacentes. L'équipement n'affiche aucune règle dans l'aperçu.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.2 Port Security

[Network Security > Port Security]

L'équipement vous permet de transmettre les paquets de données provenant uniquement des expéditeurs souhaités sur un port. Lorsque cette fonction est activée, l'équipement vérifie le VLAN-ID et l'adresse MAC ou le VLAN-ID et l'adresse IP de l'expéditeur avant de transmettre un paquet de données. L'équipement rejette les paquets de données provenant d'autres expéditeurs et consigne cet événement dans le fichier log.

L'équipement permet également de vérifier l'adresse IP de l'expéditeur avant qu'il ne transmette un paquet de données.

Commentaire : Si, dans le cadre *Mode*, le bouton radio *IP* est sélectionné, la fonction *Port Security* intervient indirectement sur la couche 2. Lorsque vous configurez une adresse IP autorisée, l'équipement récupère l'adresse MAC actuellement associée à l'adresse IP. L'équipement utilise une requête ARP et enregistre en interne l'adresse MAC associée. La condition préalable à la spécification d'une adresse IP autorisée est que le périphérique connecté soit accessible et réponde aux requêtes ARP.

Lorsqu'un équipement connecté envoie des paquets de données avec une adresse IP autorisée mais une adresse MAC autre que l'adresse MAC associée, l'équipement rejette les paquets de données correspondants. Si vous remplacez l'équipement connecté et que vous utilisez la même adresse IP qu'avant, veuillez indiquer à nouveau l'adresse IP tel qu'autorisé. Ensuite, l'équipement utilise la nouvelle adresse MAC associée.

Si la fonction *Auto-Disable* est activée, l'équipement désactive le port. Cette restriction rend les usurpations d'adresse MAC plus difficile. La fonction *Auto-Disable* réactive automatiquement le port concerné lorsque les paramètres cessent d'être dépassés.

Dans cette boîte de dialogue, une fenêtre *Wizard* vous aide à lier les ports à une ou plusieurs sources souhaitées. Dans l'équipement, ces adresses sont connues comme étant des *Static entries (x/y)*. Afin d'afficher les adresses statiques spécifiées, mettez en surbrillance le port concerné et cliquez sur le bouton  .

Pour simplifier le processus de configuration, l'équipement vous permet d'enregistrer automatiquement les expéditeurs souhaités. L'équipement « apprend » les expéditeurs en évaluant les paquet de données reçus. Dans l'équipement, ces adresses sont connues comme étant des *Dynamic entries*. Lorsqu'une limite supérieure définie par l'utilisateur a été atteinte (*Dynamic limit*), l'équipement cesse « l'apprentissage » du port concerné et transmet uniquement les paquets de données des expéditeurs déjà enregistrés. Lorsque vous définissez la limite supérieure sur le nombre d'expéditeurs attendus, vous rendez les attaques d'inondation d'adresses MAC (MAC flooding) plus difficile.

Commentaire : Avec l'enregistrement automatique des *Dynamic entries*, l'équipement rejette toujours le 1er paquet de données provenant d'expéditeurs inconnus. À l'aide de ce 1er paquet de données, l'équipement vérifie si la limite supérieure a été atteinte. L'équipement enregistre l'expéditeur jusqu'à ce que la limite supérieure soit atteinte. À la suite de quoi, l'équipement transmet les paquets de données reçus de la part de cet expéditeur sur le port concerné.

Operation

Operation

Active/désactive la fonction *Port Security*.

Valeurs possibles :

- `On`
  La fonction *Port Security* est activée.
  L'équipement vérifie le VLAN-ID et l'adresse MAC source avant de transmettre un paquet de données.
  L'équipement ne transmet un paquet de données reçu que lorsque le VLAN-ID et l'adresse MAC source du paquet de données sont autorisés sur le port concerné. Afin que ce réglage prenne effet, vous devez également activer la vérification de l'adresse source sur les ports concernés.
- `Off` (réglage par défaut)
  La fonction *Port Security* est désactivée.
  L'équipement transmet chaque paquet de données reçu sans vérifier l'adresse source.

Commentaire : Si, dans le cadre *Mode*, le bouton radio *MAC* est sélectionné, l'équipement vérifie l'adresse MAC source par rapport aux adresses MAC sources autorisées. Si le bouton radio *IP* est sélectionné, l'équipement vérifie l'adresse MAC source par rapport aux adresses MAC associées aux adresses IP sources autorisées.

Configuration

Auto-disable

Active/désactive la fonction *Auto-Disable* relative à la *Port Security*.

Valeurs possibles :

- `case cochée`
  La fonction *Auto-Disable* relative à la *Port Security* est activée.
  Permet également de cocher la case située dans la colonne *Auto-disable* pour les ports concernés.
- `case non cochée` (réglage par défaut)
  La fonction *Auto-Disable* relative à la *Port Security* est désactivée.

Mode

Mode

Indique si la fonction *Port Security* utilise soit les adresses MAC autorisées, soit les adresses IP autorisées pour vérifier un paquet reçu.

Valeurs possibles :

- *MAC* (réglage par défaut)
  La fonction *Port Security* utilise les adresses MAC source autorisées.
  L'équipement vérifie le VLAN-ID et l'adresse MAC source par rapport aux adresses MAC source autorisées avant de transmettre un paquet de données.
- *IP*
  La fonction *Port Security* utilise les adresses IP source autorisées.
  L'équipement vérifie le VLAN-ID et l'adresse MAC source par rapport aux adresses MAC associées aux adresses IP source autorisées avant de transmettre un paquet de données.

Table

Port

Affiche le numéro de port.

Active

Active/désactive la vérification de l'adresse source sur le port.

Valeurs possibles :

- `case cochée`
  L'équipement vérifie chaque paquet de données reçu sur le port et le transmet uniquement si l'adresse source du paquet de données est autorisée. Activez également la fonction *Port Security* dans le cadre *Operation*.
- `case non cochée` (réglage par défaut)
  L'équipement transmet chaque paquet de données reçu sur le port sans vérifier l'adresse source.

Commentaire : Lorsque vous utilisez l'équipement en tant que participant actif au sein d'un anneau *MRP* ou *HIPER Ring*, nous vous recommandons de décocher la case des ports de l'anneau.

Commentaire : Lorsque vous utilisez l'équipement en tant que participant actif d'un *Ring/Network Coupling* ou *RCP*, nous vous recommandons de décocher la case des ports de couplage concernés.

Auto-disable

Active/désactive la fonction *Auto-Disable* pour les paramètres que la fonction *Port Security* surveille sur le port.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La fonction *Auto-Disable* est activée sur le port.
  Il convient pour cela que vous cochiez préalablement la case *Auto-disable* dans le cadre *Configuration*.
  - Si le port enregistre des adresses MAC source qui ne sont pas autorisées ou un nombre d'adresses MAC source supérieur au nombre spécifié dans la colonne *Dynamic limit*, l'équipement désactive le port. La LED « État du lien » du port clignote 3x par période.
  - La boîte de dialogue *Diagnostics > Ports > Auto-Disable* affiche quels ports sont actuellement désactivés en raison du dépassement des paramètres.
  - La fonction *Auto-Disable* réactive le port automatiquement. Pour cela, accédez à la boîte de dialogue *Diagnostics > Ports > Auto-Disable* et spécifiez une période d'attente pour le port concerné dans la colonne *Reset timer [s]*.
- `case non cochée`
  La fonction *Auto-Disable* est désactivée sur le port.

Send trap

Active/désactive l'envoi de traps SNMP lorsque l'équipement rejette un paquet de données provenant d'un expéditeur non souhaité sur le port.

Valeurs possibles :

- `case cochée`
  L'envoi de traps SNMP est activé.
  Si l'équipement rejette les paquets de données provenant d'un expéditeur non autorisé sur le port, l'équipement envoie un trap SNMP.
- `case non cochée` (réglage par défaut)
  L'envoi de traps SNMP est désactivé.

Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

Trap interval [s]

Spécifie le temps de retard en secondes pendant lequel l'équipement patiente après l'envoi d'un trap SNMP avant d'envoyer le prochain trap SNMP.

Valeurs possibles :

- `0..3600` (réglage par défaut : `0`)

La valeur `0` permet de désactiver le temps de retard.

Dynamic limit

Indique la limite supérieure du nombre de sources enregistrées automatiquement (*Dynamic entries*). Lorsque la limite supérieure est atteinte, l'équipement cesse son « apprentissage » sur ce port.

Définissez la valeur sur le nombre de sources attendues.

Si le port enregistre un nombre d'expéditeurs supérieur au nombre spécifié ici, le port désactive la fonction *Auto-Disable*. Il convient pour cela de cocher préalablement la case située dans la colonne *Auto-disable* et la case *Auto-disable* située dans le cadre *Configuration*.

Valeurs possibles :

- `0`
  Désactive l'enregistrement automatique des sources sur ce port.
- `1..600` (réglage par défaut : `600`)

Static limit

Indique la limite supérieure du nombre de sources liées au port (*Static entries (x/y)*). La fenêtre *Wizard*, boîte de dialogue *MAC addresses*, vous aide à lier le port à une ou plusieurs sources souhaitées.

Valeurs possibles :

- `0..64` (réglage par défaut : `64`)

La valeur `0` contribue à éviter de lier une source au port.

Dynamic entries

Affiche le nombre d'expéditeurs que l'équipement a automatiquement déterminé.

Voir la fenêtre *Wizard*, boîte de dialogue *MAC addresses*, champ *Dynamic entries*.

Si vous sélectionnez la valeur *IP* dans le cadre *Mode*, la colonne *Dynamic entries* affiche la valeur `0`.

Static MAC entries

Affiche le nombre d'expéditeurs qui sont reliés au port.

Voir la fenêtre *Wizard*, boîte de dialogue *MAC addresses*, champ *Static entries (x/y)*.

Static IP entries

Affiche le nombre d'adresses IP autorisées sur le port.

Voir la fenêtre *Wizard*, boîte de dialogue *IP addresses*, champ *Static entries (x/y)*.

Last violating VLAN ID/MAC

Affiche le VLAN-ID et l'adresse MAC d'un expéditeur non souhaité dont les paquets de données ont été rejetés en dernier par l'équipement sur ce port.

Sent traps

Affiche le nombre de paquets de données rejetés sur ce port qui a entraîné l'envoi d'un trap SNMP par l'équipement.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Port security (Wizard)]

La fenêtre *Wizard* vous aide à lier les ports à une ou plusieurs sources souhaitées. Après avoir spécifié les réglages, cliquez sur le bouton *Finish*.

Commentaire : L'équipement sauvegarde les sources liées au port jusqu'à ce que vous désactiviez la vérification de la source sur le port concerné ou dans le cadre *Operation*.

Après avoir fermé la fenêtre *Wizard*, cliquez sur le bouton pour sauvegarder vos réglages.

[Port security (Wizard) – Select port]

Port

Indique le port que vous affectez à l'expéditeur lors de la prochaine étape.

[Port security (Wizard) – MAC addresses]

VLAN ID

Indique le VLAN-ID de la source souhaitée.

Valeurs possibles :

- `1..4042`

Pour transférer le VLAN-ID et l'adresse MAC dans le champ *Static entries (x/y)*, cliquez sur le bouton *Add*.

MAC address

Indique l'adresse MAC de la source souhaitée.

Valeurs possibles :

- Adresse MAC Unicast valide
  Indiquez la valeur avec un double point, par exemple `00:11:22:33:44:55`.

Pour transférer le VLAN-ID et l'adresse MAC dans le champ *Static entries (x/y)*, cliquez sur le bouton *Add*.

Add

Permet de transférer les valeurs des champs *VLAN ID* et *MAC address* dans le champ *Static entries (x/y)*.

Static entries (x/y)

Affiche le VLAN-ID et l'adresse MAC des expéditeurs souhaités liés au port.

L'équipement utilise ce champ pour afficher le nombre d'expéditeurs liés au port et la limite supérieure. Spécifiez la limite supérieure du nombre d'entrées de la table dans le champ *Static limit*.

Commentaire : Toute adresse MAC que vous affectez à ce port ne peut être affectée à aucun autre port.

Remove

Permet de supprimer les entrées mises en surbrillance dans le champ *Static entries (x/y)*.

Déplace les entrées mises en surbrillance du champ *Dynamic entries* dans le champ *Static entries (x/y)*.

Déplace toutes les entrées du champ *Dynamic entries* dans le champ *Static entries (x/y)*.

Lorsque le champ *Dynamic entries* contient un nombre d'entrées supérieur au nombre spécifié dans le champ *Static entries (x/y)*, l'équipement déplace les premières entrées jusqu'à ce que la limite supérieure soit atteinte.

Dynamic entries

Affiche le VLAN-ID et l'adresse MAC des expéditeurs automatiquement enregistrés sur ce port dans l'ordre croissant. L'équipement transmet les paquets de données provenant de ces expéditeurs lorsqu'il reçoit les paquets de données sur ce port.

Les conditions préalables pour que l'équipement puisse afficher les adresses MAC sont les suivantes :

- La fonction *Port Security* est activée. Voir le cadre *Operation*.
- L'équipement vérifie chaque paquet de données reçu sur le port. La case dans la colonne *Active* est cochée.

Spécifiez la limite supérieure du nombre d'entrées de la table dans le champ *Dynamic limit*.

Les boutons  et  vous permettent de transférer les entrées de ce champ dans le champ *Static entries (x/y)*. Vous liez de cette manière les expéditeurs concernés au port.

[Port security (Wizard) – IP addresses]

VLAN ID

Indique le VLAN-ID de la source souhaitée.

Valeurs possibles :

▶ `1..4042`

Commentaire : Affiche le VLAN-ID du VLAN d'administration.

Pour transférer le *VLAN ID* et la *IP address* dans le champ *Static entries (x/y)*, cliquez sur le bouton *Add*.

IP address

Indique l'adresse IP de la source souhaitée.

Valeurs possibles :
- Adresse IPv4 valide

Pour transférer le *VLAN ID* et la *IP address* dans le champ *Static entries (x/y)*, cliquez sur le bouton *Add*.

Add

Permet de transférer les valeurs des champs *VLAN ID* et *IP address* dans le champ *Static entries (x/y)*.

Static entries (x/y)

Affiche le VLAN-ID et l'adresse IP des expéditeurs souhaités liés au port.

L'équipement utilise ce champ pour afficher le nombre d'expéditeurs liés au port et la limite supérieure. Vous pouvez spécifier un nombre maximum de `10` adresses IP.

Remove

Permet de supprimer les entrées mises en surbrillance dans le champ *Static entries (x/y)*.

4.3 802.1X Port Authentication

[Network Security > 802.1X Port Authentication]

L'équipement surveille l'accès au réseau des équipements terminaux connectés grâce au contrôle d'accès basé sur port conformément à la norme technique IEEE 802.1X. L'équipement (authentificateur) permet à un équipement terminal (demandeur) d'avoir accès au réseau s'il s'authentifie avec des données d'authentification valides. L'authentificateur et les équipements terminaux communiquent via le protocole d'authentification EAPoL (Extensible Authentication Protocol over LANs).

L'équipement prend en charge les méthodes suivantes pour authentifier les équipements terminaux :
- `radius`
  Un serveur RADIUS appartenant au réseau authentifie les équipements terminaux.
- `ias`
  Le serveur IAS (Integrated Authentication Server) intégré à l'équipement authentifie les équipements terminaux. Contrairement au serveur RADIUS, le serveur IAS fournit uniquement les fonctions de base.

Le menu contient les boîtes de dialogue suivantes :
- 802.1X Global
- 802.1X Port Configuration
- 802.1X Port Clients
- 802.1X EAPOL Port Statistics
- 802.1X Port Authentication History
- 802.1X Integrated Authentication Server

4.3.1 802.1X Global

[Network Security > 802.1X Port Authentication > Global]

Cette boîte de dialogue vous permet de spécifier les réglages de base du contrôle d'accès basé sur port.

Operation

Operation

Active/désactive la fonction *802.1X Port Authentication*.

Valeurs possibles :

- `On`
  La fonction *802.1X Port Authentication* est activée.
  L'équipement contrôle l'accès au réseau des équipements terminaux connectés.
  Le contrôle d'accès basé sur port est activé.
- `Off` (réglage par défaut)
  La fonction *802.1X Port Authentication* est désactivée.
  Le contrôle d'accès basé sur port est désactivé.

Configuration

VLAN assignment

Active/désactive l'affectation du port concerné à un VLAN. Cette fonction vous permet de fournir des services sélectionnés à l'équipement terminal connecté dans ce VLAN.

Valeurs possibles :

- `case cochée`
  L'affectation est activée.
  Si l'équipement terminal s'authentifie avec succès, l'équipement affecte au port concerné le VLAN-ID transmis par le serveur d'authentification RADIUS.
- `case non cochée` (réglage par défaut)
  L'affectation est désactivée.
  Le port concerné est affecté au VLAN spécifié dans la boîte de dialogue *Network Security* > 802.1X Port Authentication > *Port Configuration*, ligne *Assigned VLAN ID*.

Dynamic VLAN creation

Active/désactive la création automatique du VLAN affecté par le serveur d'authentification RADIUS si le VLAN n'existe pas.

Valeurs possibles :

- `case cochée`
  La création automatique de VLAN est activée.
  L'équipement crée le VLAN s'il n'existe pas.
- `case non cochée` (réglage par défaut)
  La création automatique de VLAN est désactivée.
  Si le VLAN affecté n'existe pas, le port reste affecté au VLAN original.

Monitor mode

Active/désactive le mode de surveillance.

Valeurs possibles :

- `case cochée`
  Le mode de surveillance est activé.
  L'équipement surveille l'authentification et contribue à diagnostiquer les erreurs détectées. Lorsque l'authentification d'un équipement terminal a échoué, l'équipement permet à cet équipement terminal d'accéder au réseau.
- `case non cochée` (réglage par défaut)
  Le mode de surveillance est désactivé.

MAC authentication bypass format options

Group size

Indique la taille des groupes d'adresses MAC. L'équipement divise l'adresse MAC en groupes pour l'authentification. La taille des groupes est spécifiée en demi-octets, chacun d'entre eux est représenté par un caractère.

Valeurs possibles :

- *1*
  L'équipement divise l'adresse MAC en 12 groupes de un caractère.
  Exemple : `A:A:B:B:C:C:D:D:E:E:F:F`
- *2*
  L'équipement divise l'adresse MAC en 6 groupes de 2 caractères.
  Exemple : `AA:BB:CC:DD:EE:FF`
- *4*
  L'équipement divise l'adresse MAC en 3 groupes de 4 caractères.
  Exemple : `AABB:CCDD:EEFF`
- *12* (réglage par défaut)
  L'équipement formate l'adresse MAC en un groupe de 12 caractères.
  Exemple : `AABBCCDDEEFF`

Group separator

Indique le caractère de séparation des groupes.

Valeurs possibles :

- *-*
  tiret
- *:*
  double point
- *.*
  point

Upper or lower case

Indique si l'équipement formate les données d'authentification en minuscules ou en majuscules.

Valeurs possibles :

- *lower-case*
- *upper-case*

Password

Indique le mot de passe optionnel pour les clients utilisant le contournement de l'authentification.

Valeurs possibles :

- Chaîne de 0..64 caractères ASCII alphanumériques
  Après la saisie, le champ affiche *****(astérisque) au lieu du mot de passe.
- <vide>
  L'équipement utilise également le nom d'utilisateur du client en tant que mot de passe.

Information

Monitor mode clients

Affiche le nombre d'équipements terminaux auquel l'équipement a permis d'accéder au réseau malgré l'échec de l'authentification.

Il convient pour cela d'activer préalablement la fonction *Monitor mode*. Voir le cadre *Configuration*.

Non monitor mode clients

Affiche le nombre d'équipements terminaux auxquels l'équipement a permis d'accéder au réseau après une authentification réussie.

Policy 1

Affiche la méthode actuellement utilisée par l'équipement pour authentifier les équipements terminaux à l'aide de la norme technique IEEE 802.1X.

Vous pouvez spécifier la méthode utilisée dans la boîte de dialogue *Device Security > Authentication List*.

- ☐ Pour authentifier les équipements terminaux à l'aide d'un serveur RADIUS, affectez la stratégie `radius` à la liste `8021x`.
- ☐ Pour authentifier les équipements terminaux à l'aide d'un serveur IAS (Integrated Authentication Server), affectez la stratégie `ias` à la liste `8021x`.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.3.2 802.1X Port Configuration

[Network Security > 802.1X Port Authentication > Port Configuration]

Cette boîte de dialogue vous permet de spécifier les réglages de l'accès propres à chaque port.

Lorsque plusieurs équipements terminaux sont connectés à un port, l'équipement vous permet de les authentifier individuellement (authentification multi-client). Dans ce cas, l'équipement permet aux équipements terminaux connectés d'avoir accès au réseau. En revanche, l'équipement bloque l'accès pour les équipements terminaux ou pour les équipements dont l'authentification a expiré.

Table

Port

Affiche le numéro de port.

Port initialization

Active/désactive l'initialisation des ports afin d'activer le contrôle d'accès sur le port ou de le réinitialiser. Utilisez uniquement cette fonction sur des ports pour lesquels la colonne *Port control* contient la valeur `auto` ou `multiClient`.

Valeurs possibles :

- `case cochée`
  L'initialisation des ports est activée.
  Lorsque l'initialisation est terminée, l'équipement `décoche` la case correspondante.
- `case non cochée` (réglage par défaut)
  L'initialisation des ports est désactivée.
  L'équipement conserve l'état du port actuel.

Port reauthentication

Active/désactive la requête de réauthentification unique.

Utilisez uniquement cette fonction sur des ports pour lesquels la colonne *Port control* contient la valeur `auto` ou `multiClient`.

L'équipement vous permet également de d'envoyer régulièrement une nouvelle requête d'authentification à l'équipement terminal. Voir la colonne *Periodic reauthentication*.

Valeurs possibles :

- `case cochée`
  La requête de réauthentification unique est activée.
  L'équipement envoie une nouvelle requête d'authentification à l'équipement terminal. Puis, l'équipement `décoche` la case correspondante.
- `case non cochée` (réglage par défaut)
  La requête de réauthentification unique est désactivée.
  L'équipement conserve l'authentification de l'équipement terminal.

Authentication activity

Indique l'état actuel de l'authentificateur (`Authenticator PAE state`).

Valeurs possibles :

- *initialize*
- *disconnected*
- *connecting*
- *authenticating*
- *authenticated*
- *aborting*
- *held*
- *forceAuth*
- *forceUnauth*

Backend authentication state

Indique l'état actuel de la connexion au serveur d'authentification (`Backend Authentication state`).

Valeurs possibles :

- *request*
- *response*
- *success*
- *fail*
- *timeout*
- *idle*
- *initialize*

Authentication state

Indique l'état actuel du serveur d'authentification sur le port (`Controlled Port Status`).

Valeurs possibles :

- *authorized*
  L'équipement terminal s'est authentifié avec succès.
- *unauthorized*
  L'équipement terminal n'est authentifié.

Users (max.)

Indique la limite supérieure du nombre d'équipements terminaux que l'équipement authentifie simultanément sur ce port. La limite supérieure s'applique uniquement aux ports pour lesquels la colonne *Port control* contient la valeur `multiClient`.

Valeurs possibles :

- `1..16` (réglage par défaut : `16`)

Port control

Indique comment l'équipement autorise l'accès au réseau (`Port control mode`).

Valeurs possibles :

- *`forceUnauthorized`*
  L'équipement bloque l'accès au réseau. Utilisez ce réglage lorsqu'un équipement terminal non autorisé à accéder au réseau est connecté au port.
- *`auto`*
  L'équipement autorise l'accès au réseau si l'équipement terminal s'est authentifié avec succès. Utilisez ce réglage lorsqu'un équipement terminal qui s'authentifie au niveau de l'authentificateur est connecté au port.

Commentaire : Si d'autres équipements terminaux sont connectés au même port, ils sont autorisés à accéder au réseau sans authentification supplémentaire.

- *`forceAuthorized`* (réglage par défaut)
  Lorsque les équipements terminaux ne prennent pas en charge la norme technique IEEE 802.1X, l'équipement autorise l'accès au réseau. Utilisez ce réglage lorsqu'un équipement terminal autorisé à accéder au réseau sans s'authentifier est connecté au port.
- *`multiClient`*
  L'équipement autorise l'accès au réseau si l'équipement terminal s'authentifie avec succès. Si l'équipement n'envoie aucun paquet de données EAPOL, l'équipement autorise ou refuse l'accès au réseau individuellement en fonction de l'adresse MAC de l'équipement terminal. Voir la colonne *MAC authorized bypass*.
  Utilisez ce réglage lorsque plusieurs équipements terminaux sont connectés au port ou si la fonction *MAC authorized bypass* est requise.

Quiet period [s]

Indique le laps de temps en secondes pendant lequel l'authentificateur n'accepte plus de connexions supplémentaires de la part de l'équipement terminal après l'échec d'une tentative de connexion (*Quiet period [s]*).

Valeurs possibles :

- `0..65535` (réglage par défaut : `60`)

Transmit period [s]

Indique le laps de temps en secondes après lequel l'authentificateur demande à l'équipement terminal de se connecter à nouveau. Après ce temps d'attente, l'équipement terminal envoie un paquet de données EAP Request/Identity à l'équipement terminal.

Valeurs possibles :

- `1..65535` (réglage par défaut : `30`)

Supplicant timeout period [s]

Indique la période en secondes pendant laquelle l'authentificateur attend la connexion de l'équipement terminal.

Valeurs possibles :

- `1..65535` (réglage par défaut : `30`)

Server timeout [s]

Indique la période en secondes pendant laquelle l'authentificateur attend la réponse du serveur d'authentification (RADIUS ou IAS).

Valeurs possibles :

- `1..65535` (réglage par défaut : `30`)

Requests (max.)

Indique combien de fois l'authentificateur demande à l'équipement terminal de se connecter jusqu'à ce que le temps spécifié dans la colonne *Supplicant timeout period [s]* se soit écoulé. L'équipement envoie un paquet de données EAP Request/Identity à l'équipement terminal autant de fois que spécifié ici.

Valeurs possibles :

- `0..10` (réglage par défaut : `2`)

Assigned VLAN ID

Affiche l'ID du VLAN que l'authentificateur a affecté au port. Cette valeur s'applique uniquement aux ports pour lesquels la colonne *Port control* contient la valeur `auto`.

Valeurs possibles :

- `0..4042` (réglage par défaut : `0`)

La boîte de dialogue *Network Security > 802.1X Port Authentication > Port Clients* contient le VLAN-ID que l'authentificateur a affecté aux ports.

Pour les ports dont la colonne *Port control* contient la valeur `multiClient`, l'équipement affecte le tag VLAN basé sur l'adresse MAC de l'équipement lorsque celui-ci reçoit des paquets de données

sans tag de VLAN.

Assignment reason

Affiche la cause de l'affectation du VLAN-ID. Cette valeur s'applique uniquement aux ports pour lesquels la colonne *Port control* contient la valeur `auto`.

Valeurs possibles :

- `notAssigned` (réglage par défaut)
- `radius`
- `guestVlan`
- `unauthenticatedVlan`

La boîte de dialogue *Network Security > 802.1X Port Authentication > Port Clients* contient le VLAN-ID que l'authentificateur a affecté aux ports pour un demandeur.

Reauthentication period [s]

Indique le laps de temps en secondes après lequel l'authentificateur demande périodiquement à l'équipement terminal de se connecter à nouveau.

Valeurs possibles :

- `1..65535` (réglage par défaut : `3600`)

Periodic reauthentication

Active/désactive les requêtes périodiques de réauthentification.

Valeurs possibles :

- `case cochée`
  Les requêtes périodiques de réauthentification sont activées.
  L'équipement envoie périodiquement une nouvelle requête d'authentification à l'équipement terminal. Vous pouvez spécifier le laps de temps souhaité dans la colonne *Reauthentication period [s]*.
  Si l'authentificateur a affecté l'ID d'un Voice VLAN, Unauthenticated VLAN ou Guest VLAN à l'équipement terminal, ce réglage devient inefficace.
- `case non cochée` (réglage par défaut)
  Les requêtes périodiques de réauthentification sont désactivées.
  L'équipement conserve l'authentification de l'équipement terminal.

Guest VLAN ID

Indique l'ID du VLAN que l'authentificateur affecte au port lorsque l'équipement terminal ne se connecte pas au cours du laps de temps spécifié dans la colonne *Guest VLAN period*. Cette valeur s'applique uniquement aux ports pour lesquels la colonne *Port control* contient la valeur `auto` ou `multiClient`.

Cette fonction vous permet d'autoriser les équipements terminaux ne prenant pas en charge la norme technique IEEE 802.1X à accéder à certains services sélectionnés du réseau.

Valeurs possibles :

- `0` (réglage par défaut)
  L'authentificateur n'affecte pas de Guest VLAN au port.
  Lorsque vous activez l'authentification basée sur l'adresse MAC dans la colonne *MAC authorized bypass*, l'équipement définit automatiquement la valeur sur `0`.
- `1..4042`

Commentaire : Les fonctions *MAC authorized bypass* et *Guest VLAN ID* ne peuvent pas être utilisées simultanément.

Guest VLAN period

Indique la période en secondes pendant laquelle l'authentificateur attend les paquets de données EAPOL après la connexion de l'équipement terminal. Lorsque cette période est écoulée, l'authentificateur autorise l'équipement terminal à accéder au réseau et affecte le port au Guest VLAN spécifié dans la colonne *Guest VLAN ID*.

Valeurs possibles :

- `1..300` (réglage par défaut : `90`)

Unauthenticated VLAN ID

Indique l'ID du VLAN que l'authentificateur affecte au port lorsque l'authentification de l'équipement terminal échoue. Cette valeur s'applique uniquement aux ports pour lesquels la colonne *Port control* contient la valeur *`auto`*.

Cette fonction vous permet d'autoriser les équipements terminaux ne disposant pas de données d'authentification valides à accéder à certains services sélectionnés du réseau.

Valeurs possibles :

- `0..4042` (réglage par défaut : `0`)

Lorsque la valeur `0` est saisie, l'authentificateur n'affecte pas de Unauthenticated VLAN au port.

Commentaire : Affectez au port un VLAN configuré statiquement dans l'équipement.

MAC authorized bypass

Active/désactive l'authentification basée sur l'adresse MAC.

Cette fonction vous permet d'authentifier les équipements terminaux ne prenant pas en charge la norme technique IEEE 802.1X sur la base de leur adresse MAC.

Valeurs possibles :

- `case cochée`
  L'authentification basée sur l'adresse MAC est activée.
  L'équipement envoie l'adresse MAC de l'équipement terminal au serveur d'authentification RADIUS. L'équipement affecte le demandeur au VLAN correspondant sur la base de son adresse MAC, comme si l'authentification était directement effectuée via IEEE 802.1X.
- `case non cochée` (réglage par défaut)
  L'authentification basée sur l'adresse MAC est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.3.3 802.1X Port Clients

[Network Security > 802.1X Port Authentication > Port Clients]

Cette boîte de dialogue affiche des informations sur les équipements terminaux connectés.

Table

Port

Affiche le numéro de port.

User name

Affiche le nom de l'utilisateur avec lequel l'équipement terminal s'est authentifié.

MAC address

Affiche l'adresse MAC de l'équipement terminal.

Assigned VLAN ID

Affiche le VLAN-ID que l'authentificateur a affecté au port après l'authentification réussie de l'équipement terminal.

Si la valeur *Network Security > 802.1X Port Authentication > Port Configuration* est spécifiée pour le port dans la colonne *Port control* de la boîte de dialogue `multiClient`, l'équipement affecte le tag VLAN basé sur l'adresse MAC de l'équipement lorsque celui-ci reçoit des paquets de données sans tag de VLAN.

Assignment reason

Affiche la raison de l'affectation du VLAN.

Valeurs possibles :

- `default`
- `radius`
- `unauthenticatedVlan`
- `guestVlan`
- `monitorVlan`
- `invalid`

Le champ affiche uniquement une valeur valide tant que le client est authentifié.

Session timeout

Affiche le temps restant en secondes jusqu'à expiration de l'authentification de l'équipement terminal. Cette valeur s'applique uniquement si la valeur `auto` ou `multiClient` est spécifiée pour le port s'affichant dans la colonne *Port control* de la boîte de dialogue *Network Security > 802.1X Port Authentication > Port Configuration*.

Le serveur d'authentification affecte le délai d'attente à l'équipement via le serveur RADIUS. La valeur `0` signifie que le serveur d'authentification n'a pas affecté de délai d'attente.

Termination action

Affiche l'action effectuée par l'équipement après écoulement du délai d'authentification.

Valeurs possibles :

- *default*
- *reauthenticate*

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.3.4 802.1X EAPOL Port Statistics

[Network Security > 802.1X Port Authentication > Statistics]

Cette boîte de dialogue affiche les paquets de données EAPOL que l'équipement terminal a envoyés et reçus pour l'authentification des équipements terminaux.

Table

Port

Affiche le numéro de port.

Received packets

Affiche le nombre total de paquets de données EAPOL que l'équipement a reçus sur le port.

Transmitted packets

Affiche le nombre total de paquets de données EAPOL que l'équipement a envoyés sur le port.

Start packets

Affiche le nombre de paquets de données EAPOL Start que l'équipement a reçus sur le port.

Logoff packets

Affiche le nombre de paquets de données EAPOL Logoff que l'équipement a reçus sur le port.

Response/ID packets

Affiche le nombre total de paquets de données EAP Response/Identity que l'équipement a reçus sur le port.

Response packets

Affiche le nombre de paquets de données EAP Response valides que l'équipement a reçus sur le port (sans paquets de données EAP Response/Identity).

Request/ID packets

Affiche le nombre total de paquets de données EAP Request/Identity que l'équipement a reçus sur le port.

Request packets

Affiche le nombre de paquets de données EAP Request valides que l'équipement a reçus sur le port (sans paquets de données EAP Request/Identity).

Invalid packets

Affiche le nombre de paquets de données EAPOL présentant un type de trame inconnu que l'équipement a reçus sur le port.

Received error packets

Affiche le nombre de paquets de données EAPOL présentant un champ Packet Body Length non valide que l'équipement a reçus sur le port.

Packet version

Affiche le numéro de version du protocole du dernier paquet de données EAPOL reçu par l'équipement sur le port.

Source of last received packet

Affiche l'adresse MAC de l'expéditeur du dernier paquet de données EAPOL reçu par l'équipement sur le port.

La valeur `00:00:00:00:00:00` signifie que le port n'a pas encore reçu de paquets de données EAPOL.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.3.5 802.1X Port Authentication History

[Network Security > 802.1X Port Authentication > Port Authentication History]

L'équipement enregistre le processus d'authentification des équipements terminaux connectés à ses ports. Cette boîte de dialogue affiche les informations enregistrées pendant l'authentification.

Table

Port

Affiche le numéro de port.

Authentification time stamp

Affiche l'heure à laquelle l'authentificateur a authentifié l'équipement terminal.

Result age

Affiche depuis combien de temps cette entrée est inscrite dans la table.

MAC address

Affiche l'adresse MAC de l'équipement terminal.

VLAN ID

Affiche l'ID du VLAN qui a été affecté à l'équipement terminal avant l'authentification.

Authentication status

Indique l'état du serveur d'authentification sur le port.

Valeurs possibles :

- *success*
  L'authentification a réussi.
- *failure*
  L'authentification a échoué.

Access status

Indique si l'équipement autorise l'équipement terminal à accéder au réseau.

Valeurs possibles :

- *granted*
  L'équipement autorise l'équipement terminal à accéder au réseau.
- *denied*
  L'équipement n'autorise pas l'équipement terminal à accéder au réseau.

Assigned VLAN ID

Affiche l'ID du VLAN que l'authentificateur a affecté au port.

Assignment type

Affiche le type de VLAN que l'authentificateur a affecté au port.

Valeurs possibles :

- *default*
- *radius*
- *unauthenticatedVlan*
- *guestVlan*
- *monitorVlan*
- *notAssigned*

Assignment reason

Affiche la raison de l'affectation de l'ID du VLAN-ID et du type de VLAN.

802.1X Port Authentication History

Port

Simplifie la table et affiche uniquement les entrées relatives au port sélectionné ici. Vous êtes ainsi en mesure d'enregistrer la table plus facilement et de le trier selon vos souhaits.

Valeurs possibles :

- `all`
  La table affiche les entrées pour chaque port.
- `<Numéro de port>`
  La table affiche les entrées qui s'appliquent au port sélectionné ici.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.3.6 802.1X Integrated Authentication Server

Le serveur IAS (Integrated Authentication Server) vous permet d'authentifier les équipements terminaux à l'aide de la norme technique IEEE 802.1X. Contrairement au serveur RADIUS, le serveur IAS dispose d'un nombre très limité de fonctions. L'authentification repose uniquement sur le nom d'utilisateur et le mot de passe.

Cette boîte de dialogue vous permet de gérer les données d'authentification des équipements terminaux. L'équipement vous permet de configurer jusqu'à 100 jeux de données d'authentification.

Pour authentifier les équipements terminaux à l'aide d'un serveur Integrated Authentication Server, affectez la stratégie *Device Security > Authentication List* à la liste 8021x dans la boîte de dialogue `ias`.

Table

User name

Affiche le nom de l'utilisateur de l'appareil terminal.

Pour créer un nouvel utilisateur, cliquez sur le bouton  .

Password

Indique le mot de passe avec lequel l'utilisateur s'authentifie.

Valeurs possibles :

- Chaîne de 0..64 caractères ASCII alphanumériques

L'équipement fait la distinction entre les majuscules et les minuscules.

Active

Active/désactive les données d'authentification.

Valeurs possibles :

- `case cochée`
  Les données d'authentification sont activées. Un équipement terminal peut choisir l'option d'authentification basée sur la norme technique IEEE 802.1X en utilisant ces données de d'authentification.
- `case non cochée` (réglage par défaut)
  Les données d'authentification sont désactivées.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.4 RADIUS

[Network Security > RADIUS]

Avec ses réglages par défaut, l'équipement authentifie les utilisateurs en se basant sur la gestion locale des utilisateurs. Cependant, à mesure que la taille d'un réseau augmente, il devient de plus en plus difficile de préserver la cohérence des données d'authentification pour l'ensemble des équipements.

Le serveur RADIUS (Remote Authentication Dial-In User Service) vous permet d'authentifier et d'autoriser les utilisateurs au niveau d'un point central du réseau. Un serveur RADIUS effectue les tâches suivantes à ce niveau :

- Authentication
  Le serveur d'authentification authentifie les utilisateurs lorsque le client RADIUS situé au niveau du point d'accès transmet au serveur les données d'authentification des utilisateurs.
- Autorisation
  Le serveur d'authentification octroie aux utilisateurs authentifiés une autorisation pour des services sélectionnés en affectant divers paramètres de l'équipement terminal concerné au client RADIUS au niveau du point d'accès.
- Traçabilité
  Le serveur de traçabilité enregistre les données de trafic générées pendant l'authentification du port conformément à la norme technique IEEE 802.1X. Cela vous permet de déterminer par la suite les services que les utilisateurs ont utilisés et dans quelle mesure.

Si vous affectez la stratégie `radius` à une application dans la boîte de dialogue *Device Security > Authentication List*, l'équipement fonctionne en tant que client RADIUS. L'équipement transmet les données d'authentification des utilisateurs au serveur d'authentification primaire. Le serveur d'authentification décide si les données de connexion sont valides et transmet les autorisations de l'utilisateur à l'équipement.

L'équipement affecte le type de service transmis dans la réponse d'un serveur RADIUS à un rôle d'utilisateur existant dans l'équipement de la manière suivante :

- `Administrative-User`: *`administrator`*
- `Login-User`: *`operator`*
- `NAS-Prompt-User`: *`guest`*

L'équipement vous permet également d'authentifier les équipements terminaux avec la norme technique IEEE 802.1X via un serveur d'authentification. Pour ce faire, affectez la stratégie `radius` à la liste `8021x` dans la boîte de dialogue *Device Security > Authentication List*.

Le menu contient les boîtes de dialogue suivantes :

- RADIUS Global
- RADIUS Authentication Server
- RADIUS Accounting Server
- RADIUS Authentication Statistics
- RADIUS Accounting Statistics

4.4.1 RADIUS Global

[Network Security > RADIUS > Global]

Cette boîte de dialogue vous permet de spécifier les réglages de base du serveur RADIUS.

RADIUS configuration

Retransmits (max.)

Indique combien de fois l'équipement retransmet un requête n'ayant pas reçu de réponse au serveur d'authentification avant que l'équipement n'envoie la requête à un autre serveur d'authentification.

Valeurs possibles :

- `1..15` (réglage par défaut : `4`)

Timeout [s]

Indique la période en secondes pendant laquelle l'équipement patiente après la transmission d'une requête à un serveur d'authentification avant transmette à nouveau la requête.

Valeurs possibles :

- `1..30` (réglage par défaut : `5`)

Accounting

Active/désactive la traçabilité.

Valeurs possibles :

- `case cochée`
  La traçabilité est activée.
  L'équipement envoie les données de trafic à un serveur de traçabilité spécifié dans la boîte de dialogue *Network Security > RADIUS > Accounting Server*.
- `case non cochée` (réglage par défaut)
  La traçabilité est désactivée.

NAS IP address (attribute 4)

Indique l'adresse IP que l'équipement transmet au serveur d'authentification en tant qu'attribut 4. Indique l'adresse IP de l'équipement ou une autre adresse disponible.

Commentaire : L'équipement n'inclut l'attribut 4 que si le paquet a été déclenché par la requête d'authentification *802.1X* d'un équipement terminal (demandeur).

Valeurs possibles :

- Adresse IPv4 valide (réglage par défaut : `0.0.0.0`)

Dans de nombreux cas, un pare-feu est installé entre l'équipement et le serveur d'authentification. Le procédé NAT (Network Address Translation) du pare-feu modifie l'adresse IP originale, et le serveur d'authentification reçoit l'adresse IP traduite de l'équipement.

L'équipement transmet l'adresse IP non modifiée dans ce champ au procédé NAT (Network Address Translation).

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Supprime les statistiques des boîtes de dialogue *Network Security > RADIUS > Authentication Statistics* et *Network Security > RADIUS > Accounting Statistics*.

4.4.2 RADIUS Authentication Server

[Network Security > RADIUS > Authentication Server]

Cette boîte de dialogue vous permet de spécifier jusqu'à 8 serveurs d'authentification. Un serveur d'authentification authentifie et autorise les utilisateurs lorsque l'équipement transmet les données d'authentification au serveur.

L'équipement transmet les données de connexion au serveur d'authentification primaire spécifié. Lorsque le serveur ne répond pas, l'équipement contacte le serveur d'authentification spécifié figurant en premier dans la table. Si ce serveur ne répond pas non plus, l'équipement contacte le prochain serveur figurant dans la table.

Table

Index

Affiche l'index auquel l'entrée de table se réfère.

Name

Affiche le nom du serveur.

Pour modifier cette valeur, cliquez sur le champ correspondant.

Valeurs possibles :

- Chaîne de 1..32 caractères ASCII alphanumériques
  (réglage par défaut : `Default-RADIUS-Server`)

Address

Indique l'adresse IP du serveur.

Valeurs possibles :

- Adresse IPv4 valide

Destination UDP port

Indique le numéro du port UDP sur lequel le serveur reçoit des requêtes.

Valeurs possibles :

- `0..65535` (réglage par défaut : `1812`)
  Exception : le port `2222` est réservé à des fonctions internes.

Secret

Affiche ****** (astérisques) lorsque vous spécifiez un mot de passe avec lequel l'équipement se connecte au serveur. Pour modifier le mot de passe, cliquez sur le champ correspondant.

Valeurs possibles :

- Chaîne de 1..64 caractères ASCII alphanumériques

Le mot de passe vous est transmis par l'administrateur du serveur d'authentification.

Primary server

Définit le serveur d'authentification comme primaire ou secondaire.

Valeurs possibles :

- `case cochée`
  Le serveur est défini en tant que serveur d'authentification primaire. L'équipement envoie vers ce serveur d'authentification les données d'authentification permettant d'authentifier les utilisateurs.
  Lorsque vous activez plusieurs serveurs, l'équipement indique le dernier serveur activé en tant que serveur d'authentification primaire.
- `case non cochée` (réglage par défaut)
  Le serveur est défini en tant que serveur d'authentification secondaire. Lorsque l'équipement ne reçoit pas de réponse de la part du serveur d'authentification primaire, l'équipement n'envoie pas les données d'authentification au serveur d'authentification secondaire.

Active

Active/désactive la connexion avec le serveur.

L'équipement utilise le serveur si vous spécifiez la valeur *Device Security > Authentication List* dans la boîte de dialogue `radius` dans l'une des lignes *Policy 1* à *Policy 5*.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La connexion est activée. L'équipement envoie à ce serveur les données d'authentification permettant d'authentifier les utilisateurs lorsque les conditions préalables précitées sont remplies.
- `case non cochée`
  La connexion est désactivée. L'équipement n'envoie pas de données d'authentification à ce serveur.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée à la table.

- Spécifiez l'index dans le champ *Index*.
- Spécifiez l'adresse IP du serveur dans le champ *Address*.

4.4.3 RADIUS Accounting Server

[Network Security > RADIUS > Accounting Server]

Cette boîte de dialogue vous permet de spécifier jusqu'à 8 serveurs de traçabilité. Un serveur de traçabilité enregistre les données de trafic générées pendant l'authentification du port conformément à la norme technique IEEE 802.1X. Pour cela, il convient préalablement d'activer la fonction *Accounting* dans le menu *Network Security > RADIUS > Global*.

L'équipement envoie les données de trafic au premier serveur de traçabilité pouvant être joint. Si le serveur de traçabilité ne répond pas, l'équipement contacte le prochain serveur figurant dans la table.

Table

Index

Affiche l'index auquel l'entrée de table se réfère.

Valeurs possibles :

- `1..8`

Name

Affiche le nom du serveur.

Pour modifier cette valeur, cliquez sur le champ correspondant.

Valeurs possibles :

- Chaîne de 1..32 caractères ASCII alphanumériques
  (réglage par défaut : `Default-RADIUS-Server`)

Address

Indique l'adresse IP du serveur.

Valeurs possibles :

- Adresse IPv4 valide

Destination UDP port

Indique le numéro du port UDP sur lequel le serveur reçoit des requêtes.

Valeurs possibles :

- `0..65535` (réglage par défaut : `1813`)
  Exception : le port `2222` est réservé à des fonctions internes.

Secret

Affiche ****** (astérisques) lorsque vous spécifiez un mot de passe avec lequel l'équipement se connecte au serveur. Pour modifier le mot de passe, cliquez sur le champ correspondant.

Valeurs possibles :

- Chaîne de 1..16 caractères ASCII alphanumériques

Le mot de passe vous est transmis par l'administrateur du serveur d'authentification.

Active

Active/désactive la connexion avec le serveur.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La connexion est activée. L'équipement envoie les données de trafic à ce serveur lorsque les conditions préalables précitées sont remplies.
- `case non cochée`
  La connexion est désactivée. L'équipement n'envoie pas de données de trafic à ce serveur.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée à la table.

- Spécifiez l'index dans le champ *Index*.
- Spécifiez l'adresse IP du serveur dans le champ *Address*.

4.4.4 RADIUS Authentication Statistics

[Network Security > RADIUS > Authentication Statistics]

Cette boîte de dialogue affiche les informations relatives à la communication entre l'équipement et le serveur d'authentification. La table affiche les informations relatives à chaque serveur dans une ligne séparée.

Pour supprimer les statistiques, cliquez sur le bouton ☰ dans la boîte de dialogue *Network Security > RADIUS > Global*, puis sur l'élément *Reset*.

Table

Name

Affiche le nom du serveur.

Address

Affiche l'adresse IP du serveur.

Round trip time

Affiche l'intervalle de temps en centièmes de seconde entre la dernière réponse reçue de la part du serveur (Access Reply/Access Challenge) et le paquet de données correspondant envoyé (Access Request).

Access requests

Affiche le nombre de paquets de données Access que l'équipement a envoyés au serveur. Cette valeur ne prend pas en compte les répétitions.

Retransmitted access-request packets

Affiche le nombre de paquets de données Access que l'équipement a retransmis au serveur.

Access accepts

Affiche le nombre de paquets de données Access Accept que l'équipement a reçus de la part du serveur.

Access rejects

Affiche le nombre de paquets de données Access Reject que l'équipement a reçus de la part du serveur.

Access challenges

Affiche le nombre de paquets de données Access Challenge que l'équipement a reçus de la part du serveur.

Malformed access responses

Affiche le nombre de paquets de données Access Response mal formés que l'équipement a reçus de la part du serveur (y compris les paquets de données présentant une longueur invalide).

Bad authenticators

Affiche le nombre de paquets de données Access Response présentant un authentificateur invalide que l'équipement a reçus de la part du serveur.

Pending requests

Affiche le nombre de paquets de données Access Request que l'équipement a envoyés au serveur pour lesquels il n'a pas encore reçu de réponse de la part du serveur.

Timeouts

Affiche combien de fois aucune réponse du serveur n'a été reçue avant l'écoulement du temps d'attente spécifié.

Unknown types

Affiche le nombre de paquets de données présentant un type de données inconnu que l'équipement a reçus de la part du serveur sur le port d'authentification.

Packets dropped

Affiche le nombre de paquets de données que l'équipement a reçus de la part du serveur sur le port d'authentification avant de les rejeter.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.4.5 RADIUS Accounting Statistics

[Network Security > RADIUS > Accounting Statistics]

Cette boîte de dialogue affiche les informations relatives à la communication entre l'équipement et le serveur de traçabilité. La table affiche les informations relatives à chaque serveur dans une ligne séparée.

Pour supprimer les statistiques, cliquez sur le bouton ☰ dans la boîte de dialogue *Network Security > RADIUS > Global*, puis sur l'élément *Reset*.

Table

Name

Affiche le nom du serveur.

Address

Affiche l'adresse IP du serveur.

Round trip time

Affiche l'intervalle de temps en centièmes de seconde entre la dernière réponse reçue de la part du serveur (Accounting Response) et le paquet de données correspondant envoyé (Accounting Request).

Accounting-request packets

Affiche le nombre de paquets de données Accounting Request que l'équipement a envoyés au serveur. Cette valeur ne prend pas en compte les répétitions.

Retransmitted accounting-request packets

Affiche le nombre de paquets de données Accounting Request que l'équipement a retransmis au serveur.

Received packets

Affiche le nombre de paquets de données Accounting Response que l'équipement a reçus de la part du serveur.

Malformed packets

Affiche le nombre de paquets de données Accounting Response mal formés que l'équipement a reçus de la part du serveur (y compris les paquets de données présentant une longueur invalide).

Bad authenticators

Affiche le nombre de paquets de données Accounting Response présentant un authentificateur invalide que l'équipement a reçus de la part du serveur.

Pending requests

Affiche le nombre de paquets de données Accounting Request que l'équipement a envoyés au serveur pour lesquels il n'a pas encore reçu de réponse de la part du serveur.

Timeouts

Affiche combien de fois aucune réponse du serveur n'a été reçue avant l'écoulement du temps d'attente spécifié.

Unknown types

Affiche le nombre de paquets de données présentant un type de données inconnu que l'équipement a reçus de la part du serveur sur le port de traçabilité.

Packets dropped

Affiche le nombre de paquets de données que l'équipement a reçus de la part du serveur sur le port de traçabilité avant de les rejeter.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.5 DoS

[Network Security > DoS]

Le déni de service (« denial of service », DoS) est une cyber-attaque dont le but est de provoquer la défaillance de services ou d'équipements spécifiques. Cette boîte de dialogue vous permet de configurer plusieurs filtres contribuant à protéger l'équipement lui-même et d'autres équipements du réseau contre les attaques DoS.

