GUIDE D'ADMINISTRATION

Guide d’administration du commutateur intelligent Cisco Small Business série 200

Table des matières

Chapitre 1: Table des matières 1

Chapitre 2: Démarrage 8

Démarrage de l'utilitaire Web de configuration 8
Configuration de l'appareil - Démarrage rapide 12
Conventions de nommage de l'interface 13
Navigation dans les fenêtres 14

Chapitre 3: État et statistiques 18

Récapitulatif système 18
Interfaces Ethernet 18
Statistiques Etherlike 20
Statistiques EAP 802.1X 21
Intégrité 22
RMON 22
Afficher le journal 29

Chapitre 4: Administration : Journal système 30

Définition des paramètres de journalisation système 30
Définition des paramètres de journalisation distante 32
Afficher les journaux de la mémoire 33

Chapitre 5: Administration : Gestion de fichiers 35

Fichiers système 35
Mettre à niveau/sauvegarder micrologiciel/langue 38
Télécharger/sauvegarder configuration/journal 41

Propriétés des fichiers de configuration 46
Copier/enregistrer la configuration 47
Configuration/Mise à jour automatique de l'image via DHCP 48

Chapitre 6: Administration 58

Modèles de périphériques 59
Paramètres système 60
Interface de gestion 63
Comptes d'utilisateur 63
Définition du délai d'expiration en cas de session inactive 63
Paramètres de l'heure 63
Journal système 63
Gestion de fichiers 64
Redémarrage du périphérique 64
Intégrité 66
Diagnostic 67
Détection - Bonjour 67
Détection - LLDP 67
Détection - CDP 67
Ping 68

Chapitre 7: Administration : Paramètres d'heure 70

Options d'heure système 71
Modes SNTP 72
Configuration de l'heure système 73

Chapitre 8: Administration : Diagnostics 80

Tests des ports en cuivre 80
Affichage de l'état des modules optiques 82
Configuration de la mise en miroir des ports et de VLAN 83

Affichage de l'utilisation du CPU et fonction Secure Core Technology (SCT) 85

Chapitre 9: Administration : Détection 86

Bonjour 86

LLDP et CDP 87

Configuration de LLDP 88

Configuration de CDP 108

Statistiques CDP 115

Chapitre 10: Gestion des ports 117

Configuration des ports 117

Détection de bouclage 121

Agrégation de liaison 124

UDLD 131

PoE 131

Configuration de Green Ethernet 131

Chapitre 11: Gestion des ports : Unidirectional Link Detection 139

Présentation de la fonction UDLD 139

Fonctionnement de UDLD 140

Instructions d'utilisation 142

Dépendances envers les autres fonctions 143

Configuration et paramètres par défaut 143

Avant de commencer 143

Tâches UDLD courantes 144

Configuration de UDLD 144

Chapitre 12: Port intelligent 148

Présentation 148

Qu'est-ce qu'un port intelligent ? 149

Types de port intelligent 149
Macros Port intelligent 152
Échec de la macro et opération de réinitialisation 153
Fonctionnement de la fonction Port intelligent 153
Port intelligent automatique 154
Gestion des erreurs 157
Configuration par défaut 158
Relations avec les autres fonctions et compatibilité descendante 158
Tâches courantes de port intelligent 158
Configuration de port intelligent à l'aide de l'interface Web 161
Macros Port intelligent intégrées 165

Chapitre 13: Gestion des ports : PoE 176

PoE sur l'appareil 176
Propriétés PoE 179
Paramètres PoE 180

Chapitre 14: Gestion des VLAN 183

Présentation 183
VLAN standard 185
VLAN voix 192

Chapitre 15: Spanning Tree 205

Types de STP 205
État STP et paramètres globaux 206
Paramètres d'interface Spanning Tree 207
Paramètres Rapid Spanning Tree 209