Le menu contient les boîtes de dialogue suivantes :
- DoS Global

4.5.1 DoS Global

[Network Security > DoS > Global]

Cette boîte de dialogue vous permet de spécifier les réglages DoS pour les protocoles TCP/UDP, IP et ICMP.

TCP/UDP

Un scanner effectue des balayages de ports pour préparer des attaques contre le réseau. Le scanner utilise différentes techniques pour identifier les équipements utilisés et les ports ouverts. Ce cadre vous permet d'activer les filtres des techniques de balayage spécifiques.

L'équipement prend en charge la détection des types de balayage suivants :
- Balayages de type Null
- Balayages de type Xmas
- Balayages de type SYN/FIN
- Attaques TCP Offset
- Attaques TCP SYN
- Attaques de port L4
- Balayages d'en-tête minimal

Null Scan filter

Active/désactive le filtre des balayages de type Null.

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.

Valeurs possibles :
- `case cochée`
  Le filtre est activé.
- `case non cochée` (réglage par défaut)
  Le filtre est désactivé.

Xmas filter

Active/désactive le filtre Xmas.

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.

Valeurs possibles :
- `case cochée`
  Le filtre est activé.
- `case non cochée` (réglage par défaut)
  Le filtre est désactivé.

SYN/FIN filter

Active/désactive le filtre SYN/FIN.

L'équipement détecte les paquets de données entrants présentant des drapeaux *SYN* et *FIN* définis simultanément et les rejette.

Valeurs possibles :

- `case cochée`
  Le filtre est activé.
- `case non cochée` (réglage par défaut)
  Le filtre est désactivé.

TCP Offset protection

Active/désactive la protection contre les attaques TCP Offset.

La protection contre les attaques TCP Offset détecte les paquets de données TCP entrants dont le champ Fragment Offset de l'en-tête IP est égal à 1 et les rejette.

La protection contre les attaques TCP Offset accepte les paquets UDP et ICMP dont le champ Fragment Offset de l'en-tête IP est égal à 1 et les rejette.

Valeurs possibles :

- `case cochée`
  La protection est activée.
- `case non cochée` (réglage par défaut)
  La protection est désactivée.

TCP SYN protection

Active/désactive la protection contre les attaques TCP SYN.

Le filtre TCP SYN détecte les paquets de données entrants présentant un drapeau TCP SYN défini et un port source L4 <1024 et les rejette.

Valeurs possibles :

- `case cochée`
  La protection est activée.
- `case non cochée` (réglage par défaut)
  La protection est désactivée.

L4 Port protection

Active/désactive la protection contre les attaques de port L4.

La protection contre les attaques de port L4 détecte les paquets de données TCP et UDP entrants dont le numéro de port source et le numéro de port cible sont identiques et les rejette.

Valeurs possibles :

- `case cochée`
  La protection est activée.
- `case non cochée` (réglage par défaut)
  La protection est désactivée.

IP

Ce cadre vous permet d'activer ou de désactiver le filtre des attaques Land. Avec la méthode d'attaque Land, la station attaquante envoie des paquets de données dont les adresses source et cible sont identiques à celles du destinataire. Lorsque vous activez ce filtre, l'équipement détecte les paquets de données présentant des adresses source et cible identiques et rejette ces paquets de données.

Land Attack filter

Active/désactive le filtre des attaques Land.

Le filtre des attaques Land détecte les paquets de données IP entrants dont les adresses IP source et cible sont identiques et les rejette.

Valeurs possibles :

- `case cochée`
  Le filtre est activé.
- `case non cochée` (réglage par défaut)
  Le filtre est désactivé.

ICMP

Cette boîte de dialogue vous fournit les options de filtre pour les paramètres ICMP suivants :
- Paquets de données fragmentés
- Paquets ICMP à partir d'une taille spécifique
- Pings Broadcast

Filter fragmented packets

Active/désactive le filtre des paquets ICMP fragmentés.

Le filtre détecte les paquets ICMP fragmentés et les rejette.

Valeurs possibles :

- `case cochée`
  Le filtre est activé.
- `case non cochée` (réglage par défaut)
  Le filtre est désactivé.

Filter by packet size

Active/désactive le filtre des paquets ICMP entrants.

Le filtre détecte les paquets ICMP dont la taille des données utiles dépasse la taille spécifiée dans le champ *Allowed payload size [byte]* et les rejette.

Valeurs possibles :

- `case cochée`
  Le filtre est activé.
- `case non cochée` (réglage par défaut)
  Le filtre est désactivé.

Allowed payload size [byte]

Indique la taille maximale des données utiles des paquets ICMP en octets.

Cochez la case *Filter by packet size* si vous souhaitez que l'équipement rejette les paquets de données entrants dont la taille des données utiles dépasse la taille maximale autorisée pour les paquets ICMP.

Valeurs possibles :

- `0..1472` (réglage par défaut : `512`)

Drop broadcast ping

Active/désactive le filtre des pings Broadcast. Les pings Broadcast constituent des preuves de l'existence d'attaques par réflexion.

Valeurs possibles :

- `case cochée`
  Le filtre est activé.
  L'équipement détecte les pings Broadcast et les rejette.
- `case non cochée` (réglage par défaut)
  Le filtre est désactivé.

Information

Packets dropped

Affiche le nombre de paquets de données que l'équipement a rejetés.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.6 DHCP Snooping

[Network Security > DHCP Snooping]

DHCP Snooping est une fonction qui prend en charge la sécurité du réseau. DHCP Snooping surveille les paquets DHCP entre le client DHCP et le serveur DHCP et agit comme un pare-feu entre les hôtes non sécurisés et les serveurs DHCP sécurisés.

Dans cette boîte de dialogue, vous configurez et surveillez les propriétés d'équipement suivantes :

- Valider les paquets DHCP provenant de sources non fiables et filtrer les paquets non valides.
- Limiter le trafic de données DHCP provenant de sources fiables et non fiables.
- Configurer et mettre à jour la base de données de liaison DHCP Snooping. Cette base de données contient l'adresse MAC, l'adresse IP, le VLAN et le port des clients DHCP sur les ports non fiables.
- Valider les requêtes ultérieures des hôtes non fiables à partir de la base de données de liaison DHCP Snooping.

Vous pouvez activer DHCP Snooping globalement et pour un VLAN spécifique. Vous spécifiez l'état de sécurité (fiable ou non fiable) sur les ports individuels. Vérifiez que le service DHCP peut être atteint via les ports fiables. Pour DHCP Snooping, vous configurez généralement les ports utilisateur/client comme non fiables et les ports uplink comme fiables.

Le menu contient les boîtes de dialogue suivantes :

- DHCP Snooping Global
- DHCP Snooping Configuration
- DHCP Snooping Statistics
- DHCP Snooping Bindings

4.6.1 DHCP Snooping Global

[Network Security > DHCP Snooping > Global]

Cette boîte de dialogue vous permet de configurer les paramètres globaux de DHCP Snooping pour votre équipement :

- Activer/désactiver *DHCP Snooping* globalement.
- Activer/désactiver *Auto-Disable* globalement.
- Activer/désactiver la vérification de l'adresse MAC source.
- Configurer le nom, l'emplacement de stockage et l'intervalle de stockage de la base de données des liaisons.

Operation

Operation

Active/désactive la fonction DHCP Snooping globalement.

Valeurs possibles :

- `On`
- `Off` (réglage par défaut)

Configuration

Verify MAC

Active/désactive la vérification de l'adresse MAC source dans le paquet Ethernet.

Valeurs possibles :

- `case cochée`
  La vérification de l'adresse MAC source est activée.
  L'équipement compare l'adresse MAC source avec l'adresse MAC du client dans le paquet DHCP reçu.
- `case non cochée` (réglage par défaut)
  La vérification de l'adresse MAC source est désactivée.

Auto-disable

Active/désactive la fonction *Auto-Disable* relative à la *DHCP Snooping*.

Valeurs possibles :

- `case cochée`
  La fonction *Auto-Disable* relative à la *DHCP Snooping* est activée.
  Cochez également la case de la colonne *Auto-disable* dans l'onglet *Port* de la boîte de dialogue *Network Security > DHCP Snooping > Configuration* pour les ports concernés.
- `case non cochée` (réglage par défaut)
  La fonction *Auto-Disable* relative à la *DHCP Snooping* est désactivée.

Binding database

Remote file name

Spécifie le nom du fichier dans lequel l'équipement enregistre la base de données de liaison DHCP Snooping.

Commentaire :

L'équipement enregistre uniquement les liaisons dynamiques dans la base de données des liaisons persistantes. L'équipement enregistre les liaisons statiques dans le profil de configuration.

Remote IP address

Spécifie l'adresse IP distante sous laquelle l'équipement enregistre la base de données des liaisons persistantes DHCP Snooping. Si la valeur est `0.0.0.0`, l'équipement enregistre la base de données des liaisons localement.

Valeurs possibles :

- Adresse IPv4 valide
- `0.0.0.0` (réglage par défaut)
  L'équipement enregistre la base de données de liaison localement.

Store interval [s]

Spécifie le délai en secondes après lequel l'équipement enregistre la base de données de liaison DHCP Snooping lorsqu'il identifie un changement dans la base de données.

Valeurs possibles :

- `15..86400` (réglage par défaut : `300`)

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.6.2 DHCP Snooping Configuration

[Network Security > DHCP Snooping > Configuration]

Cette boîte de dialogue vous permet de configurer DHCP Snooping pour des ports individuels et pour des VLANs individuels.

La boîte de dialogue contient les onglets suivants :
- [Port]
- [VLAN ID]

[Port]

Dans cet onglet, vous configurez la fonction *DHCP Snooping* pour des ports individuels.
- Configurer un port comme étant fiable/non fiable.
- Activer/désactiver la consignation des paquets invalides pour les ports individuels.
- Limiter le nombre de paquets DHCP.
- Désactiver automatiquement un port si le trafic de données DHCP dépasse la limite spécifiée.

Table

Port

Affiche le numéro de port.

Trust

Active/désactive l'état de sécurité (fiable, non fiable) du port.

Lorsque cette fonction est activée, le port est configuré comme étant fiable. En général, vous avez connecté le port fiable à un serveur DHCP.

Lorsque cette fonction est activée, le port est configuré comme n'étant pas fiable.

Valeurs possibles :
- `case cochée`
  Le port est spécifié comme étant fiable. DHCP Snooping transfère les paquets clients autorisés via les ports fiables.
- `case non cochée` (réglage par défaut)
  Le port est configuré comme n'étant pas fiable. Sur les ports non fiables, l'équipement compare le port récepteur avec le port client dans la base de données des liaisons.

Log

Active/désactive la consignation des paquets invalides que l'équipement détermine sur ce port.

Valeurs possibles :
- `case cochée`
  La consignation de paquets invalides est activée.
- `case non cochée` (réglage par défaut)
  La consignation de paquets invalides est désactivée.

Rate limit

Spécifie le nombre maximum de paquets DHCP par intervalle de rafale pour ce port. Si le nombre de paquets DHCP entrants dépasse actuellement la limite spécifiée dans un intervalle de rafale, l'équipement rejette les paquets DHCP entrants supplémentaires.

Valeurs possibles :

- `-1` (réglage par défaut)
  Désactive le nombre limite de paquets DHCP par intervalle de rafale sur ce port.
- `0..150` paquets par intervalle
  Limite le nombre maximum de paquets DHCP par intervalle de rafale sur ce port.

Vous spécifiez l'intervalle de rafale dans la colonne *Burst interval*.

Si vous activez la fonction d'auto-désactivation, l'équipement désactive également le port. Vous trouverez la fonction d'auto-désactivation dans la colonne *Auto-disable*.

Burst interval

Spécifie la durée de l'intervalle de rafale en secondes sur ce port. L'intervalle de rafale est pertinent pour la fonction de limitation de charge.

Vous spécifiez le nombre maximum de paquets DHCP par intervalle de rafale dans la colonne *Rate limit*.

Valeurs possibles :

- `1..15` (réglage par défaut : `1`)

Auto-disable

Active/désactive la fonction *Auto-Disable* pour les paramètres que la fonction *DHCP Snooping* surveille sur le port.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La fonction *Auto-Disable* est activée sur le port.
  La condition préalable est que dans la boîte de dialogue *Network Security > DHCP Snooping > Global*, la case *Auto-disable* dans le cadre *Configuration* soit cochée.
  - Si le port reçoit plus de paquets DHCP que le nombre spécifié dans le champ *Rate limit* dans le délai spécifié dans la colonne *Burst interval*, l'équipement désactive le port. La LED « État du lien » du port clignote 3x par période.
  - La boîte de dialogue *Diagnostics > Ports > Auto-Disable* affiche quels ports sont actuellement désactivés en raison du dépassement des paramètres.
  - La fonction *Auto-Disable* réactive le port automatiquement. Pour cela, accédez à la boîte de dialogue *Diagnostics > Ports > Auto-Disable* et spécifiez une période d'attente pour le port concerné dans la colonne *Reset timer [s]*.
- `case non cochée`
  La fonction *Auto-Disable* est désactivée sur le port.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[VLAN ID]

Dans cet onglet, vous configurez la fonction *DHCP Snooping* pour des VLAN individuels.

Table

VLAN ID

Affiche le VLAN-ID auquel l'entrée de table se réfère.

Active

Active/désactive la fonction *DHCP Snooping* dans ce VLAN.

La fonction *DHCP Snooping* transmet les messages du client DHCP valides aux ports fiables dans les VLAN sans fonction *Routing*.

Valeurs possibles :

- `case cochée`
  La fonction *DHCP Snooping* est activée dans ce VLAN.
- `case non cochée` (réglage par défaut)
  La fonction *DHCP Snooping* est désactivée dans ce VLAN.
  L'équipement transfère les paquets DHCP conformément aux réglages de commutation sans surveiller les paquets. La base de données des liaisons reste inchangée.

Commentaire : Pour activer DHCP Snooping pour un port, activez la fonction *DHCP Snooping* globalement dans la boîte de dialogue *Network Security > DHCP Snooping > Global*. Vérifiez que vous avez affecté le port à un VLAN dans lequel DHCP Snooping est activé.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.6.3 DHCP Snooping Statistics

[Network Security > DHCP Snooping > Statistics]

DHCP Snooping permet à l'équipement de consigner les erreurs détectées et de générer des statistiques. Dans cette boîte de dialogue, vous surveillez les statistiques DHCP Snooping pour chaque port.

L'équipement consigne les informations suivantes :
- Erreurs détectées lors de la validation de l'adresse MAC du client DHCP
- Messages du client DHCP avec un port détecté comme incorrect
- Messages du serveur DHCP vers des ports non fiables

Table

Port

Affiche le numéro de port.

MAC verify failures

Affiche le nombre de discordances entre l'adresse MAC du client DHCP dans le champ « chaddr » du paquet de données DHCP et l'adresse source dans le paquet Ethernet.

Invalid client messages

Affiche le nombre de messages du client DHCP entrants reçus sur le port pour lequel l'équipement attend le client sur un autre port selon la base de données de liaison DHCP Snooping.

Invalid server messages

Affiche le nombre de messages du serveur DHCP que l'équipement a reçu sur le port non fiable.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Réinitialise toute la table.

4.6.4 DHCP Snooping Bindings

[Network Security > DHCP Snooping > Bindings]

DHCP Snooping utilise les messages DHCP pour configurer et mettre à jour la base de données de liaison.

- Liaisons statiques
  L'équipement vous permet de saisir jusqu'à 256 liaisons statiques DHCP Snooping dans la base de données.
- Liaisons dynamiques
  La base de données des liaisons dynamiques contient des données pour les clients uniquement sur les ports non fiables.

Ce menu vous permet de spécifier les paramètres des liaisons statiques et dynamiques.

- Configurer de nouvelles liaisons statiques et les définir comme actives/inactives.
- Afficher, activer/désactiver ou supprimer les liaisons statiques qui ont été configurées.

Table

MAC address

Spécifie l'adresse MAC dans l'entrée de la table que vous liez à une *IP address* et un *VLAN ID*.

Valeurs possibles :

- Adresse MAC Unicast valide
  Indiquez la valeur avec un double point, par exemple `00:11:22:33:44:55`.

IP address

Spécifie l'adresse IP pour la liaison statique DHCP Snooping.

Valeurs possibles :

- Adresse IPv4 unicast valide inférieure à `224.x.x.x` et en dehors de la plage `127.0.0.0/8` (réglage par défaut : `0.0.0.0`)

VLAN ID

Spécifie l'ID du VLAN auquel l'entrée de table s'applique.

Valeurs possibles :

- `<ID des VLANs qui sont configurés>`

Port

Spécifie le port pour la liaison statique DHCP Snooping.

Valeurs possibles :

- Ports disponibles

Remaining binding time

Affiche le temps restant pour la liaison dynamique DHCP Snooping.

Active

Active/désactive la liaison statique DHCP Snooping spécifiée.

Valeurs possibles :

- `case cochée`
  La liaison statique DHCP Snooping est activée.
- `case non cochée` (réglage par défaut)
  La liaison statique DHCP Snooping est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée à la table.

Dans le champ *MAC address*, vous spécifiez l'adresse MAC que vous liez à une adresse IP et à un VLAN-ID.

Supprime l'entrée de table mise en surbrillance.

La condition préalable est que la case dans la colonne *Active* est décochée.

En outre, l'équipement supprime les liaisons dynamiques de ce port créées avec la fonction IP *IP Source Guard*.

4.7 IP Source Guard

[Network Security > IP Source Guard]

IP Source Guard (IPSG) est une fonction qui prend en charge la sécurité du réseau. Cette fonction filtre les paquets de données IP en fonction de l'ID source (adresse IP source ou adresse MAC source) de l'abonné. IPSG vous aide à protéger le réseau contre les attaques par usurpation d'adresse IP/MAC.

IPSG et DHCP Snooping
IP Source Guard fonctionne en combinaison avec la fonction *DHCP Snooping* du port.

DHCP Snooping rejette les paquets de données IP sur les ports non fiables, à l'exception des messages DHCP. Lorsque l'équipement reçoit des réponses DHCP et que la base de données de liaison DHCP Snooping est configurée, l'équipement crée une liste de contrôle d'accès VLAN (VACL) pour chaque port contenant les ID source des abonnés.

Vous pouvez configurer les paramètres de la fonction *DHCP Snooping* pour les ports individuels et les VLAN individuels dans la boîte de dialogue *Network Security > DHCP Snooping > Configuration*.

IPSG et la sécurité des ports
IP Source Guard coopère avec la fonction *Port Security*. Voir la boîte de dialogue *Network Security > Port Security*. Sur demande, l'IPSG informe la fonction *Port Security* si une adresse MAC appartient à une liaison valide.

- Si vous avez désactivé IPSG sur le port d'entrée, IPSG identifie le paquet de données comme étant valide.
- Si vous avez activé IPSG sur le port d'entrée, IPSG vérifie l'adresse MAC à l'aide de la base de données de liaison. Si l'adresse MAC est saisie dans la base de données de liaison, IPSG identifie le paquet de données comme étant valide ou non.

La fonction *Port Security* prend en charge le traitement ultérieur des paquets de données non valides. Vous pouvez spécifier les réglages de la fonction *Port Security* dans la boîte de dialogue *Network Security > Port Security*.

Commentaire : Pour que l'équipement vérifie l'adresse IP et l'adresse MAC des paquets de données reçus sur le port, activez la fonction *Verify MAC*.

Pour que l'équipement vérifie le VLAN-ID et l'adresse MAC de la source avant de transférer le paquet de données, activez également la fonction *Port Security*. Voir la boîte de dialogue *Network Security > Port Security*.

Le menu contient les boîtes de dialogue suivantes :

- IP Source Guard Port
- IP Source Guard Bindings

4.7.1 IP Source Guard Port

[Network Security > IP Source Guard > Port]

Cette boîte de dialogue vous permet d'afficher et de configurer les propriétés d'équipement suivantes pour chaque port :
- Inclure/exclure les adresses MAC source pour le filtrage.
- Activer/désactiver la fonction *IP Source Guard*.

Table

Port

Affiche le numéro de port.

Verify MAC

Active/désactive le filtrage basé sur l'adresse MAC source si la fonction *IP Source Guard* est activée. L'équipement exécute ce filtrage en plus du filtrage basé sur l'adresse IP source.

Valeurs possibles :

- `case cochée`
  Le filtrage basé sur l'adresse MAC source est activé.
  Pour activer la fonction, cochez la case *Active*.
- `case non cochée` (réglage par défaut)
  Le filtrage basé sur l'adresse MAC source est désactivé.
  Pour désactiver la fonction, décochez également la case *Active*.

Active

Active/désactive la fonction *IP Source Guard* sur le port.

Valeurs possibles :

- `case cochée`
  La fonction *IP Source Guard* est activée.
  Vous activez également la fonction *DHCP Snooping* dans la boîte de dialogue *Network Security* > DHCP Snooping > *Global*.
- `case non cochée` (réglage par défaut)
  La fonction *IP Source Guard* est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.7.2 IP Source Guard Bindings

[Network Security > IP Source Guard > Bindings]

Cette boîte de dialogue affiche les liaisons statiques et dynamiques d'IP Source Guard.

- L'équipement apprend les liaisons dynamiques via DHCP Snooping. Voir la boîte de dialogue *Network Security > DHCP Snooping > Configuration*.
- Les liaisons statiques sont des liaisons IP Source Guard configurées manuellement par l'utilisateur. La boîte de dialogue vous permet de modifier les liaisons statiques.

Table

MAC address

Affiche l'adresse MAC de la liaison.

IP address

Affiche l'adresse IP de la liaison.

VLAN ID

Affiche le VLAN-ID de la liaison.

Port

Affiche le numéro du port de la liaison.

Hardware status

Affiche le statut matériel de la liaison.

L'équipement applique la liaison au matériel uniquement si les réglages sont corrects. Avant que l'équipement n'applique la liaison statique IPSG au matériel, il vérifie les conditions préalables suivantes :

- La case *Active* est cochée.
- La fonction *IP Source Guard* sur le port est activée ; dans la boîte de dialogue *Network Security > IP Source Guard > Port*, la case *Active* est cochée.

Valeurs possibles :

- `case cochée`
  La liaison est activée, l'équipement applique la liaison au matériel.
- `case non cochée`
  La liaison est désactivée.

Active

Active/désactive la liaison statique IPSG spécifiée entre l'adresse MAC spécifiée et l'adresse IP spécifiée, pour le VLAN spécifié sur le port spécifié.

Valeurs possibles :

- `case cochée`
  La liaison statique IPSG est activée.
- `case non cochée` (réglage par défaut)
  La liaison statique IPSG est désactivée.

Commentaire : Pour que la liaison statique soit effective, activez la fonction *IP Source Guard* sur le port correspondant. Dans la boîte de dialogue *Network Security > IP Source Guard > Port*, cochez la case *Active*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée à la table.

- Dans le champ *MAC address*, vous spécifiez l'adresse MAC pour la liaison statique.
- Dans le champ *IP address*, vous spécifiez l'adresse ID pour la liaison statique.
- Dans le champ *VLAN ID*, vous spécifiez le VLAN-ID.
- Dans le champ *Port*, vous spécifiez l'ID du VLAN.

Supprime l'entrée de table mise en surbrillance.

La condition préalable est que la case dans la colonne *Active* est décochée.

4.8 Dynamic ARP Inspection

[Network Security > Dynamic ARP Inspection]

Dynamic ARP Inspection est une fonction qui prend en charge la sécurité du réseau. Cette fonction analyse les paquets ARP les consigne et rejette les paquets ARP invalides et hostiles.

La fonction *Dynamic ARP Inspection* permet d'éviter toute une série d'attaques de type intermédiaire. Avec ce type d'attaque, une station hostile écoute le trafic de données des autres abonnés en empiétant sur le cache ARP de ses voisins peu méfiants. La station hostile envoie des requêtes ARP et des réponses ARP et saisit l'adresse IP d'un autre abonné pour sa propre adresse MAC dans la relation (liaison) entre l'adresse IP et l'adresse MAC.

À l'aide des mesures suivantes, la fonction *Dynamic ARP Inspection* permet de s'assurer que l'équipement ne transmet que des requêtes ARP et des réponses ARP valides.

- Écouter les requêtes ARP et les réponses ARP sur les ports non fiables.
- Vérifier la validité de la relation (liaison) entre l'adresse IP et l'adresse MAC des paquets déterminés avant que l'équipement ne mette à jour le cache ARP local et ne transmette les paquets à l'adresse cible correspondante.
- Rejeter les paquets ARP invalides.

L'équipement vous permet de spécifier jusqu'à 100 ACL (listes d'accès) ARP actives. Vous pouvez activer jusqu'à 20 règles pour chaque ACL ARP.

Le menu contient les boîtes de dialogue suivantes :

- Dynamic ARP Inspection Global
- Dynamic ARP Inspection Configuration
- Dynamic ARP Inspection ARP Rules
- Dynamic ARP Inspection Statistics

4.8.1 Dynamic ARP Inspection Global

[Network Security > Dynamic ARP Inspection > Global]

Configuration

Verify source MAC

Active/désactive la vérification de l'adresse MAC source. L'équipement exécute la vérification à la fois dans les requêtes ARP et les réponses ARP.

Valeurs possibles :

- `case cochée`
  La vérification de l'adresse MAC source est activée.
  L'équipement vérifie l'adresse MAC source des paquets ARP reçus.
  - L'équipement transmet des paquets ARP avec une adresse MAC source valide à l'adresse cible correspondante et met à jour le cache ARP local.
  - L'équipement rejette les paquets ARP dont l'adresse MAC source n'est pas valide.
- `case non cochée` (réglage par défaut)
  La vérification de l'adresse MAC source est désactivée.

Verify destination MAC

Active/désactive la vérification de l'adresse MAC cible. L'équipement exécute la vérification dans les réponses ARP.

Valeurs possibles :

- `case cochée`
  La vérification de l'adresse MAC cible est activée.
  L'équipement vérifie l'adresse MAC cible des paquets ARP entrants.
  - L'équipement transmet des paquets ARP avec une adresse MAC cible valide à l'adresse cible correspondante et met à jour le cache ARP local.
  - L'équipement rejette les paquets ARP dont l'adresse MAC cible n'est pas valide.
- `case non cochée` (réglage par défaut)
  La vérification de l'adresse MAC cible des paquets ARP entrants est désactivée.

Verify IP address

Active/désactive la vérification de l'adresse IP.

Dans les requêtes ARP, l'équipement vérifie l'adresse IP source. Dans les réponses ARP, l'équipement vérifie l'adresse IP cible et l'adresse IP source.

L'équipement désigne les adresses IP suivantes comme non valides :

- `0.0.0.0`
- Adresses broadcast `255.255.255.255`
- Adresses multicast `224.0.0.0/4` (classe D)
- Adresses classe E `240.0.0.0/4` (réservées à des fins ultérieures)
- Adresses de loopback dans la plage `127.0.0.0/8`.

Valeurs possibles :

- `case cochée`
  La vérification de l'adresse IP est activée.
  L'équipement vérifie l'adresse IP des paquets ARP entrants. L'équipement transmet des paquets ARP avec une adresse IP valide à l'adresse cible correspondante et met à jour le cache ARP local. L'équipement rejette les paquets ARP dont l'adresse IP n'est pas valide.
- `case non cochée` (réglage par défaut)
  La vérification de l'adresse IP est désactivée.

Auto-disable

Active/désactive la fonction *Auto-Disable* relative à la *Dynamic ARP Inspection*.

Valeurs possibles :

- `case cochée`
  La fonction *Auto-Disable* relative à la *Dynamic ARP Inspection* est activée.
  Cochez également la case de la colonne *Port* dans l'onglet *Auto-disable* de la boîte de dialogue *Network Security > Dynamic ARP Inspection > Configuration* pour les ports concernés.
- `case non cochée` (réglage par défaut)
  La fonction *Auto-Disable* relative à la *Dynamic ARP Inspection* est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.8.2 Dynamic ARP Inspection Configuration

[Network Security > Dynamic ARP Inspection > Configuration]

La boîte de dialogue contient les onglets suivants :
- [Port]
- [VLAN ID]

[Port]

Table

Port

Affiche le numéro de port.

Trust

Active/désactive la surveillance des paquets ARP sur les ports non fiables.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  L'équipement surveille les paquets ARP sur les ports non fiables.
  L'équipement transfère immédiatement les paquets ARP sur les ports fiables.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Rate limit

Spécifie le nombre maximum de paquets ARP par intervalle sur ce port. Si le nombre de paquets ARP entrants dépasse actuellement la limite spécifiée dans un intervalle de rafale, l'équipement rejette les paquets ARP entrants supplémentaires. Vous spécifiez l'intervalle de rafale dans la colonne *Burst interval*.

En option, l'équipement désactive également le port si vous activez la fonction d'auto-désactivation. Vous activez/désactivez la fonction *Auto-Disable* dans la colonne *Auto-disable*.

Valeurs possibles :

- `-1` (réglage par défaut)
  Désactive le nombre limite de paquets ARP par intervalle de rafale sur ce port.
- `0..300` paquets par intervalle
  Limite le nombre maximum de paquets ARP par intervalle de rafale sur ce port.

Burst interval

Spécifie la durée de l'intervalle de rafale en secondes sur ce port. L'intervalle de rafale est pertinent pour la fonction de limitation de charge.

Vous spécifiez le nombre maximum de paquets ARP par intervalle de rafale dans la colonne *Rate limit*.

Valeurs possibles :

- `1..15` (réglage par défaut : `1`)

Auto-disable

Active/désactive la fonction *Auto-Disable* pour les paramètres que la fonction *Dynamic ARP Inspection* surveille sur le port.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La fonction *Auto-Disable* est activée sur le port.
  La condition préalable est que dans la boîte de dialogue *Network Security > Dynamic ARP Inspection > Global*, la case *Auto-disable* dans le cadre *Configuration* soit cochée.
  - Si le port reçoit plus de paquets ARP que le nombre spécifié dans le champ *Rate limit* dans le délai spécifié dans la colonne *Burst interval*, l'équipement désactive le port. La LED « État du lien » du port clignote 3x par période.
  - La boîte de dialogue *Diagnostics > Ports > Auto-Disable* affiche quels ports sont actuellement désactivés en raison du dépassement des paramètres.
  - La fonction *Auto-Disable* réactive le port automatiquement. Pour cela, accédez à la boîte de dialogue *Diagnostics > Ports > Auto-Disable* et spécifiez une période d'attente pour le port concerné dans la colonne *Reset timer [s]*.
- `case non cochée`
  La fonction *Auto-Disable* est désactivée sur le port.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[VLAN ID]

Table

VLAN ID

Affiche le VLAN-ID auquel l'entrée de table se réfère.

Log

Active/désactive la consignation des paquets invalides que l'équipement détermine dans ce VLAN. Si l'équipement détecte une erreur lors de la vérification de l'adresse IP, de l'adresse MAC source ou de l'adresse MAC cible, ou lors de la vérification de la relation (liaison) entre l'adresse IP et l'adresse MAC, l'équipement identifie un paquet ARP comme étant non valide.

Valeurs possibles :

- `case cochée`
  La consignation de paquets invalides est activée.
  L'équipement enregistre les paquets ARP invalides.
- `case non cochée` (réglage par défaut)
  La consignation de paquets invalides est désactivée.

Binding check

Active/désactive la vérification des paquets ARP entrants que l'équipement reçoit sur les ports non fiables et sur les VLAN pour lesquels la fonction *Dynamic ARP Inspection* est activée. Pour ces paquets ARP, l'équipement vérifie l'ACL ARP et la relation DHCP Snooping (liaisons).

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La vérification de la liaison des paquets ARP est activée.
- `case non cochée`
  La vérification de la liaison des paquets ARP est désactivée.

ACL strict

Active/désactive la vérification stricte des paquets ARP entrants en fonction des règles ACL ARP spécifiées.

Valeurs possibles :

- `case cochée`
  La vérification stricte est activée.
  L'équipement vérifie les paquets ARP entrants en fonction de la règle ACL ARP spécifiée dans la colonne *ARP ACL*.
- `case non cochée` (réglage par défaut)
  La vérification stricte est désactivée.
  L'équipement vérifie les paquets ARP entrants en fonction de la règle ACL ARP spécifiée dans la colonne *ARP ACL*, puis des entrées de la base de données DHCP Snooping.

ARP ACL

Spécifie l'ACL ARP que l'équipement utilise.

Valeurs possibles :

- `<nom de règle>`
  Vous pouvez créer et modifier les règles dans la boîte de dialogue *Network Security > Dynamic ARP Inspection > ARP Rules*.

Active

Active/désactive la fonction *Dynamic ARP Inspection* dans ce VLAN.

Valeurs possibles :

- `case cochée`
  La fonction *Dynamic ARP Inspection* est activée dans ce VLAN.
- `case non cochée` (réglage par défaut)
  La fonction *Dynamic ARP Inspection* est désactivée dans ce VLAN.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

4.8.3 Dynamic ARP Inspection ARP Rules

[Network Security > Dynamic ARP Inspection > ARP Rules]

Cette boîte de dialogue vous permet de spécifier les règles de vérification et de filtrage des paquets ARP.

Table

Name

Affiche le nom de la règle ARP.

Source IP address

Indique l'adresse source des paquets de données IP auxquels l'équipement applique la règle.

Valeurs possibles :

- Adresse IPv4 valide
  L'équipement applique la règle aux paquets de données IP associés à l'adresse source spécifiée.

Source MAC address

Indique l'adresse source des paquets de données MAC auxquels l'équipement applique la règle.

Valeurs possibles :

- Adresse MAC valide
  L'équipement applique la règle aux paquets de données MAC associés à l'adresse source spécifiée.

Active

Active/désactive la règle *ARP*.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La règle est activée.
- `case non cochée`
  La règle est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée à la table.

- Spécifiez le nom de la règle ARP dans le champ *Name*.
- Spécifiez l'adresse IP source de la règle ARP dans le champ *Source IP address*.
- Spécifiez l'adresse MAC source de la règle ARP dans le champ *Source MAC address*.

4.8.4 Dynamic ARP Inspection Statistics

[Network Security > Dynamic ARP Inspection > Statistics]

Cette fenêtre affiche le nombre de paquets ARP rejetés et transférés dans une vue d'ensemble.

Table

VLAN ID

Affiche le VLAN-ID auquel l'entrée de table se réfère.

Packets forwarded

Affiche le nombre de paquets ARP que l'équipement transfère après les avoir vérifiés à l'aide de la fonction *Dynamic ARP Inspection*.

Packets dropped

Affiche le nombre de paquets ARP que l'équipement rejette après les avoir vérifiés à l'aide de la fonction *Dynamic ARP Inspection*.

DHCP drops

Affiche le nombre de paquets ARP que l'équipement rejette après avoir vérifié la relation DHCP Snooping (liaison).

DHCP permits

Affiche le nombre de paquets ARP que l'équipement transfère après avoir vérifié la relation DHCP Snooping (liaison).

ACL drops

Affiche le nombre de paquets ARP que l'équipement rejette après les avoir vérifiés à l'aide des règles ACL ARP.

ACL permits

Affiche le nombre de paquets ARP que l'équipement transfère après les avoir vérifiés à l'aide des règles ACL ARP.

Bad source MAC

Affiche le nombre de paquets ARP que l'équipement rejette après que la fonction *Dynamic ARP Inspection* a détecté une erreur dans l'adresse MAC source.

Bad destination MAC

Affiche le nombre de paquets ARP que l'équipement rejette après que la fonction *Dynamic ARP Inspection* a détecté une erreur dans l'adresse MAC cible.

Invalid IP address

Affiche le nombre de paquets ARP que l'équipement rejette après que la fonction *Dynamic ARP Inspection* a détecté une erreur dans l'adresse IP.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Réinitialise toute la table.

4.9 ACL

[Network Security > ACL]

Ce menu vous permet de spécifier les réglages des listes de contrôle d'accès (ACL, Access Control Lists). Les listes de contrôle d'accès contiennent les règles que l'équipement applique les unes à la suite des autres au flux de données sur ses ports ou ses VLAN.

Si un paquet de données respecte les critères d'une ou de plusieurs règles, l'équipement applique l'action spécifiée dans la première règle qui s'applique au flux de données. L'équipement ignore les règles suivantes. Les actions possibles incluent :
- *permit*: l'équipement transmet les paquets de données à un port ou à un VLAN.
- *deny*: l'équipement rejette le paquet de données.

Avec le réglage par défaut, l'équipement transmet tous les paquets de données. Une fois que vous affectez une liste de contrôle d'accès à une interface ou un VLAN, ce comportement subi une modification. L'équipement ajoute à la fin d'une liste de contrôle d'accès une règle Deny-All implicite. En conséquence de quoi, l'équipement rejette les paquets de données qui ne respectent aucune règle. Si vous souhaitez modifier ce comportement, ajoutez une règle « permit » à la fin de vos listes de contrôle d'accès.

Procédez comme suit pour configurer des listes de contrôle d'accès et des règles :
- ☐ Créez une règle et spécifiez les réglages de la règle. Voir les boîtes de dialogue *Network Security > ACL > IPv4 Rule* ou *Network Security > ACL > MAC Rule*.
- ☐ Affectez la liste de contrôle d'accès aux ports et VLAN de l'équipement. Voir la boîte de dialogue *Network Security > ACL > Assignment*.

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

4.9.1 ACL IPv4 Rule

[Network Security > ACL > IPv4 Rule]

Cette boîte de dialogue vous permet de spécifier les règles que l'équipement applique aux paquets de données IP.

Une liste de contrôle d'accès (groupe) contient une ou plusieurs règles. L'équipement applique les règles d'une liste de contrôle d'accès les unes à la suite des autres, en commençant par la règle présentant la valeur la moins élevée dans la colonne *Index*.

L'équipement vous permet de procéder au filtrage selon les critères suivants :
- Adresse IP source ou cible d'un paquet de données
- Type du protocole de transmission
- Port source ou cible d'un paquet de données

Table

Group name

Affiche le nom de la liste de contrôle d'accès. La liste de contrôle d'accès contient les règles.

Index

Affiche le numéro de la règle contenue dans la liste de contrôle d'accès.

Si la liste de contrôle d'accès contient plusieurs règles, l'équipement traite d'abord la règle présentant la valeur la moins élevée.

Match every packet

Indique le paquet de données IP auquel l'équipement applique la règle.

Valeurs possibles :
- `case cochée` (réglage par défaut)
  L'équipement applique la règle à chaque paquet de données IP.
- `case non cochée`
  L'équipement applique la règle aux paquets de données IP en fonction de la valeur indiquée dans les champs *Source IP address*, *Destination IP address* et *Protocol*.

Source IP address

Indique l'adresse source des paquets de données IP auxquels l'équipement applique la règle.

Valeurs possibles :
- `?.?.?.?` (réglage par défaut)
  L'équipement applique la règle aux paquets de données IP associés à une adresse source quelconque.

- Adresse IPv4 valide
  L'équipement applique la règle aux paquets de données IP associés à l'adresse source spécifiée.
  Le `?` s'utilise comme caractère générique.
  Par exemple, `192.?.?.32` : l'équipement applique la règle aux paquets de données IP dont l'adresse source commence par `192.` et se termine par `.32`.
- Adresse IPv4 valide/masque de bits
  L'équipement applique la règle aux paquets de données IP associés à l'adresse source spécifiée. Le masque de bits inversé vous permet de spécifier la plage d'adresses avec une précision de l'ordre du bit.
  Par exemple, `192.168.1.0/0.0.0.127` : l'équipement applique la règle aux paquets de données IP dont l'adresse source est comprise dans une plage allant de `192.168.1.0` à `….127`.

Destination IP address

Indique l'adresse cible des paquets de données IP auxquels l'équipement applique la règle.

Valeurs possibles :

- `?.?.?.?` (réglage par défaut)
  L'équipement applique la règle aux paquets de données associés à une adresse cible quelconque.
- Adresse IPv4 valide
  L'équipement applique la règle aux paquets de données associés à l'adresse cible spécifiée.
  Le `?` s'utilise comme caractère générique.
  Par exemple, `192.?.?.32` : l'équipement applique la règle aux paquets de données IP dont l'adresse source commence par `192.` et se termine par `.32`.
- Adresse IPv4 valide/masque de bits
  L'équipement applique la règle aux paquets de données associés à l'adresse cible spécifiée. Le masque de bits inversé vous permet de spécifier la plage d'adresses avec une précision de l'ordre du bit.
  Par exemple, `192.168.1.0/0.0.0.127` : l'équipement applique la règle aux paquets de données IP dont l'adresse cible est comprise dans une plage allant de `192.168.1.0` à `….127`.

Protocol

Indique le type de protocole des paquets de données IP auxquels l'équipement applique la règle.

Valeurs possibles :

- `any` (réglage par défaut)
  L'équipement applique la règle à tous les paquets de données IP sans prendre en compte le type de protocole.
- `icmp`
- `igmp`
- `ip-in-ip`
- `tcp`
- `udp`
- `ip`

Source TCP/UDP port

Indique le port source des paquets de données IP auxquels l'équipement applique la règle. Il convient pour cela de spécifier préalablement la valeur `TCP` ou `UDP` dans la colonne *Protocol*.

Valeurs possibles :

- `any` (réglage par défaut)
  L'équipement applique la règle à tous les paquets de données IP sans prendre en compte le port source.
- `1..65535`
  L'équipement applique uniquement la règle aux paquets de données IP contenant le port source spécifié.

Destination TCP/UDP port

Indique le port cible des paquets de données IP auxquels l'équipement applique la règle. Il convient pour cela de spécifier préalablement la valeur `TCP` ou `UDP` dans la colonne *Protocol*.

Valeurs possibles :

- `any` (réglage par défaut)
  L'équipement applique la règle à tous les paquets de données IP sans prendre en compte le port cible.
- `1..65535`
  L'équipement applique uniquement la règle aux paquets de données IP contenant le port cible spécifié.

Action

Indique comment l'équipement traite les paquets de données IP lorsque l'équipement applique la règle.

Valeurs possibles :

- *permit* (réglage par défaut)
  L'équipement transmet les paquets de données IP.
- *deny*
  L'équipement rejette les paquets de données IP.

Log

Active/désactive la consignation dans le fichier log. Voir la boîte de dialogue *Diagnostics > Report > System Log*.

Valeurs possibles :

- `case cochée`
  La consignation dans le fichier log est activée.
  Il convient pour cela d'affecter préalablement la liste de contrôle d'accès à un VLAN ou un port dans la boîte de dialogue *Network Security > ACL > Assignment*.
  À intervalle de 30 s, l'équipement enregistre dans le fichier log combien de fois il a appliqué la règle « deny » à des paquets de données IP.
- `case non cochée` (réglage par défaut)
  La consignation dans le fichier log est désactivée.

L'équipement vous permet d'activer cette fonction pour un nombre maximum de 128 règles « deny ».

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée à la table.

- Dans le champ *Group name*, spécifiez le nom de la liste de contrôle d'accès à laquelle la règle appartient.
- Dans le champ *Index*, spécifiez le numéro de la règle au sein de la liste de contrôle d'accès. Si la liste de contrôle d'accès contient plusieurs règles, l'équipement traite d'abord la règle présentant la valeur la moins élevée.

4.9.2 ACL MAC Rule

[Network Security > ACL > MAC Rule]

Cette boîte de dialogue vous permet de spécifier les règles que l'équipement applique aux paquets de données MAC.

Une liste de contrôle d'accès (groupe) contient une ou plusieurs règles. L'équipement applique les règles d'une liste de contrôle d'accès les unes à la suite des autres, en commençant par la règle présentant la valeur la moins élevée dans la colonne *Index*.

L'équipement vous permet de filtrer l'adresse MAC source ou cible d'un paquet de données.

Table

Group name

Affiche le nom de la liste de contrôle d'accès. La liste de contrôle d'accès contient les règles.

Index

Affiche le numéro de la règle contenue dans la liste de contrôle d'accès.

Si la liste de contrôle d'accès contient plusieurs règles, l'équipement traite d'abord la règle présentant la valeur la moins élevée.

Match every packet

Indique les paquets de données MAC auxquels l'équipement applique la règle.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'équipement applique la règle à tous les paquets de données MAC.
- `case non cochée`
  L'équipement applique la règle aux paquets de données MAC en fonction de la valeur indiquée dans les champs *Source MAC address* et *Destination MAC address*.

Source MAC address

Indique l'adresse source des paquets de données MAC auxquels l'équipement applique la règle.

Valeurs possibles :

- `??:??:??:??:??:??` (réglage par défaut)
  L'équipement applique la règle aux paquets de données MAC associés à une adresse source quelconque.

- Adresse MAC valide
  L'équipement applique la règle aux paquets de données MAC associés à l'adresse source spécifiée.
  Le `?` s'utilise comme caractère générique.
  Par exemple, `00:11:??:??:??:??` : l'équipement applique la règle aux paquets de données MAC dont l'adresse source commence par `00:11`.
- Adresse MAC valide/masque de bits
  L'équipement applique la règle aux paquets de données MAC associés à l'adresse source spécifiée. Le masque de bits vous permet de spécifier la plage d'adresses avec une précision de l'ordre du bit.
  Par exemple, `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC` : l'équipement applique la règle aux paquets de données MAC dont l'adresse source est comprise dans une plage allant de `00:11:22:33:44:54` à `…:57`.

Destination MAC address

Indique l'adresse cible des paquets de données MAC auxquels l'équipement applique la règle.

Valeurs possibles :

- `??:??:??:??:??:??` (réglage par défaut)
  L'équipement applique la règle aux paquets de données MAC associés à une adresse cible quelconque.
- Adresse MAC valide
  L'équipement applique la règle aux paquets de données MAC associés à l'adresse cible spécifiée.
  Le `?` s'utilise comme caractère générique.
  Par exemple, `00:11:??:??:??:??` : l'équipement applique la règle aux paquets de données MAC dont l'adresse cible commence par `00:11`.
- Adresse MAC valide/masque de bits
  L'équipement applique la règle aux paquets de données MAC associés à l'adresse source spécifiée. Le masque de bits vous permet de spécifier la plage d'adresses avec une précision de l'ordre du bit.
  Par exemple, `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC` : l'équipement applique la règle aux paquets de données MAC dont l'adresse cible est comprise dans une plage allant de `00:11:22:33:44:54` à `…:57`.

Action

Indique comment l'équipement traite les paquets de données MAC lorsque l'équipement applique la règle.

Valeurs possibles :

- *`permit`* (réglage par défaut)
  L'équipement transmet les paquets de données MAC.
- *`deny`*
  L'équipement rejette les paquets de données MAC.

Log

Active/désactive la consignation dans le fichier log. Voir la boîte de dialogue *Diagnostics > Report > System Log*.

Valeurs possibles :

- `case cochée`
  La consignation dans le fichier log est activée.
  Il convient pour cela d'affecter préalablement la liste de contrôle d'accès à un VLAN ou un port dans la boîte de dialogue *Network Security > ACL > Assignment*.
  À intervalle de 30 s, l'équipement enregistre dans le fichier log combien de fois il a appliqué la règle « deny » à des paquets de données MAC.
- `case non cochée` (réglage par défaut)
  La consignation dans le fichier log est désactivée.

L'équipement vous permet d'activer cette fonction pour un nombre maximum de 128 règles « deny ».

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée à la table.

- Dans le champ *Group name*, spécifiez le nom de la liste de contrôle d'accès à laquelle la règle appartient.
- Dans le champ *Index*, spécifiez le numéro de la règle au sein de la liste de contrôle d'accès. Si la liste de contrôle d'accès contient plusieurs règles, l'équipement traite d'abord la règle présentant la valeur la moins élevée.

4.9.3 ACL Assignment

[Network Security > ACL > Assignment]

Cette boîte de dialogue vous permet d'affecter une ou plusieurs listes de contrôle d'accès aux ports et aux VLAN de l'équipement. L'affectation d'une priorité vous permet de définir un ordre de traitement, à condition que vous affectiez une ou plusieurs listes de contrôle d'accès à un port ou à un VLAN.

L'équipement applique les règles les unes à la suite des autres, en suivant l'ordre de priorité indiqué par l'index de chaque règle. Vous pouvez spécifier la priorité d'un groupe dans la colonne *Priority*. Plus le nombre spécifié est petit, plus la priorité est élevée. Au cours de ce processus, l'équipement applique les règles présentant une priorité élevée avant les règles présentant une priorité faible.

L'affectation de listes de contrôle d'accès à des ports et à des VLAN implique les différents types d'ACL suivants :
- ACL IPv4 basés sur port
- ACL MAC basés sur port
- ACL IPv4 basés sur VLAN
- ACL MAC basés sur VLAN

L'équipement vous permet d'appliquer les listes de contrôle d'accès aux paquets de données reçus (`inbound`).

Commentaire : Avant d'activer cette fonction, vérifiez qu'au moins une entrée active de la table vous permet l'accès. Sinon, la connexion à l'équipement prend fin lorsque vous modifiez les réglages. Il n'est possible d'accéder à l'administration de l'équipement qu'en utilisant la CLI (interface de ligne de commande) via l'interface série de l'équipement.

Table

Group name

Affiche le nom de la liste de contrôle d'accès. La liste de contrôle d'accès contient les règles.

Type

Indique si la liste de contrôle d'accès contient des règles MAC ou IPv4.

Valeurs possibles :
- *mac*
  La liste de contrôle d'accès contient des règles MAC.
- *ip*
  La liste de contrôle d'accès contient des règles IPv4.

La boîte de dialogue *Network Security > ACL > IPv4 Rule* vous permet de modifier les listes de contrôle d'accès contenant des règles IPv4. La boîte de dialogue *Network Security > ACL > MAC Rule* vous permet de modifier les listes de contrôle d'accès contenant des règles MAC.

Port

Affiche le port auquel la liste de contrôle d'accès est affectée. Ce champ reste vide lorsque la liste de contrôle d'accès est affectée à un VLAN.

VLAN ID

Affiche le VLAN auquel la liste de contrôle d'accès est affectée. Ce champ reste vide lorsque la liste de contrôle d'accès est affectée à un port.

Direction

Indique que l'équipement applique la liste de contrôle d'accès aux paquets de données reçus.

Priority

Affiche la priorité de la liste de contrôle d'accès.

Cette priorité vous permet de définir l'ordre suivant lequel l'équipement applique les listes de contrôle d'accès au flux de données. L'équipement applique les règles dans l'ordre croissant en commençant par la priorité n° `1`.

Valeurs possibles :

- `1..4294967295`

lorsqu'une liste de contrôle d'accès est affectée à un port et à un VLAN présentant le même numéro de priorité, l'équipement applique d'abord les règles au port.

Active

Affiche si la liste de contrôle d'accès sur le port ou dans le VLAN est activée.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La liste de contrôle d'accès est activée.
- `case non cochée`
  La liste de contrôle d'accès est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la boîte de dialogue *Create* pour affecter une règle à un port ou à un VLAN.

- Spécifiez le port ou le VLAN-ID dans le champ *Port/VLAN*.
- Spécifiez l'adresse MAC source de la règle ARP dans le champ *Priority*.
- Spécifiez les paquets de données auxquels l'équipement applique la règle dans le champ *Direction*.
- Spécifiez la règle que l'équipement affecte au port ou au VLAN dans le champ *Group name*.

5 Switching

Le menu contient les boîtes de dialogue suivantes :
- Switching Global
- Rate Limiter
- Filter for MAC Addresses
- IGMP Snooping
- Time-Sensitive Networking
- MRP-IEEE
- GARP
- QoS/Priority
- VLAN
- L2-Redundancy

5.1 Switching Global

[Switching > Global]

Cette boîte de dialogue vous permet de spécifier les réglages suivants :
- Modification de la durée de vieillissement de la table d'adresses
- Activation du contrôle de flux dans l'équipement

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.

Ainsi, les équipements connectés n'envoient plus de paquets de données tant que le signal est présent. Sur les ports uplink, cela peut provoquer des interruptions d'envoi indésirables dans le segment de réseau de niveau supérieur (« wandering backpressure »).