Chapitre 16: Gestion des tables d'adresses MAC 212

Adresses MAC statiques 213
Adresses MAC dynamiques 214

Chapitre 17: Multidiffusion 215

Réacheminement multidestination 215
Propriétés de multidiffusion 220
Adresse de groupe MAC 220
Adresses IP de groupe de multidiffusion 222
Configuration de la multidiffusion IPv4 223
Configuration de la multidiffusion IPv6 225
Groupe de multidiffusion IP de surveillance IGMP/MLD 228
Ports de routeur de multidiffusion 229
Tout transférer 230
Multidiffusion non enregistrée 231

Chapitre 18: Configuration IP 232

Présentation 232
IPv4 Management and Interfaces (Interfaces et gestion IPv4) 234
Nom de domaine 248

Chapitre 19: Sécurité 253

Définition d'utilisateurs 254
Configuration de RADIUS 257
Méthode d'accès de gestion 260
Authentification de l'accès de gestion 265
Gestion sécurisée des données confidentielles 266
Serveur SSL 266
Client SSH 269
Configuration des services TCP/UDP 269
Définition du contrôle des tempêtes 270
Configuration de la sécurité des ports 271
802.1X 273
Prévention du déni de service 274

Chapitre 20: Sécurité : Authentification 802.1X 278

Présentation de 802.1X 278
Présentation de l'authentificateur 280
Tâches courantes 284
Configuration de 802.1X via l'interface utilisateur graphique (GUI) 285

Chapitre 21: Sécurité : Client SSH 291

Secure Copy (SCP) et SSH 291
Méthodes de protection 292
Authentification du serveur SSH 294
Authentification du client SSH 294
Avant de commencer 295
Tâches courantes 295
Configuration du client SSH via l'interface utilisateur graphique (GUI) 297

Chapitre 22: Sécurité : Gestion sécurisée des données confidentielles 301

Introduction 301
Règles SSD 302
Propriétés SSD 307
Fichiers de configuration 310
Canaux de gestion SSD 314
Interface de ligne de commande (CLI) et récupération du mot de passe 315
Configuration de SSD 316

Chapitre 23: Qualité de service 319

Fonctions et composants QoS 320
Configuration de la QoS - Général 321
Gestion des statistiques de QoS 330

Chapitre 24: SNMP 332

Versions et flux de travail SNMP 332
ID d'objet du modèle 335
ID de moteur SNMP 336
Configuration de vues SNMP 338
Création de groupes SNMP 339
Création d'utilisateurs SNMP 341
Définition de communautés SNMP 342
Définition de paramètres d'interceptions 344
Destinataires de notifications 345
Filtres de notification SNMP 349

2

Démarrage

Cette section offre une introduction à l'utilitaire de configuration Web et inclut les rubriques suivantes :

- **Démarrage de l'utilitaire Web de configuration**
- **Configuration de l'appareil - Démarrage rapide**
- **Conventions de nommage de l'interface**
- **Navigation dans les fenêtres**

Démarrage de l'utilitaire Web de configuration

Cette section explique comment naviguer dans l'utilitaire Web de configuration du commutateur.

Si vous utilisez un bloqueur de fenêtres publicitaires intempestives, assurez-vous qu'il est désactivé.

Restrictions s'appliquant aux navigateurs

Si vous utilisez des interfaces IPv6 sur votre station de gestion, utilisez l'adresse globale IPv6 au lieu de l'adresse de liaison locale IPv6 pour accéder au périphérique à partir de votre navigateur.

Lancement de l'utilitaire de configuration

Pour lancer l'utilitaire de configuration Web :

ÉTAPE 1 Ouvrez un navigateur Web.

ÉTAPE 2 Saisissez l'adresse IP du périphérique que vous configurez dans la barre d'adresse du navigateur, puis appuyez sur **Entrée**.

REMARQUE Lorsque le périphérique utilise l'adresse IP par défaut 192.168.1.254, sa LED d'alimentation clignote de façon continue. Lorsque le périphérique utilise une adresse IP affectée par DHCP ou une adresse IP statique configurée par un administrateur, sa LED d'alimentation reste allumée.

Connexion

Le nom d'utilisateur par défaut est **cisco** tandis que le mot de passe par défaut est **cisco**. Lors de votre première ouverture de session avec le nom d'utilisateur et le mot de passe par défaut, vous devez saisir un nouveau mot de passe.

REMARQUE Si vous n'avez pas encore choisi la langue de l'interface utilisateur graphique, la page de connexion s'affiche dans la ou les langues demandées par votre navigateur et dans les langues configurées sur votre périphérique. Si votre navigateur demande le chinois par exemple, et si le chinois a été chargé sur votre périphérique, la page de connexion s'affiche automatiquement en chinois. Si le chinois n'a pas été chargé sur votre périphérique, la page de connexion s'affiche en anglais.

Les langues chargées sur le périphérique sont désignées par le code de la langue et le code du pays (en-US, en-GB, etc.). Pour que la page de connexion s'ouvre automatiquement dans une langue particulière, en fonction de la demande du navigateur, le code de la langue et le code du pays indiqués dans la demande du navigateur doivent correspondre aux langues chargées sur le périphérique. Si la demande du navigateur ne contient que le code de la langue, mais pas celui du pays (par exemple : fr), la première langue intégrée dont le code de la langue correspond est sélectionnée (sans code de pays correspondant, par exemple : fr_CA).

Pour vous connecter à l'utilitaire de configuration de l'appareil :

ÉTAPE 1 Saisissez le nom d'utilisateur/le mot de passe. Le mot de passe peut comporter au maximum 64 caractères ASCII. Les règles de complexité du mot de passe sont décrites à la section **Définition de règles de complexité des mots de passe**.

ÉTAPE 2 Si vous n'utilisez pas l'anglais, sélectionnez la langue souhaitée dans le menu déroulant *Langue*. Pour ajouter une nouvelle langue au périphérique ou mettre à jour une langue déjà enregistrée, reportez-vous à la section **Mettre à niveau/ sauvegarder micrologiciel/langue**.

ÉTAPE 3 S'il s'agit de votre première ouverture de session avec l'ID utilisateur par défaut (**cisco**) et le mot de passe par défaut (**cisco**), ou si votre mot de passe a expiré, la page Modifier le mot de passe s'ouvre. Pour plus d'informations, reportez-vous à la section **Expiration du mot de passe**.

ÉTAPE 4 Vous avez la possibilité de sélectionner **Désactiver l'application de la complexité du mot de passe**. Pour plus d'informations sur la complexité des mots de passe, reportez-vous à la section **Définition de règles de complexité des mots de passe**.

ÉTAPE 5 Saisissez le nouveau mot de passe, puis cliquez sur **Appliquer**.

Une fois la connexion établie, la page Mise en route s'ouvre.

Si vous avez saisi un nom d'utilisateur ou un mot de passe erroné, un message d'erreur apparaît et la page Connexion reste affichée sur la fenêtre. Si vous rencontrez des problèmes pour vous connecter, reportez-vous à la section **Lancement de l'utilitaire de configuration** du Guide d'administration pour obtenir des informations supplémentaires.

Sélectionnez **Ne pas afficher cette page au démarrage** pour empêcher la page Mise en route de s'ouvrir à chaque fois que vous vous connectez au système. Si vous sélectionnez cette option, la page System Summary s'ouvre à la place de la page Getting Started.

HTTP/HTTPS

Vous pouvez ouvrir une session HTTP (non sécurisée) en cliquant sur **Se connecter**. Vous pouvez également ouvrir une session HTTPS (sécurisée) en cliquant sur **Navigation sécurisée (HTTPS)**. Vous serez invité à approuver la connexion avec une clé RSA par défaut, puis une session HTTPS s'ouvrira.