Configuration

MAC address

Affiche l'adresse MAC de l'équipement.

Aging time [s]

Spécifie la durée de vieillissement en secondes.

Valeurs possibles :

- `10..500000` (réglage par défaut : `30`)

L'équipement surveille l'âge des adresses MAC unicast apprises. L'équipement supprime les entrées d'adresses excédant un âge donné (aging time) de sa table d'adresses.

Vous trouverez la table d'adresses dans la boîte de dialogue *Switching > Filter for MAC Addresses*.

Flow control

Active/désactive le contrôle de flux dans l'équipement.

Valeurs possibles :

- `case cochée`
  Le contrôle de flux est actif dans l'équipement.
  Activez par ailleurs le contrôle de flux sur les ports requis. Voir la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*, case à cocher dans la colonne *Flow control*.
- `case non cochée` (réglage par défaut)
  Le contrôle de flux est inactif dans l'équipement.

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.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.2 Rate Limiter

[Switching > Rate Limiter]

L'équipement vous permet de limiter le trafic sur les ports afin de garantir un fonctionnement stable, même avec un volume de trafic important. Si le trafic sur un port excède la valeur de trafic saisie, l'équipement rejette le trafic excédentaire sur ce port.

La fonction de limiteur de charge n'intervient que sur la couche 2 et permet de limiter les effets des tempêtes de paquets de données qui submergent l'équipement (typiquement des broadcasts).

La fonction de limiteur de charge ignore les informations des protocoles des couches supérieures, comme IP ou TCP.

La boîte de dialogue contient les onglets suivants :
- [Ingress]
- [Egress]

[Ingress]

Dans cet onglet, vous activez la fonction *Rate Limiter*. La valeur seuil spécifie la quantité maximale de trafic que le port reçoit. Si le trafic sur ce port excède la valeur seuil, l'équipement rejette le trafic excédentaire sur ce port.

Table

Port

Affiche le numéro de port.

Threshold unit

Spécifie l'unité de la valeur seuil :

Valeurs possibles :
- *percent* (réglage par défaut)
  Spécifie la valeur seuil en pourcentage du débit de données du port.
- *pps*
  Spécifie la valeur seuil en paquets de données par seconde.

Broadcast mode

Active/désactive la fonction de limiteur de charge pour les paquets de données de broadcast reçus.

Valeurs possibles :
- `case cochée`
- `case non cochée` (réglage par défaut)

Si la valeur seuil est dépassée, l'équipement rejette les paquets de données de broadcast excédentaires sur ce port.

Broadcast threshold

Spécifie la valeur seuil pour les broadcasts reçus sur ce port.

Valeurs possibles :

- `0..14880000` (réglage par défaut : `0`)
  La valeur `0` désactive la fonction de limiteur de charge sur ce port.
  - Si vous sélectionnez la valeur *`percent`* dans la colonne *Threshold unit*, saisissez une valeur de pourcentage comprise entre `1` et `100`.
  - Si vous sélectionnez la valeur *`pps`* dans la colonne *Threshold unit*, saisissez une valeur absolue pour le débit de données.

Known multicast mode

Active/désactive la fonction de limiteur de charge pour les paquets de données multicast connus reçus.

Valeurs possibles :

- `case cochée`
- `case non cochée` (réglage par défaut)

Si la valeur seuil est dépassée, l'équipement rejette les paquets de données de multicast excédentaires sur ce port.

Known multicast threshold

Spécifie la valeur seuil pour les multicasts reçus sur ce port.

Valeurs possibles :

- `0..14880000` (réglage par défaut : `0`)
  La valeur `0` désactive la fonction de limiteur de charge sur ce port.
  - Si vous sélectionnez la valeur *`percent`* dans la colonne *Threshold unit*, saisissez une valeur de pourcentage comprise entre `0` et `100`.
  - Si vous sélectionnez la valeur *`pps`* dans la colonne *Threshold unit*, saisissez une valeur absolue pour le débit de données.

Unknown frame mode

Active/désactive la fonction de limiteur de charge pour les paquets de données unicast et multicast reçus avec une adresse cible inconnue.

Valeurs possibles :

- `case cochée`
- `case non cochée` (réglage par défaut)

Si la valeur seuil est dépassée, l'équipement rejette les paquets de données unicast excédentaires sur ce port.

Unknown frame threshold

Spécifie la valeur seuil pour les unicasts avec une adresse cible inconnue reçus sur ce port.

Valeurs possibles :

- `0..14880000` (réglage par défaut : `0`)
  La valeur `0` désactive la fonction de limiteur de charge sur ce port.
  - Si vous sélectionnez la valeur *`percent`* dans la colonne *Threshold unit*, saisissez une valeur de pourcentage comprise entre `0` et `100`.
  - Si vous sélectionnez la valeur *`pps`* dans la colonne *Threshold unit*, saisissez une valeur absolue pour le débit de données.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Egress]

Dans cet onglet, vous spécifiez le débit de transmission sur le port.

Table

Port

Affiche le numéro de port.

Bandwidth [%]

Spécifie le débit de transmission.

Valeurs possibles :

- `0` (réglage par défaut)
  La limitation de la bande passante est désactivée.
- `1..100`
  La limitation de la bande passante est activée.
  Cette valeur spécifie le pourcentage de la vitesse de liaison globale pour le port par incréments de 1 %.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.3 Filter for MAC Addresses

[Switching > Filter for MAC Addresses]

Cette boîte de dialogue vous permet d'afficher et de modifier les filtres d'adresses pour la table d'adresses. Les filtres d'adresses spécifient de quelle manière les paquets de données sont transmis dans l'équipement sur la base de l'adresse MAC cible.

Chaque ligne de la table correspond à un filtre. L'équipement définit automatiquement les filtres. L'équipement vous permet de définir manuellement des filtres supplémentaires.

L'équipement transmet les paquets de données comme suit :

- Lorsque la table contient une entrée pour l'adresse cible d'un paquet de données, l'équipement transmet le paquet de données depuis le port de réception vers le port spécifié dans l'entrée de la table.
- Lorsque la table ne contient pas d'entrée pour l'adresse cible, l'équipement transmet le paquet de données depuis le port de réception vers tout autre port.

Table

Pour supprimer les adresses MAC apprises de la table d'adresses, cliquez dans la boîte de dialogue *Basic Settings > Restart* sur le bouton *Reset MAC address table*.

Address

Affiche l'adresse MAC cible à laquelle l'entrée de la table s'applique.

VLAN ID

Affiche l'ID du VLAN auquel l'entrée de la table s'applique.

L'équipement apprend les adresses MAC pour chaque VLAN séparément (apprentissage VLAN indépendant).

Status

Affiche comment l'équipement a défini le filtre d'adresses.

Valeurs possibles :

- *learned*
  Filtre d'adresses défini automatiquement par l'équipement sur la base des paquets de données reçus.
- *permanent*
  Filtre d'adresses défini manuellement. Le filtre d'adresses est défini de façon permanente.
- *IGMP*
  Filtre d'adresses défini automatiquement par IGMP Snooping.
- *mgmt*
  Adresse MAC de l'équipement. Le filtre d'adresses est protégé contre les modifications.
- *MRP-MMRP*
  Filtre d'adresses multicast défini automatiquement par MMRP.
- *GMRP*
  Filtre d'adresses multicast défini automatiquement par GMRP.

<Numéro de port>

Affiche comment le port correspondant transmet les paquets de données qu'il dirige vers les adresses cibles adjacentes.

Valeurs possibles :

- `-`
  Le port ne transmet aucun paquet de données à l'adresse cible.
- `learned`
  Le port transmet des paquets de données à l'adresse cible. L'équipement a créé le filtre automatiquement sur la base des paquets de données reçus.
- `IGMP learned`
  Le port transmet des paquets de données à l'adresse cible. L'équipement a créé le filtre automatiquement sur la base de l'IGMP.
- `unicast static`
  Le port transmet des paquets de données à l'adresse cible. Un utilisateur a créé le filtre.
- `multicast static`
  Le port transmet des paquets de données à l'adresse cible. Un utilisateur a créé le filtre.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée à la table.

- Dans le champ *Address*, vous spécifiez l'adresse MAC cible.
- Dans le champ *VLAN ID*, vous spécifiez l'ID du VLAN.
- Dans le champ *Port*, vous spécifiez le port.
  - Sélectionnez un port si l'adresse MAC cible est une adresse unicast.
  - Sélectionnez un ou plusieurs ports si l'adresse MAC cible est une adresse multicast.
  - Ne sélectionnez aucun port pour créer un filtre de rejet. L'équipement rejette les paquets de données avec l'adresse MAC cible spécifiée dans l'entrée de la table.

Reset MAC address table

Supprime de la table de transfert les adresses MAC qui ont la valeur `learned` dans la colonne *Status*.

5.4 IGMP Snooping

[Switching > IGMP Snooping]

L'Internet Group Management Protocol (IGMP) est un protocole pour la gestion dynamique des groupes multicast. Il décrit la distribution des paquets de données multicast entre les routeurs et les équipements terminaux sur la couche 3.

L'équipement vous permet d'utiliser la fonction IGMP Snooping, afin d'utiliser aussi les mécanismes IGMP sur la couche 2.
- Sans IGMP Snooping, l'équipement transmet les paquets de données multicast à tous les ports.
- Avec la fonction IGMP Snooping activée, l'équipement transmet les paquets de données multicast uniquement sur les ports auxquels des destinataires multicast sont connectés. La charge du réseau est ainsi réduite. L'équipement évalue les paquets de données IGMP transmis sur la couche 3 et utilise les informations sur la couche 2.

N'activez pas la fonction IGMP Snooping tant que les conditions suivantes ne sont pas remplies :
- Il y a, dans le réseau, un routeur multicast qui génère des requêtes IGMP (requêtes périodiques).
- Les équipements qui participent à l'IGMP Snooping transfèrent les requêtes IGMP.

L'équipement associe les rapports IGMP aux entrées dans sa table d'adresses. Lorsqu'un destinataire multicast rejoint un groupe multicast, l'équipement crée une entrée de table pour ce port dans la boîte de dialogue *Switching > Filter for MAC Addresses*. Lorsque le destinataire multicast quitte le groupe multicast, l'équipement supprime l'entrée de la table.

Le menu contient les boîtes de dialogue suivantes :
- IGMP Snooping Global
- IGMP Snooping Configuration
- IGMP Snooping Enhancements
- IGMP Snooping Querier
- IGMP Snooping Multicasts

5.4.1 IGMP Snooping Global

[Switching > IGMP Snooping > Global]

Cette boîte de dialogue vous permet d'activer le protocole *IGMP Snooping* dans l'équipement et de le configurer pour chaque port et chaque VLAN.

Operation

Operation

Active/désactive la fonction *IGMP Snooping* dans l'équipement.

Valeurs possibles :

- `On`
  La fonction *IGMP Snooping* est activée dans l'équipement conformément à RFC 4541 (« Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches »).
- `Off` (réglage par défaut)
  La fonction *IGMP Snooping* est désactivée dans l'équipement.
  L'équipement transmet une requête reçue, génère un rapport et laisse les paquets de données sans les évaluer. Les paquets de données reçus avec une adresse cible multicast sont transmis à tous les ports par l'équipement.

Information

Multicast control packets processed

Affiche le nombre de paquets de données de contrôle multicast traités.

Cette statistique englobe les types de paquets suivants :

- Rapports IGMP
- Requêtes IGMP version V1
- Requêtes IGMP version V2
- Requêtes IGMP version V3
- Requêtes IGMP avec une version incorrecte
- Paquets PIM ou DVMRP

L'équipement utilise les paquets de données de contrôle multicast pour créer la table d'adresses afin de transmettre les paquets de données multicast.

Valeurs possibles :

- `0..2^31-1`

Vous utilisez le bouton *Reset IGMP snooping data* dans la boîte de dialogue *Basic Settings > Restart* ou la commande `clear igmp-snooping` à l'aide l'interface de ligne de commande pour réinitialiser les entrées IGMP Snooping, y compris le compteur de paquets de données de contrôle multicast traités.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset IGMP snooping counters

Supprime les entrées IGMP Snooping et remet le compteur dans le cadre *Information* à `0`.

5.4.2 IGMP Snooping Configuration

[Switching > IGMP Snooping > Configuration]

Cette boîte de dialogue vous permet d'activer la fonction *IGMP Snooping* dans l'équipement et de la configurer pour chaque port et chaque VLAN.

La boîte de dialogue contient les onglets suivants :
- [VLAN ID]
- [Port]

[VLAN ID]

Dans cet onglet, vous configurez la fonction *IGMP Snooping* pour chaque VLAN.

Table

VLAN ID

Affiche l'ID du VLAN auquel l'entrée de la table s'applique.

Active

Active/désactive la fonction *IGMP Snooping* pour ce VLAN.

La condition préalable est que la fonction *IGMP Snooping* soit activée globalement.

Valeurs possibles :
- `case cochée`
  IGMP Snooping est activé pour ce VLAN. Le VLAN a rejoint le flux de données multicast.
- `case non cochée` (réglage par défaut)
  IGMP Snooping est désactivé pour ce VLAN. Le VLAN a quitté le flux de données multicast.

Group membership interval

Spécifie la durée en secondes pendant laquelle un VLAN d'un groupe multicast dynamique reste dans la table d'adresses lorsque l'équipement ne reçoit plus de paquets de données de rapport du VLAN.

Indiquez une valeur supérieure à la valeur dans la colonne *Max. response time*.

Valeurs possibles :
- `2..3600` (réglage par défaut : `260`)

Max. response time

Spécifie la durée en secondes pendant laquelle les membres d'un groupe multicast répondent à un paquet de données de requête. Pour leur réponse, les membres indiquent une durée aléatoire comprise dans le temps de réponse. Vous évitez ainsi que tous les membres du groupe multicast ne répondent simultanément à la requête.

Indiquez une valeur inférieure à la valeur de la colonne *Group membership interval*.

Valeurs possibles :

- `1..25` (réglage par défaut : `10`)

Fast leave admin mode

Active/désactive la fonction Fast Leave pour ce VLAN.

Valeurs possibles :

- `case cochée`
  Lorsque la fonction Fast Leave est activée et que l'équipement reçoit un message IGMP Leave d'un groupe multicast, l'équipement supprime immédiatement l'entrée de sa table d'adresses.
- `case non cochée` (réglage par défaut)
  Lorsque la fonction Fast Leave est désactivée, l'équipement envoie d'abord les requêtes basées MAC aux membres du groupe multicast et supprime une entrée lorsqu'un VLAN n'envoie plus de messages de rapport.

MRP expiration time

Délai d'expiration actuel du routeur multicast. Spécifie la durée en secondes pendant laquelle l'équipement attend une requête sur ce port appartenant à un VLAN. Si le port ne reçoit pas de paquet de données de requête, l'équipement supprime le port de la liste des ports avec routeurs multicast connectés.

Vous pouvez configurer ce paramètre uniquement si le port appartient à un VLAN existant.

Valeurs possibles :

- `0`
  temporisation illimitée - pas de délai d'expiration
- `1..3600` (réglage par défaut : `260`)

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Port]

Dans cet onglet, vous configurez la fonction *IGMP Snooping* pour chaque port.

Table

Port

Affiche le numéro de port.

Active

Active/désactive la fonction *IGMP Snooping* pour ce port.

La condition préalable est que la fonction *IGMP Snooping* soit activée globalement.

Valeurs possibles :

- `case cochée`
  IGMP Snooping est activé sur ce port. L'équipement inclut le port dans le flux de données multicast.
- `case non cochée` (réglage par défaut)
  IGMP Snooping est désactivé sur ce port. Le port a quitté le flux de données multicast.

Group membership interval

Spécifie la durée en secondes pendant laquelle un port d'un groupe multicast dynamique reste dans la table d'adresses lorsque l'équipement ne reçoit plus de paquets de données de rapport du port.

Valeurs possibles :

- `2..3600` (réglage par défaut : `260`)

Indiquez une valeur supérieure à la valeur dans la colonne *Max. response time*.

Max. response time

Spécifie la durée en secondes pendant laquelle les membres d'un groupe multicast répondent à un paquet de données de requête. Pour leur réponse, les membres indiquent une durée aléatoire comprise dans le temps de réponse. Vous évitez ainsi que tous les membres du groupe multicast ne répondent simultanément à la requête.

Valeurs possibles :

- `1..25` (réglage par défaut : `10`)

Indiquez une valeur inférieure à la valeur dans la colonne *Group membership interval*.

MRP expiration time

Spécifie le délai d'expiration actuel du routeur multicast. Le délai d'expiration MRP est la durée en secondes pendant laquelle l'équipement attend un paquet de requête sur ce port. Si le port ne reçoit pas de paquet de données de requête, l'équipement supprime le port de la liste des ports avec routeurs multicast connectés.

Valeurs possibles :

- `0`
  temporisation illimitée - pas de délai d'expiration
- `1..3600` (réglage par défaut : `260`)

Fast leave admin mode

Active/désactive la fonction Fast Leave pour ce port.

Valeurs possibles :

- `case cochée`
  Lorsque la fonction Fast Leave est activée et que l'équipement reçoit un message IGMP Leave d'un groupe multicast, l'équipement supprime immédiatement l'entrée de sa table d'adresses.
- `case non cochée` (réglage par défaut)
  Lorsque la fonction Fast Leave est désactivée, l'équipement envoie d'abord des requêtes basées MAC aux membres du groupe multicast et supprime une entrée lorsqu'un port n'envoie plus de messages de rapport.

Static query port

Active/désactive le mode *Static query port*.

Valeurs possibles :

- `case cochée`
  Le mode *Static query port* est activé.
  Le port est un port de requête statique dans les VLAN qui sont définis.
  Si vous utilisez la fonction *Redundant Coupling Protocol* et que l'équipement fonctionne en tant qu'esclave, n'activez pas le mode *Static query port* pour les ports sur l'anneau secondaire/le réseau.
- `case non cochée` (réglage par défaut)
  Le mode *Static query port* est désactivé.
  Le port n'est pas un port de requête statique. L'équipement ne transmet les messages de rapport IGMP au port que s'il reçoit des requêtes IGMP.

VLAN IDs

Affiche l'ID des VLAN auxquels l'entrée de table s'applique.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.4.3 IGMP Snooping Enhancements

[Switching > IGMP Snooping > Snooping Enhancements]

Cette boîte de dialogue vous permet de sélectionner un port pour un VLAN-ID et de configurer ce port.

Table

VLAN ID

Affiche l'ID du VLAN auquel l'entrée de la table s'applique.

<Numéro de port>

Affiche, pour chaque VLAN défini dans l'équipement, si le port concerné est un port de requête. De plus, le champ affiche si l'équipement transmet chaque flux multicast dans le VLAN à ce port.

Valeurs possibles :

- `-`
  Le port n'est pas un port de requête dans ce VLAN.
- `L`= Learned
  L'équipement a détecté le port en tant que port de requête car le port a reçu des requêtes IGMP dans ce VLAN. Le port n'est pas un port de requête configuré de manière statique.
- `A`= Automatic
  L'équipement a détecté le port en tant que port de requête. La condition préalable est que vous configuriez le port en tant que *`Learn by LLDP`*.
- `S`= Static (réglage manuel)
  Un utilisateur a spécifié le port en tant que port de requête statique. L'équipement transmet des rapports IGMP uniquement aux ports sur lesquels il a précédemment reçu des requêtes IGMP – ainsi qu'aux ports de requête configurés de manière statique.
  Pour affecter cette valeur, exécutez les étapes suivantes :
  - ☐ Ouvrez la fenêtre *Wizard*.
  - ☐ Dans la boîte de dialogue *Configuration*, cochez la case *`Static`*.
- `P`= Learn by LLDP (réglage manuel)
  Un utilisateur a spécifié le port en tant que *`Learn by LLDP`*.
  Avec le Link Layer Discovery Protocol (LLDP), l'équipement détecte les équipements Schneider Electric connectés directement au port. L'équipement identifie les ports de requête détectés avec `A`.
  Pour affecter cette valeur, exécutez les étapes suivantes :
  - ☐ Ouvrez la fenêtre *Wizard*.
  - ☐ Dans la boîte de dialogue *Configuration*, cochez la case *`Learn by LLDP`*.
- `F`= Forward All (réglage manuel)
  Un utilisateur a spécifié le port de telle manière que l'équipement transmet chaque flux multicast reçu dans le VLAN sur ce port. Utilisez ce réglage à des fins de diagnostic, par exemple.
  Pour affecter cette valeur, exécutez les étapes suivantes :
  - ☐ Ouvrez la fenêtre *Wizard*.
  - ☐ Dans la boîte de dialogue *Configuration*, cochez la case *`Forward all`*.

Display categories

Améliore la clarté de l'affichage. La table met en surbrillance les cellules contenant la valeur spécifiée. Cela vous permet d'analyser et de trier la table en fonction de vos besoins.

- *Learned (L)*
  La table affiche les cellules qui contiennent la valeur `L` et éventuellement d'autres valeurs. Pour les cellules contenant d'autres valeurs que `L` uniquement, la table affiche l'icône « - ».
- *Static (S)*
  La table affiche les cellules qui contiennent la valeur `S` et éventuellement d'autres valeurs. Pour les cellules contenant d'autres valeurs que `S` uniquement, la table affiche l'icône « - ».
- *Automatic (A)*
  La table affiche les cellules qui contiennent la valeur `A` et éventuellement d'autres valeurs. Pour les cellules contenant d'autres valeurs que `A` uniquement, la table affiche l'icône « - ».
- *Learned by LLDP (P)*
  La table affiche les cellules qui contiennent la valeur `P` et éventuellement d'autres valeurs. Pour les cellules contenant d'autres valeurs que `P` uniquement, la table affiche l'icône « - ».
- *Forward all (F)*
  La table affiche les cellules qui contiennent la valeur `F` et éventuellement d'autres valeurs. Pour les cellules contenant d'autres valeurs que `F` uniquement, la table affiche l'icône « - ».

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Wizard*, qui vous permet de sélectionner et de configurer les ports.

[Selection VLAN/Port (Wizard)]

Dans la boîte de dialogue *Selection VLAN/Port*, vous affectez un VLAN-ID au port.

Dans la boîte de dialogue *Configuration*, vous spécifiez les réglages pour le port.

Après avoir fermé la fenêtre *Wizard*, cliquez sur le bouton  pour sauvegarder vos réglages.

[Selection VLAN/Port (Wizard) – Selection VLAN/Port]

VLAN ID

Sélectionnez l'ID du VLAN.

Valeurs possibles :

- `1..4042`

Port

Sélectionnez le port.

Valeurs possibles :

- `<Numéro de port>`

[Selection VLAN/Port (Wizard) – Configuration]

VLAN ID

Affiche l'ID du VLAN sélectionné.

Port

Affiche le numéro du port sélectionné.

Static

Spécifie le port en tant que port de requête statique dans les VLAN qui sont définis. L'équipement transmet les messages de rapport IGMP aux ports sur lesquels il reçoit des requêtes IGMP. Cela vous permet également de transmettre des messages de rapport IGMP à d'autres ports sélectionnés (activer) ou équipements Schneider Electric connectés (`Automatic` (Automatique)).

Learn by LLDP

Spécifie le port en tant que *`Learn by LLDP`*. Permet à l'équipement de détecter les équipements Schneider Electric directement connectés par LLDP et d'apprendre les ports liés en tant que ports de requête.

Forward all

Spécifie le port en tant que *`Forward all`*. Avec le réglage *`Forward all`*, l'équipement transmet sur ce port tous les paquets de données avec une adresse multicast dans le champ d'adresse cible.

5.4.4 IGMP Snooping Querier

[Switching > IGMP Snooping > Querier]

L'équipement vous permet d'envoyer un flux multicast uniquement sur les ports auxquels un destinataire multicast est connecté.

Pour déterminer à quels ports les destinataires multicast sont connectés, l'équipement envoie des paquets de données de requête aux ports à intervalles définissables. Lorsqu'un destinataire multicast est connecté, il rejoint le flux multicast en répondant à l'équipement avec un paquet de données de rapport.

Cette boîte de dialogue vous permet de configurer les réglages du Snooping Querier de manière globale et pour les VLAN qui sont définis.

Operation

Operation

Active/désactive la fonction IGMP Querier de manière globale dans l'équipement.

Valeurs possibles :

- *On*
- *Off* (réglage par défaut)

Configuration

Dans ce cadre, vous spécifiez les réglages de l'IGMP Snooping Querier pour les paquets de données de requête généraux.

Protocol version

Spécifie la version IGMP des paquets de données de requête généraux.

Valeurs possibles :

- 1
  IGMP v1
- 2 (réglage par défaut)
  IGMP v2
- 3
  IGMP v3

Query interval [s]

Spécifie la durée en secondes après laquelle l'équipement génère lui-même des paquets de données de requête généraux s'il a reçu des paquets de données de requête du routeur multicast.

Valeurs possibles :

- `1..1800` (réglage par défaut : `60`)

Expiry interval [s]

Spécifie la durée en secondes après laquelle un requérant actif repasse de l'état passif à l'état actif s'il n'a reçu aucun paquet de requête durant le temps spécifié ici.

Valeurs possibles :

- `60..300` (réglage par défaut : `125`)

Table

Dans la table, vous spécifiez les réglages du Snooping Querier pour les VLAN qui sont définis.

VLAN ID

Affiche l'ID du VLAN auquel l'entrée de la table s'applique.

Active

Active/désactive la fonction IGMP Snooping Querier pour ce VLAN.

Valeurs possibles :

- `case cochée`
  La fonction IGMP Snooping Querier est activée pour ce VLAN.
- `case non cochée` (réglage par défaut)
  La fonction IGMP Snooping Querier est désactivée pour ce VLAN.

Current state

Affiche si le Snooping Querier est activé pour ce VLAN.

Valeurs possibles :

- `case cochée`
  Le Snooping Querier est activé pour ce VLAN.
- `case non cochée`
  Le Snooping Querier est désactivé pour ce VLAN.

Address

Spécifie l'adresse IP que l'équipement ajoute en tant qu'adresse source dans les paquets de données de requête généraux générés. Vous utilisez l'adresse du routeur multicast.

Valeurs possibles :

- Adresse IPv4 valide (réglage par défaut : `0.0.0.0`)

Protocol version

Affiche la version de l'IGMP des paquets de données de requête généraux.

Valeurs possibles :

- `1`
  IGMP v1
- `2`
  IGMP v2
- `3`
  IGMP v3

Max. response time

Affiche la durée en secondes pendant laquelle les membres d'un groupe multicast répondent à un paquet de données de requête. Pour leur réponse, les membres indiquent une durée aléatoire comprise dans le temps de réponse. Cela évite ainsi que tous les membres du groupe multicast ne répondent simultanément à la requête.

Last querier address

Affiche l'adresse IP du routeur multicast à partir duquel la dernière requête IGMP reçue a été envoyée.

Last querier version

Affiche la version IGMP utilisée par le routeur multicast pour envoyer la dernière requête IGMP reçue dans ce VLAN.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.4.5 IGMP Snooping Multicasts

[Switching > IGMP Snooping > Multicasts]

L'équipement vous permet de spécifier comment il transmet les paquets de données avec des adresses multicast inconnues : soit il rejette ces paquets de données, soit il les envoie à tous les ports, soit il ne les transmet qu'aux ports ayant précédemment reçu des paquets de requête.

L'équipement vous permet également de transmettre les paquets de données avec des adresses multicast connues aux ports de requête.

Configuration

Unknown multicasts

Spécifie comment l'équipement transmet les paquets de données avec des adresses multicast inconnues.

Valeurs possibles :

- *discard*
  L'équipement rejette les paquets de données avec une adresse multicast MAC/IP inconnue.
- *flood* (réglage par défaut)
  L'équipement transfère à chaque port les paquets de données avec une adresse multicast MAC/IP inconnue.

Table

Dans la table, vous spécifiez les réglages des multicasts connus pour les VLAN qui sont définis.

VLAN ID

Affiche l'ID du VLAN auquel l'entrée de la table s'applique.

Known multicasts

Spécifie comment l'équipement transmet les paquets de données avec des adresses multicast connues.

Valeurs possibles :

- *send to query and registered ports*
  L'équipement transfère aux ports de requête et aux ports enregistrés les paquets de données avec une adresse multicast MAC/IP inconnue.
- *send to registered ports* (réglage par défaut)
  L'équipement transfère aux ports enregistrés les paquets de données avec une adresse multicast MAC/IP inconnue.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.5 Time-Sensitive Networking

[Switching > TSN]

Le menu contient les boîtes de dialogue suivantes :

- TSN Configuration
- TSN Gate Control List

5.5.1 TSN Configuration

[Switching > TSN > Configuration]

Dans cette boîte de dialogue, vous activez la fonction *TSN* et spécifiez les réglages temporels.

L'équipement prend en charge la mise en file d'attente sensible au temps définie dans IEEE 802.1 Qbv. Cette fonction *TSN* permet aux ports compatibles TSN de transmettre des paquets de données de chaque classe de trafic programmée par rapport à un cycle défini dans la Gate Control List. Le tag VLAN d'un paquet Ethernet ou, dans le cas d'un paquet non taggé, la priorité du port indique la priorité.

Cette fonction permet d'éviter la latence et la perte de congestion pour les flux de données réservés. La synchronisation précise des cycles et des états de porte à l'aide de la norme IEEE1588 (PTP) permet une communication sans congestion et à faible latence. La condition préalable est que tous les équipements du réseau prennent en charge la norme IEEE 802.1 Qbv.

Commentaire : Contrairement à l'interface de ligne de commande, vous validez les réglages immédiatement si vous cliquez sur le bouton .

Operation

Operation

Active/désactive la fonction *TSN* dans l'équipement.

Valeurs possibles :

- *On*
  La fonction *TSN* est activée globalement.
  L'équipement traite les link local frames sur les ports compatibles TSN avec la priorité de la classe de trafic6. Par conséquent, les link local frames entrent en concurrence avec d'autres paquets de données ayant une priorité identique ou supérieure lors du transfert. Cela affecte les types de frame suivants :
  - RSTP
  - LLDP
  - IEEE 802.1AS
  - PTP Peer Delay
- *Off* (réglage par défaut)
  La fonction *TSN* est désactivée globalement.
  Tant que la fonction *TSN* est activée sur un port, ce dernier utilise les portes ouvertes 0,1,2,3,4,5,6,7. Ce réglage est prédéfini par le fabricant.

Base time

Date
Time
[ns]

Spécifie l'heure à laquelle le cycle commence par rapport à l'heure UTC.

L'équipement convertit directement la valeur dans l'échelle de temps PTP sans tenir compte des secondes intercalaires.

Valeurs possibles :

- `MM/DD/YY`
  Mois/Jour/Année
  (en fonction des préférences linguistiques de votre navigateur Web)
- `hh:mm:ss`
  Heure:Minute:Seconde
- `0..999999999`
  Spécifie la dérive en nanosecondes.

Commentaire : Lorsque vous spécifiez l'heure de base dans le futur, le cycle commence autant de secondes plus tôt que ce qui est spécifié dans le champ *UTC offset [s]*. Voir la boîte de dialogue *Time > PTP > Boundary Clock > Global*.

Configuration

Cycle time [ns]

Spécifie la durée d'un cycle en nanosecondes.

Valeurs possibles :

- `50000..10000000` (réglage par défaut : `1000000`)
  50 µs .. 10 ms

Table

Port

Affiche le numéro de port.

Active

Active/désactive la fonction *TSN* sur le port.

Valeurs possibles :

- `case cochée`
  La fonction *TSN* est activée sur le port.
  Lorsque vous spécifiez l'heure de base dans le futur, le cycle commence à l'heure spécifiée dans le cadre *Base time*.
  La condition préalable est que la fonction *PTP* soit activée et que l'équipement soit synchronisé.
  Tant que la fonction *TSN* est activée globalement, le port utilise le cycle spécifié dans la boîte de dialogue *Switching > TSN > Gate Control List > Configured*.
- `case non cochée` (réglage par défaut)
  La fonction *TSN* est désactivée sur le port.
  Tant que la fonction *TSN* est activée globalement, le port utilise les portes ouvertes `0,1,2,3,4,5,6,7`.

Port state

Affiche l'état du cycle sur le port.

Valeurs possibles :

- *running*
  Le cycle est en cours.
  Le port utilise le cycle spécifié dans la boîte de dialogue *Switching > TSN > Gate Control List >* Configured.
- *waitForTimeSync*
  Le cycle n'a pas encore commencé.
  L'horloge de l'équipement n'est pas synchronisée.
  Vérifiez les réglages *PTP*.
- *pending*
  Le cycle n'a pas encore commencé.
  L'heure de base est spécifiée dans le futur.
- *disabled*
  Le cycle n'est pas en cours.
  La fonction *TSN* est désactivée sur le port.
  – Vérifiez le réglage dans le cadre *Operation*.
  – Vérifiez le réglage dans la colonne *Active*.
  Le port utilise les états de porte spécifiés dans la colonne *Default gate states*.
- *error*
  Le cycle n'est pas en cours.
  Une erreur a été détectée.

Time of last activation

Affiche la date et l'heure auxquelles les réglages de temps sont devenus actifs la dernière fois.

Cette valeur se rapporte à l'heure PTP.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.5.2 TSN Gate Control List

[Switching > TSN > Gate Control List]

Le menu contient les boîtes de dialogue suivantes :

- TSN Configured Gate Control List
- TSN Current Gate Control List

5.5.2.1 TSN Configured Gate Control List

[Switching > TSN > Gate Control List > Configured]

Dans cette boîte de dialogue, vous spécifiez les plages horaires du cycle pour les ports compatibles TSN. En ajoutant une entrée de table, vous spécifiez les portes ouvertes et la durée de la plage horaire.

Commentaire : Contrairement à l'interface de ligne de commande, vous validez les réglages immédiatement si vous cliquez sur le bouton ✓.

La boîte de dialogue contient les onglets suivants :

- Un onglet pour chaque port compatible TSN.
  Le nombre de ports compatibles TSN dépend de l'équipement.

[<Numéro de port>]

Configuration

Status

Affiche le modèle affecté à la Gate Control List.

Valeurs possibles :

- `-`
  Pas de modèle. Aucune entrée n'est affectée à la Gate Control List.
- *`default 2 time slots`*
  Modèle avec 3 entrées :
  - La première entrée est la classe de trafic `7`.
  - La seconde entrée est la classe de trafic `6` à `0`.
  - La troisième entrée est une bande de garde.
- *`default 3 time slots`*
  Modèle avec 5 entrées :
  - La première entrée est la classe de trafic `7`.
  - La deuxième entrée est une bande de garde.
  - La troisième entrée est la classe de trafic `6`.
  - La quatrième entrée est la classe de trafic `5` à `0`.
  - La cinquième entrée est une bande de garde.
- <`any other template name`>
  Le modèle a été affecté à l'aide de l'interface de ligne de commande.

Template

Ouvre la fenêtre *Template* pour affecter un modèle différent à la Gate Control List. Lorsque vous sélectionnez un modèle différent et que vous cliquez sur le bouton *Ok*, l'équipement remplace les entrées dans la table.

Dans la liste déroulante, vous sélectionnez l'un des modèles suivants :

- *default 2 time slots*
- *default 3 time slots*

L'équipement vous permet d'affecter des modèles supplémentaires à l'aide de l'interface de ligne de commande.

Delete

Supprime le modèle affecté à la Gate Control List. Plus aucune entrée n'est alors affectée à la Gate Control List.

Table

Index

Affiche le numéro d'index de l'entrée dans la Gate Control List, qui spécifie l'ordre chronologique des plages horaires.

Gate states

Spécifie les portes ouvertes dans le cas où la fonction *TSN* est activée sur le port.

- Les paquets de données dont la classe de trafic est affectée à une porte sélectionnée sont sélectionnés pour la transmission – état de la porte OPEN.
- Les paquets de données dont la classe de trafic est affectée à une porte non sélectionnée ne sont pas sélectionnés pour la transmission – état de la porte CLOSED.

Valeurs possibles :

- `-` (réglage par défaut)
  Aucune porte sélectionnée.
  L'équipement n'ouvre aucune porte sur le port pendant le traitement de la plage horaire. Désélectionnez chaque porte dans la liste déroulante.
- `0..7`
  L'équipement ouvre les portes sélectionnées sur le port pendant le traitement de la plage horaire. Sélectionnez une ou plusieurs portes dans la liste déroulante.
  Vous affectez les priorités VLAN à une classe de trafic dans la boîte de dialogue *Switching > QoS/Priority > 802.1D/p Mapping*.

Interval [ns]

Spécifie la durée de la plage horaire en nanosecondes.

Valeurs possibles :

▶ `1000..10000000`

Lorsque vous spécifiez la durée des plages horaires, tenez compte des conditions suivantes :

- Une plage horaire unique
  - Confirmez qu'une plage horaire est suffisamment longue pour que le port puisse transmettre le plus long paquet de données attendu.
  - Confirmez qu'une plage horaire est inférieure ou égale à la durée du cycle.
- La somme des plages horaires spécifiées
  - Nous recommandons que la somme des plages horaires soit égale à la durée du cycle.
  - Si la somme est supérieure à la durée du cycle, les plages qui se chevauchent sont rejetées et le cycle redémarre.
  - Si la somme est inférieure à la durée du cycle, l'intervalle de la dernière plage est prolongé pour s'insérer dans le cycle.

Commentaire : Les discordances entre les plages horaires spécifiées et la durée du cycle ne sont pas mises en surbrillance dans la boîte de dialogue *Switching > TSN > Gate Control List > Current*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.5.2.2 TSN Current Gate Control List

[Switching > TSN > Gate Control List > Current]

Dans cette boîte de dialogue, vous surveillez les réglages actuels du cycle pour les ports compatibles TSN. Chaque entrée de la table représente une plage horaire spécifiée.

Si l'heure de début du cycle (*Base time*) se situe dans le futur, les valeurs affichées sont différentes des valeurs spécifiées dans la boîte de dialogue *Switching > TSN > Gate Control List > Configured*.

Dans la boîte de dialogue *Switching > TSN > Configuration*, la colonne *Port state* indique si le cycle est en cours d'exécution sur un port.

La boîte de dialogue contient les onglets suivants :
- Un onglet pour chaque port compatible TSN.
  Le nombre de ports compatibles TSN dépend de l'équipement.

[<Numéro de port>]

Table

Index

Affiche le numéro d'index de l'entrée dans la Gate Control List, qui spécifie l'ordre chronologique des plages horaires.

Gate states

Affiche les portes ouvertes dans le cas où la fonction *TSN* est activée sur le port.

Interval [ns]

Affiche la durée de la plage horaire en nanosecondes.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.6 MRP-IEEE

[Switching > MRP-IEEE]

L'amendement IEEE 802.1ak apporté à la norme technique IEEE 802.1Q a introduit Multiple Registration Protocol (MRP) pour remplacer Generic Attribute Registration Protocol (GARP). L'IEEE a également modifié et remplacé les applications GARP, GARP Multicast Registration Protocol (GMRP) et GARP VLAN Registration Protocol (GVRP). Ces protocoles sont remplacés par Multiple MAC Registration Protocol (MMRP) et Multiple VLAN Registration Protocol (MVRP).

MRP-IEEE permet de confiner le trafic aux zones requises du LAN. Pour confiner le trafic, les applications MRP-IEEE distribuent des valeurs d'attribut aux équipements MRP-IEEE impliqués à travers un LAN en enregistrant et désenregistrant l'appartenance à un groupe multicast ainsi que les identifiants de VLAN.

L'enregistrement des participants au groupe vous permet de réserver des ressources pour le trafic propre à un LAN. La définition des besoins en ressources régule le niveau du trafic, permettant aux équipements de déterminer les ressources requises et d'assurer une gestion dynamique des ressources attribuées.

Le menu contient les boîtes de dialogue suivantes :
- MRP-IEEE Configuration
- MRP-IEEE Multiple MAC Registration Protocol
- MRP-IEEE Multiple VLAN Registration Protocol

5.6.1 MRP-IEEE Configuration

[Switching > MRP-IEEE > Configuration]

Cette boîte de dialogue vous permet de définir les différents temporisateurs MRP. Grâce à la gestion du lien entre les différentes valeurs de temporisation, le protocole fonctionne efficacement et les désenregistrements et ré-enregistrements inutiles d'attributs sont moins susceptibles de se produire. Les valeurs de temporisation par défaut assurent une gestion efficace de ces liens.

Si vous reconfigurez les temporisateurs, gérez les liens suivants :
- Pour permettre un ré-enregistrement après un événement Leave ou LeaveAll, même en cas de perte de message, spécifiez la valeur LeaveTime sur : `≥ (2x JoinTime) + 60`.
- Pour minimiser le volume du trafic à réintégrer généré suite à un événement LeaveAll, spécifiez une valeur du temporisateur LeaveAll supérieure à la valeur du temporisateur LeaveTime.

Table

Port

Affiche le numéro de port.

Join time [1/100s]

Spécifie le temporisateur Join, qui contrôle l'intervalle entre les opportunités de transmission appliqué à la machine à état Applicant.

Valeurs possibles :
- `10..100` (réglage par défaut : `20`)

Leave time [1/100s]

Spécifie le temporisateur Leave, qui contrôle le délai pendant lequel la machine à état Registrar attend à l'état Leave (LV) avant de passer à l'état Empty (MT).

Valeurs possibles :
- `20..600` (réglage par défaut : `60`)

Leave all time [1/100s]

Spécifie le temporisateur LeaveAll, qui contrôle la fréquence à laquelle la machine à état LeaveAll génère des PDU LeaveAll.

Valeurs possibles :
- `200..6000` (réglage par défaut : `1000`)

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.6.2 MRP-IEEE Multiple MAC Registration Protocol

[Switching > MRP-IEEE > MMRP]

Multiple MAC Registration Protocol (MMRP) permet aux équipements terminaux et aux commutateurs MAC d'enregistrer et de désenregistrer l'appartenance à un groupe ainsi que les informations d'adresses MAC individuelles avec des interrupteurs situés dans le même LAN. Les commutateurs au sein du LAN répartissent les informations sur des interrupteurs prenant en charge des services de filtrage étendus. À l'aide des informations d'adresses MAC, MMRP vous permet de confiner le trafic multicast aux zones requises d'un réseau de couche 2.

Pour comprendre comment MMRP fonctionne, prenons le cas d'une caméra de sécurité montée sur un mât pour surveiller un bâtiment. Cette caméra envoie des paquets multicast sur un LAN. Vous avez 2 équipements terminaux installés pour la surveillance en des endroits distincts. Vous enregistrez les adresses MAC de la caméra et des 2 équipements terminaux dans le même groupe multicast. Vous spécifiez ensuite les réglages MMRP sur les ports pour envoyer les paquets du groupe multicast aux 2 équipements terminaux.

La boîte de dialogue contient les onglets suivants :
- [Configuration]
- [Service requirement]
- [Statistics]

[Configuration]

Dans cet onglet, vous sélectionnez les participants du port MMRP activé et vous réglez l'équipement pour qu'il transmette des événements périodiques. La boîte de dialogue vous permet également d'activer la diffusion d'adresses MAC enregistrées sur le VLAN.

Une machine à état périodique existe pour chaque port et transmet régulièrement des événements périodiques aux machines à état Applicant associées aux ports activés. Les événements périodiques contiennent des informations indiquant l'état des équipements associés au port activé.

Operation

Operation

Active/désactive la fonction *MMRP* globale dans l'équipement. L'équipement participe aux échanges de messages MMRP.

Valeurs possibles :
- *On*
  L'équipement est un participant normal aux échanges de messages MMRP.
- *Off* (réglage par défaut)
  L'équipement ignore les messages MMRP.

Configuration

Periodic state machine

Active/désactive la machine à état périodique global dans l'équipement.

Valeurs possibles :

- *On*
  L'option *Operation* MMRP étant activé globalement, l'équipement transmet, à intervalles d'une seconde, des messages MMRP aux ports participant à MMRP.
- *Off* (réglage par défaut)
  Désactive la machine à état périodique dans l'équipement.

Table

Port

Affiche le numéro de port.

Active

Active/désactive la participation du port à MMRP.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  MMRP étant activé globalement et sur ce port, l'équipement envoie et reçoit des messages MMRP sur ce port.
- `case non cochée`
  Désactive la participation du port à MMRP.

Restricted group registration

Active/désactive la restriction d'enregistrement d'adresse MAC dynamique par MMRP sur le port.

Valeurs possibles :

- `case cochée`
  Si cette option est cochée et qu'une entrée de filtre statique existe pour l'adresse MAC sur le VLAN concerné, l'équipement enregistre les attributs d'adresse MAC de manière dynamique.
- `case non cochée` (réglage par défaut)
  Active/désactive la restriction d'enregistrement d'adresse MAC dynamique par MMRP sur le port.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Service requirement]

Cet onglet contient les paramètres de transfert pour chaque VLAN activé et spécifie les ports sur lesquels le transfert multicast s'applique. L'équipement vous permet de définir de manière statique les ports VLAN sur *Forward all* ou Forbidden. Vous définissez l'exigence de service MMRP Forbidden de manière statique uniquement via l'interface utilisateur graphique ou l'interface de ligne de commande.

Un port ne peut être défini que sur ForwardAll ou Forbidden.

Table

VLAN ID

Affiche l'ID du VLAN.

<Numéro de port>

Spécifie le traitement de l'exigence de service pour le port.

Valeurs possibles :

- FA
  Spécifie le réglage du trafic ForwardAll sur le port. L'équipement transfère le trafic destiné aux adresses MAC multicast enregistrées MMRP sur le VLAN. L'équipement transfère le trafic aux ports définis de manière dynamique par MMRP ou aux ports définis de manière statique par l'administrateur en tant que ports ForwardAll.
- F
  Spécifie le réglage du trafic Forbidden sur le port. L'équipement bloque les exigences de service ForwardAll dynamiques de MMRP. Les requêtes ForwardAll étant bloquées sur ce port dans ce VLAN, l'équipement bloque le trafic destiné aux adresses MAC multicast enregistrées MMRP sur ce port. De plus, l'équipement bloque la requête de service MMRP visant à modifier cette valeur sur ce port.
- \- (réglage par défaut)
  Désactive les fonctions de transfert sur ce port.
- Learned
  Affiche les valeurs définies par les requêtes de service MMRP.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Statistics]

Les équipements sur un LAN échangent des Multiple MAC Registration Protocol Data Units (MMRPDU) pour gérer les états des équipements sur un port MMRP activé. Cet onglet vous permet de surveiller les statistiques de trafic MMRP pour chaque port.

Information

Transmitted MMRP PDU

Affiche le nombre de MMRPDU transmises dans l'équipement.

Received MMRP PDU

Affiche le nombre de MMRPDU reçues dans l'équipement.

Received bad header PDU

Affiche le nombre de MMRPDU reçues avec un en-tête incorrect dans l'équipement.

Received bad format PDU

Affiche le nombre de MMRPDU avec un champ de données incorrect qui n'ont pas été transmises dans l'équipement.

Transmission failed

Affiche le nombre de MMRPDU non transmises dans l'équipement.

Table

Port

Affiche le numéro de port.

Transmitted MMRP PDU

Affiche le nombre de MMRPDU transmises sur le port.

Received MMRP PDU

Affiche le nombre de MMRPDU reçues sur le port.

Received bad header PDU

Affiche le nombre de MMRPDU avec un en-tête incorrect qui n'ont pas été reçues sur le port.

Received bad format PDU

Affiche le nombre de MMRPDU avec un champ de données incorrect qui n'ont pas été transmises sur le port.

Transmission failed

Affiche le nombre de MMRPDU non transmises sur le port.

Last received MAC address

Affiche la dernière adresse MAC de laquelle le port a reçu des MMRPDU.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Réinitialise les compteurs statistiques du port et les valeurs dans la colonne *Last received MAC address*.

5.6.3 MRP-IEEE Multiple VLAN Registration Protocol

[Switching > MRP-IEEE > MVRP]

Multiple VLAN Registration Protocol (MVRP) constitue un mécanisme qui vous permet de distribuer les informations de VLAN et de configurer les VLAN de manière dynamique. Par exemple, lorsque vous configurez un VLAN sur un port MVRP activé, l'équipement distribue les informations du VLAN aux autres équipements compatibles MVRP. À l'aide des informations reçues, un équipement compatible MVRP crée de manière dynamique les trunks de VLAN sur d'autres équipements compatibles MVRP selon les besoins.

La boîte de dialogue contient les onglets suivants :
- [Configuration]
- [Statistics]

[Configuration]

Dans cet onglet, vous sélectionnez les participants du port MVRP activé et vous réglez l'équipement pour qu'il transmette des événements périodiques.

Une machine à état périodique existe pour chaque port et transmet régulièrement des événements périodiques aux machines à état Applicant associées aux ports activés. Les événements périodiques contiennent des informations indiquant l'état des VLAN associés au port activé. À l'aide des événements périodiques, les commutateurs compatibles MVRP gèrent les VLAN de manière dynamique.

Operation

Operation

Active/désactive l'Applicant Administrative Control global qui spécifie si la machine à état Applicant participe à l'échange de messages MMRP.

Valeurs possibles :
- *On*
  Participant normal. La machine à état Applicant participe à l'échange de messages MMRP.
- *Off* (réglage par défaut)
  Non-participant. La machine à état Applicant ignore les messages MMRP.

Configuration

Periodic state machine

Active/désactive la machine à état périodique dans l'équipement.

Valeurs possibles :

- `On`
  La machine à état périodique est activée.
  L'option *Operation* MVRP étant activée de manière globale, l'équipement transmet, à intervalles de 1 seconde, des événements périodiques MVRP sur les ports participant à MVRP.
- `Off` (réglage par défaut)
  La machine à état périodique est désactivée.
  Désactive la machine à état périodique dans l'équipement.

Table

Port

Affiche le numéro de port.

Active

Active/désactive la participation du port à MVRP.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  MVRP étant activé de manière globale et sur ce port, l'équipement distribue les informations d'appartenance au VLAN aux équipements compatibles MVRP connectés à ce port.
- `case non cochée`
  Désactive la participation du port à MVRP.

Restricted VLAN registration

Active/désactive la fonction *Restricted VLAN registration* sur ce port.

Valeurs possibles :

- `case cochée`
  Si cette option est cochée et qu'une entrée d'enregistrement de VLAN statique existe, l'équipement vous permet de créer un VLAN dynamique pour cette entrée.
- `case non cochée` (réglage par défaut)
  Désactive la fonction *Restricted VLAN registration* sur ce port.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Statistics]

Les équipements sur un LAN échangent des Multiple VLAN Registration Protocol Data Units (MVRPDU) pour gérer les états des VLAN sur des ports activés. Cet onglet vous permet de surveiller le trafic MVRP.

Information

Transmitted MVRP PDU

Affiche le nombre de MVRPDU transmises dans l'équipement.

Received MVRP PDU

Affiche le nombre de MVRPDU reçues dans l'équipement.

Received bad header PDU

Affiche le nombre de MVRPDU reçues avec un en-tête incorrect dans l'équipement.

Received bad format PDU

Affiche le nombre de MVRPDU avec un champ de données incorrect bloquées par l'équipement.

Transmission failed

Affiche le nombre de défaillances détectées tout en ajoutant un message dans la file d'attente MVRP.

Message queue failures

Affiche le nombre de MVRPDU bloquées par l'équipement.

Table

Port

Affiche le numéro de port.

Transmitted MVRP PDU

Affiche le nombre de MVRPDU transmises sur le port.

Received MVRP PDU

Affiche le nombre de MVRPDU reçues sur le port.

Received bad header PDU

Affiche le nombre de MVRPDU avec un en-tête incorrect reçues par l'équipement sur le port.

Received bad format PDU

Affiche le nombre de MVRPDU avec un champ de données incorrect bloquées par l'équipement sur le port.

Transmission failed

Affiche le nombre de MVRPDU bloquées par l'équipement sur le port.