REMARQUE Vous n'avez pas besoin de saisir le nom d'utilisateur et le mot de passe avant de cliquer sur le bouton **Navigation sécurisée (HTTPS).**

Pour savoir comment configurer HTTPS, reportez-vous à la section **Serveur SSL**.

Expiration du mot de passe

La page Nouveau mot de passe s'affiche dans les cas suivants :

- La première fois que vous accédez au périphérique avec le nom d'utilisateur **cisco** et le mot de passe **cisco** par défaut, cette page vous oblige à remplacer le mot de passe par défaut.
- Lorsque le mot de passe expire, cette page vous oblige à sélectionner un nouveau mot de passe.

Déconnexion

L'application se déconnecte par défaut au bout de dix minutes d'inactivité. Vous pouvez modifier cette valeur par défaut en suivant la procédure décrite à la section **Définition du délai d'expiration en cas de session inactive**.

ATTENTION Sauf si la Configuration d'exécution est copiée dans la Configuration de démarrage, toutes les modifications apportées depuis le dernier enregistrement du fichier sont perdues en cas de redémarrage du périphérique. Enregistrez la Configuration d'exécution dans la Configuration de démarrage avant de vous déconnecter, afin de conserver toute modification apportée au cours de cette session.

Une icône X rouge clignotante qui s'affiche à gauche du lien d'application **Enregistrer** indique que des changements apportés à la Configuration d'exécution n'ont pas encore été enregistrés dans le fichier de Configuration de démarrage. Vous pouvez désactiver le clignotement en cliquant sur le bouton **Désactiver clignotement icône d'enr.** de la page Copier/enregistrer la configuration.

Lorsque le périphérique détecte automatiquement un périphérique, tel qu'un téléphone IP (reportez-vous à la section **Qu'est-ce qu'un port intelligent ?**), il configure le port de manière adéquate pour ce périphérique. Ces commandes de configuration sont écrites dans le fichier de configuration de fonctionnement. L'icône Enregistrer se met alors à clignoter lorsque vous vous connectez, même si

vous n'avez apporté aucune modification à la configuration.

Lorsque vous cliquez sur **Enreg.**, la page Copier/enregistrer la configuration s'affiche. Enregistrez le fichier de configuration de fonctionnement en le copiant dans le fichier de configuration de démarrage. Une fois cet enregistrement effectué, l'icône X rouge et le lien d'application Enregistrer ne s'affichent plus.

Pour vous déconnecter, cliquez sur **Se déconnecter** en haut à droite de n'importe quelle page. Le système se déconnecte du périphérique.

En cas d'expiration du délai ou si vous vous déconnectez intentionnellement du système, un message apparaît et la page de connexion s'ouvre tout en indiquant que vous êtes déconnecté. Une fois que vous vous êtes connecté, l'application retourne à la page initiale.

La page initiale qui s'affiche varie selon que l'option « Ne pas afficher cette page au démarrage » de la page Mise en route a été activée ou non. Si vous n'avez pas sélectionné cette option, la page initiale qui apparaît est la page Mise en route. Si vous avez sélectionné cette option, la page initiale qui apparaît est la page Récapitulatif système.

Configuration de l'appareil - Démarrage rapide

Afin de simplifier la configuration du périphérique, des liens vous permettant d'accéder rapidement aux pages les plus fréquemment utilisées ont été mis à votre disposition sur la page Mise en route.

Catégorie	Nom du lien (sur la page)	Page correspondante
	Change Management Applications and Services	Page Services TCP/UDP
	Change Device IP Address	Page Interface IPv4
	Create VLAN	Page Créer un VLAN
	Configure Port Settings	Page Paramètres des ports
État du périphérique	System Summary	Page Récapitulatif système
	Port Statistics	Page Interface
	RMON Statistics	Page Statistiques
	View Log	Page Mémoire RAM
Accès rapide	Change Device Password	Page Comptes d'utilisateur
	Upgrade Device Software	Page Mettre à niveau/sauvegarder micrologiciel/langue
	Backup Device Configuration	Page Télécharger/sauvegarder configuration/journal
	Configure QoS	Page Propriétés de QoS
	Configure Port Mirroring	Page Mise en miroir des ports et VLAN

La page Getting Started comporte deux liens qui vous redirigent vers des pages Web Cisco sur lesquelles vous trouverez des informations supplémentaires. Cliquez sur le lien **Assistance** pour accéder à la page d'assistance produit du périphérique, puis sélectionnez le lien **Forums** pour accéder à la page Communauté d'assistance Cisco Small Business.