Registrations failed

Affiche le nombre de tentatives d'enregistrement ayant échoué sur le port.

Last received MAC address

Affiche la dernière adresse MAC de laquelle le port a reçu des MMRPDU.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Réinitialise les compteurs statistiques du port et les valeurs dans la colonne *Last received MAC address*.

5.7 GARP

[Switching > GARP]

Generic Attribute Registration Protocol (GARP) est défini par l'IEEE pour fournir un cadre générique afin que les commutateurs puissent enregistrer et désenregistrer des valeurs d'attribut, comme des identifiants de VLAN et l'appartenance à un groupe multicast.

Lorsqu'un attribut est enregistré ou désenregistré conformément à GARP pour un participant, ce dernier est modifié selon des règles spécifiques. Les participants sont un ensemble d'équipements terminaux et d'équipements réseau accessibles. L'ensemble défini de participants à un moment quelconque, ainsi que leurs attributs, constituent l'arbre d'accessibilité pour le sous-ensemble de la topologie de 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.

Commentaire : Avant d'activer la fonction *GMRP*, vérifiez que la fonction *MMRP* est désactivée.

Le menu contient les boîtes de dialogue suivantes :
- GMRP
- GVRP

5.7.1 GMRP

[Switching > GARP > GMRP]

GARP Multicast Registration Protocol (GMRP) est un Generic Attribute Registration Protocol (GARP) constituant un mécanisme qui permet aux équipements de réseau et équipements terminaux d'enregistrer de manière dynamique l'appartenance à un groupe. Les équipements enregistrent les informations d'appartenance à un groupe avec les équipements liés au même segment de LAN. GARP permet également aux équipement de distribuer les informations aux équipements de réseau qui prennent en charge les services de filtrage étendus.

GMRP et GARP sont des protocoles industriels standard définis par la norme technique IEEE 802.1P.

Operation

Operation

Active/désactive la fonction *GMRP* globale dans l'équipement. L'équipement participe aux échanges de messages GMRP.

Valeurs possibles :

- *On*
  GMRP est activé.
- *Off* (réglage par défaut)
  L'équipement ignore les messages GMRP.

Multicasts

Unknown multicasts

Active/désactive soit le transfert, soit le rejet des données multicast inconnues.

Valeurs possibles :

- *discard*
  L'équipement rejette les données multicast inconnues.
- *flood* (réglage par défaut)
  L'équipement transfère les données multicast inconnues à tous les ports.

Table

Port

Affiche le numéro de port.

GMRP active

Active/désactive la participation du port à *GMRP*.

La condition préalable est que la fonction *GMRP* soit activée globalement.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La participation du port à *GMRP* est activée.
- `case non cochée`
  La participation du port à *GMRP* est désactivée.

Service requirement

Spécifie les ports sur lesquels le transfert multicast s'applique.

Valeurs possibles :

- *`Forward all unregistered groups`* (réglage par défaut)
  L'équipement transfère les données destinées aux adresses MAC multicast enregistrées *GMRP* sur le VLAN. L'équipement transfère les données aux groupes non enregistrés.
- *`Forward all groups`*
  L'équipement transfère les données destinées à tous les groupes, qu'ils soient enregistrés ou non.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.7.2 GVRP

[Switching > GARP > GVRP]

GARP VLAN Registration Protocol (GVRP) ou Generic VLAN Registration Protocol est un protocole qui facilite le contrôle des réseaux locaux virtuels (VLAN) au sein d'un réseau plus vaste. GVRP est un protocole réseau de couche 2 utilisé pour configurer automatiquement les équipements dans un réseau VLAN.

GVRP est une application GARP qui permet un élagage VLAN compatible IEEE 802.1Q et qui crée un VLAN dynamique sur les ports de trunk 802.1Q. Avec GVRP, l'équipement échange des informations de configuration VLAN avec d'autres équipements GVRP. Ainsi, l'équipement réduit le broadcast inutile et le trafic unicast inconnu. L'échange des informations de configuration VLAN vous permet également de créer de manière dynamique et de gérer des VLAN connectés par le biais de ports de trunk 802.1Q.

Operation

Operation

Active/désactive la fonction *GVRP* de manière globale dans l'équipement. L'équipement participe aux échanges de messages *GVRP*. Si la fonction est désactivée, l'équipement ignore les messages *GVRP*.

Valeurs possibles :

- *On*
  La fonction *GVRP* est activée.
- *Off* (réglage par défaut)
  La fonction *GVRP* est désactivée.

Table

Port

Affiche le numéro de port.

GVRP active

Active/désactive la participation du port à *GVRP*.

La condition préalable est que la fonction *GVRP* soit activée globalement.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La participation du port à *GVRP* est activée.
- `case non cochée`
  La participation du port à *GVRP* est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.8 QoS/Priority

[Switching > QoS/Priority]

Les réseaux de communication transmettent simultanément plusieurs applications présentant différentes exigences en termes de disponibilité, de bande passante et de périodes de latence.

QoS (Quality of Service) est une procédure définie dans IEEE 802.1D. Elle est utilisée pour distribuer les ressources dans le réseau. Vous pouvez ainsi fournir une bande passante minimale aux applications requises. La condition préalable est que les équipements terminaux et les équipements dans le réseau prennent en charge la transmission priorisée de données. Les paquets de données avec une priorité élevée sont transmis en priorité par les équipements dans le réseau. Vous transférez les paquets de données avec une priorité moindre lorsqu'il n'y a aucun paquet de données avec une priorité supérieure à transmettre.

L'équipement dispose des options de réglage suivantes :
- Vous spécifiez comment l'équipement évalue les informations de QoS/priorisation pour les paquets de données entrants.
- Pour les paquets sortants, vous spécifiez quelles informations de QoS/priorisation l'équipement inscrit dans les paquets de données (par exemple, priorité pour la gestion des paquets, priorité pour les ports).

Commentaire : Si vous utilisez les fonctions dans ce menu, désactivez le contrôle de flux. Le contrôle de flux est désactivé si, dans la boîte de dialogue *Switching > Global* cadre *Configuration*, la case *Flow control* est `décochée`.

Le menu contient les boîtes de dialogue suivantes :
- QoS/Priority Global
- QoS/Priority Port Configuration
- 802.1D/p Mapping
- IP DSCP Mapping
- Queue Management

5.8.1 QoS/Priority Global

[Switching > QoS/Priority > Global]

L'équipement vous permet de gérer l'accès à l'administration de l'équipement, même dans des situations d'utilisation intensive. Dans cette boîte de dialogue, vous spécifiez les réglages de QoS/priorité requis.

Configuration

VLAN priority for management packets

Spécifie la priorité de VLAN pour l'envoi de paquets de données de gestion. En fonction de la priorité de VLAN, l'équipement affecte les paquets de données à une classe de trafic spécifique, et ainsi à une file d'attente priorisée spécifique du port.

Valeurs possibles :

- `0..7` (réglage par défaut : `0`)

Dans la boîte de dialogue *Switching > QoS/Priority > 802.1D/p Mapping*, vous affectez une classe de trafic à chaque priorité de VLAN.

IP DSCP value for management packets

Spécifie la valeur IP DSCP pour l'envoi de paquets de données de gestion. En fonction de la valeur IP DSCP, l'équipement affecte les paquets de données à une classe de trafic spécifique, et ainsi à une file d'attente priorisée spécifique du port.

Valeurs possibles :

- *`0 (be/cs0)..63`* (réglage par défaut : *`0 (be/cs0)`*)

Certaines valeurs dans la liste ont aussi un mot-clé DSCP, par exemple *`0 (be/cs0)`*, *`10 (af11)`* et *`46 (ef)`*. Ces valeurs sont compatibles avec le modèle de priorisation.

Dans la boîte de dialogue *Switching > QoS/Priority > IP DSCP Mapping*, vous affectez une classe de trafic à chaque valeur IP DSCP.

Queues per port

Affiche le nombre de files d'attente priorisées par port.

Affiche le nombre de files d'attente 8 priorisées par port. Vous affectez chaque file d'attente priorisée à une classe de trafic spécifique (classe de trafic conformément à IEEE 802.1D).

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.8.2 QoS/Priority Port Configuration

[Switching > QoS/Priority > Port Configuration]

Dans cette boîte de dialogue, vous spécifiez pour chaque port comment l'équipement traite les paquets de données reçus sur la base de leurs informations de QoS/priorité.

Table

Port

Affiche le numéro de port.

Port priority

Spécifie quelles informations de priorité de VLAN l'équipement inscrit dans un paquet de données si ce dernier ne contient aucune information de priorité. Ensuite, l'équipement transmet le paquet de données en fonction de la valeur spécifiée dans la colonne *Trust mode*.

Valeurs possibles :

- `0..7` (réglage par défaut : `0`)

Trust mode

Spécifie comment l'équipement traite un paquet de données reçu si ce dernier contient des informations de QoS/priorité.

Valeurs possibles :

- *untrusted*
  L'équipement transmet le paquet de données conformément à la priorité spécifiée dans la colonne *Port priority*. L'équipement ignore les informations de priorité contenues dans le paquet de données.
  Dans la boîte de dialogue *Switching > QoS/Priority > 802.1D/p Mapping*, vous affectez une classe de trafic à chaque priorité de VLAN.
- *trustDot1p* (réglage par défaut)
  L'équipement transmet le paquet de données conformément aux informations de priorité dans le tag de VLAN.
  Dans la boîte de dialogue *Switching > QoS/Priority > 802.1D/p Mapping*, vous affectez une classe de trafic à chaque priorité de VLAN.
- *trustIpDscp*
  - Si le paquet de données est un paquet IP :
    L'équipement transmet le paquet de données conformément à la valeur IP DSCP contenue dans le paquet de données.
    Dans la boîte de dialogue *Switching > QoS/Priority > IP DSCP Mapping*, vous affectez une classe de trafic à chaque valeur IP DSCP.
  - Si le paquet de données n'est pas un paquet IP :
    L'équipement transmet le paquet de données conformément à la priorité spécifiée dans la colonne *Port priority*.
    Dans la boîte de dialogue *Switching > QoS/Priority > 802.1D/p Mapping*, vous affectez une classe de trafic à chaque priorité de VLAN.

Untrusted traffic class

Affiche la classe de trafic affectée à l'information de priorité de VLAN spécifiée dans la colonne *Port priority*. Dans la boîte de dialogue *Switching > QoS/Priority > 802.1D/p Mapping*, vous affectez une classe de trafic à chaque priorité de VLAN.

Valeurs possibles :

- `0..7`

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.8.3 802.1D/p Mapping

[Switching > QoS/Priority > 802.1D/p Mapping]

L'équipement transmet des paquets de données avec un tag de VLAN conformément aux informations de QoS/priorité contenues présentant une priorité supérieure ou inférieure.

Dans cette boîte de dialogue, vous affectez une classe de trafic à chaque priorité de VLAN. Vous affectez les classes de trafic aux files d'attente priorisées des ports.

Table

VLAN priority

Affiche la priorité de VLAN.

Traffic class

Spécifie la classe de trafic affectée à la priorité de VLAN.

Valeurs possibles :

- `0..7`
  `0` affectée à la file d'attente avec la priorité la plus basse.
  `7` affectée à la file d'attente avec la priorité la plus haute.

Commentaire : Les mécanismes de redondance utilisent notamment la classe de trafic la plus élevée. Aussi, sélectionnez une autre classe de trafic pour les données d'application.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Affectation par défaut de la priorité de VLAN aux classes de trafic

Priorité de VLAN	Classe de trafic	Description du contenu conformément à IEEE 802.1D
`0`	2	`Best Effort` Données normales sans priorisation
`1`	0	`Background` Données non sensibles au temps et services en arrière-plan
`2`	1	`Standard` Données normales
`3`	3	`Excellent Effort` Données cruciales
`4`	4	`Controlled Load` Données sensibles au temps avec une priorité élevée

Priorité de VLAN	Classe de trafic	Description du contenu conformément à IEEE 802.1D
5	5	Video Transmission vidéo avec délais et gigue < 100 ms
6	6	Voice Transmission vocale avec délais et gigue < 10 ms
7	7	Network Control Données pour la gestion du réseau et les mécanismes de redondance

5.8.4 IP DSCP Mapping

[Switching > QoS/Priority > IP DSCP Mapping]

L'équipement transmet les paquets de données IP conformément à la valeur DSCP contenue dans le paquet de données avec une priorité supérieure ou inférieure.

Dans cette boîte de dialogue, vous affectez une classe de trafic à chaque valeur DSCP. Vous affectez les classes de trafic aux files d'attente priorisées des ports.

Table

DSCP value

Affiche la valeur DSCP.

Traffic class

Spécifie la classe de trafic affectée à la valeur DSCP.

Valeurs possibles :

- `0..7`
  `0` affectée à la file d'attente avec la priorité la plus basse.
  `7` affectée à la file d'attente avec la priorité la plus haute.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Affectation par défaut des valeurs DSCP aux classes de trafic

Valeur DSCP	Nom DSCP	Classe de trafic
0	Best Effort /CS0	2
1-7		2
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	1
17,19,21,23		1
18,20,22	AF21,AF22,AF23	1
24	CS3	3
25,27,29,31		3
26,28,30	AF31,AF32,AF33	3
32	CS4	4
33,35,37,39		4
34,36,38	AF41,AF42,AF43	4

Valeur DSCP	Nom DSCP	Classe de trafic
40	CS5	5
41,42,43,44,45,47		5
46	EF	5
48	CS6	6
49-55		6
56	CS7	7
57-63		7

5.8.5 Queue Management

[Switching > QoS/Priority > Queue Management]

Cette boîte de dialogue vous permet d'activer et de désactiver la fonction *Strict priority* pour les classes de trafic. Lorsque vous désactivez la fonction *Strict priority*, l'équipement traite les files d'attente priorisées des ports selon le principe du « Weighted Fair Queuing ».

Vous pouvez également affecter une bande passante minimum à chaque classe de trafic utilisée par l'équipement pour traiter les files d'attente priorisées avec « Weighted Fair Queuing ».

Table

Traffic class

Affiche la classe de trafic.

Strict priority

Active/désactive le traitement de la file d'attente priorisée *Strict priority* du port pour cette classe de trafic.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  Le traitement de la file d'attente priorisée *Strict priority* du port est activé.
  - Le port transmet uniquement les paquets de données qui se trouvent dans la file d'attente avec la priorité la plus élevée. Lorsque cette file d'attente priorisée est vide, le port transmet les paquets de données dans la file d'attente priorisée avec la priorité immédiatement inférieure.
  - Le port transmet les paquets de données avec une classe de trafic inférieure une fois que les files d'attente avec une priorité supérieure sont vides. Dans les situations défavorables, le port n'envoie pas ces paquets de données.
  - Lorsque vous sélectionnez ce réglage pour une classe de trafic, l'équipement active également la fonction pour les classes de trafic avec une priorité supérieure.
  - Utilisez ce réglage pour des applications comme la VoIP ou la vidéo, qui requièrent le moins de retard possible.
- `case non cochée`
  Le traitement de la file d'attente priorisée avec *Strict priority* du port est désactivé. L'équipement utilise «Weighted Fair Queuing »/« Weighted Round Robin » (WRR) pour traiter la file d'attente priorisée du port.
  - L'équipement affecte une bande passante minimum à chaque classe de trafic.
  - Même en cas de charge élevée du réseau, le port transmet les paquets de données avec une classe de trafic basse.
  - Lorsque vous sélectionnez ce réglage pour une classe de trafic, l'équipement désactive également la fonction pour les classes de trafic avec une priorité inférieure.

Min. bandwidth [%]

Spécifie la bande passante minimum pour cette classe de trafic lorsque l'équipement traite les files d'attente priorisées des ports avec « Weighted Fair Queuing ».

Valeurs possibles :

- `0..100` (réglage par défaut : `0` = l'équipement ne réserve aucune bande passante pour cette classe de trafic)

La valeur spécifiée en pourcentage se rapporte à la bande passante disponible sur le port. Lorsque vous désactivez la fonction *Strict priority* pour chaque classe de trafic, la bande passante maximum est disponible sur le port pour « Weighted Fair Queuing ».

Le total maximum des bandes passantes affectées est de 100 %.

Max. bandwidth [%]

Indique le débit de régulation avec lequel une classe de trafic transmet les paquets de données (régulation du débit des files d'attente).

Valeurs possibles :

- `0` (réglage par défaut)
  L'équipement ne réserve aucune bande passante pour cette classe de trafic.
- `1..100`
  L'équipement réserve la bande passante spécifiée pour cette classe de trafic. La valeur spécifiée en pourcentage se rapporte à la bande passante maximale disponible sur ce port.

Par exemple, l'utilisation de la régulation du débit des files d'attente vous permet de limiter le débit d'une file d'attente de haute priorité stricte. La limitation du débit d'une file d'attente de haute priorité stricte permet également à l'équipement de traiter les files d'attente de faible priorité. Pour utiliser la régulation du débit de file d'attente, définissez la bande passante maximale pour une file d'attente particulière.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.9 VLAN

[Switching > VLAN]

Avec un VLAN (réseau local virtuel), vous distribuez le trafic de données dans le réseau physique entre les sous-réseaux logiques. Cela vous offre les avantages suivants :

- Flexibilité élevée
  - Avec un VLAN, vous distribuez le trafic de données entre des réseaux logiques de l'infrastructure existante. Sans VLAN, il serait nécessaire d'avoir des équipements supplémentaires et un câblage complexe.
  - Avec un VLAN, vous spécifiez les segments de réseau indépendamment de l'emplacement des équipements terminaux individuels.

- Débit amélioré
  - Dans les VLAN, les paquets de données peuvent être transférés par priorité.
    Lorsque la priorité est élevée, l'équipement transfère les données d'un VLAN de manière préférentielle, par exemple pour des applications sensibles au temps comme les appels téléphoniques VoIP.
  - Lorsque les paquets de données et les broadcasts sont distribués dans de petits segments de réseaux et non dans le réseau entier, la charge du réseau est considérablement réduite.
- Sécurité accrue
  La distribution du trafic de données sur des réseaux individuels logiques rend les accès indésirables plus difficiles et renforce le système contre les attaques de type MAC Flooding ou MAC Spoofing.

L'équipement prend en charge les VLAN « taggés » basés sur les paquets conformément à la norme technique IEEE 802.1Q. Le taggage VLAN dans le paquet de données indique le VLAN auquel le paquet de données appartient.

L'équipement transmet les paquets de données taggés d'un VLAN uniquement aux ports qui sont affectés au même VLAN. La charge du réseau est ainsi réduite.

L'équipement apprend les adresses MAC pour chaque VLAN séparément (apprentissage VLAN indépendant).

L'équipement priorise le flux de données reçus selon la séquence suivante :
- Voice VLAN
- VLAN basé sur des ports

Le menu contient les boîtes de dialogue suivantes :
- VLAN Global
- VLAN Configuration
- VLAN Port
- VLAN Voice

5.9.1 VLAN Global

[Switching > VLAN > Global]

Cette boîte de dialogue vous permet de visualiser les paramètres de VLAN généraux pour l'équipement.

Configuration

Max. VLAN ID

ID le plus élevé affectable à un VLAN.

Voir la boîte de dialogue *Switching > VLAN > Configuration*.

VLANs (max.)

Affiche le nombre maximum possible de VLAN.

Voir la boîte de dialogue *Switching > VLAN > Configuration*.

VLANs

Nombre de VLAN actuellement configurés dans l'équipement.

Voir la boîte de dialogue *Switching > VLAN > Configuration*.

Le VLAN-ID 1 est toujours présent dans l'équipement.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Clear...

Rétablit les réglages VLAN par défaut de l'équipement.

Notez que vous perdrez la connexion à l'équipement si vous modifiez le VLAN-ID pour l'administration de l'équipement dans la boîte de dialogue *Basic Settings > Network*.

5.9.2 VLAN Configuration

[Switching > VLAN > Configuration]

Dans cette boîte de dialogue, vous gérez les VLAN. Pour définir un VLAN, créez une nouvelle ligne dans la table. Spécifiez ensuite pour chaque port s'il transmet les paquets de données de ce VLAN et si les paquets de données contiennent un tag de VLAN.

Vous distinguez les VLAN suivants :

- L'utilisateur définit des VLAN statiques.
- L'équipement définit automatiquement des VLAN dynamiques et les supprime si les conditions requises cessent de s'appliquer.
  Pour les fonctions suivantes, l'équipement crée des VLAN dynamiques :
  - *MRP* : si vous affectez aux ports de l'anneau un VLAN inexistant, l'équipement crée ce VLAN.
  - *MVRP* : l'équipement crée un VLAN sur la base des messages des équipements voisins.

Table

VLAN ID

ID du VLAN.

L'équipement prend en charge jusqu'à 128 VLAN définis simultanément.

Valeurs possibles :

- `1..4042`

Status

Affiche comment le VLAN est défini.

Valeurs possibles :

- *`other`*
  VLAN `1`
  ou
  VLAN défini à l'aide de la fonction *802.1X Port Authentication*. Voir la boîte de dialogue *Network Security > 802.1X Port Authentication*.
- *`permanent`*
  VLAN défini par l'utilisateur.
  ou
  VLAN défini à l'aide de la fonction *MRP*. Voir la boîte de dialogue *Switching > L2-Redundancy > MRP*.
  Si vous sauvegardez les modifications dans la mémoire non volatile, les VLAN avec ce réglage restent définis après un redémarrage.
- *`dynamicMvrp`*
  VLAN défini à l'aide de la fonction *MVRP*. Voir la boîte de dialogue *Switching > MRP-IEEE > MVRP*.
  Les VLAN avec ce réglage sont protégés en écriture. L'équipement supprime un VLAN de la table dès que le dernier port quitte le VLAN.

Creation time

Affiche l'heure de création du VLAN.

Ce champ affiche l'horodatage pour le temps de fonctionnement (disponibilité du système).

Name

Spécifie le nom du VLAN.

Valeurs possibles :

- Chaîne de 1..32 caractères ASCII alphanumériques

<Numéro de port>

Spécifie si le port concerné transmet les paquets de données du VLAN et si les paquets de données contiennent un tag de VLAN.

Valeurs possibles :

- `-` (réglage par défaut)
  Le port n'est pas membre du VLAN et ne transmet pas les paquets de données du VLAN.
- `T` = Tagged
  Le port est un membre du VLAN et transmet les paquets de données avec un tag de VLAN. Vous utilisez ce réglage pour les ports uplink, par exemple.
- `LT` = Tagged Learned
  Le port est un membre du VLAN et transmet les paquets de données avec un tag de VLAN. L'équipement crée l'entrée automatiquement sur la base de la fonction *GVRP* ou *MVRP*.
- `F` = Forbidden
  Le port n'est pas membre du VLAN et ne transmet pas les paquets de données de ce VLAN. De plus, l'équipement empêche le port de devenir un membre du VLAN par le biais de la fonction *MVRP*.
- `U` = Untagged (réglage par défaut pour le VLAN 1)
  Le port est un membre du VLAN et transmet les paquets de données sans tag de VLAN. Utilisez ce réglage si l'équipement connecté n'évalue aucun tag de VLAN, par exemple sur les ports terminaux.
- `LU` = Untagged Learned
  Le port est un membre du VLAN et transmet les paquets de données sans tag de VLAN. L'équipement crée l'entrée automatiquement sur la base de la fonction *GVRP* ou *MVRP*.

Commentaire : Vérifiez que le port sur lequel la station d'administration réseau est connectée est un membre du VLAN dans lequel l'équipement transmet les données de gestion. Dans le réglage par défaut, l'équipement transmet les données de gestion sur le VLAN 1. Sinon, la liaison à l'équipement prend fin lorsque vous transférez les modifications à l'équipement. 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.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée à la table.

Dans le champ *VLAN ID*, vous spécifiez l'ID du VLAN.

5.9.3 VLAN Port

[Switching > VLAN > Port]

Dans cette boîte de dialogue, vous spécifiez comment l'équipement traite les paquets de données reçus qui n'ont pas de tag de VLAN ou dont le tag de VLAN diffère du VLAN-ID du port.

Cette boîte de dialogue vous permet d'affecter un VLAN aux ports, et ainsi de spécifier le VLAN-ID des ports.

De plus, vous spécifiez également pour chaque port comment l'équipement transmet les paquets de données, et l'une des situations suivantes se produit :
- Le port reçoit des paquets de données sans taggage VLAN.
- Le port reçoit des paquets de données avec des informations de priorité de VLAN (VLAN-ID `0`, avec tag de priorité).
- Le taggage VLAN du paquet de données diffère du VLAN-ID du port.

Table

Port

Affiche le numéro de port.

Port-VLAN ID

Spécifie l'ID du VLAN que l'équipement affecte aux paquets de données sans tag de VLAN.

Conditions préalables :
- Dans la colonne *Acceptable packet types*, spécifiez la valeur `admitAll`.

Valeurs possibles :
- ID d'un VLAN défini par vous (réglage par défaut : `1`)

Si vous utilisez la fonction *MRP* et que vous n'avez pas affecté de VLAN aux ports de l'anneau, spécifiez ici la valeur `1` pour les ports de l'anneau. Sinon, l'équipement affecte automatiquement la valeur aux ports de l'anneau.

Acceptable packet types

Spécifie si le port transmet ou rejette les paquets de données reçus sans tag de VLAN.

Valeurs possibles :
- `admitAll` (réglage par défaut)
  Le port accepte les paquets de données avec et sans tag de VLAN.
- `admitOnlyVlanTagged`
  Le port accepte uniquement les paquets de données taggés avec un VLAN-ID ≥ `1`.

Ingress filtering

Active/désactive le filtrage à l'entrée.

Valeurs possibles :

- `case cochée`
  Le filtre à l'entrée est activé.
  L'équipement compare le VLAN-ID dans le paquet de données aux VLAN dont l'équipement est un membre. Voir la boîte de dialogue *Switching > VLAN > Configuration*. Si le VLAN-ID dans le paquet de données correspond à l'un de ces VLAN, le port transmet le paquet de données. Sinon, l'équipement rejette le paquet de données.
- `case non cochée` (réglage par défaut)
  Le filtrage à l'entrée est désactivé.
  L'équipement transmet les paquets de données reçus sans comparer le VLAN-ID. Ainsi, le port transmet des paquets de données avec un VLAN-ID dont le port n'est pas un membre.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.9.4 VLAN Voice

[Switching > VLAN > Voice]

Utilisez la fonctionnalité Voice VLAN pour séparer les trafics de voix et de données sur un port, par VLAN et/ou par priorité. Un avantage essentiel de la fonctionnalité Voice VLAN est la préservation de la qualité du trafic de voix lorsque le trafic de données sur le port est élevé.

L'équipement détecte les téléphones VoIP à l'aide de Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED). L'équipement ajoute ensuite le port approprié à l'ensemble de membres du Voice VLAN configuré. L'ensemble de membres est soit taggé, soit non taggé. Le taggage dépend du mode de l'interface du Voice VLAN (VLAN-ID, Dot1p, Aucun, Non taggé).

Un autre avantage de la fonctionnalité Voice VLAN est que le téléphone VoIP obtient de l'équipement un VLAN-ID ou des informations de priorité via LLDP-MED. Par conséquent, le téléphone VoIP envoie des données de voix taggées comme étant prioritaires ou bien non taggées. Cela dépend du mode configuré pour l'interface du Voice VLAN. Vous activez le Voice VLAN sur le port qui se connecte au téléphone VoIP.

Operation

Operation

Active/désactive la fonction *VLAN Voice* de l'équipement de manière globale.

Valeurs possibles :

- *On*
- *Off* (réglage par défaut)

Table

Port

Affiche le numéro de port.

Voice VLAN mode

Spécifie si le port transmet ou rejette les paquets de données reçus sans taggage du Voice VLAN ou avec des informations de priorité du Voice VLAN.

Valeurs possibles :

- *disabled* (réglage par défaut)
  Désactive la fonction *VLAN Voice* pour cette entrée de table.
- *none*
  Permet au téléphone IP d'utiliser sa propre configuration pour envoyer le trafic de voix non taggé.
- *vlan/dot1p-priority*
  Le port filtre les paquets de données du Voice VLAN à l'aide des tags de priorité vlan et dot1p.
- *untagged*
  Le port filtre les paquets de données sans tag du Voice VLAN.

- *vlan*
  Le port filtre les paquets de données du Voice VLAN à l'aide du tag vlan.
- *dot1p-priority*
  Le port filtre les paquets de données du Voice VLAN à l'aide des tags de priorité dot1p. Si vous sélectionnez cette valeur, spécifiez aussi une valeur propre dans la colonne *Priority*.

Data priority mode

Spécifie le mode Trust pour le trafic de données sur ce port particulier.

L'équipement utilise ce mode pour le trafic de données sur le Voice VLAN lorsqu'il détecte un téléphone VoIP et un PC et que ces équipements utilisent le même câble de données pour transmettre et recevoir des données.

Valeurs possibles :

- *trust* (réglage par défaut)
  Si le trafic de voix est présent sur l'interface, le trafic de données utilise la priorité normale avec ce réglage.
- *untrust*
  Si le trafic de voix est présent et que le *Voice VLAN mode* est défini sur *dot1p-priority*, les données ont la priorité 0. Si l'interface ne transmet que les données, alors les données ont la priorité normale.

Status

Affiche l'état du Voice VLAN sur le port.

Valeurs possibles :

- case cochée
  Le Voice VLAN est activé.
- case non cochée
  La Voice VLAN est désactivé.

VLAN ID

Spécifie l'ID du VLAN auquel l'entrée de table s'applique.

Pour transférer le trafic à ce VLAN-ID à l'aide de ce filtre, sélectionnez dans la colonne *Voice VLAN mode* la valeur *vlan*.

Valeurs possibles :

- 0..4042

Priority

Spécifie la priorité du Voice VLAN du port.

Conditions préalables :

- Dans la colonne *Voice VLAN mode*, spécifiez la valeur *dot1p-priority*.

Valeurs possibles :

- *0..7*
- *none*
  Désactive la priorité du Voice VLAN du port.

Bypass authentication

Active le mode d'authentification du Voice VLAN.

Si vous désactivez la fonction et définissez la valeur dans la colonne *Voice VLAN mode* sur `dot1p-priority`, les équipements de voix requièrent une authentification.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  Si vous avez activé la fonction dans la boîte de dialogue *Network Security > 802.1X Port Authentication > Global*, définissez le paramètre *Port control* pour ce port sur la valeur `multiClient` avant d'activer cette fonction. Vous trouverez le paramètre *Port control* dans la boîte de dialogue *Network Security > 802.1X Port Authentication > Global*.
- `case non cochée`

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.10 L2-Redundancy

[Switching > L2-Redundancy]

Le menu contient les boîtes de dialogue suivantes :

- MRP
- HIPER Ring
- Spanning Tree
- Link Aggregation
- Link Backup
- FuseNet

5.10.1 MRP

[Switching > L2-Redundancy > MRP]

⚠ 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.

Media Redundancy Protocol (MRP) est un protocole qui vous permet de définir des structures de réseau en anneau à tolérance fautive. Un anneau MRP avec des équipements Schneider Electric comprend jusqu'à 100 équipements prenant en charge le protocole MRP conformément à la norme technique IEC 62439.

Si une section ne fonctionne pas, la structure annulaire d'un anneau MRP bascule de nouveau sur une structure linéaire. Le délai de récupération maximum peut être configuré.

La fonction Gestionnaire d'anneau de l'équipement ferme les extrémités d'un backbone dans une structure linéaire en un couplage d'anneau redondant.

Commentaire : *Spanning Tree* et la redondance d'anneau s'influencent mutuellement. Désactivez le protocole *Spanning Tree* pour les ports connectés à l'anneau MRP. Voir la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*.

Lorsque vous travaillez avec des paquets Ethernet surdimensionnés (la valeur dans la colonne *MTU* pour le port est > `1518`, voir la boîte de dialogue *Basic Settings > Port*), le temps de commutation pour la reconfiguration de l'anneau MRP dépend des paramètres suivants :

- Bande passante de la ligne annulaire
- Taille des paquets Ethernet
- Nombre d'équipements dans l'anneau

Définissez un délai de récupération suffisamment important pour éviter les retards des paquets MRP du fait de latences dans les équipements. Vous trouverez la formule pour calculer le temps de commutation dans la norme technique CEI 62439-2, section 9.5.

Operation

Operation

Active/désactive la fonction *MRP*.

Après avoir configuré les paramètres pour l'anneau MRP, activez la fonction ici.

Valeurs possibles :

- `On`
  La fonction *MRP* est activée.
  Après avoir configuré les équipements dans l'anneau MRP, la redondance est active.
- `Off` (réglage par défaut)
  La fonction *MRP* est désactivée.

Ring port 1/Ring port 2

Port

Spécifie le numéro du port fonctionnant en tant que port de l'anneau.

Valeurs possibles :

- `<Numéro de port>`
  Numéro du port de l'anneau

Operation

Affiche le mode opérationnel du port de l'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.

Fixed backup

Active/désactive la fonction de port de secours pour le *Ring port 2*.

Commentaire : La commutation sur le port principal peut excéder le délai de récupération maximum de l'anneau.

Valeurs possibles :

- `case cochée`
  La fonction de secours *Ring port 2* est activée. Lorsque l'anneau est fermé, le gestionnaire de l'anneau bascule de nouveau sur le port principal de l'anneau.
- `case non cochée` (réglage par défaut)
  La fonction de secours *Ring port 2* est désactivée. Lorsque l'anneau est fermé, le gestionnaire de l'anneau continue d'envoyer des données sur le port secondaire de l'anneau.

Configuration

Ring manager

Active/désactive la fonction *Ring manager*.

Si un équipement est présent à chaque extrémité de la ligne, vous activez cette fonction.

Valeurs possibles :

- *On*
  La fonction *Ring manager* est activée.
  L'équipement fonctionne en tant que gestionnaire de l'anneau.
- *Off* (réglage par défaut)
  La fonction *Ring manager* est désactivée.
  L'équipement fonctionne en tant que client de l'anneau.

Advanced mode

Active/désactive le mode avancé pour des délais de récupération rapides.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  Mode avancé activé.
  Les équipements Schneider Electric compatibles MRP prennent en charge ce mode.
- `case non cochée`
  Mode avancé désactivé.
  Sélectionnez ce réglage si un autre équipement dans l'anneau ne prend pas en charge ce mode.

Ring recovery

Spécifie le délai de récupération maximum en millisecondes pour la reconfiguration de l'anneau. Ce réglage est effectif si l'équipement fonctionne en tant que gestionnaire de l'anneau.

Valeurs possibles :

- *500ms*
- *200ms* (réglage par défaut)

Des délais de commutation plus courts génèrent un plus grand nombre de demandes sur le délai de réponse de chaque équipement individuel dans l'anneau. Utilisez des valeurs inférieures à *500ms* si les autres équipements dans l'anneau prennent également en charge ce délai de récupération plus court.

Lorsque vous travaillez avec des paquets Ethernet surdimensionnés, le nombre d'équipements dans l'anneau est limité. Notez que le délai de commutation dépend de différents paramètres. Voir la description ci-dessus.

VLAN ID

Spécifie l'ID du VLAN que vous affectez aux ports de l'anneau.

Valeurs possibles :

- `0` (réglage par défaut)
  Aucun VLAN affecté.
  Dans la boîte de dialogue *Switching > VLAN > Configuration*, affectez aux ports de l'anneau pour le VLAN `1` la valeur `U`.
- `1..4042`
  VLAN affecté.
  Si vous affectez aux ports de l'anneau un VLAN inexistant, l'équipement crée ce VLAN. Dans la boîte de dialogue *Switching > VLAN > Configuration*, l'équipement crée une entrée dans la table pour le VLAN et affecte la valeur `T` aux ports de l'anneau.

Information

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.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Delete ring configuration

Désactive la fonction de redondance et réinitialise les réglages par défaut dans la boîte de dialogue.

5.10.2 HIPER Ring

[Switching > L2-Redundancy > 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 du HIPER Ring permet la mise en œuvre de réseaux annulaires à tolérance fautive. Cet équipement constitue un client du HIPER Ring. Cette fonction vous permet d'étendre un HIPER Ring existant ou de remplacer un équipement participant déjà en tant que client dans un HIPER Ring.

Un HIPER Ring contient un gestionnaire d'anneau (RM) qui contrôle l'anneau. Le RM envoie des paquets watchdog dans l'anneau sur les ports principal et secondaire. Lorsque le RM reçoit les paquets watchdog sur les deux ports, le port principal reste à l'état de transfert et le port secondaire reste à l'état de rejet.

L'équipement fonctionne uniquement en mode client de l'anneau. Cela signifie que l'équipement est capable de détecter et de transférer les paquets watchdog sur les ports de l'anneau, mais aussi de transférer la modification de l'état du lien au RM, par exemple des paquets LinkDown et LinkUp.

L'équipement ne prend en charge que les ports Fast Ethernet et Gigabit Ethernet en tant que ports d'anneau. De plus, l'équipement ne prend en charge que le HIPER Ring dans le VLAN `1`.

Commentaire : *Spanning Tree* et la redondance d'anneau s'influencent mutuellement. Désactivez le protocole *Spanning Tree* pour les ports connectés au HIPER Ring. Voir la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*.

Commentaire : Configurez individuellement les équipements du HIPER Ring. Avant de connecter la liaison redondante, terminez la configuration de chaque équipement sur le HIPER Ring. Vous évitez ainsi les boucles pendant la phase de configuration.

Operation

Operation

Active/désactive le client *HIPER Ring*.

Valeurs possibles :

- `On`
  Le client *HIPER Ring* est activé.
- `Off` (réglage par défaut)
  Le client *HIPER Ring* est désactivé.

Ring port 1/Ring port 2

Port

Spécifie le numéro du port principal/secondaire de l'anneau.

Valeurs possibles :

- `-` (réglage par défaut)
  Aucun port principal/secondaire de l'anneau sélectionné.
- `<Numéro de port>`
  Numéro du port de l'anneau

State

Affiche l'état du port principal/secondaire de l'anneau.

Valeurs possibles :

- *`not-available`*
  Le client *HIPER Ring* est désactivé.
  ou
  Aucun port principal ou secondaire de l'anneau n'est sélectionné.
- *`active`*
  Le port de l'anneau est activé et logiquement opérationnel.
- *`inactive`*
  Le port de l'anneau est logiquement inopérationnel.
  Dès que la liaison devient inopérationnelle sur un port de l'anneau, l'équipement envoie un paquet LinkDown au gestionnaire de l'anneau sur l'autre port de l'anneau.

Information

Mode

Affiche que l'équipement est capable de fonctionner en mode client de l'anneau.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.10.3 Spanning Tree

[Switching > L2-Redundancy > Spanning Tree]

⚠ 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.

Spanning Tree Protocol (STP) est un protocole qui désactive les chemins redondants d'un réseau afin d'éviter les boucles. Si un composant du réseau devient inexploitable sur le chemin, l'équipement calcule la nouvelle topologie et réactive ce chemin.

Rapid Spanning Tree Protocol (RSTP) permet une commutation rapide sur une nouvelle topologie calculée sans interrompre les liaisons existantes. RSTP présente des temps de reconfiguration moyens inférieurs à une seconde. Lorsque vous utilisez RSTP dans un anneau avec 10 ou 20 équipements, vous pouvez obtenir des temps de reconfiguration de quelques millisecondes.

Commentaire : Lorsque vous connectez l'équipement au réseau par le biais de SFP à paire torsadée au lieu des ports à paire torsadée usuels, la reconfiguration du réseau est légèrement plus longue.

Le menu contient les boîtes de dialogue suivantes :

- Spanning Tree Global
- Spanning Tree Dual RSTP (MCSESM-E)
- Spanning Tree Port

5.10.3.1 Spanning Tree Global

[Switching > L2-Redundancy > Spanning Tree > Global]

Dans cette boîte de dialogue, vous activez/désactivez la fonction *Spanning Tree* et vous spécifiez les réglages du commutateur réseau.

Operation

Operation

Active/désactive la fonction Spanning Tree dans l'équipement.

Valeurs possibles :

- `On` (réglage par défaut)
- `Off`
  L'équipement se comporte de manière transparente. L'équipement transmet les paquets de données Spanning Tree reçus comme les paquets de données multicast aux ports.

Variant

Variant

Affiche le protocole utilisé pour la fonction *Spanning Tree* :

Valeurs possibles :

- `rstp`
  Le protocole `RSTP` est activé.
  Avec RSTP (IEEE 802.1Q-2005), la fonction *Spanning Tree* opère pour la couche physique sous-jacente.

Traps

Send trap

Active/désactive l'envoi de traps SNMP pour les événements suivants :

- Un autre commutateur réseau joue le rôle de commutateur racine.
- La topologie change. Un port modifie son *Port state* de *forwarding* en *discarding* ou de *discarding* en *forwarding*.

Valeurs possibles :

- `case cochée`
  L'envoi de traps SNMP est activé.
- `case non cochée` (réglage par défaut)
  L'envoi de traps SNMP est désactivé.

Bridge configuration

Bridge ID

Affiche l'ID de commutateur réseau de l'équipement.

L'équipement doté de l'ID de commutateur réseau avec la plus petite valeur numérique joue le rôle de commutateur racine dans le réseau.

Valeurs possibles :

- `<Priorité du commutateur réseau> / <Adresse MAC>`
  Valeur dans le champ *Priority* / adresse MAC de l'équipement

Priority

Spécifie la priorité du commutateur réseau de l'équipement.

Valeurs possibles :

- `0..61440` par incréments de 4096 (réglage par défaut : `32768`)

Pour faire de cet équipement le commutateur racine, affectez lui la valeur numérique de priorité la plus basse du réseau.

Hello time [s]

Spécifie la durée en secondes entre l'envoi de deux messages de configuration (paquets de données Hello).

Valeurs possibles :

- `1..2` (réglage par défaut : `2`)

Si l'équipement joue le rôle de commutateur racine, les autres équipements dans le réseau utilisent la valeur spécifiée ici.

Sinon, l'équipement utilise la valeur spécifiée par le commutateur racine. Voir le cadre *Root information*.

En raison de l'interaction avec le paramètre *Tx holds*, il est recommandé de ne pas modifier le réglage par défaut.

Forward delay [s]

Spécifie le délai en secondes pour le changement d'état.

Valeurs possibles :

- `4..30` (réglage par défaut : `15`)

Si l'équipement joue le rôle de commutateur racine, les autres équipements dans le réseau utilisent la valeur spécifiée ici.

Sinon, l'équipement utilise la valeur spécifiée par le commutateur racine. Voir le cadre *Root information*.

Dans le protocole RSTP, les commutateurs réseau négocient un changement d'état sans délai spécifié.

Le protocole *Spanning Tree* utilise le paramètre pour retarder le changement entre les états `disabled`, `discarding`, `learning`, `forwarding`.

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.

Max age

Spécifie la longueur de branche maximum admissible, par exemple le nombre d'équipements pour le commutateur racine.

Valeurs possibles :

- `6..40` (réglage par défaut : `20`)

Si l'équipement joue le rôle de commutateur racine, les autres équipements dans le réseau utilisent la valeur spécifiée ici.

Sinon, l'équipement utilise la valeur spécifiée par le commutateur racine. Voir le cadre *Root information*.

Le protocole *Spanning Tree* utilise le paramètre pour spécifier la validité des STP-BPDU en secondes.

Tx holds

Limite le débit de transmission maximum pour l'envoi de BPDU.

Valeurs possibles :

- `1..40` (réglage par défaut : `10`)

Lorsque l'équipement envoie une BPDU, il incrémente un compteur sur ce port.

Si le compteur atteint la valeur spécifiée ici, le port arrête d'envoyer des BPDU. D'une part, cela réduit la charge générée par RSTP et d'autre part, le fait que l'équipement ne reçoive pas de BPDU peut entraîner une interruption de la communication.

L'équipement décrémente le compteur de `1` toutes les secondes. La seconde suivante, l'équipement envoie un maximum de `1` nouvelle BPDU.

BPDU guard

Active/désactive la fonction BPDU Guard dans l'équipement.

Avec cette fonction, l'équipement contribue à préserver votre réseau des configurations incorrectes, des attaques avec STP-BPDU et des modifications indésirables de la topologie.

Valeurs possibles :

- `case cochée`
  Le *BPDU guard* est activé.
  - L'équipement applique la fonction aux ports marginaux spécifiés manuellement. Pour ces ports, la case dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*, onglet *CIST*, colonne *Admin edge port* est cochée.
  - Si un port marginal reçoit une STP-BPDU, l'équipement désactive le port. Pour ce port, dans la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*, la case dans la colonne *Port on* est `décochée`.
- `case non cochée` (réglage par défaut)
  Le *BPDU guard* est désactivé.

Pour réinitialiser l'état du port à la valeur `forwarding`, procédez comme suit :

- ☐ Si le port reçoit toujours des BPDU :
  - Dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*, onglet *CIST*, décochez la case dans la colonne *Admin edge port*.
    ou
  - Dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*, décochez la case *BPDU guard*.
- ☐ Pour réactiver le port, utilisez la fonction *Auto-Disable*. Sinon, procédez comme suit :
  - Ouvrez la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.
  - Cochez la case dans la colonne *Port on*.

BPDU filter (all admin edge ports)

Active/désactive le filtre STP-BPDU sur chaque port marginal spécifié manuellement. Pour ces ports, la case dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*, onglet *CIST*, colonne *Admin edge port* est cochée.

Valeurs possibles :

- `case cochée`
  Le filtre BPDU est activé sur chaque port marginal.
  La fonction n'utilise pas ces ports dans les opérations *Spanning Tree*.
  - L'équipement n'envoie pas de STP-BPDU sur ces ports.
  - L'équipement rejette toutes les STP-BPDU reçues sur ces ports.
- `case non cochée` (réglage par défaut)
  Le filtre BPDU global est désactivé.
  Vous avez la possibilité d'activer explicitement le filtre BPDU pour les ports uniques. Voir la colonne *Port BPDU filter* dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*.

Auto-disable

Active/désactive la fonction *Auto-Disable* pour les paramètres que *BPDU guard* surveille sur le port.

Valeurs possibles :

- `case cochée`
  La fonction *Auto-Disable* pour le *BPDU guard* est activée.
  - Lorsque le port reçoit une STP-BPDU, l'équipement désactive un port marginal. La LED « État du lien » du port clignote 3x par période.
  - La boîte de dialogue *Diagnostics > Ports > Auto-Disable* affiche quels ports sont actuellement désactivés en raison du dépassement des paramètres.
  - La fonction *Auto-Disable* réactive le port automatiquement. Pour cela, accédez à la boîte de dialogue *Diagnostics > Ports > Auto-Disable* et spécifiez une période d'attente pour le port concerné dans la colonne *Reset timer [s]*.
- `case non cochée` (réglage par défaut)
  La fonction *Auto-Disable* pour le *BPDU guard* est désactivée.

Root information

Bridge ID

Affiche l'ID du commutateur racine actuel.

Valeurs possibles :

- `<Priorité du commutateur réseau> / <Adresse MAC>`

Priority

Affiche la priorité du commutateur racine actuel.

Valeurs possibles :

- `0..61440` par incréments de 4096

Hello time [s]

Affiche la durée en secondes spécifiée par le commutateur racine entre l'envoi de deux messages de configuration (paquets de données Hello).

Valeurs possibles :

- `1..2`

L'équipement utilise cette valeur spécifiée. Voir le cadre *Bridge configuration*.

Forward delay [s]

Spécifie le délai en secondes défini par le commutateur racine pour les changements d'état.

Valeurs possibles :

- `4..30`

L'équipement utilise cette valeur spécifiée. Voir le cadre *Bridge configuration*.

Dans le protocole RSTP, les commutateurs réseau négocient un changement d'état sans délai spécifié.

Le protocole *Spanning Tree* utilise le paramètre pour retarder le changement entre les états `disabled`, `discarding`, `learning`, `forwarding`.

Max age

Spécifie la longueur de branche maximum admissible définie par le commutateur racine, par exemple le nombre d'équipements pour le commutateur racine.

Valeurs possibles :

- `6..40` (réglage par défaut : `20`)

Le protocole *Spanning Tree* utilise le paramètre pour spécifier la validité des STP-BPDU en secondes.

Topology information

Bridge is root

Affiche si l'équipement joue actuellement le rôle de commutateur racine.

Valeurs possibles :

- `case cochée`
  L'équipement joue actuellement le rôle de commutateur racine.
- `case non cochée`
  Un autre équipement joue actuellement le rôle de commutateur racine.

Root port

Affiche le numéro du port à partir duquel le chemin actuel mène au commutateur racine.

Si l'équipement joue le rôle de commutateur racine, le champ affiche la valeur `no Port`.

Root path cost

Spécifie le coût du chemin menant du port racine de l'équipement au commutateur racine du réseau de couche 2.

Valeurs possibles :

- `0..200000000`
  Si la valeur `0` est spécifiée, l'équipement joue le rôle de commutateur racine.

Topology changes

Affiche combien de fois l'équipement a basculé un port sur l'état `forwarding` à l'aide de la fonction *Spanning Tree* depuis le démarrage de l'instance *Spanning Tree*.

Time since topology change

Affiche le temps écoulé depuis la dernière modification de la topologie.

Valeurs possibles :

- `<jours, heures:minutes:secondes>`

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.10.3.2 Spanning Tree Dual RSTP (MCSESM-E)

[Switching > L2-Redundancy > Spanning Tree > Dual RSTP]

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Pour éviter les boucles durant la phase de configuration, configurez chaque équipement de la configuration *RCP* et *Dual RSTP* configuration 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.

Dans cette boîte de dialogue, vous spécifiez les réglages du commutateur réseau correspondant à la deuxième *Spanning Tree* instance.

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 2 *Spanning Tree* segments, 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*.

Vous spécifiez les réglages de la fonction *RCP* dans la boîte de dialogue *Switching > L2-Redundancy > FuseNet > RCP*.

Operation

Operation

Indique si la fonction *Dual RSTP* est activée/désactivée dans l'équipement.

Valeurs possibles :

- `On`
  La fonction *Dual RSTP* est activée dans l'équipement.
  L'équipement active la fonction *Dual RSTP* si les conditions préalables suivantes sont remplies :
  - Dans la boîte de dialogue *Switching > L2-Redundancy > FuseNet > RCP*, vous avez spécifié les ports pour les réglages *Primary ring/network* et *Secondary ring/network*.
  - Dans la boîte de dialogue *Switching > L2-Redundancy > FuseNet > RCP*, cadre *Operation*, vous avez activé la fonction *RCP*.
  - Dans la boîte de dialogue *Spanning Tree Global*, cadre *Operation*, vous avez activé la fonction *Spanning Tree*.
  - Aucun protocole de redondance n'est configuré dans l'anneau secondaire.
- `Off` (réglage par défaut)
  La fonction *Dual RSTP* est désactivée dans l'équipement.

Traps

Send trap

Active/désactive l'envoi de traps SNMP pour les événements suivants :

- Un autre commutateur réseau joue le rôle de commutateur racine.
- La topologie change. Un port modifie son *Port state* de *forwarding* en *discarding* ou de *discarding* en *forwarding*.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'envoi de traps SNMP est activé.
- `case non cochée`
  L'envoi de traps SNMP est désactivé.

Bridge configuration

Bridge ID

Affiche l'ID de commutateur réseau de l'équipement.

L'équipement doté de l'ID de commutateur réseau avec la plus petite valeur numérique joue le rôle de commutateur racine dans le réseau.

Valeurs possibles :

- `<Priorité du commutateur réseau> / <Adresse MAC>`
  Valeur dans le champ *Priority* / adresse MAC de l'équipement

Priority

Spécifie la priorité du commutateur réseau de l'équipement.

Valeurs possibles :

- `0..61440` par incréments de 4096 (réglage par défaut : `32768`)

Pour faire de cet équipement le commutateur racine, affectez lui la valeur numérique de priorité la plus basse du réseau.

Hello time [s]

Spécifie la durée en secondes entre l'envoi de deux messages de configuration (paquets de données Hello).

Valeurs possibles :

- `1..2` (réglage par défaut : `2`)

Si l'équipement joue le rôle de commutateur racine, les autres équipements dans le réseau utilisent la valeur spécifiée ici.

Sinon, l'équipement utilise la valeur spécifiée par le commutateur racine. Voir le cadre *Root information*.

En raison de l'interaction avec le paramètre *Tx holds*, il est recommandé de ne pas modifier le réglage par défaut.

Forward delay [s]

Spécifie le délai en secondes pour le changement d'état.

Valeurs possibles :

- `4..30` (réglage par défaut : `15`)

Si l'équipement joue le rôle de commutateur racine, les autres équipements dans le réseau utilisent la valeur spécifiée ici. Sinon, l'équipement utilise la valeur spécifiée par le commutateur racine. Voir le cadre *Root information*.

Dans le protocole RSTP, les commutateurs réseau négocient un changement d'état sans délai spécifié.

Le protocole *Spanning Tree* utilise le paramètre pour retarder le changement entre les états *disabled*, *discarding*, *learning*, *forwarding*.

Les paramètres *Forward delay [s]* et *Max age* ont la relation suivante :

Forward delay [s] ≥ (*Max age*/2) + 1

Max age

Spécifie le nombre maximum admissible d'équipements dans le chemin jusqu'au commutateur racine.

Valeurs possibles :

- `6..40` (réglage par défaut : `20`)

Si l'équipement joue le rôle de commutateur racine, les autres équipements dans le réseau utilisent la valeur spécifiée ici. Sinon, l'équipement utilise la valeur spécifiée par le commutateur racine. Voir le cadre *Root information*.

Tx holds

Limite le débit de transmission maximum pour l'envoi de BPDU.

Valeurs possibles :

- `1..40` (réglage par défaut : `10`)

Lorsque l'équipement envoie une BPDU, il incrémente un compteur sur ce port.

Lorsque le compteur atteint la valeur spécifiée ici, le port arrête d'envoyer des BPDU. D'une part, cela réduit la charge générée par RSTP et d'autre part, le fait que l'équipement ne reçoive pas de BPDU peut entraîner une interruption de la communication.

L'équipement décrémente le compteur de `1` toutes les secondes. La seconde suivante, l'équipement envoie un maximum de `1` nouvelle BPDU.

BPDU guard

Active/désactive la fonction BPDU Guard dans l'équipement.

Avec cette fonction, l'équipement contribue à préserver votre réseau des configurations incorrectes, des attaques avec STP-BPDU et des modifications indésirables de la topologie.

Valeurs possibles :

- `case cochée`
  Le *BPDU guard* est activé.
  - L'équipement applique la fonction aux ports marginaux spécifiés manuellement. Pour ces ports, la case dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*, onglet *CIST*, colonne *Admin edge port* est cochée.
  - Si un port marginal reçoit une STP-BPDU, l'équipement désactive le port. Pour ce port, dans la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*, la case dans la colonne *Port on* est `décochée`.
- `case non cochée` (réglage par défaut)
  Le *BPDU guard* est désactivé.

Pour réinitialiser l'état du port à la valeur *`forwarding`*, procédez comme suit :

- ☐ Si le port reçoit toujours des BPDU :
  - Dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*, onglet *CIST*, décochez la case dans la colonne *Admin edge port*.
    ou
  - Dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Dual RSTP*, décochez la case *BPDU guard*.
- ☐ Pour réactiver le port, procédez comme suit :
  - Ouvrez la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.
  - Cochez la case dans la colonne *Port on*.

BPDU filter (all admin edge ports)

Active/désactive le filtre STP-BPDU sur chaque port marginal spécifié manuellement. Pour ces ports, la case dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*, onglet *CIST*, colonne *Admin edge port* est cochée.

Valeurs possibles :

- `case cochée`
  Le filtre BPDU est activé sur chaque port marginal.
  La fonction n'utilise pas ces ports dans les opérations *Spanning Tree*.
  - L'équipement n'envoie pas de STP-BPDU sur ces ports.
  - L'équipement rejette toutes les STP-BPDU reçues sur ces ports.
- `case non cochée` (réglage par défaut)
  Le filtre BPDU global est désactivé.
  Vous avez la possibilité d'activer explicitement le filtre BPDU pour les ports uniques. Voir la colonne *Port BPDU filter* dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*.

Root information

Root ID

Affiche l'ID du commutateur racine actuel.

Valeurs possibles :

- `<Priorité du commutateur réseau> / <Adresse MAC>`

Priority

Affiche la priorité du commutateur racine actuel.

Valeurs possibles :

- `0..61440` par incréments de 4096

Hello time [s]

Affiche la durée en secondes spécifiée par le commutateur racine entre l'envoi de deux messages de configuration (paquets de données Hello).

Valeurs possibles :

- `1..2`

L'équipement utilise cette valeur spécifiée. Voir le cadre *Bridge configuration*.

Forward delay [s]

Spécifie le délai en secondes défini par le commutateur racine pour les changements d'état.

Valeurs possibles :

- `4..30`

L'équipement utilise cette valeur spécifiée. Voir le cadre *Bridge configuration*.

Dans le protocole RSTP, les commutateurs réseau négocient un changement d'état sans délai spécifié.

Le protocole *Spanning Tree* utilise le paramètre pour retarder le changement entre les états *disabled*, *discarding*, *learning*, *forwarding*.

Max age

Spécifie la longueur de branche maximum admissible définie par le commutateur racine, par exemple le nombre d'équipements pour le commutateur racine.

Valeurs possibles :

- `6..40` (réglage par défaut : `20`)

Le protocole *Spanning Tree* utilise le paramètre pour spécifier la validité des STP-BPDU en secondes.

Topology information

Bridge is root

Affiche si l'équipement joue actuellement le rôle de commutateur racine.

Valeurs possibles :

- `case cochée`
  L'équipement joue actuellement le rôle de commutateur racine.
- `case non cochée`
  Un autre équipement joue actuellement le rôle de commutateur racine.

Root port

Affiche le numéro du port à partir duquel le chemin actuel mène au commutateur racine.

Si l'équipement joue le rôle de commutateur racine, le champ affiche la valeur `no Port`.

Root path cost

Spécifie le coût du chemin menant du port racine de l'équipement au commutateur racine du réseau de couche 2.

Valeurs possibles :

- `0..200000000`
  Si la valeur `0` est spécifiée, l'équipement joue le rôle de commutateur racine.

Topology changes

Affiche combien de fois l'équipement a basculé un port sur l'état *`forwarding`* à l'aide de la fonction *Spanning Tree* depuis le démarrage de l'instance *Spanning Tree*.

Time since topology change

Affiche le temps écoulé depuis la dernière modification de la topologie.

Valeurs possibles :

- `<jours, heures:minutes:secondes>`

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.10.3.3 Spanning Tree Port

[Switching > L2-Redundancy > Spanning Tree > Port]

Dans cette boîte de dialogue, vous activez la fonction Spanning Tree sur les ports et vous spécifiez les ports marginaux ainsi que les réglages des différentes fonctions de protection.

La boîte de dialogue contient les onglets suivants :
- [CIST]
- [Guards]

[CIST]

Dans cet onglet, vous pouvez activer individuellement la fonction Spanning Tree sur les ports, spécifier les réglages des ports marginaux et afficher les valeurs actuelles. L'abréviation CIST signifie Common and Internal Spanning Tree.

Commentaire : Désactivez la fonction *Spanning Tree* sur les ports participant à d'autres protocoles de redondance de couche 2. Sinon, il est possible que les protocoles de redondance ne fonctionnent pas comme prévu. Cela peut générer des boucles.

Table

Port

Affiche le numéro de port.

STP active

Active/désactive la fonction Spanning Tree sur le port.

Valeurs possibles :
- `case cochée` (réglage par défaut)
  La fonction *Spanning Tree* est activée sur le port.
- `case non cochée`
  La fonction *Spanning Tree* est désactivée sur le port.
  Si la fonction *Spanning Tree* est activée dans l'équipement et désactivée sur le port, le port n'envoie pas de STP-BPDU et rejette toutes les STP-BPDU reçues.

Port state

Affiche l'état de transmission du port.

Valeurs possibles :
- *discarding*
  Le port est bloqué et transfère uniquement des STP-BPDU.
- *learning*
  Le port est bloqué, mais il apprend les adresses MAC des paquets de données reçus.
- *forwarding*
  Le port transfère des paquets de données.

- *disabled*
  Le port est désactivé. Voir la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.
- *manualFwd*
  La fonction *Spanning Tree* est désactivée sur le port. Le port transfère des STP-BPDU.
- *notParticipate*
  Le port ne participe pas à STP.

Port role

Affiche le rôle actuel du port dans CIST.

Valeurs possibles :

- *root*
  Port avec le chemin le moins cher jusqu'au commutateur racine.
- *alternate*
  Port avec le chemin alternatif jusqu'au commutateur racine (actuellement bloqué).
- *designated*
  Port pour le côté de l'arbre évité depuis le commutateur racine (actuellement bloqué).
- *backup*
  Le port reçoit des STP-BPDU de son propre équipement
- *disabled*
  Le port est désactivé. Voir la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.

Port path cost

Spécifie les coûts de chemin du port.

Valeurs possibles :

- `0..200000000` (réglage par défaut : `0`)

Lorsque la valeur est `0`, l'équipement calcule automatiquement les coûts de chemin en fonction du débit de données du port.

Port priority

Spécifie la priorité du port.

Valeurs possibles :

- `16..240` par incréments de 16 (réglage par défaut : `128`)

Cette valeur représente les 4 premiers bits de l'ID du port.

Received bridge ID

Affiche l'ID du dernier commutateur réseau de l'équipement duquel ce port a reçu une STP-BPDU.

Valeurs possibles :

- Pour les ports avec le rôle *designated*, l'équipement affiche les informations de la dernière STP-BPDU reçue par le port. Cela facilite le diagnostic d'éventuels problèmes STP dans le réseau.
- Pour les rôles de port *alternate*, *backup*, *master* et *root*, ces informations sont identiques aux informations du rôle de port *designated* à l'état stationnaire (topologie statique).
- Si un port n'a pas de liaison ou s'il n'a pas encore reçu de STP-BDU, l'équipement affiche les valeurs que le port peut envoyer avec le rôle *designated*.

Received port ID

Affiche l'ID du dernier port de l'équipement duquel ce port a reçu une STP-BPDU.

Valeurs possibles :

- Pour les ports avec le rôle *designated*, l'équipement affiche les informations de la dernière STP-BPDU reçue par le port. Cela facilite le diagnostic d'éventuels problèmes STP dans le réseau.
- Pour les rôles de port *alternate*, *backup*, *master* et *root*, ces informations sont identiques aux informations du rôle de port *designated* à l'état stationnaire (topologie statique).
- Si un port n'a pas de liaison ou s'il n'a pas encore reçu de STP-BDU, l'équipement affiche les valeurs que le port peut envoyer avec le rôle *designated*.

Received path cost

Affiche, pour le commutateur réseau de niveau supérieur, le coût du chemin entre son port racine et le commutateur racine.

Valeurs possibles :

- Pour les ports avec le rôle *designated*, l'équipement affiche les informations de la dernière STP-BPDU reçue par le port. Cela facilite le diagnostic d'éventuels problèmes STP dans le réseau.
- Pour les rôles de port *alternate*, *backup*, *master* et *root*, ces informations sont identiques aux informations du rôle de port *designated* à l'état stationnaire (topologie statique).
- Si un port n'a pas de liaison ou s'il n'a pas encore reçu de STP-BDU, l'équipement affiche les valeurs que le port peut envoyer avec le rôle *designated*.

Admin edge port

Active/désactive le mode *Admin edge port*. Si le port est connecté à un équipement terminal, utilisez le mode *Admin edge port*. Ce réglage permet au port marginal de passer plus rapidement à l'état de transfert après établissement de la liaison, et ainsi une accessibilité plus rapide de l'équipement terminal.

Valeurs possibles :

- `case cochée`
  Le mode *Admin edge port* est activé.
  Le port est connecté à un équipement terminal.
  - Une fois la liaison établie, le port passe à l'état *forwarding* sans passer d'abord par l'état *learning*.
  - Si le port reçoit une STP-BPDU et que la fonction BPDU Guard est activée, l'équipement désactive le port. Voir la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*.
- `case non cochée` (réglage par défaut)
  Le mode *Admin edge port* est désactivé.
  Le port est connecté à un autre commutateur réseau STP.
  Une fois la liaison établie, le port passe à l'état *learning* avant de passer à l'état *forwarding*, le cas échéant.

Auto edge port

Active/désactive la détection automatique du raccordement d'un équipement terminal au port. La condition préalable est que la case dans la colonne *Admin edge port* soit `décochée`.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La détection automatique est activée.
  Après l'établissement de la liaison et après 1,5 × *Hello time [s]* l'équipement définit le port sur l'état *`forwarding`* (réglage par défaut 1,5 × 2 s) si le port n'a reçu aucune STP-BPDU durant cette période.
- `case non cochée`
  La détection automatique est désactivée.
  Après l'établissement de la liaison et après *Max age*, l'équipement définit le port sur l'état *`forwarding`*.
  (réglage par défaut : 20 s)

Oper edge port

Affiche si un équipement terminal ou un commutateur réseau STP est connecté au port.

Valeurs possibles :

- `case cochée`
  Un équipement terminal est connecté au port. Le port ne reçoit aucune STP-BPDU.
- `case non cochée`
  Un commutateur réseau STP est connecté au port. Le port reçoit des STP-BPDU.

Oper PointToPoint

Affiche si le port est connecté à un équipement STP via une liaison full duplex.

Valeurs possibles :

- `case cochée`
  Le port est connecté directement à un équipement STP via une liaison full duplex. La communication décentralisée directe entre 2 commutateurs réseau permet des délais de reconfiguration courts.
- `case non cochée`
  Le port est connecté d'une autre manière, par exemple via une liaison half duplex ou via un hub.

Port BPDU filter

Active/désactive le filtrage des STP-BPDU sur le port de manière explicite.

La condition préalable est que le port soit un port marginal spécifié manuellement. Pour ces ports, la case dans la colonne *Admin edge port* est cochée.

Valeurs possibles :

- `case cochée`
  Le filtre BPDU est activé sur le port.
  La fonction exclut le port des opérations *Spanning Tree*.
  – L'équipement n'envoie pas de STP-BPDU sur le port.
  – L'équipement rejette toutes les STP-BPDU reçues sur le port.
- `case non cochée` (réglage par défaut)
  Le filtre BPDU est désactivé sur le port.
  Vous avez la possibilité d'activer globalement le filtre BPDU pour chaque port marginal. Voir la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*, cadre *Bridge configuration*.
  Si la case *BPDU filter (all admin edge ports)* est cochée, le filtre BPDU est toujours activé sur le port.

BPDU filter status

Affiche si le filtre BPDU est activé sur le port.

Valeurs possibles :

- `case cochée`
  Le filtre BPDU est activé sur le port en conséquence des réglages suivants :
  – La case dans la colonne *Port BPDU filter* est cochée.
  et/ou
  – La case dans la colonne *BPDU filter (all admin edge ports)* est cochée. Voir la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*, cadre *Bridge configuration*.
- `case non cochée`
  Le filtre BPDU est désactivé sur le port.

BPDU flood

Active/désactive le mode *BPDU flood* sur le port même si la fonction *Spanning Tree* est désactivée sur le port. L'équipement transmet les STP-BPDU reçues sur le port aux ports pour lesquels la fonction *Spanning Tree* est désactivée et le mode *BPDU flood* est également activé.

Valeurs possibles :

- `case cochée`
  Le mode *BPDU flood* est activé.
- `case non cochée` (réglage par défaut)
  Le mode *BPDU flood* est désactivé.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Guards]

Cet onglet vous permet de spécifier les réglages de différentes fonctions de protection sur les ports.

Table

Port

Affiche le numéro de port.

Root guard

Active/désactive la surveillance des STP-BDU sur le port. La condition préalable est que le fonction *Loop guard* soit désactivée.

Avec ce réglage, l'équipement contribue à préserver votre réseau des configurations incorrectes et des attaques avec STP-BPDU visant à modifier la topologie. Ce réglage n'est pertinent que pour les ports avec le rôle STP `designated`.

Valeurs possibles :

- `case cochée`
  La surveillance des STP-BPDU est activée.
  - Si le port reçoit une STP-BPDU avec de meilleures informations de chemin jusqu'au commutateur racine, l'équipement rejette la STP-BPDU et définit l'état du port sur la valeur `discarding` au lieu de `root`.
  - En l'absence de STP-BPDU avec de meilleures informations de chemin jusqu'au commutateur racine, l'équipement réinitialise l'état du port après 2 × *Hello time [s]*.
- `case non cochée` (réglage par défaut)
  La surveillance des STP-BPDU est désactivée.

TCN guard

Active/désactive la surveillance des « notifications de modification de la topologie » sur le port. Avec ce réglage, l'équipement contribue à préserver votre réseau des attaques avec STP-BPDU visant à modifier la topologie.

Valeurs possibles :

- `case cochée`
  La surveillance des « notifications de modification de la topologie » est activée.
  - Le port ignore la marque Modification de la topologie dans les STP-BPDU reçues.
  - Si la BPDU reçue contient d'autres informations entraînant une modification de la topologie, l'équipement traite la BPDU même si la protection TCN est activée.
    Exemple : l'équipement reçoit des informations sur un meilleur chemin pour le commutateur racine.
- `case non cochée` (réglage par défaut)
  La surveillance des « notifications de modification de la topologie » est désactivée.
  Si l'équipement reçoit des STP-BPDU avec une marque Modification de la topologie, l'équipement supprime la table d'adresses du port et transfère les notifications de modification de la topologie.

Loop guard

Active/désactive la surveillance des boucles sur le port. La condition préalable est que le fonction *Root guard* soit désactivée.

Avec ce réglage, l'équipement contribue à prévenir les boucles si le port ne reçoit plus de STP-BPDU. N'utilisez ce réglage que pour les ports avec le rôle STP `alternate`, `backup` ou `root`.

Valeurs possibles :

- `case cochée`
  La surveillance des boucles est activée. Cela contribue à prévenir les boucles, par exemple si vous désactivez la fonction Spanning Tree sur l'équipement distant ou si la liaison est interrompue uniquement dans le sens de réception.
  - Si le port ne reçoit aucune STP-BPDU pendant un moment, l'équipement définit l'état du port sur la valeur *discarding* et coche la case dans la colonne *Loop state*.
  - Si le port reçoit de nouveau des STP-BPDU, l'équipement définit l'état du port sur une valeur selon *Port role* et décoche la case dans la colonne *Loop state*.
- `case non cochée` (réglage par défaut)
  La surveillance des boucles est désactivée.
  Si le port ne reçoit aucune STP-BPDU pendant un moment, l'équipement définit l'état du port sur la valeur *forwarding*.

Loop state

Affiche si l'état de boucle du port est incohérent.

Valeurs possibles :

- `case cochée`
  L'état de boucle du port est incohérent :
  - Le port ne reçoit aucune STP-BPDU et la fonction *Loop guard* est activée.
  - L'équipement définit l'état du port sur la valeur *discarding*. L'équipement contribue ainsi à prévenir toute boucle éventuelle.
- `case non cochée`
  L'état de boucle du port est cohérent. Le port reçoit des STP-BPDU.

Trans. into loop

Affiche le nombre de fois où l'état de boucle du port est devenu incohérent (case cochée dans la colonne *Loop state*).

Trans. out of loop

Affiche le nombre de fois où l'état de boucle du port est devenu cohérent (case décochée dans la colonne *Loop state*).

BPDU guard effect

Affiche si le port a reçu une STP-BPDU en tant que port marginal.

Condition préalable :

- Le port est un port marginal spécifié manuellement. Dans la boîte de dialogue *Port*, la case dans la colonne *Admin edge port* est `cochée` pour ce port.
- Dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*, la fonction BPDU Guard est activée.

Valeurs possibles :

- `case cochée`
  Le port est un port marginal et a reçu une STP-BPDU.
  L'équipement désactive le port. Pour ce port, dans la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*, la case dans la colonne *Port on* est `décochée`.
- `case non cochée`
  Le port est un port marginal et n'a reçu aucune STP-BPDU, ou bien le port n'est pas un port marginal.

Pour réinitialiser l'état du port à la valeur `forwarding`, procédez comme suit :

- ☐ Si le port reçoit toujours des BPDU :
  - Dans l'onglet *CIST*, décochez la case dans la colonne *Admin edge port*.
    ou
  - Dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*, décochez la case *BPDU guard*.
- ☐ Pour activer le port, procédez comme suit :
  - Ouvrez la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.
  - Cochez la case dans la colonne *Port on*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.10.4 Link Aggregation

[Switching > L2-Redundancy > Link Aggregation]

⚠ 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.

La fonction *Link Aggregation* vous permet d'agréger plusieurs liaisons parallèles. La condition préalable est que les liaisons aient la même vitesse et soient full duplex. Les avantages par rapport aux liaisons gérées utilisant une ligne unique sont une tolérance fautive plus importante et une bande passante de transmission supérieure.

Link Aggregation Control Protocol (LACP) permet de surveiller l'état continu du lien basé sur des paquets sur les ports physiques. LACP permet également de s'assurer que les partenaires de la liaison satisfont aux conditions préalables en matière d'agrégation.

Si le côté distant ne prend pas en charge Link Aggregation Control Protocol (LACP), vous pouvez utiliser la fonction *Static link aggregation*. Dans ce cas, l'équipement agrège les liaisons sur la base de la liaison, de la vitesse de la liaison et du réglage duplex.

Table

Trunk port

Affiche le numéro d'interface LAG.

Name

Spécifie le nom de l'interface LAG.

Valeurs possibles :

- Chaîne de 1..15 caractères ASCII alphanumériques

Link/Status

Affiche l'état opérationnel actuel de l'interface LAG et des ports physiques.

Valeurs possibles :

- *up* (ligne `lag/…`)
  L'interface LAG est opérationnelle.
  Les conditions préalables sont :
  - La fonction *Static link aggregation* est activée sur cette interface LAG.
    ou
  - LACP est activé sur les ports physiques affectés à l'interface LAG, voir la colonne *LACP active*.
    et
    La clé spécifiée pour l'interface LAG dans la colonne *LACP admin key* correspond aux clés spécifiées pour les ports physiques dans la colonne *LACP port actor admin key*.
    et
    Le nombre de ports physiques opérationnels affectés à l'interface LAG est supérieur ou égal à la valeur spécifiée dans la colonne *Active ports (min.)*.
- *up*
  Le port physique est opérationnel.
- *down* (ligne `lag/…`)
  L'interface LAG est inopérationnelle.
- *down*
  Le port physique est désactivé.
  ou
  Aucun câble de données n'est connecté ou aucune liaison n'est activée.

Active

Active/désactive l'interface LAG.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'interface LAG est activée.
  Tenez compte du fait que les protocoles suivants ne fonctionnent pas correctement sur les ports physiques lorsque vous activez l'interface LAG :
  - *PTP*
  - *802.1AS*
- `case non cochée`
  L'interface LAG est désactivée.

STP active

Active/désactive le protocole *Spanning Tree* sur cette interface LAG. La condition préalable est l'activation de la fonction *Spanning Tree* de manière globale dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*.

Vous pouvez aussi activer/désactiver le protocole *Spanning Tree* sur les interfaces LAG dans la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Port*.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  Le protocole *Spanning Tree* est activé sur cette interface LAG.
- `case non cochée`
  Le protocole *Spanning Tree* est désactivé sur cette interface LAG.

Static link aggregation

Active/désactive la fonction *Static link aggregation* sur l'interface LAG. L'équipement agrège les ports physiques affectés sur l'interface LAG, même si le site distant ne prend pas en charge LACP.

Valeurs possibles :

- `case cochée`
  La fonction *Static link aggregation* est activée sur cette interface LAG. L'équipement agrège un port physique affecté sur l'interface LAG dès que le port physique établit une liaison. L'équipement n'envoie pas de LACPDU et rejette les LACPDU reçues.
- `case non cochée` (réglage par défaut)
  La fonction *Static link aggregation* est désactivée sur cette interface LAG. Si la liaison a été négociée avec succès à l'aide de LACP, l'équipement agrège un port physique affecté sur l'interface LAG.

MTU

Spécifie la taille maximum admissible des paquets Ethernet sur l'interface LAG en octets. Les éventuels tags de VLAN ne sont pas pris en compte.

Ce réglage vous permet d'augmenter la taille des paquets Ethernet pour des applications spécifiques.

Valeurs possibles :

- `1518..9720` (réglage par défaut : `1518`)
  Avec la valeur `1518`, l'interface LAG transmet les paquets Ethernet jusqu'à la taille suivante :
  - 1518 octets sans tag de VLAN
    (1514 octets + 4 octets CRC)
  - 1522 octets avec tag de VLAN
    (1518 octets + 4 octets CRC)

Active ports (min.)

Spécifie le nombre minimum de ports physiques activés pour que l'interface LAG reste activée. Si le nombre de ports physiques activés est inférieur à la valeur spécifiée, l'équipement désactive l'interface LAG.

Si une fonction de redondance comme *Spanning Tree* ou *MRP* over LAG est activée dans l'équipement, utilisez cette fonction pour forcer l'équipement à basculer automatiquement sur la ligne redondante.

Valeurs possibles :

- `1` (réglage par défaut)
- `2`
- En fonction du matériel :
  `4`
  `8`
  `32`

Type

Affiche si l'interface LAG est basée sur la fonction *Static link aggregation* ou sur LACP.

Valeurs possibles :

- `static`
  L'interface LAG est basée sur la fonction *Static link aggregation*.
- `dynamic`
  L'interface LAG est basée sur LACP.

Send trap (Link up/down)

Active/désactive l'envoi de traps SNMP lorsque l'équipement détecte un changement dans l'état up/down du lien pour cette interface.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'envoi de traps SNMP est activé.
  Si l'équipement détecte un changement d'état up/down du lien, l'équipement envoie un trap SNMP.
- `case non cochée`
  L'envoi de traps SNMP est désactivé.

Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

LACP admin key

Spécifie la clé de l'interface LAG. L'équipement utilise cette clé pour identifier les ports qui peuvent être agrégés sur l'interface LAG.

Valeurs possibles :

- `0..65535`
  Vous spécifiez la valeur correspondante pour les ports physiques dans la colonne *LACP port actor admin key*.

Port

Affiche les numéros des ports physiques affectés à l'interface LAG.

Aggregation port status

Affiche si l'interface LAG agrège le port physique.

Valeurs possibles :

- `active`
  L'interface LAG agrège le port physique.
- `inactive`
  L'interface LAG n'agrège pas le port physique.

LACP active

Active/désactive LACP sur le port physique.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  LACP est activé sur le port physique.
- `case non cochée`
  LACP est désactivé sur le port physique.

LACP port actor admin key

Spécifie la clé du port physique. L'équipement utilise cette clé pour identifier les ports qui peuvent être agrégés sur l'interface LAG.

Valeurs possibles :

- `0`
  L'équipement ignore la clé sur ce port physique lorsqu'il décide d'agréger le port sur l'interface LAG.
- `1..65535`
  Si cette valeur correspond à la valeur de l'interface LAG spécifiée dans la colonne *LACP admin key*, l'équipement agrège uniquement ce port physique sur l'interface LAG.

LACP actor admin state

Spécifie les valeurs d'état actor que l'interface LAG transmet dans les LACPDU. Cela vous permet de contrôler les paramètres LACPDU.

L'équipement vous permet de mélanger les valeurs. Dans la liste déroulante, sélectionnez une ou plusieurs valeurs.

Valeurs possibles :

- *ACT*
  (état `LACP_Activity`)
  Lorsque cette valeur est sélectionnée, la liaison transmet les LACPDU de manière cyclique, ou sinon à la demande.
- *STO*
  (état `LACP_Timeout`)
  Lorsque cette valeur est sélectionnée, la liaison transmet les LACPDU de manière cyclique à l'aide de la temporisation courte, ou sinon à l'aide de la temporisation longue.
- *AGG*
  (état `Aggregation`)
  Lorsque cette valeur est sélectionnée, l'équipement interprète la liaison comme étant un candidat à l'agrégation, sinon comme une liaison individuelle.

Pour plus d'informations sur les valeurs, voir la norme technique IEEE 802.1AX-2014.

LACP actor oper state

Affiche les valeurs de l'état actor que l'interface LAG transmet dans les LACPDU.

Valeurs possibles :

- *ACT*
  (état `LACP_Activity`)
  Lorsque cette valeur est visible, la liaison transmet les LACPDU de manière cyclique, ou sinon à la demande.

- *STO*
  (état `LACP_Timeout`)
  Lorsque cette valeur est visible, la liaison transmet les LACPDU de manière cyclique à l'aide de la temporisation courte, ou sinon à l'aide de la temporisation longue.
- *AGG*
  (état `Aggregation`)
  Lorsque cette valeur est visible, l'équipement interprète la liaison comme étant un candidat à l'agrégation, sinon comme une liaison individuelle.
- *SYN*
  (état `Synchronization`)
  Lorsque cette valeur est visible, l'équipement interprète la liaison comme `IN_SYNC`, ou sinon comme `OUT_OF_SYNC`.
- *COL*
  (état `Collecting`)
  Lorsque cette valeur est visible, la collecte des trames entrantes est activée sur cette liaison, ou sinon elle est désactivée.
- *DST*
  (état `Distributing`)
  Lorsque cette valeur est visible, la distribution des trames sortantes est activée sur cette liaison, ou sinon elle est désactivée.
- *DFT*
  (état `Defaulted`)
  Lorsque cette valeur est visible, la liaison utilise les informations opérationnelles par défaut, spécifiées administrativement pour le Partner. Sinon, la liaison utilise les informations opérationnelles reçues d'une LACPDU.
- *EXP*
  (état `Expired`)
  Lorsque cette valeur est visible, le lien récepteur est à l'état `EXPIRED`

LACP partner oper SysID

Affiche l'adresse MAC de l'équipement distant connecté à ce port physique.

L'interface LAG a reçu ces informations dans une LACPDU du partner.

LACP partner oper port

Affiche le numéro de port de l'équipement distant connecté à ce port physique.

L'interface LAG a reçu ces informations dans une LACPDU du partner.

LACP partner oper port state

Affiche les valeurs d'état partner que l'interface LAG reçoit dans les LACPDU.

Valeurs possibles :

- *ACT*
- *STO*
- *AGG*
- *SYN*
- *COL*
- *DST*

- *DFT*
- *EXP*

Pour plus d'informations sur les valeurs, voir la description de la colonne *LACP actor oper state* et la norme technique IEEE 802.1AX-2014.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée d'interface LAG dans la table ou pour affecter un port physique à une interface LAG.

- Dans la liste déroulante *Trunk port*, vous sélectionnez le numéro d'interface LAG.
- Dans la liste déroulante *Port*, vous sélectionnez le numéro d'un port physique à affecter à l'interface LAG.

Après avoir créé une interface LAG, l'équipement ajoute l'interface LAG à la table dans la boîte de dialogue *Basic Settings > Port*, onglet *Statistics*.

5.10.5 Link Backup

[Switching > L2-Redundancy > Link Backup]

⚠ 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.

Avec Link Backup, vous configurez des paires de liaisons redondantes. Chaque paire dispose d'un port principal et d'un port de secours. Le port principal transfère le trafic jusqu'à ce que l'équipement détecte une erreur. Si l'équipement détecte une erreur sur le port principal, la fonction Link Backup transfère le trafic au port de secours.

La boîte de dialogue vous permet de définir une option de retour. Si vous activez la fonction de retour et que le port principal 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.

Operation

Operation

Active/désactive la fonction Link Backup de manière globale dans l'équipement.

Valeurs possibles :

- `On`
  Active la fonction Link Backup.
- `Off` (réglage par défaut)
  Désactive la fonction Link Backup.

Table

Primary port

Affiche le port principal de la paire de l'interface. Lorsque vous activez la fonction Link Backup, ce port est chargé de transférer le trafic.

Valeurs possibles :

- Ports physiques

Backup port

Affiche le port de secours sur lequel l'équipement transfère le trafic si l'équipement détecte une erreur sur le port principal.

Valeurs possibles :

- Ports physiques, à l'exception du port que vous définissez comme étant le port principal.

Description

Spécifie la paire Link Backup. Saisissez un nom pour identifier la paire Link Backup.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

Primary port status

Affiche l'état du port principal pour cette paire Link Backup.

Valeurs possibles :

- *forwarding*
  La liaison est up, pas d'interruption et transfert du trafic.
- *blocking*
  La liaison est up, pas d'interruption et blocage du trafic.
- *down*
  La liaison du port est down, le câble de données est débranché ou le port est désactivé dans le logiciel, interruption.
- *unknown*
  La fonctionnalité Line Backup est désactivée de manière globale, ou la paire de ports est désactivée. L'équipement ignore les réglages de la paire de ports

Backup port status

Affiche l'état du port de secours pour cette paire Link Backup.

Valeurs possibles :

- *forwarding*
  La liaison est up, pas d'interruption et transfert du trafic.
- *blocking*
  La liaison est up, pas d'interruption et blocage du trafic.

- *down*
  La liaison du port est down, le câble de données est débranché ou le port est désactivé dans le logiciel, interruption.
- *unknown*
  La fonctionnalité Line Backup est désactivée de manière globale, ou la paire de ports est désactivée. L'équipement ignore les réglages de la paire de ports

Fail back

Active/désactive le retour automatique.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  Le retour automatique est activé.
  Une fois le temporisateur à échéance, le port de secours passe sur *blocking* et le port principal passe sur *forwarding*.
- `case non cochée`
  Le retour automatique est désactivé.
  Le port de secours continue de transférer le trafic même après que le port principal a rétabli une liaison ou que vous avez changé manuellement l'état du port principal de `shutdown` à `no shutdown`.

Fail back delay [s]

Spécifie le délai en secondes durant lequel l'équipement attend après que le port principal a rétabli une liaison. De plus, ce temporisateur s'applique aussi lorsque vous changez manuellement l'état du port principal de `shutdown` à `no shutdown`. Une fois le temporisateur à échéance, le port de secours passe sur *blocking* et le port principal passe sur *forwarding*.

Valeurs possibles :

- `0..3600` (réglage par défaut : `30`)
  Lorsqu'il est défini sur `0`, immédiatement après que le port principal a rétabli une liaison, le port de secours passe à *blocking* et le port principal passe à *forwarding*. De plus, immédiatement après que vous avez changé manuellement l'état de `shutdown` à `no shutdown`, le port de secours passe à *blocking* et le port principal passe à *forwarding*.

Active

Active/désactive la configuration de la paire Link Backup.

Valeurs possibles :

- `case cochée`
  La paire Link Backup est active. L'équipement détecte la liaison et l'état d'administration et transfère le trafic en fonction de la configuration de la paire.
- `case non cochée` (réglage par défaut)
  La paire Link Backup est désactivée. Les ports transfèrent le trafic selon la commutation standard.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Create

Primary port

Spécifie le port principal de la paire de l'interface de secours. Dans le cadre d'une utilisation normale, ce port est chargé de transférer le trafic.

Valeurs possibles :

- Ports physiques

Backup port

Spécifie le port de secours sur lequel l'équipement transfère le trafic si l'équipement détecte une erreur sur le port principal.

Valeurs possibles :

- Ports physiques, à l'exception du port que vous définissez comme étant le port principal.

5.10.6 FuseNet

[Switching > L2-Redundancy > FuseNet]

Les protocoles *FuseNet* vous permettent de couples des anneaux fonctionnant avec l'un des protocoles de redondance suivants :

- MRP
- HIPER Ring
- RSTP

Commentaire : Si vous utilisez le protocole *Ring/Network Coupling* pour coupler des réseaux, vérifiez que les réseaux ne contiennent que des équipements Schneider Electric.

Utilisez la table suivante pour sélectionner 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*

– aucun protocole de couplage adapté

1) avec *MRP* configuré sur différents VLAN

Le menu contient les boîtes de dialogue suivantes :

- Sub Ring
- Ring/Network Coupling
- Redundant Coupling Protocol (MCSESM-E)

5.10.6.1 Sub Ring

[Switching > L2-Redundancy > FuseNet > Sub Ring]

⚠ 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.

Cette boîte de dialogue vous permet de définir l'équipement en tant gestionnaire de sous-anneau.

La fonction *Sub Ring* vous permet de coupler facilement des segments de réseau à des couplages d'anneaux redondants. Le gestionnaire de sous-anneau (SRM) couple un sous-anneau à un anneau existant (anneau de base).

Dans le sous-anneau, vous pouvez utiliser tout équipement prenant en charge MRP en tant que participant à l'anneau. Ces équipement ne nécessitent pas de gestionnaire de sous-anneau.

Lorsque vous définissez des sous-anneaux, appliquez les règles suivantes :
- L'équipement prend en charge *Link Aggregation* dans le sous-anneau
- Pas de Spanning Tree sur les ports du sous-anneau
- *MRP domain* identique sur les équipement au sein d'un sous-anneau
- VLAN différents pour l'anneau de base et le sous-anneau

Spécifiez les réglages de VLAN comme suit :
- VLAN `X` pour anneau de base
  - sur les ports d'anneau des participants à l'anneau de base
  - sur les ports de l'anneau de base du gestionnaire de sous-anneau
- VLAN `Y` pour sous-anneau
  - sur les ports d'anneau des participants au sous-anneau
  - sur les ports de sous-anneau du gestionnaire de sous-anneau

Commentaire : Pour éviter les boucles, fermez simplement la ligne redondante lorsque les réglages sont spécifiés pour chaque équipement participant à l'anneau.

Operation

Operation

Active/désactive la fonction *Sub Ring*.

Valeurs possibles :

- `On`
  La fonction *Sub Ring* est activée.
- `Off` (réglage par défaut)
  La fonction *Sub Ring* est désactivée.

Information

Table entries (max.)

Affiche le nombre maximum de sous-anneaux pris en charge par l'équipement.

Table

Sub ring ID

Affiche l'identifiant unique de ce sous-anneau.

Valeurs possibles :

- `1..8`

Name

Spécifie le nom facultatif du sous-anneau.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

Active

Active/désactive le sous-anneau.

Active le sous-anneau lorsque la configuration de chaque équipement du sous-anneau est terminée. Fermez le sous-anneau uniquement après avoir activé la fonction *Sub Ring*.

Valeurs possibles :

- `case cochée`
  Le sous-anneau est activé.
- `case non cochée` (réglage par défaut)
  Le sous-anneau est désactivé.

Configuration status

Affiche l'état opérationnel de la configuration du sous-anneau

Valeurs possibles :

- *noError*
  L'équipement détecte une configuration de sous-anneau acceptable.
- *ringPortLinkError*
  - Le port d'anneau n'a pas de liaison.
  - L'une de lignes du sous-anneau est connectée à un port supplémentaire de l'équipement. Néanmoins, la ligne du sous-anneau n'est pas connectée à l'un des ports d'anneau de l'équipement.
- *multipleSRM*
  Le gestionnaire de sous-anneau reçoit des paquets de plusieurs gestionnaires de sous-anneau dans le sous-anneau.
- *noPartnerManager*
  Le gestionnaire de sous-anneau reçoit ses propres trames.

- *concurrentVLAN*
  Le protocole MRP dans l'anneau de base utilise le VLAN du domaine du gestionnaire de sous-anneau.
- *concurrentPort*
  Un protocole de redondance supplémentaire utilise le port d'anneau du domaine du gestionnaire de sous-anneau.
- *concurrentRedundancy*
  Le domaine du gestionnaire de sous-anneau est désactivé en raison d'un autre protocole de redondance activé.
- *trunkMember*
  Le port d'anneau du domaine du gestionnaire de sous-anneau est membre d'une liaison *Link Aggregation*.
- *sharedVLAN*
  Le domaine du gestionnaire de sous-anneau est désactivé parce que le VLAN partagé est activé et que l'anneau principal utilise également le protocole MRP.

Redundancy available

Affiche l'état opérationnel de la redondance d'anneau dans le sous-anneau.

Valeurs possibles :

- *redGuaranteed*
  Une réserve de redondance est disponible.
- *redNotGuaranteed*
  Perte de la réserve de redondance.

Port

Spécifie le port qui connecte l'équipement au sous-anneau.

Valeurs possibles :

- <Numéro de port>

SRM mode

Spécifie le mode du gestionnaire de sous-anneau.

Un sous-anneau dispose simultanément de 2 gestionnaires qui couplent le sous-anneau à l'anneau de base. Tant que le sous-anneau est physiquement fermé, un gestionnaire bloque son port de sous-anneau.

Valeurs possibles :

- *manager* (réglage par défaut)
  Le port de sous-anneau transfère des paquets de données.
  Lorsque cette valeur est définie sur les deux équipements qui couplent le sous-anneau à l'anneau de base, l'équipement avec l'adresse MAC la plus élevée fonctionne en tant que *redundantManager*.

- *redundantManager*
  Le port de sous-anneau est bloqué alors que le sous-anneau est physiquement fermé. Si le sous-anneau est interrompu, le port de sous-anneau transmet les paquets de données. Lorsque cette valeur est définie sur les deux équipements qui couplent le sous-anneau à l'anneau de base, l'équipement avec l'adresse MAC la plus élevée fonctionne en tant que *redundantManager*.
- *singleManager*
  Utilisez cette valeur lorsque le sous-anneau est couplé à l'anneau de base via un seul équipement. La condition requise est que la table contienne 2 instances du sous-anneau. Affectez cette valeur aux deux instances. Le port du sous-anneau de l'instance avec le numéro de port le plus élevé est bloqué alors que le sous-anneau est physiquement fermé.

SRM status

Affiche le mode actuel du gestionnaire de sous-anneau.

Valeurs possibles :

- *manager*
  Le port de sous-anneau transfère des paquets de données.
- *redundantManager*
  Le port de sous-anneau est bloqué alors que le sous-anneau est physiquement fermé. Si le sous-anneau est interrompu, le port de sous-anneau transmet les paquets de données.
- *singleManager*
  Le sous-anneau est couplé à l'anneau de base via un seul équipement. Le port du sous-anneau de l'instance avec le numéro de port le plus élevé est bloqué alors que le sous-anneau est physiquement fermé.
- *disabled*
  Le sous-anneau est désactivé.

Port status

Affiche l'état du lien du port de sous-anneau.

Valeurs possibles :

- *forwarding*
  Le port transmet des trames conformément au comportement de transmission décrit dans IEEE 802.1D.
- *disabled*
  Le port rejette toutes les trames.
- *blocked*
  Le port rejette toutes les trames à l'exception des cas suivants :
  - Le port transmet les trames utilisées par le protocole d'anneau sélectionné spécifié pour passer les ports bloqués.
  - Le port transmet les trames d'autres protocoles spécifiés pour passer les ports bloqués.
- *not-connected*
  La liaison du port est down.

VLAN

Spécifie le VLAN auquel ce sous-anneau est affecté. S'il n'existe aucun VLAN pour le VLAN-ID saisi, l'équipement le crée automatiquement.

Valeurs possibles :

- VLAN configurés disponibles (réglage par défaut : `0`)
  Si vous ne souhaitez pas utiliser un VLAN distinct pour ce sous-anneau, laissez l'entrée avec la valeur 0.

Partner MAC

Affiche l'adresse MAC du gestionnaire de sous-anneau à l'autre extrémité du sous-anneau.

MRP domain

Spécifie le domaine MRP du gestionnaire de sous-anneau. Affectez le même nom de domaine MRP à chaque membre d'un sous-anneau. Si vous n'utilisez que des équipements Schneider Electric, utilisez la valeur par défaut pour le domaine MRP ; sinon, ajustez la valeur si nécessaire. Avec plusieurs sous-anneaux, la fonction vous permet d'utiliser le même nom de domaine MRP pour les sous-anneaux.

Valeurs possibles :

- Noms de domaine MRP autorisés (réglage par défaut : `255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255`)

Protocol

Spécifie le protocole.

Valeurs possibles :

- *`iec-62439-mrp`*

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

5.10.6.2 Ring/Network Coupling

[Switching > L2-Redundancy > FuseNet > 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.

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Vous utilisez la fonction *Ring/Network Coupling* pour coupler de manière redondante un HIPER Ring, un MRP Ring ou un Fast HIPER Ring existant à un autre réseau ou anneau. Vérifiez que les partenaires de couplage sont des équipements Schneider Electric.

Commentaire : Avec le couplage à deux commutateurs, vérifiez que vous avez configuré un HIPER Ring, un MRP Ring ou un Fast HIPER Ring avant de configurer la fonction *Ring/Network Coupling*.

Dans la boîte de dialogue *Ring/Network Coupling*, vous pouvez effectuer les tâches suivantes :
- afficher une vue d'ensemble du *Ring/Network Coupling* existant
- configurer un *Ring/Network Coupling*
- créer un nouveau *Ring/Network Coupling*
- supprimer un *Ring/Network Coupling*
- Activer/désactiver *Ring/Network Coupling*

Lors de la configuration des ports de couplage, spécifiez les réglages suivants dans la boîte de dialogue *Basic Settings > Port* :

Type de port	Débit	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	`case cochée`	`case non cochée`	*100 Mbit/s FDX*
TX	1 Gbit/s	`case cochée`	`case cochée`	–
Optical	100 Mbit/s	`case cochée`	`case non cochée`	*100 Mbit/s FDX*
Optical	1 Gbit/s	`case cochée`	`case cochée`	–
Optique	2.5 Gbit/s	`case cochée`	–	*2.5 Gbit/s FDX*

Commentaire : Les modes opérationnels du port actuellement disponibles dépendent de la configuration de l'équipement.

Si vous avez configuré des VLAN, notez la configuration de VLAN du couplage et des ports de couplage partenaires. Dans la configuration *Ring/Network Coupling*, sélectionnez les valeurs suivantes pour le couplage et les ports de couplage partenaires :
- `VLAN ID 1` et *Ingress filtering* désactivés dans la table de port
- Appartenance VLAN `T` dans la table *VLAN Configuration*

Indépendamment des réglages de VLAN, l'équipement envoie les trames de couplage d'anneau avec le `VLAN ID 1` et la priorité `7`. Vérifiez que l'équipement envoie des trames VLAN 1 taggées dans l'anneau local et dans le réseau connecté. Le taggage des trames de VLAN gère la priorité des trames de couplage d'anneaux.

La fonction *Ring/Network Coupling* utilise des paquets de test. Les équipements envoient leurs paquets de test avec un tag de VLAN, y compris le VLAN-ID `1` et la priorité de VLAN la plus élevée `7`. Si le port de transfert est un membre du VLAN `1` et transmet les paquets de données sans tag de VLAN, l'équipement envoie aussi des paquets de test.

Operation

Operation

Active/désactive la fonction *Ring/Network Coupling*.

Valeurs possibles :

- `On`
  La fonction *Ring/Network Coupling* est activée.
- `Off` (réglage par défaut)
  La fonction *Ring/Network Coupling* est désactivée.

Mode

Type

Spécifie la méthode utiliser pour coupler les réseaux ensemble.

Valeurs possibles :

- `one-switch coupling`
  Vous permet de spécifier les réglages de port dans les trames *Coupling port* et *Partner coupling port*.
- `two-switch coupling, master`
  Vous permet de spécifier les réglages de port dans la trame *Coupling port*.
- `two-switch coupling, slave`
  Vous permet de spécifier les réglages de port dans la trame *Coupling port*.
- `two-switch coupling with control line, master`
  Vous permet de spécifier les réglages de port dans les trames *Coupling port* et *Control port*.
- `two-switch coupling with control line, slave`
  Vous permet de spécifier les réglages de port dans les trames *Coupling port* et *Control port*.

Coupling port

Port

Spécifie le port auquel vous raccordez la liaison redondante.

Valeurs possibles :

- `-`
  Aucun port sélectionné.
- `<Numéro de port>`

Si vous avez également configuré des ports d'anneau, spécifiez les ports de couplage et d'anneau sur les différents ports.

Pour éviter des boucles continues, l'équipement désactive le port de couplage dans les cas suivants :

- désactivation de la fonction
- modification de la configuration alors que des liaisons sont opérationnelles sur les ports

Lorsque l'équipement a désactivé le port de couplage, la case *Port on* est décochée dans la boîte de dialogue *Basic Settings > Port*, onglet *Configuration*.

State

Affiche l'état du port sélectionné.

Valeurs possibles :

- *active*
  Le port est activé.
- *standby*
  Le port est en mode standby.
- *not-connected*
  Le port n'est pas connecté.
- *not-applicable*
  Le port est incompatible avec le mode de contrôle configuré.

Partner coupling port

Port

Spécifie le port sur lequel vous raccordez le port partenaire.

Valeurs possibles :

- `-`
  Aucun port sélectionné.
- `<Numéro de port>`

Si vous avez également configuré des ports d'anneau, spécifiez les ports de couplage et d'anneau sur les différents ports.

State

Affiche l'état du port sélectionné.

Valeurs possibles :

- *active*
  Le port est activé.
- *standby*
  Le port est en mode standby.
- *not-connected*
  Le port n'est pas connecté.
- *not-applicable*
  Le port est incompatible avec le mode de contrôle configuré.

IP address

Affiche l'adresse IP du partenaire lorsque les équipements sont connectés.

La condition préalable est que vous sélectionniez une méthode de couplage à deux commutateurs et que vous activiez le partenaire dans le réseau.

Control port

Port

Affiche le port sur lequel vous raccordez la ligne de contrôle.

Valeurs possibles :

- -
  Aucun port sélectionné.
- <Numéro de port>

State

Affiche l'état du port sélectionné.

Valeurs possibles :

- *active*
  Le port est activé.
- *standby*
  Le port est en mode standby.
- *not-connected*
  Le port n'est pas connecté.
- *not-applicable*
  Le port est incompatible avec le mode de contrôle configuré.

Configuration

Redundancy mode

Spécifie si l'équipement répond à une défaillance détectée dans l'anneau ou le réseau distant.

Valeurs possibles :

- *redundant ring/network coupling*
  La ligne principale ou la ligne redondante est active. Les deux lignes ne sont pas actives simultanément. Si l'équipement détecte que le lien est down entre les équipements dans le réseau connecté, l'équipement en standby maintient le port redondant en mode standby.
- *extended redundancy*
  La ligne principale et la ligne redondante sont actives simultanément. Si l'équipement détecte un problème dans la liaison entre les équipements dans le réseau connecté, l'équipement en standby transfère les données sur le port redondant. Avec le réglage, vous pouvez maintenir la continuité dans le réseau distant.

Commentaire : Durant la période de reconfiguration, des dédoublements de paquets peuvent se produire. Aussi, si votre application est capable de détecter les dédoublements de paquets, vous pouvez sélectionner ce réglage.

Coupling mode

Spécifie le mode de couplage d'un type spécifique de réseau.

Valeurs possibles :

- *ring coupling*
  L'équipement couple des anneaux redondants. L'équipement vous permet de coupler des anneaux qui utilisent les protocoles de redondance suivants :
  - HIPER Ring
  - Fast HIPER ring
  - MRP ring
- *network coupling*
  L'équipement couple des segments de réseau. La fonction vous permet de coupler ensemble des réseaux maillés et des réseaux en bus.

Information

Redundancy available

Affiche si la redondance est disponible.

Lorsqu'un composant de l'anneau est défaillant, la ligne redondante prend le relais.

Valeurs possibles :

- *redGuaranteed*
  La redondance est disponible.
- *redNotGuaranteed*
  La redondance n'est pas disponible.

Configuration failure

Vous avez configuré la fonction de manière incorrecte ou la liaison du port d'anneau n'est pas disponible.

Valeurs possibles :

- *noError*
- *slaveCouplingLinkError*
  La ligne de couplage n'est pas connectée au port de couplage de l'équipement esclave. En revanche, la ligne de couplage est connectée à un autre port de l'équipement esclave.
- *slaveControlLinkError*
  Le port de contrôle de l'équipement esclave n'a pas de liaison de données.
- *masterControlLinkError*
  La ligne de contrôle n'est pas connectée au port de contrôle de l'équipement maître. En revanche, la ligne de contrôle est connectée à un autre port de l'équipement maître.
- *twoSlaves*
  La ligne de contrôle connecte deux équipements esclaves.
- *localPartnerLinkError*
  La ligne de couplage partenaire n'est pas connectée au port de couplage partenaire de l'équipement esclave. En revanche, la ligne de couplage partenaire est connectée à un autre port de l'équipement esclave en mode *one-switch coupling*.
- *localInvalidCouplingPort*
  En mode *one-switch coupling*, la ligne de couplage n'est pas connectée sur le même équipement que la ligne partenaire. En revanche, la ligne de couplage est connectée à un autre équipement.
- *couplingPortNotAvailable*
  Le port de couplage n'est pas disponible parce que le module auquel le port se rapporte n'est pas disponible ou parce que le port n'existe pas sur ce module.
- *controlPortNotAvailable*
  Le port de contrôle n'est pas disponible parce que le module auquel le port se réfère n'est pas disponible ou parce que le port n'existe pas sur ce module.
- *partnerPortNotAvailable*
  Le port de couplage partenaire n'est pas disponible parce que le module auquel le port se rapporte n'est pas disponible ou parce que le port n'existe pas sur ce module.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Désactive la fonction de redondance et réinitialise les paramètres par défaut dans la boîte de dialogue.

5.10.6.3 Redundant Coupling Protocol (MCSESM-E)

⚠ 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.

⚠ 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.

Une topologie en anneau fournit des délais de transition courts avec une utilisation minimale des ressources. Toutefois, coupler ces anneaux de manière redondante à un réseau de niveau supérieur s'avère une tâche ardue.

Si vous souhaitez utiliser un protocole standard tel que MRP pour la redondance d'anneau et RSTP pour coupler les anneaux, *Redundant Coupling Protocol* vous offre des options.

N'utilisez pas les protocoles de redondance suivants sur les ports de l'anneau principal *RCP* et des anneaux secondaires *RCP* :

- *Sub Ring*
- *Ring/Network Coupling*

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 spécifiez les réglages de la fonction *Dual RSTP* dans la boîte de dialogue *Switching > L2-Redundancy*.

Si vous configurez la fonction *RCP* dans un réseau et que la configuration n'est pas terminée, il est possible que les équipement déconnectent temporairement l'anneau secondaire et l'anneau principal. Dans ce cas, l'administration de l'équipement des commutateurs *RCP* ne peut pas être atteinte depuis l'anneau secondaire. Durant cette phase de configuration, connectez votre station d'administration réseau à l'anneau principal.

Operation

Operation

Active/désactive la fonction *RCP*.

Valeurs possibles :

- *On*
  La fonction *RCP* est activée.
- *Off* (réglage par défaut)
  La fonction *RCP* est désactivée.

Primary ring/network / Secondary ring/network

Si l'équipement opère en tant qu'esclave (la valeur dans le champ *Role* est *slave*, n'activez pas le mode *Static query port* pour les ports sur l'anneau/le réseau secondaire.

Inner port

Spécifie le numéro de port interne dans l'anneau principal/secondaire. Le port est directement connecté au commutateur partenaire.

Valeurs possibles :

- - (réglage par défaut)
  Aucun port sélectionné.
- <Numéro de port>

Outer port

Spécifie le numéro de port externe dans l'anneau principal/secondaire.

Valeurs possibles :

- - (réglage par défaut)
  Aucun port sélectionné.
- <Numéro de port>

Primary Ring protocol/Secondary Ring protocol

Affiche le protocole qui est activé sur le port de couplage redondant dans les équipements dans l'anneau principal/secondaire.

Coupler configuration

Role

Spécifie le rôle de l'équipement local.

Valeurs possibles :

- `master`
  L'équipement fonctionne en tant que maître.
- `slave`
  L'équipement fonctionne en tant qu'esclave.
- `single`
  L'équipement couple 2 réseaux RSTP avec une instance *Dual RSTP* à l'aide d'un commutateur réseau.
- `auto` (réglage par défaut)
  L'équipement sélectionne automatiquement son rôle en tant que *master* ou *slave*.

Current role

Affiche le rôle actuel de l'équipement local. La valeur peut différer du rôle configuré :

- Si vous avez configuré les deux commutateurs partenaires en tant que `auto`, le commutateur partenaire qui couple actuellement les instances joue le rôle de `master`. L'autre commutateur partenaire joue le rôle de `slave`.
- Si les deux commutateurs partenaires sont configurés en tant que `master` ou en tant que `slave`, le commutateur partenaire avec la plus petite adresse MAC de base joue le rôle de `master`. L'autre commutateur partenaire joue le rôle de `slave`.
- Si le protocole est démarré et que le commutateur partenaire est introuvable pour un commutateur réseau dans le rôle configuré `master`, `slave` ou `auto`, le commutateur définit son propre rôle sur `listening`.
- Si l'équipement détecte un problème de configuration, par exemple si les ports d'anneau internes sont connectés de manière transversale, l'équipement définit son rôle sur `error`.

Timeout [ms]

Spécifie la durée maximum en millisecondes pendant laquelle l'équipement esclave attend des paquets de test de l'équipement maître sur les ports externes avant que l'équipement esclave ne procède au couplage. Cela ne s'applique que lorsque les deux ports internes de l'équipement esclave ont perdu la liaison à l'équipement maître.

Configurez la temporisation plus longue que la durée d'interruption la plus longue envisageable pour le protocole de redondance de l'instance plus rapide. Sinon, des boucles peuvent se produire.

Valeurs possibles :

- `5..60000` (réglage par défaut : `45`)

Partner MAC address

Affiche l'adresse MAC de base de l'équipement partenaire.

Partner IP address

Affiche l'adresse IP de l'équipement partenaire.

Coupling state

Affiche l'état de couplage de l'équipement local.

Valeurs possibles :

- *forwarding*
  Le couplage du port est à l'état de transfert.
- *blocking*
  Le couplage du port est à l'état de blocage.

Redundancy state

Affiche si la redondance est disponible.

Pour une configuration maître-esclave, les deux commutateurs réseau affichent ces informations.

Valeurs possibles :

- *redAvailable*
  La redondance est disponible.
- *redNotAvailable*
  La redondance n'est pas disponible.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6 Diagnostics

Le menu contient les boîtes de dialogue suivantes :

- Status Configuration
- System
- Email Notification
- Syslog
- Ports
- Loop Protection
- LLDP
- Report

6.1 Status Configuration

[Diagnostics > Status Configuration]

Le menu contient les boîtes de dialogue suivantes :

- Device Status
- Security Status
- Signal Contact
- MAC Notification
- Alarms (Traps)

6.1.1 Device Status

[Diagnostics > Status Configuration > Device Status]

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 affiche les erreurs détectées dans l'onglet *Status* et dans la boîte de dialogue *Basic Settings > System*, dans le cadre *Device Status*.

La boîte de dialogue contient les onglets suivants :
- [Global]
- [Port]
- [Status]

[Global]

Device status

Device status

Affiche l'état actuel de l'équipement. L'équipement détermine l'état à partir des paramètres individuels surveillés.

Valeurs possibles :

- *error*
  L'équipement affiche cette valeur pour indiquer une erreur détectée dans l'un des paramètres surveillés.
- *ok*

Traps

Send trap

Active/désactive l'envoi de traps SNMP lorsque l'équipement détecte un changement dans une fonction surveillée.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'envoi de traps SNMP est activé.
  Lorsque l'équipement détecte une modification dans les fonctions surveillées, l'équipement envoie un trap SNMP.
- `case non cochée`
  L'envoi de traps SNMP est désactivé.

Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

Table

Temperature

Active/désactive la surveillance de la température dans l'équipement.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque la température est supérieure ou inférieure à la limite spécifiée, la mention `error` est indiquée dans le cadre *Device status*.
- `case non cochée`
  La surveillance est désactivée.

Spécifiez les valeurs limites de la température dans les champs *Upper temp. limit [°C]* et *Lower temp. limit [°C]* de la boîte de dialogue *Basic Settings > System*.

Ring redundancy

Active/désactive la surveillance de la redondance d'anneau.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Dans le cadre *Device status*, la mention indiquée 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.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Connection errors

Active/désactive la surveillance d'état du lien du port/de l'interface.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  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`.
  Dans l'onglet *Port*, vous pouvez sélectionner les ports/interfaces devant faire l'objet d'une surveillance individuelle.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

External memory removal

Active/désactive la surveillance de la mémoire externe active.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Lorsque vous retirez la mémoire externe active de l'équipement, la mention indiquée dans le cadre *Device status* passe à `error`.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

External memory not in sync

Active/désactive la surveillance du profil de configuration de l'équipement et de la mémoire externe.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Dans le cadre *Device status*, la mention indiquée 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.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Power supply

Active/désactive la surveillance du bloc d'alimentation.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque l'équipement détecte une erreur de l'alimentation en tension, la mention indiquée dans le cadre *Device status* passe à `error`.
- `case non cochée`
  La surveillance est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Port]

Table

Port

Affiche le numéro de port.

Propagate connection error

Active/désactive la surveillance du lien du port/de l'interface.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Lorsque le lien est interrompu sur le port ou l'interface sélectionné, la mention indiquée dans le cadre *Device status* passe à `error`.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Ce réglage prend effet lorsque vous cochez la case *Connection errors* dans l'onglet *Global*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Status]

Table

Timestamp

Affiche la date et l'heure de l'évènement au format `Mois Jour, Année hh:mm:ss AM/PM`.

Cause

Affiche l'événement à l'origine du trap SNMP.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6.1.2 Security Status

[Diagnostics > Status Configuration > Security Status]

Cette boîte de dialogue fournit un aperçu de l'état des réglages de sécurité de l'équipement.

L'équipement affiche son état actuel en indiquant la mention `error` ou `ok` dans le cadre *Security status*. L'équipement détermine cet état à partir des résultats de surveillance individuels.

L'équipement affiche les erreurs détectées dans l'onglet *Status* et dans la boîte de dialogue *Basic Settings > System*, dans le cadre *Security status*.

La boîte de dialogue contient les onglets suivants :
- [Global]
- [Port]
- [Status]

[Global]

Security status

Security status

Affiche l'état actuel des réglages de sécurité de l'équipement. L'équipement détermine l'état à partir des paramètres individuels surveillés.

Valeurs possibles :

- `error`
  L'équipement affiche cette valeur pour indiquer une erreur détectée dans l'un des paramètres surveillés.
- `ok`

Traps

Send trap

Active/désactive l'envoi de traps SNMP lorsque l'équipement détecte un changement dans une fonction surveillée.

Valeurs possibles :

- `case cochée`
  L'envoi de traps SNMP est activé.
  Lorsque l'équipement détecte une modification dans les fonctions surveillées, l'équipement envoie un trap SNMP.
- `case non cochée` (réglage par défaut)
  L'envoi de traps SNMP est désactivé.

Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

Table

Password default settings unchanged

Active/désactive la surveillance du mot de passe pour les comptes d'utilisateurs `user` et `admin` créés localement.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque le mot de passe est défini sur le réglage par défaut pour les comptes d'utilisateur `user` ou `admin`, la mention indiquée dans le cadre *Security status* passe à `error`.
- `case non cochée`
  La surveillance est désactivée.

Définissez le mot de passe dans la boîte de dialogue *Device Security > User Management*.

Min. password length < 8

Active/désactive la surveillance de la stratégie *Min. password length*.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque la valeur de la stratégie *Min. password length* est inférieure à `8`, la mention indiquée dans le cadre *Security status* passe à `error`.
- `case non cochée`
  La surveillance est désactivée.

Spécifiez la stratégie *Min. password length* dans le cadre *Configuration* de la boîte de dialogue *Device Security > User Management*.

Password policy settings deactivated

Active/désactive la surveillance des réglages des stratégies relatives au mot de passe.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque la valeur d'au moins l'une des stratégies suivantes est inférieure à `1`, la mention indiquée dans le cadre *Security status* passe à `error`.
  - *Upper-case characters (min.)*
  - *Lower-case characters (min.)*
  - *Digits (min.)*
  - *Special characters (min.)*
- `case non cochée`
  La surveillance est désactivée.

Spécifiez les réglages de la stratégie dans le cadre *Password policy* de la boîte de dialogue *Device Security > User Management*.

User account password policy check deactivated

Active/désactive la surveillance de la fonction *Policy check*.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Lorsque la fonction *Policy check* est désactivée pour au moins un compte d'utilisateur, la mention indiquée dans le cadre *Security status* passe à `error`.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Activez la fonction *Policy check* dans la boîte de dialogue *Device Security > User Management*.

Telnet server active

Active/désactive la surveillance du serveur Telnet.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque vous activez le serveur Telnet, la mention indiquée dans le cadre *Security status* passe à `error`.
- `case non cochée`
  La surveillance est désactivée.

Désactivez/activez le serveur Telnet dans l'onglet *Telnet* de la boîte de dialogue *Device Security > Management Access > Server*.

HTTP server active

Active/désactive la surveillance du serveur HTTP.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque vous activez le serveur HTTP, la mention indiquée dans le cadre *Security status* passe à `error`.
- `case non cochée`
  La surveillance est désactivée.

Désactivez/activez le serveur HTTP dans l'onglet *HTTP* de la boîte de dialogue *Device Security* > Management Access > *Server*.

SNMP unencrypted

Active/désactive la surveillance du serveur SNMP.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque 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 la colonne *SNMP encryption type* de la boîte de dialogue *Device Security > User Management*.
- `case non cochée`
  La surveillance est désactivée.

Spécifiez les réglages de l'agent SNMP dans l'onglet *SNMP* de la boîte de dialogue *Device Security* > Management Access > *Server*.

Access to system monitor with serial interface possible

Active/désactive la surveillance du moniteur du système.

Lorsque le moniteur du système est activé, vous avez la possibilité de passer au moniteur du système via une connexion série.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Lorsque vous activez le moniteur du système, la mention indiquée dans le cadre *Security status* passe à `error`.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Activez/désactivez le moniteur du système dans la boîte de dialogue *Diagnostics > System > Selftest*.

Saving the configuration profile on the external memory possible

Active/désactive la surveillance du profil de configuration dans la mémoire externe.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Lorsque vous activez la sauvegarde du profil de configuration dans la mémoire externe, la mention indiquée dans le cadre *Security status* passe à `error`.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Activez/désactivez la sauvegarde du profil de configuration dans la mémoire externe dans la boîte de dialogue *Basic Settings > External Memory*.

Link interrupted on enabled device ports

Active/désactive la surveillance du lien sur les ports activés.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Lorsque le lien est interrompu sur un port activé, la mention indiquée dans le cadre *Security status* passe à `error`. Dans l'onglet *Port*, vous pouvez sélectionner les ports devant faire l'objet d'une surveillance individuelle.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Access with Ethernet Switch Configurator possible

Active/désactive la surveillance de la fonction Ethernet Switch Configurator.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque vous activez la fonction Ethernet Switch Configurator, la mention indiquée dans le cadre *Security status* passe à `error`.
- `case non cochée`
  La surveillance est désactivée.

Activez/désactivez la fonction Ethernet Switch Configurator dans la boîte de dialogue *Basic Settings > Network*.

Load unencrypted config from external memory

Active/désactive la surveillance du chargement des profils de configuration non chiffrés depuis la mémoire externe.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque les réglages permettent à l'équipement de charger un profil de configuration non chiffré depuis la mémoire externe, la mention indiquée dans le cadre *Security status* passe à `error`.
  Lorsque les conditions préalables suivantes sont remplies, le cadre *Security status* de la boîte de dialogue *Basic Settings > System*, affiche une alarme.
  - Le profil de configuration sauvegardé dans la mémoire externe est non chiffré.
    et
  - La colonne *Config priority* de la boîte de dialogue *Basic Settings > External Memory* présente la mention `first`.
- `case non cochée`
  La surveillance est désactivée.

IEC61850-MMS active

Active/désactive la surveillance de la fonction *IEC61850-MMS*.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque vous activez la fonction *IEC61850-MMS*, la mention indiquée dans le cadre *Security status* passe à `error`.
- `case non cochée`
  La surveillance est désactivée.

Activez/désactivez la fonction *IEC61850-MMS* dans la boîte de dialogue *Industrial Protocols* > IEC61850-MMS, cadre *Operation*.

Self-signed HTTPS certificate present

Active/désactive la surveillance du certificat HTTPS.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque le serveur HTTPS utilise un certificat numérique auto-créé, la mention indiquée dans le cadre *Security status* passe à `error`.
- `case non cochée`
  La surveillance est désactivée.

Modbus TCP active

Active/désactive la surveillance de la fonction *Modbus TCP*.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque vous activez la fonction *Modbus TCP*, la mention indiquée dans le cadre *Security status* passe à `error`.
- `case non cochée`
  La surveillance est désactivée.

Activez/désactivez la fonction *Modbus TCP* dans la boîte de dialogue *Advanced > Industrial Protocols >* Modbus TCP, cadre *Operation*.

EtherNet/IP active

Active/désactive la surveillance de la fonction *EtherNet/IP*.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque vous activez la fonction *EtherNet/IP*, la mention indiquée dans le cadre *Security status* passe à `error`.
- `case non cochée`
  La surveillance est désactivée.

Activez/désactivez la fonction *EtherNet/IP* dans la boîte de dialogue *Advanced > Industrial Protocols >* EtherNet/IP, cadre *Operation*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Port]

Table

Port

Affiche le numéro de port.

Link interrupted on enabled device ports

Active/désactive la surveillance du lien sur les ports activés.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Lorsque le port est activé (boîte de dialogue *Basic Settings > Port*, onglet *Configuration*, case *Port on*`cochée`) et que le lien est interrompu sur le port, la mention indiquée dans le cadre *Security status* passe à *`error`*.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Ce réglage prend effet lorsque vous cochez la case *Link interrupted on enabled device ports* dans l'onglet *Global* de la boîte de dialogue *Diagnostics > Status Configuration > Security Status*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Status]

Table

Timestamp

Affiche la date et l'heure de l'évènement au format `Mois Jour, Année hh:mm:ss AM/PM`.

Cause

Affiche l'événement à l'origine du trap SNMP.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6.1.3 Signal Contact

[Diagnostics > Status Configuration > Signal Contact]

Le contact sec est un contact à relais libre de potentiel. L'équipement vous permet ainsi d'effectuer des télédiagnostics. L'équipement utilise le contact à relais afin de signaler la survenue d'événements en ouvrant le contact à relais et en interrompant le circuit fermé.

Commentaire : L'équipement peut contenir plusieurs contacts secs. Chaque contact contient les mêmes fonctions de surveillance. L'utilisation de plusieurs contacts vous permet de regrouper ensemble différentes fonctions, contribuant ainsi à rendre la surveillance du système plus flexible.

Le menu contient les boîtes de dialogue suivantes :

- Signal Contact 1 / Signal Contact 2

6.1.3.1 Signal Contact 1 / Signal Contact 2

[Diagnostics > Status Configuration > Signal Contact > Signal Contact 1]

Cette boîte de dialogue vous permet de spécifier les conditions de déclenchement du contact sec.

Le contact sec vous offre les options suivantes :
- Surveillance du bon fonctionnement de l'équipement.
- Signalement de l'état de l'équipement.
- Signalement de l'état de sécurité de l'équipement.
- Commande des équipements externes par le biais du réglage manuel des contacts secs.

L'équipement affiche les erreurs détectées dans l'onglet *Status* et dans la boîte de dialogue *Basic Settings > System*, dans le cadre *Signal contact status*.

La boîte de dialogue contient les onglets suivants :
- [Global]
- [Port]
- [Status]

[Global]

Configuration

Mode

Indique les événements signalés par le contact sec.

Valeurs possibles :

- `Manual setting` (réglage par défaut du *Signal Contact 2*, le cas échéant)
  Utilisez ce réglage pour ouvrir ou fermer manuellement le contact sec, par exemple afin d'allumer ou d'éteindre un équipement distant. Voir la liste d'options *Contact*.
- `Monitoring correct operation` (réglage par défaut)
  Lorsque ce réglage est utilisé, le contact sec indique l'état des paramètres spécifiés dans la table ci-dessous.
- `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*. Vous pouvez également consulter l'état dans le cadre *Signal contact 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*. Vous pouvez également consulter l'état dans le cadre *Signal contact 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*. Vous pouvez également consulter l'état dans le cadre *Signal contact status*.

Contact

Permet de basculer manuellement entre les contacts secs. La condition préalable est que vous sélectionniez, dans la liste déroulante *Mode*, l'élément `Manual setting`.

Valeurs possibles :

- `open`
  Le contact sec est ouvert.
- `close`
  Le contact sec est fermé.

Signal contact status

Signal contact status

Affiche l'état actuel du contact sec.

Valeurs possibles :

- `Opened (error)`
  Le contact sec est ouvert. Le circuit est interrompu.
- `Closed (ok)`
  Le contact sec est fermé. Le circuit est fermé.

Trap configuration

Send trap

Active/désactive l'envoi de traps SNMP lorsque l'équipement détecte un changement dans une fonction surveillée.

Valeurs possibles :

- `case cochée`
  L'envoi de traps SNMP est activé.
  Lorsque l'équipement détecte une modification dans les fonctions surveillées, l'équipement envoie un trap SNMP.
- `case non cochée` (réglage par défaut)
  L'envoi de traps SNMP est désactivé.

Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

Monitoring correct operation

Dans la table, spécifiez les paramètres surveillés par l'équipement. L'équipement signale la survenue d'un événement en ouvrant le contact sec.

Connection errors

Active/désactive la surveillance d'état du lien du port/de l'interface.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Lorsque le lien est interrompu sur un port ou une interface faisant l'objet d'une surveillance, le contact sec s'ouvre.
  Dans l'onglet *Port*, vous pouvez sélectionner les ports/interfaces devant faire l'objet d'une surveillance individuelle.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Temperature

Active/désactive la surveillance de la température dans l'équipement.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque la température est inférieure ou supérieure aux valeurs limites, le contact sec s'ouvre.
- `case non cochée`
  La surveillance est désactivée.

Spécifiez les valeurs limites de la température dans les champs *Upper temp. limit [°C]* et *Lower temp. limit [°C]* de la boîte de dialogue *Basic Settings > System*.

Ring redundancy

Active/désactive la surveillance de la redondance d'anneau.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  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.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

External memory removed

Active/désactive la surveillance de la mémoire externe active.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Lorsque vous retirez la mémoire externe active de l'équipement, le contact sec s'ouvre.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

External memory not in sync with NVM

Active/désactive la surveillance du profil de configuration de l'équipement et de la mémoire externe.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  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.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Ethernet loops

Active/désactive la surveillance des boucles Ethernet de couche 2. Vous spécifiez les réglages de la fonction *Loop Protection* dans la boîte de dialogue *Diagnostics > Loop Protection*.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Lorsque l'équipement détecte une boucle Ethernet, le contact sec s'ouvre.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Power supply

Active/désactive la surveillance du bloc d'alimentation.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La surveillance est activée.
  Lorsque l'équipement détecte une erreur de l'alimentation en tension, le contact sec s'ouvre.
- `case non cochée`
  La surveillance est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Port]

Table

Port

Affiche le numéro de port.

Propagate connection error

Active/désactive la surveillance du lien du port/de l'interface.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  Lorsque le lien est interrompu sur un port ou une interface sélectionné, le contact sec s'ouvre.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Ce réglage prend effet lorsque vous cochez la case *Connection errors* dans l'onglet *Global*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Status]

Table

Timestamp

Affiche la date et l'heure de l'évènement au format `Mois Jour, Année hh:mm:ss AM/PM`.

Cause

Affiche l'événement à l'origine du trap SNMP.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6.1.4 MAC Notification

[Diagnostics > Status Configuration > MAC Notification]

L'équipement vous permet d'effectuer un suivi des modifications du réseau à l'aide de l'adresse MAC des équipements intégrés au réseau. L'équipement sauvegarde l'association du port et de l'adresse MAC dans sa table d'adresses MAC. Lorsque l'équipement apprend ou désapprend l'adresse MAC d'un équipement connecté ou déconnecté, l'équipement envoie un trap SNMP.

Cette fonction est destinée aux ports auxquels vous connectez des équipements terminaux dont l'adresse MAC change ainsi peu souvent.

Operation

Operation

Active/désactive la fonction *MAC Notification* dans l'équipement.

Valeurs possibles :

- `On`
  La fonction *MAC Notification* est activée.
- `Off` (réglage par défaut)
  La fonction *MAC Notification* est désactivée.

Configuration

Interval [s]

Indique l'intervalle d'envoi en secondes. Lorsque l'équipement apprend ou désapprend l'adresse MAC d'un équipement connecté ou déconnecté, l'équipement envoie un trap SNMP une fois ce laps de temps expiré.

Valeurs possibles :

- `0..2147483647` (réglage par défaut : `30`)

Avant d'envoyer un trap SNMP, l'équipement enregistre jusqu'à 20 adresses MAC. Lorsque l'équipement détecte un nombre élevé de modifications, l'équipement envoie le trap SNMP avant l'expiration de l'intervalle d'envoi.

Table

Port

Affiche le numéro de port.

Active

Active/désactive la fonction *MAC Notification* sur le port.

Valeurs possibles :

- `case cochée`
  La fonction *MAC Notification* est activée sur le port.
  L'équipement envoie un trap SNMP en cas de survenue de l'un des événements suivants :
  - L'équipement apprend l'adresse MAC d'un équipement nouvellement connecté.
  - L'équipement désapprend l'adresse MAC d'un équipement déconnecté.
- `case non cochée` (réglage par défaut)
  La fonction *MAC Notification* est désactivée sur le port.

Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

Last MAC address

Affiche l'adresse MAC du dernier équipement connecté ou déconnecté sur le port.

L'équipement détecte les adresses MAC des équipements :

- directement connectés au port
- connectés au port à travers d'autres équipements du réseau

Last MAC status

Indique l'état de la valeur *Last MAC address* sur le port.

Valeurs possibles :

- `added`
  L'équipement a détecté qu'un autre équipement était connecté au port.
- `removed`
  L'équipement a détecté que l'équipement connecté a été retiré du port.
- `other`
  L'équipement n'a pas détecté d'état.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6.1.5 Alarms (Traps)

[Diagnostics > Status Configuration > Alarms (Traps)]

L'équipement vous permet d'envoyer un trap SNMP en réaction à des événements spécifiques. Cette boîte de dialogue vous permet de spécifier les destinations de trap auxquelles l'équipement envoie les traps SNMP.

Spécifiez les événements pour lesquels l'équipement déclenche un trap SNMP dans les boîtes de dialogue suivantes, par exemple :
- dans la boîte de dialogue *Diagnostics > Status Configuration > Device Status*
- dans la boîte de dialogue *Diagnostics > Status Configuration > Security Status*
- dans la boîte de dialogue *Diagnostics > Status Configuration > MAC Notification*

Operation

Operation

Active/désactive l'envoi de traps SNMP aux destinations de trap.

Valeurs possibles :
- *On* (réglage par défaut)
  L'envoi de traps SNMP est activé.
- *Off*
  L'envoi de traps SNMP est désactivé.

Table

Name

Indique le nom de la destination de trap.

Valeurs possibles :
- Chaîne de 1..32 caractères ASCII alphanumériques

Address

Indique l'adresse IP et le numéro de port de la destination de trap.

Valeurs possibles :
- `<Adresse IPv4 valide>:<numéro de port>`

Active

Active/désactive l'envoi de traps SNMP à cette destination de trap.

Valeurs possibles :
- `case cochée` (réglage par défaut)
  L'envoi de traps SNMP à cette destination de trap est activé.
- `case non cochée`
  L'envoi de traps SNMP à cette destination de trap est désactivé.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Ouvre la fenêtre *Create* pour ajouter une nouvelle entrée à la table.

- Spécifiez le nom d'une destination de trap dans le champ *Name*.
- Spécifiez l'adresse IP et le numéro de port de la destination de trap dans le champ *Address*. Si vous choisissez de ne pas saisir de numéro de port, l'équipement ajoute automatiquement le numéro de port `162`.

6.2 System

[Diagnostics > System]

Le menu contient les boîtes de dialogue suivantes :

- System Information
- Hardware State
- IP Address Conflict Detection
- ARP
- Selftest

6.2.1 System Information

[Diagnostics > System > System Information]

Cette boîte de dialogue affiche l'état de fonctionnement actuel des composants individuels de l'équipement. Les valeurs affichées représentent un aperçu instantané de l'état de fonctionnement des composants au moment du chargement de la boîte de dialogue sur la page.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Save system information

Ouvre la page HTML dans une nouvelle fenêtre ou un nouvel onglet de navigateur Web. Vous pouvez sauvegarder la page HTML sur votre PC à l'aide de la commande de navigateur Web appropriée.

6.2.2 Hardware State

[Diagnostics > System > Hardware State]

Cette boîte de dialogue fournit des informations sur la distribution et l'état de la mémoire flash de l'équipement.

Information

Uptime

Affiche le temps de fonctionnement total de l'équipement depuis sa livraison.

Valeurs possibles :

▶ `..d ..h ..m ..s`
Jours(s) Heures(s) Minute(s) Seconde(s)

Table

Flash region

Affiche le nom de la zone de mémoire concernée.

Description

Affiche une description de ce pourquoi l'équipement utilise la zone de mémoire.

Flash sectors

Affiche le nombre de secteurs affectés à la zone de mémoire.

Sector erase operations

Affiche combien de fois l'équipement a écrasé les secteurs de la zone de mémoire.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6.2.3 IP Address Conflict Detection

[Diagnostics > System > IP Address Conflict Detection]

La fonction *IP Address Conflict Detection* permet de vérifier si l'adresse IP est unique sur le réseau. L'équipement analyse à cette fin les paquets ARP reçus.

Cette boîte de dialogue vous permet de spécifier la procédure avec laquelle l'équipement détecte les conflits d'adresses et de configurer les réglages correspondants.

L'équipement affiche les conflits d'adresses détectés dans la table.

Lorsque l'équipement détecte un conflit d'adresses, la LED d'état de l'équipement clignote en rouge 4 fois.

Operation

Operation

Active/désactive la fonction *IP Address Conflict Detection*.

Valeurs possibles :

- `On` (réglage par défaut)
  La fonction *IP Address Conflict Detection* est activée.
  L'équipement vérifie que son adresse IP est unique sur le réseau.
- `Off`
  La fonction *IP Address Conflict Detection* est désactivée.

Configuration

Detection mode

Indique la procédure avec laquelle l'équipement détecte les conflits d'adresses.

Valeurs possibles :

- `active and passive` (réglage par défaut)
  La détection des conflits d'adresses IP utilisée par l'équipement peut être active ou passive.

▶ *active*
Détection active des conflits d'adresses IP. L'équipement contribue activement à éviter la communication avec une adresse IP qui existe déjà sur le réseau. La détection des conflits d'adresses IP commence dès que vous connectez l'équipement au réseau ou modifiez ses paramètres.
- L'équipement envoie 4 paquets de données de sonde ARP avec un intervalle spécifié dans le champ *Detection delay [ms]*. Toute réponse à ces paquets de données reçue par l'équipement confirme la présence d'un conflit d'adresses IP.
- Lorsque l'équipement ne détecte pas de conflit d'adresses, il envoie 2 paquets de données gratuitous ARP en guise d'annonce. L'équipement envoie également ces paquets de données lorsque la détection des conflits d'adresses IP est désactivée.
- Lorsque l'adresse IP existe déjà sur le réseau, l'équipement rétablit les paramètres IP utilisés dans leur état antérieur (si possible).
  Lorsque l'équipement reçoit ses paramètres IP de la part d'un serveur DHCP, il renvoie un message DHCPDECLINE au serveur DHCP.
- Après une période spécifiée dans le champ *Release delay [s]*, l'équipement vérifie si le conflit d'adresses est toujours présent. Lorsque l'équipement détecte successivement 10 conflits d'adresses, il prolonge le délai d'attente de 60 s lors de la prochaine vérification.
- Lorsque l'équipement résout un conflit d'adresses, l'administration de l'équipement retourne sur le réseau.

▶ *passive*
Détection passive des conflits d'adresses IP. L'équipement analyse le trafic de données du réseau. Lorsqu'un autre équipement du réseau utilise la même adresse IP, l'équipement « défend » d'abord son adresse IP. L'équipement cesse toute émission lorsque l'autre équipement continue à émettre avec la même adresse IP.
- En guise de « défense », l'équipement envoie des paquets de données gratuitous ARP. L'équipement répète cette procédure autant de fois que spécifié dans le champ *Address protections*.
- Si l'autre équipement continue à émettre avec la même adresse IP, l'équipement vérifie périodiquement si le conflit d'adresses est toujours présent après la période spécifiée dans le champ *Release delay [s]*.
- Lorsque l'équipement résout un conflit d'adresses, l'administration de l'équipement retourne sur le réseau.

Send periodic ARP probes

Active/désactive la détection périodique des conflits d'adresses IP.

Valeurs possibles :

▶ `case cochée` (réglage par défaut)
La détection périodique des conflits d'adresses IP est activée.
- L'équipement envoie périodiquement un paquet de données de sonde ARP toutes les 90 à 150 secondes et attend une réponse pendant la période spécifiée dans le champ *Detection delay [ms]*.
- Lorsque l'équipement détecte un conflit d'adresses, l'équipement applique le mode de détection passive. Lorsque la fonction *Send trap* est activée, l'équipement envoie un trap SNMP.

▶ `case non cochée`
La détection périodique des conflits d'adresses IP est désactivée.

Detection delay [ms]

Indique la période en millisecondes pendant laquelle l'équipement attend une réponse après l'envoi de paquets de données ARP.

Valeurs possibles :

- `20..500` (réglage par défaut : `200`)

Release delay [s]

Indique la période en secondes après laquelle l'équipement vérifie à nouveau si le conflit d'adresses est toujours présent.

Valeurs possibles :

- `3..3600` (réglage par défaut : `15`)

Address protections

Indique combien de fois l'équipement envoie des paquets de données gratuitous ARP en mode de détection passive pour « défendre » son adresse IP.

Valeurs possibles :

- `0..100` (réglage par défaut : `3`)

Protection interval [ms]

Indique la période en millisecondes après laquelle l'équipement envoie à nouveau des paquets de données gratuitous ARP en mode de détection passive pour « défendre » son adresse IP.

Valeurs possibles :

- `20..5000` (réglage par défaut : `200`)

Send trap

Active/désactive l'envoi de traps SNMP lorsque l'équipement détecte un conflit d'adresses.

Valeurs possibles :

- `case cochée`
  L'envoi de traps SNMP est activé.
  Lorsque l'équipement détecte un conflit d'adresses, l'équipement envoie un trap SNMP.
- `case non cochée` (réglage par défaut)
  L'envoi de traps SNMP est désactivé.

Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

Information

Conflict detected

Indique si un conflit d'adresses existe actuellement.

Valeurs possibles :

- `case cochée`
  L'équipement détecte un conflit d'adresses.
- `case non cochée`
  L'équipement ne détecte pas de conflit d'adresses.

Table

Timestamp

Affiche l'heure à laquelle l'équipement a détecté un conflit d'adresses.

Port

Affiche le numéro du port sur lequel l'équipement a détecté le conflit d'adresses.

IP address

Affiche l'adresse IP à l'origine du conflit d'adresses.

MAC address

Affiche l'adresse MAC de l'équipement concerné par le conflit d'adresses.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6.2.4 ARP

[Diagnostics > System > ARP]

Cette boîte de dialogue affiche les adresses MAC et IP des équipements voisins connectés à l'administration de l'équipement.

L'équipement peut afficher les adresses IPv4 et IPv6. Pour le protocole IPv6, les adresses des équipements voisins sont obtenues à l'aide du protocole NDP (Neighbor Discovery Protocol).

Table

Port

Affiche le numéro de port.

IP address

Affiche l'adresse IPv4 ou l'adresse IPv6 d'un équipement voisin.

MAC address

Affiche l'adresse MAC d'un équipement voisin.

Last updated

Affiche le laps de temps en secondes depuis lequel les réglages actuels de l'entrée ont été enregistrés dans la table ARP.

Type

Affiche le type de l'entrée.

Valeurs possibles :

- `static`
  Entrée statique. Lorsque la table ARP est supprimé, l'équipement conserve l'entrée statique.
- `dynamic`
  Entrée dynamique. Lorsque la valeur *Aging time [s]* a été dépassée et que l'équipement ne reçoit pas de données de la part de cet équipement au cours de ce laps de temps, l'équipement supprime l'entrée dynamique.
- `local`
  Les adresses IP et MAC de l'administration de l'équipement.

Active

Indique si la table ARP contient l'affectation d'adresses IP/MAC en tant qu'entrée active.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset ARP table

Supprime les adresses configurées dynamiquement de la table ARP.

6.2.5 Selftest

[Diagnostics > System > Selftest]

Cette boîte de dialogue vous permet d'effectuer les actions suivantes :
- Activer/désactiver le test RAM lorsque l'équipement est démarré.
- Activer/désactiver l'option de saisie du moniteur du système au démarrage du système.
- Spécifier comment l'équipement se comporte en cas d'erreur détectée.

Configuration

Lorsque l'équipement ne détecte pas de profil de configuration lisible lors du redémarrage, les réglages suivants bloquent votre accès à l'équipement de manière permanente.
- Case *SysMon1 is available* `décochée`.
- Case *Load default config on error* `décochée`.

C'est par exemple le cas lorsque le mot de passe du profil de configuration chargé diffère du mot de passe défini dans l'équipement. Pour débloquer à nouveau l'équipement, contactez votre revendeur.

RAM test

Active/désactive le contrôle de la mémoire RAM lors du redémarrage.

Valeurs possibles :
- `case cochée` (réglage par défaut)
  Le contrôle de la mémoire RAM est activé. Lors du redémarrage, l'équipement contrôle la mémoire RAM.
- `case non cochée`
  Le contrôle de la mémoire RAM est désactivé. Il en résulte un temps de démarrage plus court pour l'équipement.

SysMon1 is available

Active/désactive l'accès au moniteur du système pendant le redémarrage.

Valeurs possibles :
- `case cochée` (réglage par défaut)
  L'équipement vous permet d'ouvrir le moniteur du système lors du redémarrage.
- `case non cochée`
  L'équipement démarre sans l'option d'ouverture du moniteur du système.

Entre autres choses, le moniteur du système vous permet de mettre à jour le logiciel de l'équipement et de supprimer les profils de configuration sauvegardés.

Load default config on error

Active/désactive le chargement des réglages par défaut lorsque l'équipement ne détecte pas de profil de configuration lisible lors du redémarrage.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'équipement charge les réglages par défaut.
- `case non cochée`
  L'équipement interrompt le redémarrage et s'arrête. 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.
  Pour bénéficier à nouveau d'un accès à l'équipement via le réseau, ouvrez le moniteur du système et réinitialisez les réglages. Lors du redémarrage, l'équipement charge les réglages par défaut.

Table

Spécifiez dans cette table comment l'équipement se comporte en cas d'erreur détectée.

Cause

Causes d'erreur détectée auxquelles l'équipement réagit.

Valeurs possibles :

- `task`
  L'équipement détecte des erreurs survenant dans les applications exécutées, par exemple lorsqu'une tâche est interrompue ou n'est pas disponible.
- `resource`
  L'équipement détecte les erreurs dans les ressources disponibles, par exemple lorsque l'espace de stockage commence à devenir insuffisant.
- `software`
  L'équipement détecte les erreurs logicielles, par exemple lors du contrôle de cohérence.
- `hardware`
  L'équipement détecte les erreurs matérielles, par exemple celles survenant au niveau des puces.

Action

Indique comment l'équipement se comporte lorsque l'événement adjacent se produit.

Valeurs possibles :

- `reboot` (réglage par défaut)
  L'équipement déclenche un redémarrage.
- `logOnly`
  L'équipement enregistre l'erreur détectée dans le fichier log. Voir la boîte de dialogue *Diagnostics > Report > System Log*.
- `sendTrap`
  L'équipement envoie un trap SNMP.
  Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6.3 Email Notification

[Diagnostics > Email Notification]

L'équipement vous permet d'informer par e-mail plusieurs destinataires des événements qui se sont produits.

L'équipement envoie les e-mails immédiatement ou périodiquement en fonction de la gravité de l'événement. En général, vous spécifiez que les événements d'un niveau de gravité élevé doivent être envoyés immédiatement.

Vous pouvez spécifier plusieurs destinataires auxquels l'équipement envoie les e-mails immédiatement ou périodiquement.

Le menu contient les boîtes de dialogue suivantes :
- Email Notification Global
- Email Notification Recipients
- Email Notification Mail Server

6.3.1 Email Notification Global

[Diagnostics > Email Notification > Global]

Dans cette boîte de dialogue, vous spécifiez les réglages de l'expéditeur. Vous spécifiez également pour quelles gravités d'événements l'équipement envoie les e-mails immédiatement et pour lesquelles périodiquement.

Operation

Operation

Active/désactove l'envoi d'emails :

Valeurs possibles :

- *On*
  L'envoi d'e-mails est activé.
- *Off* (réglage par défaut)
  L'envoi d'e-mails est désactivé.

Certificate

L'équipement peut envoyer des messages à un serveur sur des réseaux non sécurisés. Pour éviter attaque de type « intermédiaire », demandez à l'autorité de certification de créer un certificat pour le serveur. Configurez le serveur pour qu'il utilise le certificat. Transférez le certificat sur l'équipement.

Si vous spécifiez les réglages des serveurs de messagerie, utilisez l'adresse IP ou le nom DNS fournis comme `Common Name` ou `Subject Alternative Name` dans le certificat. Sinon, la validation du certificat échouera.

URL

Indique le chemin et le nom de fichier du certificat.

L'équipement accepte les certificats présentant les propriétés suivantes :

- Format X.509
- Extension de fichier `.PEM`
- Codé en Base64, compris entre les mentions
  `-----BEGIN CERTIFICATE-----`
  et
  `-----END CERTIFICATE-----`

Pour des raisons de sécurité, nous recommandons de toujours utiliser un certificat signé par une autorité de certification.

L'équipement vous offre les options suivantes pour copier le certificat sur l'équipement :

- Importation depuis le PC
  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.

- Importation depuis un serveur FTP
  Lorsque le certificat est stocké sur un serveur FTP, spécifiez l'URL pour le fichier dans la forme suivante :
  `ftp://<utilisateur>:<mot de passe>@<adresse IP>:<port>/<chemin d'accès>/<nom fichier>`
- Importation depuis un serveur TFTP
  Lorsque le certificat est stocké sur un serveur TFTP, spécifiez l'URL pour le fichier dans la forme suivante :
  `tftp://<adresse IP>/<chemin d'accès>/<nom fichier>`
- Importation depuis un serveur SCP ou SFTP
  Lorsque le certificat est stocké sur un serveur SCP ou SFTP, spécifiez l'URL pour le fichier dans la forme suivante :
  - `scp://` ou `tftp://<adresse IP>/<chemin d'accès>/<nom 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>`

Start

Copie le certificat spécifié dans le champ *URL* sur l'équipement.

Sender

Address

Spécifie l'adresse e-mail de l'équipement.

L'équipement envoie les e-mails en utilisant cette adresse e-mail comme expéditeur.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

Notification immediate

Vous spécifiez ici les réglages des e-mails que l'équipement envoie immédiatement.

Severity

Spécifie le degré de gravité minimum des événements pour lesquels l'équipement envoie immédiatement un e-mail. Si un événement de cette gravité, ou d'une gravité plus urgente, se produit, l'équipement envoie un e-mail aux destinataires.

Valeurs possibles :

- *emergency*
- *alert* (réglage par défaut)
- *critical*
- *error*
- *warning*
- *notice*

- *informational*
- *debug*

Subject

Spécifie l'objet de l'e-mail.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

Notification periodic

Vous spécifiez ici les réglages des e-mails que l'équipement envoie périodiquement.

Severity

Spécifie le degré de gravité minimum des événements pour lesquels l'équipement envoie périodiquement un e-mail. Si un événement de cette gravité, ou d'une gravité plus urgente, se produit, l'équipement enregistre l'événement dans la mémoire tampon. L'équipement envoie le contenu de la mémoire tampon périodiquement ou lorsque la mémoire tampon déborde.

Si un événement d'une gravité moindre se produit, l'équipement n'enregistre pas l'événement dans la mémoire tampon.

Valeurs possibles :

- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (réglage par défaut)
- *notice*
- *informational*
- *debug*

Subject

Spécifie l'objet de l'e-mail.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

Sending interval [min]

Spécifie l'intervalle d'envoi en minutes.

Si l'équipement a enregistré au moins un événement, il envoie un e-mail avec le fichier log après l'expiration du délai.

Valeurs possibles :

- `30..1440` (réglage par défaut : `30`)

Send

Envoie immédiatement un e-mail avec le contenu de la mémoire tampon et vide la mémoire tampon.

Information

Sent messages

Affiche combien de fois l'équipement a envoyé avec succès un e-mail au serveur de messagerie.

Undeliverable messages

Affiche combien de fois l'équipement a tenté sans succès d'envoyer un e-mail au serveur de messagerie.

Time of the last messages sent

Affiche la date et l'heure du dernier envoi d'un e-mail au serveur de messagerie par l'équipement.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Clear email notification statistics

Remet les compteurs du cadre *Information* à `0`.

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
`notice`	État normal significatif
`informational`	Message à titre informatif
`debug`	Message de débogage

6.3.2 Email Notification Recipients

[Diagnostics > Email Notification > Recipients]

Dans cette boîte de dialogue, vous spécifiez les destinataires auxquels l'équipement envoie les e-mails. L'équipement vous permet de spécifier jusqu'à 10 destinataires.

Table

Index

Affiche l'index auquel l'entrée de table se réfère.

Notification type

Spécifie si l'équipement envoie les e-mails à ce destinataire immédiatement ou périodiquement.

Valeurs possibles :

- *immediate*
  L'équipement envoie les e-mails à ce destinataire immédiatement.
- *periodic*
  L'équipement envoie les e-mails à ce destinataire périodiquement.

Address

Spécifie l'adresse e-mail du destinataire.

Valeurs possibles :

- Adresse e-mail valide comportant jusqu'à 255 caractères

Active

Active/désactive la notification du destinataire.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La notification du destinataire est activée.
- `case non cochée`
  La notification du destinataire est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6.3.3 Email Notification Mail Server

[Diagnostics > Email Notification > Mail Server]

Dans cette boîte de dialogue, vous spécifiez les réglages des serveurs de messagerie. L'équipement prend en charge les connexions chiffrées et non chiffrées au serveur de messagerie.

Table

Index

Affiche l'index auquel l'entrée de table se réfère.

Description

Spécifie le nom du serveur.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

IP address

Spécifie l'adresse IP ou le nom DNS du serveur.

Valeurs possibles :

- Adresse IPv4 valide (réglage par défaut : `0.0.0.0`)
- Nom DNS au format `domain.tld` ou `host.domain.tld`
  Si vous spécifiez un nom DNS, activez également la fonction *Client* dans la boîte de dialogue *Advanced > DNS > Client > Global*.
  Si vous établissez des connexions chiffrées à l'aide du certificat, vérifiez que le nom DNS correspond au nom DNS du serveur figurant dans le certificat.

Destination TCP port

Spécifie le port TCP du serveur.

Valeurs possibles :

- `1..65535` (réglage par défaut : `25`)
  Exception : le port `2222` est réservé à des fonctions internes.

Ports TCP fréquemment utilisés :

- SMTP `25`
- Message Submission `587`

Encryption

Spécifie le protocole qui chiffre la connexion entre l'équipement et le serveur de messagerie.

Valeurs possibles :

- `none` (réglage par défaut)
  L'équipement établit une connexion non chiffrée avec le serveur.
- `tlsv1`
  L'équipement établit une connexion chiffrée avec le serveur à l'aide de l'extension startTLS.

User name

Spécifie le nom d'utilisateur du compte que l'équipement utilise pour s'authentifier sur le serveur de messagerie.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

Password

Spécifie le mot de passe du compte que l'équipement utilise pour s'authentifier sur le serveur de messagerie.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

Timeout [s]

Spécifie le délai en secondes après lequel l'équipement envoie à nouveau un e-mail. La condition préalable est que l'équipement n'ait pas réussi à envoyer l'e-mail complet en raison d'une erreur de connexion.

Valeurs possibles :

- `1..15` (réglage par défaut : `3`)

Active

Active/désactive l'utilisation du serveur de messagerie.

Valeurs possibles :

- `case cochée`
  Le serveur de messagerie est activé.
  L'équipement envoie des e-mails à ce serveur de messagerie.
- `case non cochée` (réglage par défaut)
  Le serveur de messagerie est désactivé.
  L'équipement n'envoie pas d'e-mails à ce serveur de messagerie.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Connection test

Ouvre la boîte de dialogue *Connection test* pour envoyer un e-mail de test.

Si les réglages du serveur de messagerie sont corrects, les destinataires sélectionnés reçoivent un e-mail de test.

- Dans le champ *Recipient*, vous spécifiez les destinataires auxquels l'équipement envoie l'e-mail de test :
  - *immediate*
    L'équipement envoie l'e-mail de test aux destinataires auxquels il envoie des e-mails immédiatement.
  - *periodic*
    L'équipement envoie l'e-mail de test aux destinataires auxquels il envoie des e-mails périodiquement.
- Dans le champ *Message text*, vous spécifiez le texte de l'e-mail de test.

6.4 Syslog

[Diagnostics > Syslog]

L'équipement vous permet de signaler des événements sélectionnés à différents serveurs Syslog indépendamment de la gravité de l'événement. Cette boîte de dialogue vous permet de spécifier les réglages relatifs à cette fonction et de gérer jusqu'à 8 serveurs Syslog.

Operation

Operation

Active/désactive l'envoi des événements aux serveurs Syslog.

Valeurs possibles :

- `On`
  L'envoi des événements est activé.
  L'équipement envoie les événements indiqués dans la table aux serveurs Syslog spécifiés.
- `Off` (réglage par défaut)
  L'envoi des événements est désactivé.

Certificate

L'équipement peut envoyer des messages à un serveur sur des réseaux non sécurisés. Pour éviter attaque de type « intermédiaire », demandez à l'autorité de certification de créer un certificat pour le serveur. Configurez le serveur pour qu'il utilise le certificat. Transférez le certificat sur l'équipement.

Si vous spécifiez les paramètres sur le serveur, vérifiez que vous indiquez l'adresse IP et le nom DNS fournis dans le certificat comme `Common Name` ou `Subject Alternative Name`. Sinon, la validation du certificat échouera.

Commentaire : Afin que les changements prennent effet après le chargement d'un nouveau certificat, redémarrez la fonction *Syslog*.

URL

Indique le chemin et le nom de fichier du certificat.

L'équipement accepte les certificats présentant les propriétés suivantes :

- Format X.509
- Extension de fichier `.PEM`
- Codé en Base64, compris entre les mentions
  `-----BEGIN CERTIFICATE-----`
  et
  `-----END CERTIFICATE-----`

Pour des raisons de sécurité, nous recommandons de toujours utiliser un certificat signé par une autorité de certification.

L'équipement vous offre les options suivantes pour copier le certificat sur l'équipement :

- Importation depuis le PC
  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.
- Importation depuis un serveur FTP
  Lorsque le certificat est stocké sur un serveur FTP, spécifiez l'URL pour le fichier dans la forme suivante :
  `ftp://<utilisateur>:<mot de passe>@<adresse IP>:<port>/<chemin d'accès>/<nom fichier>`
- Importation depuis un serveur TFTP
  Lorsque le certificat est stocké sur un serveur TFTP, spécifiez l'URL pour le fichier dans la forme suivante :
  `tftp://<adresse IP>/<chemin d'accès>/<nom fichier>`
- Importation depuis un serveur SCP ou SFTP
  Lorsque le certificat est stocké sur un serveur SCP ou SFTP, spécifiez l'URL pour le fichier dans la forme suivante :
  - `scp://` ou `tftp://<adresse IP>/<chemin d'accès>/<nom 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>`

Start

Copie le certificat spécifié dans le champ *URL* sur l'équipement.

Table

Index

Affiche l'index auquel l'entrée de table se réfère.

Si vous supprimez une entrée de table, il reste un blanc dans la numérotation. Si vous créez une entrée de table, l'équipement remplit le 1er blanc.

Valeurs possibles :

- `1..8`

IP address

Indique l'adresse IP du serveur Syslog.

Valeurs possibles :

- Adresse IPv4 valide (réglage par défaut : `0.0.0.0`)
- Adresse IPv6 valide
- Nom d'hôte

Destination UDP port

Spécifie le port TCP ou UDP sur lequel le serveur Syslog s'attend à recevoir les entrées du log.

Valeurs possibles :

- `1..65535` (réglage par défaut : `514`)

Transport type

Spécifie le type de transport que l'équipement utilise pour envoyer les événements au serveur Syslog.

Valeurs possibles :

- `udp` (réglage par défaut)
  L'équipement envoie les événements via le port UDP spécifié dans la colonne *Destination UDP port*.
- `tls`
  L'équipement envoie les événements via TLS sur le port TCP spécifié dans la colonne *Destination UDP port*.

Min. severity

Indique le degré de gravité minimum de l'événement. L'équipement envoie une entrée de log au serveur Syslog pour les événements présentant ce degré de gravité et des degrés de gravité supérieurs.

Valeurs possibles :

- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (réglage par défaut)
- `notice`

- `informational`
- `debug`

Type

Indique le type de l'entrée de log transmise par l'équipement.

Valeurs possibles :

- `systemlog` (réglage par défaut)
- `audittrail`

Active

Active/désactive la transmission des événements au serveur Syslog :

- `case cochée`
  L'équipement envoie des événements au serveur Syslog.
- `case non cochée` (réglage par défaut)
  La transmission des événements au serveur Syslog est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6.5 Ports

[Diagnostics > Ports]

Le menu contient les boîtes de dialogue suivantes :

- SFP
- TP cable diagnosis
- Port Monitor
- Auto-Disable
- Port Mirroring

6.5.1 SFP

[Diagnostics > Ports > SFP]

Cette boîte de dialogue vous permet de consulter les transceivers SFP actuellement connectés à l'équipement et leurs propriétés.

Table

La table affiche des valeurs valides lorsque l'équipement est doté de transceivers SFP.

Port

Affiche le numéro de port.

Module type

Type de transceiver SFP, par exemple M-SFP-SX/LC.

Serial number

Affiche le numéro de série du transceiver SFP.

Connector type

Affiche le type de fiche.

Supported

Indique si l'équipement prend en charge le transceiver SFP.

Temperature [°C]

Température de fonctionnement du transceiver SFP en degrés Celsius.

Tx power [mW]

Puissance d'émission du transceiver SFP en mW.

Rx power [mW]

Puissance de réception du transceiver SFP en mW.

Tx power [dBm]

Puissance d'émission du transceiver SFP en dBm.

Rx power [dBm]

Puissance de réception du transceiver SFP en dBm.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6.5.2 TP cable diagnosis

[Diagnostics > Ports > TP cable diagnosis]

Cette fonctionnalité permet de tester le câble raccordé à une interface, afin de détecter un court-circuit ou un circuit ouvert. La table affiche l'état et la longueur estimée du câble. L'équipement affiche également les paires de câbles individuels raccordées au port. Lorsque l'équipement détecte un court-circuit ou un circuit ouvert dans le câble, il affiche également la distance estimée avec le problème.

Pour obtenir des résultats fiables, utilisez la fonction *TP cable diagnosis* pour les câbles à paires torsadées d'une longueur minimale de 3 mètres.

Commentaire : Ce test interrompt le trafic sur le port.

Information

Port

Affiche le numéro de port.

Status

État du testeur de câbles virtuel.

Valeurs possibles :

- *active*
  Le test des câbles est en cours.
  Pour lancer le test, cliquez sur le bouton ☰, puis sur l'élément *Start cable diagnosis...*. Cette action ouvre la boîte de dialogue *Select port*.
- *success*
  L'équipement affiche cette entrée après un test réussi.
- *failure*
  L'équipement affiche cette entrée après un test interrompu.
- *uninitialized*
  L'équipement affiche cette entrée lors de la veille.

Table

Cable pair

Affiche la paire de câbles à laquelle cette entrée se réfère. L'équipement utilise le premier index PHY pris en charge pour afficher les valeurs.

Result

Affiche les résultats du test des câbles.

Valeurs possibles :

- *normal*
  Le câble fonctionne correctement.

- *open*
  Le câble est coupé, ce qui provoque une interruption.
- *short*
  Les fils du câble se touchent et provoquent un court-circuit.
- *unknown*
  L'équipement affiche cette valeur pour les paires de câbles non testées.

L'équipement affiche des valeurs différentes que prévu dans les cas suivants :

- Si aucun câble n'est connecté au port, l'équipement affiche la valeur *unknown* au lieu de la valeur *open*.
- Si le port est désactivé, l'équipement affiche la valeur *short*.

Min. length

Affiche la longueur minimale estimée du câble, exprimée en mètres.

Si la longueur du câble est inconnue ou dans le cadre *Information*, le champ *Status* affiche la valeur *active*, *failure* ou *uninitialized*, puis l'équipement affiche la valeur 0.

Max. length

Affiche la longueur maximale estimée du câble, exprimée en mètres.

Si la longueur du câble est inconnue ou dans le cadre *Information*, le champ *Status* affiche la valeur *active*, *failure* ou *uninitialized*, puis l'équipement affiche la valeur 0.

Distance [m]

Affiche la distance estimée en mètres d'une extrémité du câble à l'autre ou à une interruption du câble.

Si la longueur du câble est inconnue ou dans le cadre *Information*, le champ *Status* affiche la valeur *active*, *failure* ou *uninitialized*, puis l'équipement affiche la valeur 0.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Start cable diagnosis...

Ouvre la boîte de dialogue *Select port*.

Dans la liste déroulante *Port*, sélectionnez le port à tester. Utilisez uniquement pour les ports à base de cuivre.

Pour lancer le test du câble sur le port sélectionné, cliquez sur le bouton *Ok*.

6.5.3 Port Monitor

[Diagnostics > Ports > Port Monitor]

La fonction *Port Monitor* permet de surveiller le respect des paramètres spécifiés au niveau des ports. Lorsque la fonction *Port Monitor* détecte que les paramètres dépassent les valeurs limites, l'équipement exécute une action.

Pour appliquer la fonction *Port Monitor*, exécutez les étapes suivantes :
- Onglet *Global*
  - Activez la fonction *Operation* dans le cadre *Port Monitor*.
  - Pour chaque port, activez les paramètres devant être surveillés par la fonction *Port Monitor*.
- Onglet *Link flap*, *CRC/Fragments* et *Overload detection*
  - Spécifiez les valeurs limites des paramètres pour chaque port.
- Onglet *Link speed/Duplex mode detection*
  - Active les combinaisons de vitesse et de mode duplex pour chaque port.
- Onglet *Global*
  - Pour chaque port, spécifiez une action que l'équipement exécute lorsque la fonction *Port Monitor* détecte que les paramètres ont dépassé les valeurs limites.
- Onglet *Auto-disable*
  - Cochez la case *Auto-disable* des paramètres surveillés si vous avez spécifié l'action `auto-disable` au moins une fois.

La boîte de dialogue contient les onglets suivants :
- [Global]
- [Auto-disable]
- [Link flap]
- [CRC/Fragments]
- [Overload detection]
- [Link speed/Duplex mode detection]

[Global]

Cet onglet vous permet d'activer la fonction *Port Monitor* et de spécifier les paramètres que la fonction *Port Monitor* surveille. Vous pouvez également spécifier l'action que l'équipement exécute lorsque la fonction *Port Monitor* détecte que les paramètres ont dépassé les valeurs limites.

Operation

Operation

Active/désactive la fonction *Port Monitor* globalement.

Valeurs possibles :
- `On`
  La fonction *Port Monitor* est activée.
- `Off` (réglage par défaut)
  La fonction *Port Monitor* est désactivée.

Table

Port

Affiche le numéro de port.

Link flap on

Active/désactive la surveillance des instabilités de lien sur le port.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  - La fonction *Port Monitor* surveille les instabilités de lien sur le port.
  - Lorsque l'équipement détecte un trop grand nombre d'instabilités de lien, il exécute l'action spécifiée dans la colonne *Action*.
  - Dans l'onglet *Link flap*, spécifiez les paramètres à surveiller.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

CRC/Fragments on

Active/désactive la surveillance des erreurs CRC/de fragments détectées sur le port.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  - La fonction *Port Monitor* surveille les erreurs CRC/de fragments détectées sur le port.
  - Lorsque l'équipement détecte un trop grand nombre d'erreurs CRC/de fragments, il exécute l'action spécifiée dans la colonne *Action*.
  - Dans l'onglet *CRC/Fragments*, spécifiez les paramètres à surveiller.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Duplex mismatch detection active

Active/désactive la surveillance des non-correspondances de duplex sur le port.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  - La fonction *Port Monitor* surveille les non-correspondances de duplex sur le port.
  - Lorsque l'équipement détecte un trop grand nombre de non-correspondances de duplex, il exécute l'action spécifiée dans la colonne *Action*.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Overload detection on

Active/désactive la fonction de détection de surcharge sur le port.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  - La fonction *Port Monitor* surveille la charge de données sur le port.
  - Lorsque l'équipement détecte une surcharge de données sur le port, il exécute l'action spécifiée dans la colonne *Action*.
  - Dans l'onglet *Overload detection*, spécifiez les paramètres à surveiller.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Link speed/Duplex mode detection on

Active/désactive la surveillance de la vitesse de lien et du mode duplex sur le port.

Valeurs possibles :

- `case cochée`
  La surveillance est activée.
  - La fonction *Port Monitor* surveille la vitesse de lien et le mode duplex sur le port.
  - Lorsque l'équipement détecte une combinaison non autorisée de vitesse de lien et de mode duplex, il exécute l'action spécifiée dans la colonne *Action*.
  - Dans l'onglet *Link speed/Duplex mode detection*, spécifiez les paramètres à surveiller.
- `case non cochée` (réglage par défaut)
  La surveillance est désactivée.

Active condition

Affiche le paramètre surveillé qui a entraîné l'action sur le port.

Valeurs possibles :

- `-`
  Pas de paramètre surveillé.
  L'équipement n'exécute aucune action.
- *`Link flap`*
  Un trop grand nombre de modifications de lien ont été détectées lors de la période observée.
- *`CRC/Fragments`*
  Un trop grand nombre d'erreurs CRC/de fragments ont été détectées lors de la période observée.
- *`Duplex mismatch`*
  Une non-concordance de duplex a été détectée.
- *`Overload detection`*
  Une surcharge a été détectée lors de la période observée.
- *`Link speed/Duplex mode detection`*
  Une combinaison non autorisée de vitesse et de mode duplex a été détectée.

Action

Indique l'action que l'équipement exécute lorsque la fonction de *Port Monitor* détecte que les paramètres ont dépassé les valeurs limites.

Valeurs possibles :

- `disable port`
  L'équipement désactive le port et envoie un trap SNMP.
  La LED « État du lien » du port clignote 3x par période.
  - Pour réactiver le port, mettez le port en surbrillance et cliquez sur le bouton ☰, puis sur l'élément *Reset*.
  - Lorsque les paramètres cessent de dépasser les valeurs limites, la fonction *Auto-Disable* réactive le port concerné après le temps d'attente spécifié. Il convient pour cela que la case correspondant au paramètre surveillé soit préalablement cochée dans l'onglet *Auto-disable*.
- `send trap`
  L'équipement envoie un trap SNMP.
  Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.
- `auto-disable` (réglage par défaut)
  L'équipement désactive le port et envoie un trap SNMP.
  La LED « État du lien » du port clignote 3x par période.
  Il convient pour cela que la case correspondant au paramètre surveillé soit préalablement cochée dans l'onglet *Auto-disable*.
  - La boîte de dialogue *Diagnostics > Ports > Auto-Disable* affiche quels ports sont actuellement désactivés en raison du dépassement des paramètres.
  - La fonction *Auto-Disable* réactive le port automatiquement. Pour cela, accédez à la boîte de dialogue *Diagnostics > Ports > Auto-Disable* et spécifiez une période d'attente pour le port concerné dans la colonne *Reset timer [s]*.

Port status

Affiche l'état de fonctionnement du port.

Valeurs possibles :

- `up`
  Le port est activé.
- `down`
  Le port est désactivé.
- `notPresent`
  Port physique non disponible.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Réactive le port mis en surbrillance dans la table et réinitialise son compteur sur `0`. Cette opération se répercute sur les compteurs des boîtes de dialogue suivantes :

- Boîte de dialogue *Diagnostics > Ports > Port Monitor*
  - Onglet *Link flap*
  - Onglet *CRC/Fragments*
  - Onglet *Overload detection*
- Boîte de dialogue *Diagnostics > Ports > Auto-Disable*

[Auto-disable]

Cet onglet vous permet d'activer la fonction *Auto-Disable* pour les paramètres surveillés par la fonction *Port Monitor*.

Table

Reason

Affiche les paramètres surveillés par la fonction *Port Monitor*.

Cochez la case afin que la fonction *Port Monitor* exécute l'action `auto-disable` lorsqu'elle détecte un dépassement des valeurs limites des paramètres.

Auto-disable

Active/désactive la fonction *Auto-Disable* pour les paramètres adjacents.

Valeurs possibles :

- `case cochée`
  La fonction *Auto-Disable* est activée pour les paramètres adjacents.
  Lorsque les paramètres adjacents dépassent les valeurs limites et que la valeur `auto-disable` est spécifiée dans la colonne *Action*, l'équipement exécute la fonction *Auto-Disable*.
- `case non cochée` (réglage par défaut)
  La fonction *Auto-Disable* est désactivée pour les paramètres adjacents.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Réactive le port mis en surbrillance dans la table et réinitialise son compteur sur `0`. Cette opération se répercute sur les compteurs des boîtes de dialogue suivantes :

- Boîte de dialogue *Diagnostics > Ports > Port Monitor*
  - Onglet *Link flap*
  - Onglet *CRC/Fragments*
  - Onglet *Overload detection*
- Boîte de dialogue *Diagnostics > Ports > Auto-Disable*

[Link flap]

Cet onglet vous permet de spécifier les réglages suivants individuellement pour chaque port :

- Le nombre de modifications de lien.
- La période pendant laquelle la fonction *Port Monitor* surveille un paramètre pour détecter des discordances.

Vous pouvez également consulter le nombre de modifications de lien que la fonction *Port Monitor* a détectées jusqu'à présent.

La fonction *Port Monitor* surveille les ports pour lesquels la case de la colonne *Link flap on* est cochée dans l'onglet *Global*.

Table

Port

Affiche le numéro de port.

Sampling interval [s]

Indique la période en secondes pendant laquelle la fonction *Port Monitor* surveille un paramètre pour détecter des discordances.

Valeurs possibles :

- `1..180` (réglage par défaut : `10`)

Link flaps

Indique le nombre de modifications de lien.

Lorsque la fonction *Port Monitor* détecte ce nombre de modifications de lien lors de la période surveillée, l'équipement exécute l'action spécifiée.

Valeurs possibles :

- `1..100` (réglage par défaut : `5`)

Last sampling interval

Affiche le nombre d'erreurs que l'équipement a détectées lors de la période écoulée.

Total

Affiche le nombre total d'erreurs que l'équipement a détectées depuis l'activation du port.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Réactive le port mis en surbrillance dans la table et réinitialise son compteur sur `0`. Cette opération se répercute sur les compteurs des boîtes de dialogue suivantes :

- Boîte de dialogue *Diagnostics > Ports > Port Monitor*
  - Onglet *Link flap*
  - Onglet *CRC/Fragments*
  - Onglet *Overload detection*
- Boîte de dialogue *Diagnostics > Ports > Auto-Disable*

[CRC/Fragments]

Cet onglet vous permet de spécifier les réglages suivants individuellement pour chaque port :

- Le taux d'erreurs de fragments détecté.
- La période pendant laquelle la fonction *Port Monitor* surveille un paramètre pour détecter des discordances.

Vous pouvez également consulter le taux d'erreurs de fragments que l'équipement a détecté jusqu'à présent.

La fonction *Port Monitor* surveille les ports pour lesquels la case de la colonne *CRC/Fragments on* est cochée dans l'onglet *Global*.

Table

Port

Affiche le numéro de port.

Sampling interval [s]

Indique la période en secondes pendant laquelle la fonction *Port Monitor* surveille un paramètre pour détecter des discordances.

Valeurs possibles :

- `5..180` (réglage par défaut : `10`)

CRC/Fragments count [ppm]

Indique le taux d'erreurs de fragments détecté (en parties par million).

Lorsque la fonction *Port Monitor* détecte ce taux d'erreurs de fragments lors de la période surveillée, l'équipement exécute l'action spécifiée.

Valeurs possibles :

- `1..1000000` (réglage par défaut : `1000`)

Last active interval [ppm]

Affiche le taux d'erreurs de fragments que l'équipement a détecté lors de la période écoulée.

Total [ppm]

Affiche le taux d'erreurs de fragments que l'équipement a détectées depuis l'activation du port.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Réactive le port mis en surbrillance dans la table et réinitialise son compteur sur `0`. Cette opération se répercute sur les compteurs des boîtes de dialogue suivantes :

- Boîte de dialogue *Diagnostics > Ports > Port Monitor*
  - Onglet *Link flap*
  - Onglet *CRC/Fragments*
  - Onglet *Overload detection*
- Boîte de dialogue *Diagnostics > Ports > Auto-Disable*

[Overload detection]

Cet onglet vous permet de spécifier les réglages suivants individuellement pour chaque port :

- Les valeurs limites de charge.
- La période pendant laquelle la fonction *Port Monitor* surveille un paramètre pour détecter des discordances.

Vous pouvez également consulter le nombre de paquets de données que l'équipement a détectés jusqu'à présent.

La fonction *Port Monitor* surveille les ports pour lesquels la case de la colonne *Overload detection on* est cochée dans l'onglet *Global*.

La fonction *Port Monitor* ne surveille pas les ports faisant partie d'un groupe d'agrégat de liens.

Table

Port

Affiche le numéro de port.

Traffic type

Indique le type de paquets de données que l'équipement prend en compte lors de la surveillance de la charge sur le port.

Valeurs possibles :

- `all`
  La fonction *Port Monitor* surveille les paquets broadcast, multicast et unicast.
- `bc` (réglage par défaut)
  La fonction *Port Monitor* surveille uniquement les paquets de données broadcast.
- `bc-mc`
  La fonction *Port Monitor* surveille uniquement les paquets broadcast et multicast.

Threshold type

Indique l'unité utilisée pour le débit de données.

Valeurs possibles :

- `pps` (réglage par défaut)
  paquets par seconde
- `kbps`
  kbit par seconde
  Il convient pour cela que la valeur de la colonne *Traffic type* soit préalablement réglée sur `all`.

Lower threshold

Indique la valeur limite inférieure du débit de données.

La fonction *Auto-Disable* réactive le port uniquement lorsque la charge détectée sur le port est inférieure à la valeur spécifiée ici.

Valeurs possibles :

- `0..10000000` (réglage par défaut : `0`)

Upper threshold

Indique la valeur limite supérieure du débit de données.

Lorsque la fonction *Port Monitor* détecte cette charge lors de la période surveillée, l'équipement exécute l'action spécifiée.

Valeurs possibles :

- `0..10000000` (réglage par défaut : `0`)

Interval [s]

Indique la période en secondes pendant laquelle la fonction *Port Monitor* observe un paramètre pour détecter un dépassement de valeur limite.

Valeurs possibles :

- `1..20` (réglage par défaut : `1`)

Packets

Affiche le nombre de paquets broadcast, multicast et unicast que l'équipement a détectés lors de la période écoulée.

Broadcast packets

Affiche le nombre de paquets broadcast que l'équipement a détectés lors de la période écoulée.

Multicast packets

Affiche le nombre de paquets multicast que l'équipement a détectés lors de la période écoulée.

Kbit/s

Affiche le débit de données en kilobits par seconde que l'équipement a détecté lors de la période écoulée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Réactive le port mis en surbrillance dans la table et réinitialise son compteur sur `0`. Cette opération se répercute sur les compteurs des boîtes de dialogue suivantes :

- Boîte de dialogue *Diagnostics > Ports > Port Monitor*
  - Onglet *Link flap*
  - Onglet *CRC/Fragments*
  - Onglet *Overload detection*
- Boîte de dialogue *Diagnostics > Ports > Auto-Disable*

[Link speed/Duplex mode detection]

Cet onglet vous permet d'activer les combinaisons de vitesse et de mode duplex pour chaque port.

La fonction *Port Monitor* surveille les ports pour lesquels la case de la colonne *Link speed/Duplex mode detection on* est cochée dans l'onglet *Global*.

La fonction *Port Monitor* surveille uniquement les ports physiques activés.

Table

Port

Affiche le numéro de port.

10 Mbit/s HDX

Active/désactive la surveillance des ports pour accepter une combinaison de half duplex et d'un débit de données de 10 Mbit/s sur le port.

Valeurs possibles :

- `case cochée`
  La surveillance des ports prend en compte cette combinaison de vitesse et de duplex.
- `case non cochée`
  Lorsque l'équipement détecte cette combinaison de vitesse et de duplex sur le port, l'équipement exécute l'action spécifiée dans l'onglet *Global*.

10 Mbit/s FDX

Active/désactive la surveillance des ports pour accepter une combinaison de full duplex et d'un débit de données de 10 Mbit/s sur le port.

Valeurs possibles :

- `case cochée`
  La surveillance des ports prend en compte cette combinaison de vitesse et de duplex.
- `case non cochée`
  Lorsque l'équipement détecte cette combinaison de vitesse et de duplex sur le port, l'équipement exécute l'action spécifiée dans l'onglet *Global*.

100 Mbit/s HDX

Active/désactive la surveillance des ports pour accepter une combinaison de half duplex et d'un débit de données de 100 Mbit/s sur le port.

Valeurs possibles :

- `case cochée`
  La surveillance des ports prend en compte cette combinaison de vitesse et de duplex.
- `case non cochée`
  Lorsque l'équipement détecte cette combinaison de vitesse et de duplex sur le port, l'équipement exécute l'action spécifiée dans l'onglet *Global*.

100 Mbit/s FDX

Active/désactive la surveillance des ports pour accepter une combinaison de full duplex et d'un débit de données de 100 Mbit/s sur le port.

Valeurs possibles :

- `case cochée`
  La surveillance des ports prend en compte cette combinaison de vitesse et de duplex.
- `case non cochée`
  Lorsque l'équipement détecte cette combinaison de vitesse et de duplex sur le port, l'équipement exécute l'action spécifiée dans l'onglet *Global*.

1,000 Mbit/s FDX

Active/désactive la surveillance des ports pour accepter une combinaison de full duplex et d'un débit de données de 1 Gbit/s sur le port.

Valeurs possibles :

- `case cochée`
  La surveillance des ports prend en compte cette combinaison de vitesse et de duplex.
- `case non cochée`
  Lorsque l'équipement détecte cette combinaison de vitesse et de duplex sur le port, l'équipement exécute l'action spécifiée dans l'onglet *Global*.

2.5 Gbit/s FDX

Active/désactive la surveillance des ports pour accepter une combinaison de full duplex et d'un débit de données de 2,5 Gbit/s sur le port.

Valeurs possibles :

- `case cochée`
  La surveillance des ports prend en compte cette combinaison de vitesse et de duplex.
- `case non cochée`
  Lorsque l'équipement détecte cette combinaison de vitesse et de duplex sur le port, l'équipement exécute l'action spécifiée dans l'onglet *Global*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Réactive le port mis en surbrillance dans la table et réinitialise son compteur sur `0`. Cette opération se répercute sur les compteurs des boîtes de dialogue suivantes :

- Boîte de dialogue *Diagnostics > Ports > Port Monitor*
  - Onglet *Link flap*
  - Onglet *CRC/Fragments*
  - Onglet *Overload detection*
- Boîte de dialogue *Diagnostics > Ports > Auto-Disable*

6.5.4 Auto-Disable

[Diagnostics > Ports > Auto-Disable]

La fonction *Auto-Disable* vous permet de désactiver automatiquement les ports surveillés et de les réactiver autant de fois que vous le souhaitez.

Par exemple, la fonction *Port Monitor* et les fonctions sélectionnées dans le menu *Network Security* utilisent la fonction *Auto-Disable* pour désactiver les ports lorsque les paramètres surveillés dépassent les valeurs limites.

Lorsque les paramètres cessent de dépasser les valeurs limites, la fonction *Auto-Disable* réactive le port concerné après le temps d'attente spécifié.

La boîte de dialogue contient les onglets suivants :
- [Port]
- [Status]

[Port]

Cet onglet affiche les ports actuellement désactivés en raison du dépassement des valeurs limites des paramètres. Lorsque les paramètres cessent de dépasser les valeurs limites et que vous spécifiez un temps d'attente dans la colonne *Reset timer [s]*, la fonction *Auto-Disable* réactive automatiquement le port concerné.

Table

Port

Affiche le numéro de port.

Reset timer [s]

Indique le temps d'attente en secondes après lequel la fonction *Auto-Disable* réactive le port.

Valeurs possibles :
- `0` (réglage par défaut)
  Le temporisateur est désactivé. Le port reste désactivé.
- `30..4294967295`
  Lorsque les paramètres cessent de dépasser les valeurs limites, la fonction *Auto-Disable* réactive le port après le temps d'attente spécifié ici.

Error time

Affiche le moment auquel l'équipement a désactivé le port en raison du dépassement des valeurs limites des paramètres.

Remaining time [s]

Affiche le temps restant en secondes jusqu'à ce que la fonction *Auto-Disable* réactive le port.

Component

Affiche le composant logiciel de l'équipement qui a désactivé le port.

Valeurs possibles :

- `PORT_MON`
  Port Monitor
  Voir la boîte de dialogue *Diagnostics > Ports > Port Monitor*.
- `PORT_ML`
  Port Security
  Voir la boîte de dialogue *Network Security > Port Security*.
- `DHCP_SNP`
  DHCP Snooping
  Voir la boîte de dialogue *Network Security > DHCP Snooping*.
- `DOT1S`
  BPDU guard
  Voir la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*.
- `DAI`
  Dynamic ARP Inspection
  Voir la boîte de dialogue *Network Security > Dynamic ARP Inspection*.

Reason

Affiche le paramètre surveillé qui a entraîné la désactivation du port.

Valeurs possibles :

- `none`
  Pas de paramètre surveillé.
  Le port est activé.
- `link-flap`
  Un trop grand nombre de modifications de lien a été détecté. Voir la boîte de dialogue *Diagnostics > Ports > Port Monitor*, onglet *Link flap*.
- `crc-error`
  Un trop grand nombre d'erreurs CRC/de fragments a été détecté. Voir la boîte de dialogue *Diagnostics > Ports > Port Monitor*, onglet *CRC/Fragments*.
- `duplex-mismatch`
  Une non-concordance de duplex a été détectée. Voir la boîte de dialogue *Diagnostics > Ports > Port Monitor*, onglet *Global*.
- `dhcp-snooping`
  Un trop grand nombre de paquets DHCP provenant de sources non fiables. Voir la boîte de dialogue *Network Security > DHCP Snooping > Configuration*, onglet *Port*.
- `arp-rate`
  Un trop grand nombre de paquets ARP provenant de sources non fiables. Voir la boîte de dialogue *Network Security > Dynamic ARP Inspection > Configuration*, onglet *Port*.
- `bpdu-rate`
  Des STP-BPDU ont été reçus. Voir la boîte de dialogue *Switching > L2-Redundancy > Spanning Tree > Global*.
- `mac-based-port-security`
  Un trop grand nombre de paquets de données provenant d'expéditeurs non souhaités a été détecté. Voir la boîte de dialogue *Network Security > Port Security*.
- `overload-detection`
  Surcharge. Voir la boîte de dialogue *Diagnostics > Ports > Port Monitor*, onglet *Overload detection*.

- `speed-duplex`
  Une combinaison non autorisée de vitesse et de mode duplex a été détectée. Voir la boîte de dialogue *Diagnostics > Ports > Port Monitor*, onglet *Link speed/Duplex mode detection*.
- `Loop protection`
  Une boucle de réseau de couche 2 a été détectée sur le port. Voir la boîte de dialogue *Diagnostics > Loop Protection*, colonne *Loop detected*.

Active

Indique si le port est actuellement désactivé en raison du dépassement des valeurs limites des paramètres.

Valeurs possibles :

- `case cochée`
  Le port est actuellement désactivé.
- `case non cochée`
  Le port est activé.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[Status]

Cet onglet affiche les paramètres surveillés pour lesquels la fonction *Auto-Disable* est activée.

Table

Reason

Affiche les paramètres surveillés par l'équipement.

Cochez la case adjacente afin que la fonction *Auto-Disable* désactive et, le cas échéant, réactive le port lorsque les paramètres surveillés dépassent les valeurs limites.

Category

Indique la fonction à laquelle le paramètre adjacent appartient.

Valeurs possibles :

- `port-monitor`
  Le paramètre appartient aux fonctions du menu *Diagnostics > Port > Port Monitor*.
- `network-security`
  Le paramètre appartient aux fonctions du menu *Network Security*.
- `l2-redundancy`
  Le paramètre appartient aux fonctions du menu *Switching > L2-Redundancy*.

Auto-disable

Indique si la fonction *Auto-Disable* est activée/désactivée pour le paramètre adjacent.

Valeurs possibles :

- `case cochée`
  La fonction *Auto-Disable* est activée pour les paramètres adjacents.
  La fonction *Auto-Disable* désactive et, le cas échéant, réactive le port concerné lorsque les paramètres surveillés dépassent les valeurs limites.
- `case non cochée` (réglage par défaut)
  La fonction *Auto-Disable* est désactivée pour les paramètres adjacents.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Réactive le port mis en surbrillance dans la table et réinitialise son compteur sur `0`. Cette opération se répercute sur les compteurs des boîtes de dialogue suivantes :

- Boîte de dialogue *Diagnostics > Ports > Port Monitor*
  - Onglet *Link flap*
  - Onglet *CRC/Fragments*
  - Onglet *Overload detection*
- Boîte de dialogue *Diagnostics > Ports > Auto-Disable*

6.5.5 Port Mirroring

[Diagnostics > Ports > Port Mirroring]

La fonction *Port Mirroring* vous permet de copier les paquets de données reçus et envoyés par les ports sélectionnés vers un port cible. Vous pouvez consulter et traiter le flux de données à l'aide d'un analyseur ou d'une sonde RMON connecté au port cible. Les paquets de données ne sont pas modifiés sur le port source.

Commentaire : Pour activer l'accès à l'administration de l'équipement à l'aide du port cible, cochez la case *Allow management* dans le cadre *Destination port* avant d'activer la fonction *Port Mirroring*.

Operation

Operation

Active/désactive la fonction *Port Mirroring*.

Valeurs possibles :

- *On*
  La fonction *Port Mirroring* est activée.
  L'équipement copie les paquets de données des ports sources sélectionnés vers le port cible.
- *Off* (réglage par défaut)
  La fonction *Port Mirroring* est désactivée.

Destination port

Primary port

Indique le port cible.

Les ports qui conviennent pour cette fonction sont ceux qui ne sont pas utilisés pour les raisons suivantes :

- Port source
- Protocoles de redondance L2

Valeurs possibles :

- `no Port` (réglage par défaut)
  Pas de port cible sélectionné.
- `<Numéro de port>`
  Numéro du port cible. L'équipement copie les paquets de données des ports sources vers ce port.

Sur le port cible, l'équipement ajoute un tag VLAN aux paquets de données que le port source transmet. Le port cible transmet les paquets de données non modifiés que le port source reçoit.

Commentaire : Le port cible a besoin d'une bande passante suffisante pour absorber le flux de données. Si le flux de données copié dépasse la bande passante du port cible, l'équipement rejette les paquets de données en surplus sur le port cible.

Secondary port

Spécifie un deuxième port cible. La condition préalable est que vous ayez spécifié un port principal.

Valeurs possibles :

- `no Port` (réglage par défaut)
  Pas de port cible sélectionné.
- `<Numéro de port>`
  Numéro du port cible. L'équipement copie les paquets de données des ports sources vers ce port.

Allow management

Active/désactive l'accès à l'administration de l'équipement à l'aide du port cible.

Valeurs possibles :

- `case cochée`
  L'accès à l'équipement à l'aide du port cible est activé.
  L'équipement permet aux utilisateurs d'avoir accès à l'administration de l'équipement à l'aide du port cible sans interrompre la session *Port Mirroring* active.
  - 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'administration de l'équipement à l'aide du port cible est que le port cible ne soit pas un membre du VLAN de l'administration de l'équipement.
- `case non cochée` (réglage par défaut)
  L'accès à l'administration de l'équipement à l'aide du port cible est désactivé.
  L'équipement interdit l'accès à l'administration de l'équipement à l'aide du port cible.

Table

Source port

Affiche le numéro de port.

Valeurs possibles :

- `<Numéro de port>`

Enabled

Active/désactive la copie des paquets de données de ce port source vers le port cible.

Valeurs possibles :

- `case cochée`
  La copie des paquets de données est activée.
  Le port est spécifié comme port source.
- `case non cochée` (réglage par défaut)
  La copie des paquets de données est désactivée.
- (Apparaît grisé)
  Il n'est pas possible de copier les paquets de données pour ce port.
  Causes possibles :
  - Le port est déjà spécifié comme port cible.
  - Le port est un port logique, pas un port physique.

Commentaire : L'équipement vous permet d'activer tous les ports physiques comme port source, sauf le port cible.

Type

Indique quels paquets de données sont copiés par l'équipement vers le port cible.

Sur le port cible, l'équipement ajoute un tag VLAN aux paquets de données que le port source transmet. Le port cible transmet les paquets de données non modifiés que le port source reçoit.

Valeurs possibles :

- `none` (réglage par défaut)
  Aucun paquets de données.
- `tx`
  Les paquets de données que le port source transmet.
- `rx`
  Les paquets de données que le port source reçoit.
- `txrx`
  Les paquets de données que le port source transmet et reçoit.

Commentaire : Avec le réglage `txrx`, l'équipement copie les paquets de données transmis et reçus. Les ports cibles ont besoin d'une bande passante correspondant au moins à la somme des canaux d'envoi et de réception des ports sources. Par exemple, pour des ports similaires, le port cible est à 100 % de capacité lorsque les canaux d'envoi et de réception d'un port source sont respectivement à 50 % de capacité.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset config

Rétablit les réglages par défaut de la boîte de dialogue et transfère les modifications vers la mémoire volatile de l'équipement (*RAM*).

6.6 LLDP

[Diagnostics > LLDP]

L'équipement vous permet de rassembler des informations sur les équipements voisins. Pour ce faire, l'équipement utilise le protocole LLDP (Link Layer Discovery Protocol). Grâce à ces informations, une station d'administration réseau est en mesure de représenter la structure de votre réseau.

Ce menu vous permet de configurer la découverte de la topologie et d'afficher les informations reçues sous forme de table.

Le menu contient les boîtes de dialogue suivantes :

- LLDP Configuration
- LLDP Topology Discovery

6.6.1 LLDP Configuration

[Diagnostics > LLDP > Configuration]

Cette boîte de dialogue vous permet de configurer la découverte de la topologie pour chaque port.

Operation

Operation

Active/désactive la fonction *LLDP*.

Valeurs possibles :

- `On` (réglage par défaut)
  La fonction *LLDP* est activée.
  La découverte de la topologie basée sur LLDP est activée sur l'équipement.
- `Off`
  La fonction *LLDP* est désactivée.

Configuration

Transmit interval [s]

Indique l'intervalle en secondes selon lequel l'équipement transmet les paquets de données LLDP.

Valeurs possibles :

- `5..32768` (réglage par défaut : `30`)

Transmit interval multiplier

Indique le facteur permettant de déterminer la valeur « Time To Live » pour les paquets de données LLDP.

Valeurs possibles :

- `2..10` (réglage par défaut : `4`)

La valeur « Time To Live » codée dans l'en-tête LLDP est obtenue en multipliant cette valeur avec la valeur du champ *Transmit interval [s]*.

Reinit delay [s]

Indique le délai en secondes pour la réinitialisation d'un port.

Valeurs possibles :

- `1..10` (réglage par défaut : `2`)

Si dans la colonne *Operation*, la valeur `Off` est spécifiée, l'équipement tente de réinitialiser le port une fois que la période spécifiée ici s'est écoulée.

Transmit delay [s]

Indique le délai en secondes pour la transmission de paquets de données LLDP successifs à la suite de modifications apportées à la configuration de l'équipement.

Valeurs possibles :

- `1..8192` (réglage par défaut : `2`)

La valeur recommandée est située entre un minimum de `1` et un maximum d'un quart de la valeur du champ *Transmit interval [s]*.

Notification interval [s]

Indique l'intervalle en secondes pour la transmission des notifications LLDP.

Valeurs possibles :

- `5..3600` (réglage par défaut : `5`)

Après la transmission d'un trap de notification, l'équipement patiente au minimum pendant le temps spécifié ici avant de transmettre le prochain trap de notification.

Table

Port

Affiche le numéro de port.

Operation

Indique si le port transmet et reçoit les paquets de données LLDP.

Valeurs possibles :

- *transmit*
  Le port transmet les paquets de données LLDP mais ne sauvegarde pas les informations relatives aux équipements voisins.
- *receive*
  Le port reçoit les paquets de données LLDP mais ne transmet pas les informations relatives aux équipements voisins.
- *receive and transmit* (réglage par défaut)
  Le port transmet les paquets de données LLDP et sauvegarde les informations relatives aux équipements voisins.
- *disabled*
  Le port ne transmet pas les paquets de données LLDP et ne sauvegarde pas les informations relatives aux équipements voisins.

Notification

Active/désactive les notifications LLDP sur le port.

Valeurs possibles :

- `case cochée`
  Les notifications LLDP sont activées sur le port.
- `case non cochée` (réglage par défaut)
  Les notifications LLDP sont désactivées sur le port.

Transmit port description

Active/désactive la transmission d'un TLV (Type Longueur Valeur) avec la description du port.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La transmission du TLV est activée.
  L'équipement transmet le TLV avec la description du port.
- `case non cochée`
  La transmission du TLV est désactivée.
  L'équipement ne transmet pas de TLV avec la description du port.

Transmit system name

Active/désactive la transmission d'un TLV (Type Longueur Valeur) avec la description du port.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La transmission du TLV est activée.
  L'équipement transmet le TLV avec la description de l'équipement.
- `case non cochée`
  La transmission du TLV est désactivée.
  L'équipement ne transmet pas de TLV avec le nom de l'équipement.

Transmit system description

Active/désactive la transmission du TLV (Type Longueur Valeur) avec la description du système.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La transmission du TLV est activée.
  L'équipement transmet le TLV avec la description du système.
- `case non cochée`
  La transmission du TLV est désactivée.
  L'équipement ne transmet pas de TLV avec la description du système.

Transmit system capabilities

Active/désactive la transmission du TLV (Type Longueur Valeur) avec les fonctionnalités système.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La transmission du TLV est activée.
  L'équipement transmet le TLV avec les fonctionnalités du système.
- `case non cochée`
  La transmission du TLV est désactivée.
  L'équipement ne transmet pas de TLV avec les fonctionnalités du système.

Neighbors (max.)

Limite le nombre d'équipements voisins à enregistrer pour ce port.

Valeurs possibles :

- `1..50` (réglage par défaut : `10`)

FDB mode

Indique quelle fonction l'équipement utilise pour enregistrer les équipements voisins sur ce port.

Valeurs possibles :

- `lldpOnly`
  L'équipement utilise uniquement les paquets de données LLDP pour enregistrer les équipements voisins sur ce port.
- `macOnly`
  L'équipement utilise les adresses MAC apprises pour enregistrer les équipements voisins sur ce port. L'équipement utilise l'adresse MAC uniquement si aucune autre entrée n'existe pour ce port dans la table d'adresses (base de données FDB, Forwarding Database).
- `both`
  L'équipement utilise les paquets de données LLDP et les adresses MAC apprises pour enregistrer les équipements voisins sur ce port.
- `autoDetect` (réglage par défaut)
  Lorsque l'équipement reçoit des paquets de données LLDP sur ce port, l'équipement fonctionne de la même manière qu'avec le réglage `lldpOnly`. Sinon, l'équipement fonctionne de la même manière qu'avec le réglage `macOnly`.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6.6.2 LLDP Topology Discovery

[Diagnostics > LLDP > Topology Discovery]

Les équipements de réseau envoient des notifications sous forme de paquets également connus sous le nom de « LLDPDU » (unités de données LLDP). Les données qui sont envoyées et reçues via des LLDPDU sont utiles pour de nombreuses raisons. L'équipement détecte ainsi les équipements voisins sur le réseau et les ports via lesquels ils sont connectés.

Cette boîte de dialogue vous permet d'afficher le réseau et de détecter les équipements connectés et leurs caractéristiques spécifiques.

La boîte de dialogue contient les onglets suivants :
- [LLDP]
- [LLDP-MED]

[LLDP]

Cet onglet affiche les informations LLDP collectées pour les équipements voisins. Grâce à ces informations, une station d'administration réseau est en mesure de représenter la structure de votre réseau.

Lorsque les équipements avec et sans fonction de découverte de la topologie sont connectés à un port, la table de topologie masque les équipements sans découverte de la topologie activée.

Lorsque seuls les équipements sans découverte de la topologie active sont connectés à un port, la table contient une ligne pour ce port afin de représenter tous les équipements. Cette ligne contient le nombre d'équipements connectés.

La table d'adresses de la base de données FDB (Forwarding Database) contient les adresses MAC des équipements que la table de topologie masque à des fins de clarté.

Lorsque vous utilisez un port pour connecter plusieurs équipements, par exemple via un concentrateur, la table contient une ligne pour chaque équipement connecté.

Table

Port

Affiche le numéro de port.

Neighbor identifier

Affiche l'identifiant du châssis de l'équipement voisin. Il peut par exemple s'agir de l'adresse MAC de base de l'équipement voisin.

FDB

Indique si l'équipement connecté prend activement en charge le protocole LLDP.

Valeurs possibles :

- `case cochée`
  L'équipement connecté ne prend pas activement en charge le protocole LLDP.
  L'équipement utilise des informations de sa table d'adresses (FDB, Forwarding Database)
- `case non cochée` (réglage par défaut)
  L'équipement connecté prend activement en charge le protocole LLDP.

Neighbor IP address

Indique l'adresse IP avec laquelle l'accès à l'administration de l'équipement voisin est possible.

Neighbor port description

Affiche une description pour le port de l'équipement voisin.

Neighbor system name

Affiche le nom de l'équipement voisin.

Neighbor system description

Affiche une description pour l'équipement voisin.

Port ID

Affiche l'ID du port via lequel l'équipement voisin est connecté à l'équipement.

Autonegotiation supported

Indique si le port de l'équipement voisin prend en charge l'auto-négociation.

Autonegotiation

Indique si l'auto-négociation est activée sur le port de l'équipement voisin.

PoE supported

Indique si le port de l'équipement voisin prend en charge Power-over-Ethernet (PoE).

PoE enabled

Indique si Power-over-Ethernet (PoE) est activé sur le port de l'équipement voisin.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[LLDP-MED]

LLDP-MED (LLDP for Media Endpoint Devices) est une extension du protocole LLDP intervenant entre les équipements terminaux et les équipements de réseau. Cette extension permet spécifiquement la prise en charge des applications VoIP. Dans cette règle de support, elle offre un ensemble supplémentaire de messages communs d'annonces Type Longueur Valeur (TLV). L'équipement utilise les TLV pour la découverte des fonctionnalités, comme la stratégie de réseau, la fonction Power-over-Ethernet, la gestion de l'inventaire et les informations de localisation.

Table

Port

Affiche le numéro de port.

Device class

Affiche la catégorie de l'équipement connecté à distance.

- Une valeur `notDefined` indique que l'équipement est doté de fonctionnalités qui ne sont couvertes par aucune catégorie *LLDP-MED*.
- Une valeur de `endpointClass1..3` indique que l'équipement est doté de fonctionnalités de « catégorie d'équipement terminal 1 ..3 ».
- Une valeur de `networkConnectivity` indique que l'équipement est doté de fonctionnalités d'équipement de connectivité réseau.

VLAN ID

Affiche l'extension de l'identifiant VLAN pour le système distant connecté à ce port, tel que défini dans IEEE 802.3.

- L'équipement utilise une valeur de `1` à `4042` pour spécifier un Port VLAN-ID.
- L'équipement affiche la valeur `0` pour les paquets dotés de tags prioritaires. Cela signifie que seule la priorité 802.1D est significative et que l'équipement utilise le VLAN-ID par défaut du port d'entrée.

Priority

Affiche la valeur de la priorité 802.1D qui est associée au système distant connecté au port.

DSCP

Affiche la valeur du DSCP (Differentiated Service Code Point) qui est associé au système distant connecté au port.

Unknown bit status

Affiche l'état de bit inconnu du trafic entrant.

- La valeur `true` indique que la stratégie de réseau associée au type d'application spécifié est actuellement inconnue. Dans ce cas, le VLAN-ID ignore la priorité de niveau 2 et la valeur du champ *DSCP*.
- La valeur `false` indique une stratégie de réseau spécifiée.

Tagged bit status

Affiche l'état de bit avec tag.

- La valeur `true` indique que l'application utilise un VLAN muni d'un tag.
- La valeur `false` indique que l'équipement utilise un VLAN muni d'un tag. Dans ce cas, l'équipement ignore les champs du VLAN-ID et de la priorité de niveau 2. Cependant, la valeur DSCP est prise en compte.

Hardware revision

Affiche la chaîne de caractères de la révision du matériel spécifique au fournisseur tel qu'annoncé par l'équipement terminal distant.

Firmware revision

Affiche la chaîne de caractères de la révision du firmware spécifique au fournisseur tel qu'annoncé par l'équipement terminal distant.

Software revision

Affiche la chaîne de caractères de la révision du logiciel spécifique au fournisseur tel qu'annoncé par l'équipement terminal distant.

Serial number

Affiche la chaîne de caractères de la révision du numéro de série spécifique au fournisseur tel qu'annoncé par l'équipement terminal distant.

Manufacturer name

Affiche la chaîne de caractères de la révision du nom du fabricant spécifique au fournisseur tel qu'annoncé par l'équipement terminal distant.

Model name

Affiche la chaîne de caractères du nom de modèle spécifique au fournisseur tel qu'annoncé par l'équipement terminal distant.

Asset ID

Affiche la chaîne de caractères du suivi des actifs spécifique au fournisseur tel qu'annoncé par l'équipement terminal distant.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

6.7 Loop Protection

[Diagnostics > Loop Protection]

La fonction *Loop Protection* 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.

Dans les topologies de réseau redondantes, plusieurs protocoles de redondance sont généralement activés. Vous désactivez généralement la fonction *Spanning Tree* sur les ports impliqués dans d'autres protocoles de redondance. Les protocoles de redondance contribuent déjà à éviter les boucles.

Operation

Operation

Active/désactive la fonction *Loop Protection*.

Valeurs possibles :

▶ `On`
La fonction *Loop Protection* est activée.
- Sur les ports actifs et passifs, l'équipement évalue les paquets de *détection de boucle* reçus. Sur les ports actifs, l'équipement envoie des paquets de *détection de boucle* à intervalles réguliers, comme spécifié dans le champ *Transmit interval*.
  La condition préalable est que la fonction *Loop Protection* soit activée sur le port.
- L'équipement vous permet de surveiller les boucles Ethernet à l'aide du contact sec. Voir la boîte de dialogue *Diagnostics > Status Configuration > Signal Contact > Signal Contact 1*, case à cocher pour le paramètre *Ethernet loops*.

▶ `Off` (réglage par défaut)
La fonction *Loop Protection* est désactivée.
L'équipement n'envoie pas de paquets de *détection de boucle* et n'évalue pas les paquets de *détection de boucle* reçus.

Global

Transmit interval

Spécifie l'intervalle en secondes selon lequel l'équipement envoie des paquets de *détection de boucle* si la fonction *Loop Protection* est activée sur le port.

Valeurs possibles :

- `1..10`

Receive threshold

Spécifie la valeur seuil pour le nombre de paquets de *détection de boucle* reçus consécutivement. Si le nombre atteint ou dépasse ce seuil, l'équipement exécute l'action spécifiée dans la colonne *Action*.

Valeurs possibles :

- `1..50`

Configuration

Auto-disable

Active/désactive la fonction *Auto-Disable* relative à la *Loop Protection*.

Valeurs possibles :

- `case cochée`
  La fonction *Auto-Disable* relative à la *Loop Protection* est activée.
  La condition préalable à la désactivation du port est que l'action *auto-disable* ou *all* soit spécifiée dans la colonne *Action*.
  L'équipement vous permet de spécifier le temps d'attente en secondes après lequel la fonction *Auto-Disable* réactive le port. Pour cela, dans la boîte de dialogue *Diagnostics > Ports > Auto-Disable*, spécifiez le temps d'attente dans la colonne *Reset timer [s]*.
- `case non cochée` (réglage par défaut)
  La fonction *Auto-Disable* relative à la *Loop Protection* est désactivée.

Table

Port

Affiche le numéro de port.

Active

Active/désactive la fonction *Loop Protection* sur le port.

Valeurs possibles :

- `case cochée`
  La fonction *Loop Protection* est activée sur le port.
  Activez la fonction uniquement sur les ports qui ne font pas partie d'un chemin réseau redondant. Cela permet d'éviter une interruption accidentelle des chemins réseau redondants.
  Si l'équipement reçoit un paquet de *détection de boucle* sur ce port, envoyé depuis un autre port du même équipement, l'équipement exécute l'action spécifiée dans la colonne *Action*.
- `case non cochée` (réglage par défaut)
  La fonction *Loop Protection* est désactivée sur le port. Le port n'envoie pas de paquets de *détection de boucle* et n'évalue pas les paquets de *détection de boucle* reçus.

Mode

Spécifie le comportement de la fonction *Loop Protection* sur le port.

Valeurs possibles :

- *active*
  L'équipement envoie des paquets de *détection de boucle* et évalue les paquets de *détection de boucle* reçus.
- *passive*
  L'équipement évalue les paquets de *détection de boucle* reçus.

Action

Spécifie l'action que l'équipement exécute lorsqu'il détecte une boucle de réseau de couche 2 sur ce port.

Valeurs possibles :

- *trap*
  L'équipement envoie un trap.
- *auto-disable*
  L'équipement désactive le port à l'aide de la fonction *Auto-Disable*.
  La condition préalable à la désactivation du port est que la case *Auto-disable* dans le cadre *Configuration* soit cochée.
- *all*
  L'équipement envoie un trap. Ensuite, l'équipement désactive le port à l'aide de la fonction *Auto-Disable*.
  La condition préalable à la désactivation du port est que la case *Auto-disable* dans le cadre *Configuration* soit cochée.

VLAN ID

Spécifie le VLAN dans lequel l'équipement envoie les paquets de *détection de boucle*.

Valeurs possibles :

- `0` (réglage par défaut)
  L'équipement envoie les paquets de *détection de boucle* sans tag de VLAN.
- `1..4042`
  L'équipement envoie les paquets de *détection de boucle* dans le VLAN spécifié. La condition préalable est que le VLAN soit déjà configuré et que le port soit membre du VLAN. Voir la boîte de dialogue *Switching > VLAN > Port*.

Loop detected

Affiche si l'équipement a détecté une boucle de réseau de couche 2 sur le port.

Valeurs possibles :

- *yes*
  L'équipement a détecté une boucle de réseau de couche 2 sur le port.
  Une fois la boucle terminée et le port à nouveau activé, l'équipement réinitialise la valeur à *no*.
- *no*
  L'équipement n'a pas détecté de boucle de réseau de couche 2 sur le port.

Loop count

Affiche le nombre de boucles que l'équipement a détectées sur le port depuis la dernière réinitialisation des statistiques du port ou depuis le dernier redémarrage de l'équipement.

Last loop time

Affiche l'heure à laquelle l'équipement a détecté la dernière boucle sur le port.

La condition préalable à l'évaluation correcte de la valeur est que vous synchronisiez l'heure système de l'équipement avec l'heure de référence appropriée. Voir la boîte de dialogue *Time* > Basic Settings.

Sent frames

Affiche le nombre de paquets de *détection de boucle* envoyés sur le port depuis la dernière réinitialisation des statistiques du port ou depuis le dernier redémarrage de l'équipement.

Received frames

Affiche le nombre de paquets de *détection de boucle* envoyés et reçus en retour sur le port depuis la dernière réinitialisation des statistiques du port ou depuis le dernier redémarrage de l'équipement.

Discarded frames

Affiche le nombre de paquets de *détection de boucle* rejetés sur le port.

Exemples de raisons expliquant le rejet de paquets :

- L'équipement détecte des paquets dont le format est incorrect.
- L'équipement détecte des paquets dont l'horodatage a expiré (paquets reçus plus de 5 secondes après l'envoi).
- L'équipement a reçu un paquet de données avec une information VLAN inattendue.
- L'équipement détecte des paquets reçus sur un port qui est désactivé.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Clear port statistics

Réinitialise les valeurs des colonnes suivantes :

- *Loop count*
- *Sent frames*
- *Received frames*

6.8 Report

[Diagnostics > Report]

Le menu contient les boîtes de dialogue suivantes :

- Report Global
- Persistent Logging
- System Log
- Audit Trail

6.8.1 Report Global

[Diagnostics > Report > Global]

L'équipement vous permet de consigner des événements spécifiques à l'aide des sorties suivantes :
- sur la console
- sur un ou plusieurs serveurs Syslog
- sur une connexion à l'interface de ligne de commande à l'aide de SSH
- sur une connexion à l'interface de ligne de commande à l'aide de Telnet

Cette boîte de dialogue vous permet de spécifier les réglages requis. L'affectation du degré de gravité vous permet de spécifier les événements que l'équipement enregistre.

La boîte de dialogue vous permet de sauvegarder une archive ZIP avec les informations système sur votre PC.

Console logging

Operation

Active/désactive la fonction *Console logging*.

Valeurs possibles :
- *On*
  La fonction *Console logging* est activée.
  L'équipement consigne les événements survenus sur la console.
- *Off* (réglage par défaut)
  La fonction *Console logging* est désactivée.

Severity

Indique le degré de gravité minimum des événements. L'équipement consigne les événements présentant ce degré de gravité ou présentant des degrés de gravité plus urgents.

L'équipement émet les messages sur l'interface série.

Valeurs possibles :
- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (réglage par défaut)
- `notice`
- `informational`
- `debug`

Buffered logging

L'équipement met en mémoire tampon les événements consignés dans 2 zones de mémoire séparées de manière à conserver les entrées du log dédiées aux événements urgents.

Cette boîte de dialogue vous permet de spécifier le degré de gravité minimum pour les événements que l'équipement met en mémoire tampon dans la zone de mémoire présentant un degré de priorité supérieur.

Severity

Indique le degré de gravité minimum des événements. L'équipement met en mémoire tampon les entrées du log dédiées aux événements présentant ce degré de gravité dans la zone de mémoire présentant un degré de priorité supérieur.

Valeurs possibles :

- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (réglage par défaut)
- `notice`
- `informational`
- `debug`

SNMP logging

Lorsque vous activez la consignation des requêtes SNMP, l'équipement les envoie comme événements à la liste des serveurs Syslog avec le degré de gravité `notice` réglé par défaut. Le degré de gravité minimum réglé par défaut pour une entrée de serveur Syslog est `critical`.

Pour envoyer des requêtes SNMP à un serveur Syslog, vous disposez de plusieurs moyens de modifier les réglages par défaut. Sélectionnez ceux qui conviennent le mieux à vos besoins.

- ☐ Réglez le degré de gravité à partir duquel l'équipement crée des requêtes SNMP comme événements sur `warning` ou `error`. Modifiez le degré de gravité minimum pour une entrée Syslog sur la même valeur pour un ou plusieurs serveurs Syslog.
  Vous pouvez également créer une entrée de serveur Syslog séparée à cette fin.
- ☐ Réglez uniquement la gravité des requêtes SNMP sur `critical` ou sur un degré de gravité supérieur. L'équipement envoie alors aux serveurs Syslog les requêtes SNMP comme événements avec le degré de gravité `critical` ou un degré de gravité supérieur.
- ☐ Réglez uniquement le degré de gravité minimum pour une ou plusieurs entrées de serveur Syslog sur `notice` ou un degré de gravité inférieur. Il est alors possible que l'équipement envoie de nombreux événements aux serveurs Syslog.

Log SNMP get request

Active/désactive la consignation des SNMP Get requests.

Valeurs possibles :

- *On*
  La consignation est activée.
  L'équipement enregistre les SNMP Get requests comme événements dans le serveur syslog.
  Dans la liste déroulante *Severity get request*, sélectionnez le degré de gravité pour cet événement.
- *Off* (réglage par défaut)
  La consignation est désactivée.

Log SNMP set request

Active/désactive la consignation des SNMP Set requests.

Valeurs possibles :

- *On*
  La consignation est activée.
  L'équipement enregistre les SNMP Set requests comme événements dans le serveur syslog.
  Dans la liste déroulante *Severity set request*, sélectionnez le degré de gravité pour cet événement.
- *Off* (réglage par défaut)
  La consignation est désactivée.

Severity get request

Spécifie le degré de gravité de l'événement que l'équipement enregistre pour les SNMP Get requests.

Valeurs possibles :

- emergency
- alert
- critical
- error
- warning
- notice (réglage par défaut)
- informational
- debug

Severity set request

Spécifie le degré de gravité de l'événement que l'équipement enregistre pour les SNMP Set requests.

Valeurs possibles :

- emergency
- alert
- critical
- error
- warning
- notice (réglage par défaut)

- `informational`
- `debug`

CLI logging

Operation

Active/désactive la fonction *CLI logging*.

Valeurs possibles :

- *On*
  La fonction *CLI logging* est activée.
  L'équipement terminal consigne toutes les commandes reçues à l'aide de l'interface de ligne de commande.
- *Off* (réglage par défaut)
  La fonction *CLI logging* est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Download support information

Génère une archive ZIP que le navigateur Web vous permet de télécharger depuis l'équipement.

L'archive ZIP contient des informations système relative à l'équipement. Vous trouverez une explication des fichiers contenus dans l'archive ZIP dans la section suivante.

Informations destinées au support : fichiers contenus dans l'archive ZIP

Nom du fichier	Format	Remarques
`audittrail.html`	HTML	Contient l'enregistrement chronologique des événements du système et des modifications de l'utilisateur sauvegardées dans l'Audit Trail.
`defaultconfig.xml`	XML	Contient le profil de configuration avec les réglages par défaut.
`script`	TEXT	Contient la sortie de la commande la `show running-config script`.
`runningconfig.xml`	XML	Contient le profil de configuration avec les réglages d'exploitation actuels.
`supportinfo.html`	TEXT	Contient les informations des services internes de l'équipement.
`systeminfo.html`	HTML	Contient les informations relatives aux réglages et aux paramètres d'exploitation actuels.
`systemlog.html`	HTML	Contient les événements consignés dans le fichier log. Voir la boîte de dialogue *Diagnostics > Report > System Log*.

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
`notice`	État normal significatif
`informational`	Message à titre informatif
`debug`	Message de débogage

6.8.2 Persistent Logging

[Diagnostics > Report > Persistent Logging]

L'équipement vous permet de sauvegarder les entrées du log de manière permanente dans un fichier stocké dans la mémoire externe. Vous pouvez ainsi accéder aux entrées du log même après le redémarrage de l'équipement.

Cette boîte de dialogue vous permet de limiter la taille du fichier log et de spécifier le degré de gravité minimum pour les événements à sauvegarder. Lorsque le fichier log atteint la taille spécifiée, l'équipement archive ce fichier et sauvegarde les prochaines entrées de log dans un nouveau fichier.

Dans la table, l'équipement affiche les fichiers log stockés dans la mémoire externe. Dès que le nombre de fichiers maximum spécifié est atteint, l'équipement supprime le fichier le plus ancien et renomme les fichiers restants. Cette mesure contribue à préserver l'espace de stockage dans la mémoire externe.

Commentaire : Vérifiez qu'une mémoire externe est connectée. Pour vérifier qu'une mémoire externe est connectée, voir la colonne *Status* dans la boîte de dialogue *Basic Settings > External Memory*. Nous recommandons de surveiller la connexion de la mémoire externe à l'aide de la fonction *Device Status*, voir le paramètre *External memory removal* dans la boîte de dialogue *Diagnostics > Status Configuration > Device Status*.

Operation

Operation

Active/désactive la fonction *Persistent Logging*.

Activez uniquement cette fonction lorsque la mémoire externe est disponible dans l'équipement.

Valeurs possibles :

- *On* (réglage par défaut)
  La fonction *Persistent Logging* est activée.
  L'équipement sauvegarde les entrées du log dans un fichier stocké dans la mémoire externe.
- *Off*
  La fonction *Persistent Logging* est désactivée.

Configuration

Max. file size [kbyte]

Spécifie la taille maximale du fichier log en kilo-octets. Lorsque le fichier log atteint la taille spécifiée, l'équipement archive ce fichier et sauvegarde les prochaines entrées de log dans un nouveau fichier.

Valeurs possibles :

- 0..4096 (réglage par défaut : 1024)

La valeur 0 désactive la sauvegarde des entrées de log dans le fichier log.

Files (max.)

Indique le nombre de fichiers log que l'équipement conserve dans la mémoire externe.

Dès que le nombre de fichiers maximum spécifié est atteint, l'équipement supprime le fichier le plus ancien et renomme les fichiers restants.

Valeurs possibles :

- `0..25` (réglage par défaut : `4`)

La valeur `0` désactive la sauvegarde des entrées de log dans le fichier log.

Severity

Indique le degré de gravité minimum de l'événement. L'équipement sauvegarde l'entrée de log pour les événements présentant ce degré de gravité et des degrés de gravité plus urgents dans le fichier log stocké dans la mémoire externe.

Valeurs possibles :

- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (réglage par défaut)
- `notice`
- `informational`
- `debug`

Log file target

Indique l'équipement de mémoire externe dédié à la consignation.

Valeurs possibles :

- `usb`
  Mémoire USB externe (EAM)

Table

Index

Affiche l'index auquel l'entrée de table se réfère.

Valeurs possibles :

- `1..25`

l'équipement affecte automatiquement ce numéro.

File name

Affiche le nom du fichier log stocké dans la mémoire externe.

Valeurs possibles :

- `messages`
- `messages.X`

File size [byte]

Affiche la taille du fichier log stocké dans la mémoire externe.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Delete persistent log file

Efface les fichiers log de la mémoire externe.

6.8.3 System Log

[Diagnostics > Report > System Log]

L'équipement consigne les événements internes de l'équipement dans un fichier log (System Log).

Cette boîte de dialogue affiche le fichier log (System Log). La boîte de dialogue vous permet de sauvegarder le fichier log au format HTML sur votre PC.

Pour rechercher des termes dans le fichier log, utilisez la fonction de recherche de votre navigateur Web.

Le fichier log est conservé jusqu'au prochain redémarrage de l'équipement. Après le redémarrage, l'équipement recrée le fichier.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Save log file

Ouvre la page HTML dans une nouvelle fenêtre ou un nouvel onglet de navigateur Web. Vous pouvez sauvegarder la page HTML sur votre PC à l'aide de la commande de navigateur Web appropriée.

Delete log file

Supprime les événements consignés dans le fichier log.

6.8.4 Audit Trail

[Diagnostics > Report > Audit Trail]

Cette boîte de dialogue affiche le fichier log (Audit Trail). La boîte de dialogue vous permet de sauvegarder le fichier log au format HTML sur votre PC.

Pour rechercher des termes dans le fichier log, utilisez la fonction de recherche de votre navigateur Web.

L'équipement consigne les événements du système et les actions d'écriture de l'utilisateur effectuées dans l'équipement. Vous êtes ainsi en mesure de garder une trace des modifications apportées à l'équipement et d'identifier QUI les a effectuées, QUAND, et ce sur QUOI elles portaient. Il convient pour cela que le rôle d'utilisateur `auditor` ou `administrator` soit préalablement affecté à votre compte d'utilisateur.

L'équipement consigne notamment les actions de l'utilisateur suivantes :
- La connexion de l'utilisateur via l'interface de ligne de commande (locale ou distante)
- La déconnexion manuelle de l'utilisateur
- La déconnexion automatique d'un utilisateur dans l'interface de ligne de commande après une période d'inactivité spécifiée
- Redémarrage de l'équipement
- Blocage d'un compte d'utilisateur dû à de trop nombreux échecs de tentatives de connexion
- Blocage de l'accès à l'administration de l'équipement dû à des échecs de tentatives de connexion
- Commandes exécutées dans l'interface de ligne de commande, à l'exception des commandes `show`
- Modifications apportées aux variables de configuration
- Modifications apportées à l'heure système
- Opérations de transfert de fichiers, y compris les mises à jour des firmwares
- Modifications de la configuration via Ethernet Switch Configurator
- Les mises à jour des firmwares et la configuration automatique de l'équipement via la mémoire externe
- L'ouverture et la fermeture de SNMP via un tunnel HTTPS

L'équipement ne consigne pas les mots de passe. Les entrées consignées sont protégées en écriture et restent sauvegardées dans l'équipement après un redémarrage.

Pendant le redémarrage, l'accès au moniteur du système est possible à l'aide des réglages par défaut de l'équipement. Si un pirate informatique parvient à accéder physiquement à l'équipement, il sera capable de rétablir les réglages par défaut de l'équipement à l'aide du moniteur du système. Il pourra alors accéder à l'équipement et au fichier log à l'aide du mot de passe standard.

⚠ AVERTISSEMENT

FONCTIONNEMENT NON INTENTIONNEL DE L'ÉQUIPEMENT

Veuillez prendre les mesures appropriées pour restreindre l'accès physique à l'équipement. Sinon, veuillez désactiver le moniteur du système. Voir la boîte de dialogue *Diagnostics > System > Selftest*, case à cocher *SysMon1 is available*

Le non-respect de ces instructions peut entraîner la mort, des blessures graves ou des dommages matériels.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Save audit trail file

Ouvre la page HTML dans une nouvelle fenêtre ou un nouvel onglet de navigateur Web. Vous pouvez sauvegarder la page HTML sur votre PC à l'aide de la commande de navigateur Web appropriée.

7 Advanced

Le menu contient les boîtes de dialogue suivantes :

- DHCP L2 Relay
- DHCP Server
- DNS
- Industrial Protocols
- Digital IO Module
- Command Line Interface

7.1 DHCP L2 Relay

[Advanced > DHCP L2 Relay]

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 L2 pour ajouter les informations client DHCP. Les *agents de relais* L3 et les serveurs DHCP ont besoin des informations client DHCP pour affecter une adresse IP et une configuration aux clients.

Lorsqu'il est actif, le relais ajoute aux paquets les informations *Option 82* configurées dans cette boîte de dialogue avant de relayer les requêtes DHCP des clients vers le serveur. Les champs *Option 82* fournissent des informations uniques sur le client et le relais. Cet identifiant unique se compose d'un *ID circuit* pour le client et d'un *ID distant* pour le relais.

En plus des champs Type, Longueur et Multicast, l'*ID circuit* comprend le VLAN-ID, le numéro de l'unité, le numéro d'emplacement et le numéro du port du client connecté.

L'*ID distant* contient un champ Type et Longueur, et soit une adresse MAC, une adresse IP, l'identifiant du client ou une description de l'équipement définie par l'utilisateur. Un identifiant client est le nom du système défini par l'utilisateur pour l'équipement.

Pour le protocole DHCPv6, l'équipement utilise un *agent de relais* 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 :

- Messages *Relay-Forward*
  L'*agent de relais* transfère les messages *Relay-Forward* qui contiennent des informations uniques sur le client. Les informations sur le client comprennent l'adresse du pair, c'est-à-dire l'adresse de lien local IPv6 du client et l'information *Interface-ID*. L'information *Interface-ID*, également connue en tant que *Option 18*, fournit des informations qui identifient l'interface sur laquelle la requête du client a été envoyée.
- Messages *Relay-Reply*
  Le serveur DHCPv6 envoie des messages *Relay-Reply*. L'*agent de relais* valide les messages pour inclure les informations encapsulées dans le message initial *Relay-Forward*. Si les informations sont valides, l'*agent de relais* transfère le paquet au client.

Le menu contient les boîtes de dialogue suivantes :

- DHCP L2 Relay Configuration
- DHCP L2 Relay Statistics

7.1.1 DHCP L2 Relay Configuration

[Advanced > DHCP L2 Relay > Configuration]

Cette boîte de dialogue vous permet d'activer la fonction relais sur une interface ou un VLAN. Lorsque vous activez cette fonction sur un port, l'équipement relaie les informations *Option 82* ou supprime les informations sur les ports non fiables. De plus, l'équipement vous permet de spécifier l'identifiant distant.

Les informations *Option 82* sont spécifiques à la fonction de relais L2 du DHCPv4. Pour la fonction de relais DHCPv6 L2, les informations *Option 18* sont utilisées dans l'échange de paquets entre le client et le serveur DHCPv6. L'équipement rejette les paquets DHCPv6 reçus sur les ports qui ne contiennent pas les informations *Option 18*.

La boîte de dialogue contient les onglets suivants :
- [Interface]
- [VLAN ID]

Operation

Operation

Active/désactive la fonction de relais DHCP L2 de l'équipement globalement.

Lorsque cette fonction est activée, les fonctions DHCPv4 L2 Relay et DHCPv6 L2 Relay peuvent fonctionner simultanément sur l'équipement.

Valeurs possibles :

- `On`
  Active la fonction *DHCP L2 Relay* dans l'équipement.
- `Off` (réglage par défaut)
  Désactive la fonction *DHCP L2 Relay* dans l'équipement.

[Interface]

Table

Port

Affiche le numéro de port.

Active

Active/désactive la fonction *DHCP L2 Relay* sur le port.

Il convient pour cela que vous activiez préalablement la fonction globalement.

Valeurs possibles :

- `case cochée`
  La fonction *DHCP L2 Relay* est activée.
- `case non cochée` (réglage par défaut)
  La fonction *DHCP L2 Relay* est désactivée.

Trusted port

Active/désactive le mode *DHCP L2 Relay* sécurisé pour le port correspondant.

Valeurs possibles :

- `case cochée`
  L'équipement accepte les paquets DHCPv4 avec les informations *Option 82*.
  L'équipement accepte les paquets DHCPv6 avec les informations *Option 18*.
- `case non cochée` (réglage par défaut)
  L'équipement ignore les paquets DHCPv4 reçus sur les ports non sécurisés contenant les informations *Option 82*.
  L'équipement rejette les paquets DHCPv6 reçus sur les ports qui ne contiennent pas les informations *Option 18*.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

[VLAN ID]

Table

VLAN ID

VLAN auquel l'entrée de table se réfère.

Active

Active/désactive la fonction *DHCP L2 Relay* sur le VLAN.

Il convient pour cela que vous activiez préalablement la fonction globalement.

Valeurs possibles :

- `case cochée`
  La fonction *DHCP L2 Relay* est activée.
- `case non cochée` (réglage par défaut)
  La fonction *DHCP L2 Relay* est désactivée.

Circuit ID

Active ou désactive l'ajout de l'*ID circuit* aux informations *Option 82*.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  Active l'*ID circuit* et l'*ID distant* à envoyer ensemble.
- `case non cochée`
  L'équipement envoie uniquement l'*ID distant*.

Remote ID type

Spécifie les composants de l'*ID distant* pour ce VLAN.

Valeurs possibles :

- `ip`
  Indique l'adresse IP de l'équipement en tant qu'*ID distant*.
- `mac` (réglage par défaut)
  Indique l'adresse MAC de l'équipement en tant qu'*ID distant*.
- `client-id`
  Spécifie le nom du système de l'équipement en tant qu'*ID distant*.
- `other`
  Lorsque vous utilisez cette valeur, entrez les informations définies par l'utilisateur dans la colonne *Remote ID*.

Remote ID

Affiche l'*ID distant* du VLAN.

Lorsque vous spécifiez la valeur `other` dans la colonne *Remote ID type*, indiquez l'identifiant.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

7.1.2 DHCP L2 Relay Statistics

[Advanced > DHCP L2 Relay > Statistics]

L'équipement surveille le trafic sur les ports et affiche les résultats sous forme de table.

Cette table est divisée en différentes catégories pour vous aider lors de l'analyse du trafic.

Les options de relais DHCPv6 ne sont pas affichées dans la table des statistiques.

Table

Port

Affiche le numéro de port.

Untrusted server messages with Option 82

Affiche le nombre de messages du serveur DHCP reçus avec les informations *Option 82* sur l'interface non fiable.

Untrusted client messages with Option 82

Affiche le nombre de messages du client DHCP reçus avec les informations *Option 82* sur l'interface non fiable.

Trusted server messages without Option 82

Affiche le nombre de messages du serveur DHCP reçus avec les informations *Option 82* sur l'interface non fiable.

Trusted client messages without Option 82

Affiche le nombre de messages du client DHCP reçus avec les informations *Option 82* sur l'interface non fiable.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Reset

Réinitialise toute la table.

7.2 DHCP Server

[Advanced > DHCP Server]

Le serveur DHCP vous permet de gérer une base de données des adresses IP disponibles et des informations de configuration. Lorsque l'équipement reçoit une requête de la part d'un client, le serveur DHCP valide le réseau du client DHCP, puis loue une adresse IP. Lorsqu'il est activé, le serveur DHCP attribue également des informations de configuration adaptées à ce client. Les informations de configuration indiquent par exemple l'adresse IP, le serveur DNS et la route par défaut utilisés par un client.

Le serveur DHCP attribue une adresse IP à un client pour une durée définie par l'utilisateur. Le client DHCP est responsable du renouvellement de l'adresse IP avant l'expiration de cette durée. Lorsque le client DHCP ne peut pas renouveler l'adresse, l'adresse est rajoutée au pool pour être réaffectée.

Le menu contient les boîtes de dialogue suivantes :

- DHCP Server Global
- DHCP Server Pool
- DHCP Server Lease Table

7.2.1 DHCP Server Global

[Advanced > DHCP Server > Global]

Activez la fonction globalement ou par port, selon vos besoins.

Operation

Operation

Active/désactive la fonction de serveur DHCP de l'équipement globalement.

Valeurs possibles :

- *On*
- *Off* (réglage par défaut)

Configuration

IP Probe

Active/désactive la recherche d'adresses IP uniques. Avant d'attribuer une adresse IP, le serveur utilise une requête *ICMP Echo* pour vérifier si cette adresse IP est déjà utilisée sur le réseau.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La fonction *IP Probe* est activée.
- `case non cochée`
  La fonction *IP Probe* est désactivée.

Table

Port

Affiche le numéro de port.

DHCP server active

Active/désactive la fonction de serveur DHCP sur ce port.

Il convient pour cela que vous activiez préalablement la fonction globalement.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  La fonction de serveur DHCP est activée.
- `case non cochée`
  La fonction de serveur DHCP est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

7.2.2 DHCP Server Pool

[Advanced > DHCP Server > Pool]

Affectez une adresse IP à un équipement terminal ou à un commutateur connecté à un port ou inclus dans un VLAN.

Le serveur DHCP fournit des pools d'adresses IP à l'aide desquels il attribue des adresses IP aux clients. Un pool est constitué d'une liste d'entrées. Spécifiez une entrée comme statique pour une adresse IP spécifique ou comme dynamique pour une plage d'adresses IP. L'équipement peut contenir un maximum de 128 pools. L'ensemble des pools peut contenir un maximum de 1000 entrées.

Avec une attribution statique, le serveur DHCP affecte une 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. Appliquez cette adresse IP à tous les ports ou à un port spécifique de l'équipement. Pour l'attribution statique, saisissez une adresse IP dans le champ *IP address* et laissez la colonne *Last IP address* vide. Entrez 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 l'équipement avec un ID matériel connu, le serveur DHCP attribue l'adresse IP statique.

Avec l'attribution dynamique, lorsqu'un client DHCP établit un contact sur un port, le serveur DHCP affecte à ce port une adresse IP issue d'un pool. Pour l'attribution dynamique, créez un pool pour les ports en affectant une plage d'adresses IP. Spécifiez la première et la dernière adresse IP de la plage d'adresses IP. Laissez les champs *MAC address*, *Client ID*, *Remote ID* et *Circuit ID* vides. Vous pouvez créer plusieurs entrées de pool. Vous pouvez ainsi créer une plage d'adresses IP contenant des blancs.

Cette boîte de dialogue affiche les différentes informations requises pour l'affectation d'une adresse IP à un port ou à un VLAN. Utilisez le bouton  pour ajouter une entrée. L'équipement ajoute une entrée pouvant être lue et éditée.

Table

Index

Affiche l'index auquel l'entrée de table se réfère.

Active

Active/désactive la fonction de serveur DHCP sur ce port.

Valeurs possibles :

- `case cochée`
  La fonction de serveur DHCP est activée.
- `case non cochée` (réglage par défaut)
  La fonction de serveur DHCP est désactivée.

IP address

Indique l'adresse IP pour l'affectation de l'adresse IP statique. Lorsque vous utilisez l'affectation d'adresses IP dynamique, cette valeur indique le début de la plage d'adresses IP.

Valeurs possibles :

- Adresse IPv4 valide

Last IP address

Lorsque vous utilisez l'affectation d'adresses IP dynamique, cette valeur indique la fin de la plage d'adresses IP.

Valeurs possibles :

- Adresse IPv4 valide

Port

Affiche le numéro de port.

VLAN ID

Affiche le VLAN auquel l'entrée de table se réfère.

Une valeur de `1` correspond au VLAN d'administration de l'équipement par défaut.

Valeurs possibles :

- `1..4042`

MAC address

Indique l'adresse MAC de l'équipement qui loue l'adresse IP.

Valeurs possibles :

- Adresse MAC Unicast valide
  Indiquez la valeur avec un double point, par exemple `00:11:22:33:44:55`.
- `-`
  Le serveur ignore cette variable pour l'affectation d'adresses IP.

DHCP relay

Indique l'adresse IP du relais DHCP à travers lequel les clients transmettent leurs requêtes au serveur DHCP. Lorsque le serveur DHCP reçoit la requête du client à travers un autre relais DHCP, il ignore cette requête.

Valeurs possibles :

- Adresse IPv4 valide
  Adresse IP du relais DHCP.
- `-`
  Aucun relais DHCP n'est installé entre le client et le serveur DHCP.

Client ID

Indique l'identification de l'équipement client qui loue l'adresse IP.

Valeurs possibles :

- 1..80 octets (format `XX XX .. XX`)
- `-`
  Le serveur ignore cette variable pour l'affectation d'adresses IP.

Remote ID

Indique l'identification de l'équipement distant qui loue l'adresse IP.

Valeurs possibles :

- 1..80 octets (format `XX XX .. XX`)
- `-`
  Le serveur ignore cette variable pour l'affectation d'adresses IP.

Circuit ID

Indique l'ID circuit de l'équipement qui loue l'adresse IP.

Valeurs possibles :

- 1..80 octets (format `XX XX .. XX`)
- `-`
  Le serveur ignore cette variable pour l'affectation d'adresses IP.

Schneider Electric device

Active/désactive les multicasts Schneider Electric.

Si l'équipement compris dans cette plage d'adresses IP dessert uniquement les équipements Schneider Electric, activez cette fonction.

Valeurs possibles :

- `case cochée`
  Dans cette plage d'adresses IP, l'équipement dessert uniquement les équipements Schneider Electric. Les multicasts Schneider Electric sont activés.
- `case non cochée` (réglage par défaut)
  Dans cette plage d'adresses IP, l'équipement dessert les équipements de différents fabricants. Les multicasts Schneider Electric sont désactivés.

Configuration URL

Indique le protocole à utiliser ainsi que le nom et le chemin d'accès du fichier de configuration.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques avec 0..70 caractères
  Exemple : `tftp://192.9.200.1/cfg/config.xml`

Lorsque vous laissez ce champ vierge, l'équipement laisse ce champ d'option vierge dans le message DHCP.

Lease time [s]

Indique la durée du bail en secondes.

Valeurs possibles :

- `60..220752000` (réglage par défaut : `86400`)
- `4294967295`
  Utilisez cette valeur pour les attributions non limitées dans le temps et pour les attributions effectuées via BOOTP.

Default gateway

Indique l'adresse IP de la passerelle par défaut.

Une valeur de `0.0.0.0` désactive l'ajout du champ d'option dans le message DHCP.

Valeurs possibles :

- Adresse IPv4 valide

Netmask

Indique le masque du réseau auquel le client appartient.

Une valeur de `0.0.0.0` désactive l'ajout du champ d'option dans le message DHCP.

Valeurs possibles :

- Masque réseau IPv4 valide

WINS server

Indique l'adresse IP du serveur WINS (Windows Internet Name Server) qui convertit les noms NetBIOS.

Une valeur de `0.0.0.0` désactive l'ajout du champ d'option dans le message DHCP.

Valeurs possibles :

- Adresse IPv4 valide

DNS server

Indique l'adresse IP du serveur DNS.

Une valeur de `0.0.0.0` désactive l'ajout du champ d'option dans le message DHCP.

Valeurs possibles :

- Adresse IPv4 valide

Hostname

Indique le nom d'hôte.

Lorsque vous laissez ce champ vierge, l'équipement laisse ce champ d'option vierge dans le message DHCP.

Valeurs possibles :

- Chaîne de 0..64 caractères ASCII alphanumériques

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

7.2.3 DHCP Server Lease Table

[Advanced > DHCP Server > Lease Table]

Cette boîte de dialogue affiche l'état de la location d'adresses IP pour chaque port.

Table

Port

Affiche le numéro de port auquel l'adresse est actuellement louée.

IP address

Affiche l'adresse IP louée à laquelle l'entrée se réfère.

Status

Affiche la phase de location.

Selon la norme technique relative aux opérations du protocole DHCP, la location d'une adresse IP se compose de 4 phases : la découverte, l'offre, la requête et l'acquittement.

Valeurs possibles :

- `bootp`
  Un client DHCP tente de découvrir un serveur DHCP pour l'attribution d'adresses IP.
- `offering`
  Le serveur DHCP confirme que l'adresse IP est adaptée au client.
- `requesting`
  Un client DHCP acquiert l'offre d'adresse IP.
- `bound`
  Le serveur DHCP loue l'adresse IP à un client.
- `renewing`
  Le client DHCP demande une extension du bail.
- `rebinding`
  Le serveur DHCP affecte l'adresse IP au client après un renouvellement réussi.
- `declined`
  Le serveur DHCP a refusé la requête d'adresse IP.
- `released`
  L'adresse IP est disponible pour d'autres clients.

Remaining lifetime

Affiche le temps restant pour l'adresse IP louée.

Leased MAC address

Affiche l'adresse MAC de l'équipement qui loue l'adresse IP.

Gateway

Indique la passerelle IP de l'équipement qui loue l'adresse IP.

Client ID

Affiche l'identifiant du client de l'équipement qui loue l'adresse IP.

Remote ID

Affiche l'identifiant distant de l'équipement qui loue l'adresse IP.

Circuit ID

Affiche l'ID circuit de l'équipement qui loue l'adresse IP.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

7.3 DNS

[Advanced > DNS]

Le menu contient les boîtes de dialogue suivantes :
- DNS Client

7.3.1 DNS Client

[Advanced > DNS > Client]

Le DNS (Domain Name System ou système de noms de domaine) est un service du réseau permettant de traduire les noms de domaine en adresses IP. Cette résolution de nom vous permet de contacter d'autres équipements en utilisant leur nom d'hôte au lieu de leur adresse IP.

La fonction *Client* permet à l'équipement d'envoyer des requêtes de résolution de noms d'hôtes en adresses IP à un serveur DNS.

Le menu contient les boîtes de dialogue suivantes :
- DNS Client Global
- DNS Client Current
- DNS Client Static
- DNS Client Static Hosts

7.3.1.1 DNS Client Global

[Advanced > DNS > Client > Global]

Dans cette boîte de dialogue, vous activez la fonction *Client* et la fonction *Cache*.

Operation

Operation

Active/désactive la fonction *Client*.

Valeurs possibles :

- *On*
  La fonction *Client* est activée.
  L'équipement envoie des requêtes de résolution de noms d'hôtes en adresses IP à un serveur DNS.
- *Off* (réglage par défaut)
  La fonction *Client* est désactivée.

Cache

Cache

Active/désactive la fonction *Cache*.

Valeurs possibles :

- *On* (réglage par défaut)
  La fonction *Cache* est activée.
  L'équipement sauvegarde temporairement jusqu'à 128 réponses du serveur DNS (nom d'hôte et adresse IP correspondante) dans le cache. Lorsque le cache contient une entrée correspondante, l'équipement résout lui-même le nom d'hôte d'une nouvelle requête. Il n'est donc pas nécessaire d'envoyer une nouvelle requête au serveur DNS.
- *Off*
  La fonction *Cache* est désactivée.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Flush cache

Supprime toutes les entrées du cache DNS.

7.3.1.2 DNS Client Current

[Advanced > DNS > Client > Current]

Cette boîte de dialogue affiche les serveurs DNS auxquels l'équipement envoie des requêtes de résolution de noms d'hôtes en adresses IP.

Table

Index

Affiche le numéro séquentiel du serveur DNS.

Address

Affiche l'adresse IP du serveur DNS. L'équipement transfère les requêtes de résolution de noms d'hôtes en adresses IP au serveur DNS avec cette adresse IP.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

7.3.1.3 DNS Client Static

[Advanced > DNS > Client > Static]

Dans cette boîte de dialogue, vous spécifiez les serveurs DNS auxquels l'équipement transfère les requêtes de résolution de noms d'hôtes en adresses IP.

L'équipement vous permet de spécifier vous-même jusqu'à 4 adresses IP ou de transférer les adresses IP à partir d'un serveur DHCP.

Configuration

Configuration source

Spécifie la source à partir de laquelle l'équipement obtient l'adresse IP des serveurs DNS auxquels l'équipement adresse les requêtes.

Valeurs possibles :

- `user`
  L'équipement utilise les adresses IP spécifiées dans la table.
- `mgmt-dhcp` (réglage par défaut)
  L'équipement utilise les adresses IP que le serveur DHCP lui fournit.

Domain name

Spécifie le nom de domaine conformément à RFC 1034 que l'équipement ajoute aux noms d'hôtes sans suffixe de domaine.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

Request timeout [s]

Spécifie l'intervalle de temps en secondes pour envoyer à nouveau une requête au serveur.

Valeurs possibles :

- `0`
  Désactive la fonction. L'équipement n'envoie pas de nouvelle requête au serveur.
- `1..3600` (réglage par défaut : `3`)

Request retransmits

Spécifie le nombre de fois que l'équipement retransmet une requête.

La condition préalable est que vous spécifiez une valeur >`0` dans le champ *Request timeout [s]*.

Valeurs possibles :

- `0..100` (réglage par défaut : `2`)

Table

Index

Affiche le numéro séquentiel du serveur DNS.

L'équipement vous permet de spécifier jusqu'à 4 serveurs DNS.

Address

Indique l'adresse IP du serveur DNS.

Valeurs possibles :

- Adresse IPv4 valide (réglage par défaut : `0.0.0.0`)
- Adresse IPv6 valide

Active

Active ou désactive l'entrée de table.

L'équipement envoie des requêtes au serveur DNS configuré dans la première entrée de table active. Lorsque l'équipement ne reçoit pas de réponse de ce serveur, il envoie des requêtes au serveur DNS configuré dans l'entrée de table active suivante.

Valeurs possibles :

- `case cochée`
  Le client DNS envoie des requêtes à ce serveur DNS.
  Conditions préalables :
  - ☐ Activez la fonction Client DNS dans la boîte de dialogue *Advanced > DNS > Global*.
  - ☐ Dans le cadre *Configuration*, liste déroulante *Configuration source*, sélectionnez la valeur `user`.
- `case non cochée` (réglage par défaut)
  L'équipement n'envoie pas de requêtes à ce serveur DNS.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

7.3.1.4 DNS Client Static Hosts

[Advanced > DNS > Client > Static Hosts]

Cette boîte de dialogue vous permet de spécifier jusqu'à 64 noms d'hôtes que vous associez chacun à une adresse IP. Lors d'une requête de résolution de noms d'hôtes en adresses IP, l'équipement recherche une entrée correspondante dans cette table. Lorsque l'équipement ne trouve pas d'entrée correspondante, il transfère la requête.

Table

Index

Affiche l'index auquel l'entrée de table se réfère.

Valeurs possibles :

- `1..64`

Name

Indique le nom d'hôte.

Valeurs possibles :

- Chaîne de caractères ASCII alphanumériques de 0..255 caractères

IP address

Spécifie l'adresse IP sous laquelle l'hôte est accessible.

Valeurs possibles :

- Adresse IPv4 valide

Active

Active ou désactive l'entrée de table.

Valeurs possibles :

- `case cochée`
  L'équipement résout une requête de nom d'hôte pour cette entrée.
- `case non cochée`
  Après avoir reçu une requête pour ce nom d'hôte, l'équipement envoie une requête à l'un des serveurs de noms configurés pour la résolution.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

7.4 Industrial Protocols

[Advanced > Industrial Protocols]

Le menu contient les boîtes de dialogue suivantes :

- IEC61850-MMS
- Modbus TCP
- EtherNet/IP

7.4.1 IEC61850-MMS

[Advanced > Industrial Protocols > IEC61850-MMS]

Le protocole CEI 61850-MMS est un protocole industriel standardisé par l'International Electrotechnical Commission (IEC). Par exemple, l'équipement de commutation automatique utilise ce protocole lorsqu'il communique avec l'équipement de la centrale électrique.

Ce protocole orienté paquet définit un langage de communication uniforme basé sur le protocole de transport TCP/IP. Ce protocole utilise un serveur MMS (Manufacturing Messaging Specification) pour les communications client-serveur. Il comprend les fonctions destinées aux systèmes SCADA, aux dispositifs électroniques intelligents (IED) et aux systèmes de contrôle réseau.

Commentaire : 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.

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.

Cette boîte de dialogue vous permet de spécifier les réglages suivants pour le serveur MMS :
- Active/désactive le serveur MMS.
- Active/désactive l'accès en écriture au serveur MMS.
- Le port TCP du serveur MMS.
- Le nombre maximum de sessions de serveur MMS.

Operation

Operation

Active/désactive le serveur *IEC61850-MMS*.

Valeurs possibles :

- `On`
  Le serveur *IEC61850-MMS* est activé.
- `Off` (réglage par défaut)
  Le serveur *IEC61850-MMS* est désactivé.
  Les MIB IEC61850 restent accessibles.

Configuration

Write access

Active/désactive l'accès en écriture au serveur MMS.

Valeurs possibles :

- `case cochée`
  L'accès en écriture au serveur MMS est activé. Ce réglage vous permet de modifier les réglages du protocole IEC 61850 MMS.
- `case non cochée` (réglage par défaut)
  L'accès en écriture au serveur MMS est désactivé. Le serveur MMS est accessible en lecture seule.

Technical key

Indique le nom IED.

Le nom IED peut être choisi indépendamment du nom du système.

Valeurs possibles :

- Chaîne de 0..32 caractères ASCII alphanumériques
  Les caractères suivants sont autorisés :
  - _
  - `0..9`
  - `a..z`
  - `A..Z` (réglage par défaut : `KEY`)

Pour que le serveur MMS utilise le nom IED, cliquez sur le bouton ☑ et redémarrez le serveur MMS. La connexion aux clients connectés est ensuite interrompue.

TCP port

Spécifie le port TCP pour l'accès au serveur MMS.

Valeurs possibles :

- `1..65535` (réglage par défaut : `102`)
  Exception : le port `2222` est réservé à des fonctions internes.

Commentaire : Le serveur redémarre automatiquement en cas de changement de port. Durant ce processus, l'équipement met fin aux connexions au serveur actives.

Sessions (max.)

Indique le nombre maximum de connexions au serveur MMS.

Valeurs possibles :

- `1..15` (réglage par défaut : `5`)

Information

Status

Affiche l'état actuel du serveur *IEC61850-MMS*.

Valeurs possibles :

- *unavailable*
- *starting*
- *running*
- *stopping*
- *halted*
- *error*

Active sessions

Affiche le nombre de connexions au serveur MMS actives.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Download ICD file

Copie le fichier ICD sur votre PC.

7.4.2 Modbus TCP

[Advanced > Industrial Protocols > Modbus TCP]

Modbus TCP est un protocole utilisé pour l'intégration du système SCADA (Supervisory Control and Data Acquisition). *Modbus TCP* est un protocole non lié à un fournisseur utilisé pour surveiller et contrôler les équipements d'automatisation industrielle tels que les automates programmables industriels (API), les capteurs et les compteurs.

Cette boîte de dialogue vous permet de spécifier les paramètres du protocole. Pour surveiller et contrôler les paramètres de l'équipement, vous devez disposer d'un logiciel d'interface homme-machine (HMI) et de la topographie mémoire. Reportez-vous aux tables situées dans le manuel d'utilisation « Configuration » pour les objets pris en charge et la topographie mémoire.

Cette boîte de dialogue vous permet d'activer la fonction, d'activer l'accès en écriture et de déterminer le port TCP qui sera interrogé par l'interface homme-machine (HMI). Vous pouvez également spécifier le nombre de sessions pouvant être ouvertes simultanément.

Commentaire : L'activation de l'accès en écriture du protocole *Modbus TCP* peut entraîner des risques de sécurité inévitables car le protocole ne procède pas à l'authentification de l'accès des utilisateurs.

Pour contribuer à minimiser les risques de sécurité inévitables, spécifiez la plage d'adresses IP située dans la boîte de dialogue *Device Security > Management Access*. Saisissez uniquement les adresses IP affectées à vos équipements avant d'activer la fonction. En outre, le réglage par défaut permettant d'activer la fonction de surveillance dans la boîte de dialogue *Diagnostics > Status Configuration > Security Status* de l'onglet *Global* est activé.

Operation

Operation

Active/désactive le serveur *Modbus TCP* de l'équipement.

Valeurs possibles :

- `On`
  Le serveur *Modbus TCP* est activé.
- `Off` (réglage par défaut)
  Le serveur *Modbus TCP* est désactivé.

Configuration

Write access

Active/désactive l'accès en écriture aux paramètres *Modbus TCP*.

Commentaire : L'activation de l'accès en écriture du protocole *Modbus TCP* peut entraîner des risques de sécurité inévitables car le protocole ne procède pas à l'authentification de l'accès des utilisateurs.

Valeurs possibles :

- `case cochée` (réglage par défaut)
  L'accès en écriture/lecture du serveur *Modbus TCP* est activé. Cela vous permet de modifier la configuration de l'équipement à l'aide du protocole *Modbus TCP*.
- `case non cochée`
  L'accès en lecture seule du serveur *Modbus TCP* est activé.

TCP port

Spécifie le numéro de port TCP que le serveur *Modbus TCP* utilise pour la communication.

Valeurs possibles :

- `<Numéro de port TCP>` (réglage par défaut : `502`)
  Il n'est pas autorisé de spécifier la valeur `0`.

Sessions (max.)

Spécifie le nombre maximum de sessions simultanées gérées par le serveur *Modbus TCP*.

Valeurs possibles :

- `1..5` (réglage par défaut : `5`)

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

7.4.3 EtherNet/IP

[Advanced > Industrial Protocols > EtherNet/IP]

Cette boîte de dialogue vous permet de spécifier les réglages *EtherNet/IP*. Vous disposez des options suivantes :

- Activer/désactiver la fonction *EtherNet/IP* dans l'équipement.
- Spécifier un VLAN qui transfère exclusivement les paquets *EtherNet/IP*.
- Activer/désactiver la fonctionnalité en lecture/écriture du protocole *EtherNet/IP*.
- Télécharger le fichier EDS (Electronic Data Sheet) de l'équipement.

Operation

Operation

Active/désactive la fonction *EtherNet/IP* dans l'équipement.

Valeurs possibles :

- `On`
  La fonction *EtherNet/IP* est activée.
- `Off` (réglage par défaut)
  La fonction *EtherNet/IP* est désactivée.

VLAN Configuration

Avantages de la configuration d'un VLAN :

- Réduction des inondations de paquets *EtherNet/IP*. L'équipement transfère les paquets *EtherNet/IP* dans le VLAN que vous avez affecté.
- Amélioration de la sécurité et de la confidentialité du réseau.

VLAN ID

Spécifie un VLAN dans lequel l'équipement transfère les paquets *EtherNet/IP*.

Valeurs possibles :

- `mgmt` (réglage par défaut)
  L'équipement transfère les paquets *EtherNet/IP* dans le VLAN dans lequel l'administration de l'équipement est accessible via le réseau. Vous spécifiez ce VLAN dans la boîte de dialogue *Basic Settings > Network > Global*, cadre *Management interface*, champ *VLAN ID*.
- `1..4042`
  Dans la liste déroulante, sélectionnez un élément. L'équipement transfère les paquets *EtherNet/IP* dans ce VLAN.
  Conditions préalables :
  - Le VLAN est déjà configuré dans l'équipement.
    Voir la boîte de dialogue *Switching > VLAN > Configuration*.
  - Le port sur lequel l'équipement transfère les paquets *EtherNet/IP* est membre du VLAN que vous avez affecté et transfère les paquets de données avec un tag de VLAN.
    Voir la boîte de dialogue *Switching > VLAN > Configuration*.
  - La fonction *IP Access Restriction* est activée.
    Voir la boîte de dialogue *Device Security > Management Access > IP Access Restriction*.

Configuration

Write access

Active/désactive la fonctionnalité en lecture/écriture du protocole *EtherNet/IP*.

Valeurs possibles :

- `case cochée`
  Le protocole *EtherNet/IP* accepte les requêtes set/get.
- `case non cochée` (réglage par défaut)
  Le protocole *EtherNet/IP* accepte uniquement les requêtes get.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Download EDS file

Copie les informations suivantes dans un fichier zip sur votre PC :

- fichier EDS (Electronic Data Sheet) contenant des informations relatives à l'équipement
- icône d'équipement

7.5 Digital IO Module

[Advanced > Digital IO Module]

Les entrées numériques vous permettent de capturer et de transmettre les signaux des capteurs numériques. Les sorties numériques vous permettent d'appliquer aux actionneurs le signal relayé à partir des entrées. La tension de sortie de 24 VCC vous permet de faire fonctionner les actionneurs, par exemple, les voyants lumineux.

L'équipement transmet les signaux des capteurs à travers le réseau pour activer les actionneurs correspondants. Le module capture les signaux via les connexions d'entrée et les transmet aux sorties. Selon l'emplacement des actionneurs, l'équipement transmet les signaux aux sorties situées sur le même module, sur un module différent au sein du même équipement, ou sur un autre équipement.

Lorsque l'équipement associe les ports d'entrée numériques aux ports de sortie numériques, la relation est de type 1:N. L'équipement met en miroir le flux de données d'un port d'entrée numérique avec un ou plusieurs ports de sortie.

Lorsque l'équipement associe les ports de sortie numériques aux ports de d'entrée numériques, la relation est de type 1:1. Un port de sortie numérique met en miroir le flux de données d'un port d'entrée numérique.

La boîte de dialogue contient les onglets suivants :
- [IO input]

[IO input]

Cet onglet vous permet :
- d'activer/désactiver l'interrogation des entrées numériques globalement
- de configurer l'intervalle avec lequel l'équipement interroge les entrées numériques pour obtenir leurs valeurs
- d'activer/de désactiver la consignation d'un événement
- d'activer/de désactiver l'envoi de traps SNMP

Operation

Operation

Active/désactive les requêtes cycliques des entrées numériques (entrée ES).

Valeurs possibles :
- *On*
  Vous permet d'interroger les valeurs des entrées numériques.
- *Off* (réglage par défaut)

Configuration

Refresh interval [ms]

Indique l'intervalle en millisecondes avec lequel l'équipement interroge les valeurs des entrées numériques.

Valeurs possibles :

- `1000..10000` (réglage par défaut : `1000`)

Table

Input ID

Affiche le numéro d'emplacement du module (x) et le numéro de l'entrée numérique (i) qui s'applique à cette entrée.

Notation : `x.i`

Valeurs possibles :

- x =`0..7`
  La valeur `0` est égale à l'unité principale (MU ou main unit).
- i =`1..4`

Value

Indique le niveau d'entrée numérique.

Valeurs possibles :

- `low`
  La tension d'entrée au niveau de l'entrée numérique est de 0 V.
- `high`
  La tension d'entrée au niveau de l'entrée numérique est de +24 VCC.
- `not-available`
  La tension d'entrée au niveau de l'entrée numérique est différente de 0 V ou de +24 VCC. Vérifiez que le module est présent et correctement inséré.

Log event

Active/désactive la consignation dans le fichier log. Voir la boîte de dialogue *Diagnostics > Report >* System Log.

Valeurs possibles :

- `case cochée`
  La consignation dans le fichier log est activée.
  L'équipement vérifie l'état des entrées numériques selon l'intervalle spécifié dans le champ *Configuration* du cadre *Refresh interval [ms]*.
  En cas de modifications survenant au niveau des entrées numériques, l'équipement consigne une entrée dans le fichier log System Log.
- `case non cochée` (réglage par défaut)
  La consignation dans le fichier log est désactivée.

Send trap

Active/désactive l'envoi de traps SNMP lorsque l'équipement détecte un changement au niveau des entrées numériques.

L'équipement vérifie l'état des entrées numériques selon l'intervalle spécifié dans le champ *Configuration* du cadre *Refresh interval [ms]*.

Valeurs possibles :

- `case cochée`
  L'envoi de traps SNMP est activé.
  Lorsque l'équipement détecte des modifications au niveau des entrées numériques, l'équipement envoie un trap SNMP.
- `case non cochée` (réglage par défaut)
  L'envoi de traps SNMP est désactivé.

Pour pouvoir envoyer des traps SNMP, il convient préalablement d'activer la fonction dans la boîte de dialogue *Diagnostics > Status Configuration > Alarms (Traps)* et de spécifier au moins une destination de trap.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

7.6 Command Line Interface

[Advanced > CLI]

Cette boîte de dialogue vous permet d'accéder à l'équipement à l'aide de l'interface de ligne de commande.

Les conditions préalables sont :
- ☐ Dans l'équipement, activez le serveur SSH dans la boîte de dialogue *Device Security > Management Access > Server*, onglet *SSH*.
- ☐ Sur votre poste de travail, installez une application client compatible avec SSH qui enregistre un gestionnaire dédié aux URL commençant par `ssh://` dans votre système d'exploitation.

Boutons

La section « Boutons » à la page 17 contient la description des boutons par défaut.

Open SSH connection

Ouvre l'application client compatible avec SSH.

Lorsque vous cliquez sur ce bouton, l'application Web transmet l'URL de l'équipement commençant par `ssh://` et le nom de l'utilisateur actuellement connecté.

Lorsque le navigateur Web identifie une application client compatible avec SSH, le client compatible avec SSH établit une connexion à l'équipement à l'aide du protocole SSH.

A Index

L

M

N

P

V

W