Conventions de nommage de l'interface

Dans l'interface utilisateur graphique, les interfaces sont désignées en concaténant les éléments suivants :

- **Type de l'interface :** les types suivants d'interface se retrouvent dans divers types de périphériques :
  - **Fast Ethernet (10/100 bits)** : celles-ci sont désignées par **FE**.
  - **Ports Gigabit Ethernet (10/100/1 000 bits)** : celles-ci sont désignées par **GE**.
  - **LAG (PortChannel)** : celles-ci sont désignées par **LAG**.
  - **VLAN** : celles-ci sont désignées par **VLAN.**
  - **Tunnel** : celles-ci sont désignées par **Tunnel.**
- **Numéro d'interface : ID du port, LAG, tunnel ou VLAN**

Navigation dans les fenêtres

Cette section décrit les fonctions de l'utilitaire Web de configuration du commutateur.

En-tête d'application

L'en-tête d'application s'affiche sur toutes les pages. Elle propose les liens d'application suivants :

Nom du lien d'application	Description
	Une icône X rouge clignotante qui s'affiche à gauche du lien d'application **Enregistrer** indique que des changements apportés à la Configuration d'exécution n'ont pas encore été enregistrés dans le fichier de Configuration de démarrage. Vous pouvez désactiver le clignotement de l'icône X rouge sur la page Copier/enregistrer la configuration. Cliquez sur **Enregistrer** pour afficher la page Copier/enregistrer la configuration. Enregistrez le fichier de Configuration d'exécution en le copiant dans le fichier de Configuration de démarrage sur le périphérique. Une fois cet enregistrement effectué, l'icône X rouge et le lien d'application Enregistrer ne s'affichent plus. Au redémarrage du périphérique, le type de fichier Configuration de démarrage est copié sur la Configuration d'exécution et les paramètres du périphérique sont définis en fonction des données de Configuration d'exécution.
Nom d'utilisateur	Affiche le nom de l'utilisateur connecté au périphérique. Le nom d'utilisateur par défaut est **cisco**. (Le mot de passe par défaut est **cisco**.)

Nom du lien d'application	Description
Language Menu	Ce menu comprend les options suivantes : ▪ **Select a language :** choisissez une des langues qui apparaît dans le menu. Il s'agira de la langue utilisée par l'utilitaire de configuration Web. ▪ **Download Language :** ajoute une nouvelle langue au périphérique. ▪ **Delete Language :** supprime la deuxième langue du périphérique. La première langue (anglais) ne peut pas être supprimée. ▪ **Débogage :** option utilisée pour la traduction. Si vous choisissez cette option, tous les intitulés de l'utilitaire de configuration Web disparaîtront et vous verrez les ID des chaînes qui correspondent aux ID du fichier de langue. **REMARQUE** Pour mettre à niveau un fichier de langue, accédez à la page Upgrade/Backup Firmware/Language.
Logout	Cliquez sur ce bouton pour vous déconnecter de l'utilitaire Web de configuration du commutateur.
About	Cliquez sur ce lien pour afficher le nom et le numéro de version du périphérique.
Help	Cliquez sur ce lien pour afficher l'aide en ligne.
	L'icône d'état d'alerte SYSLOG s'affiche en cas de journalisation d'un message SYSLOG dont le niveau de gravité se situe au-dessus du *niveau critique*. Cliquez sur l'icône pour ouvrir la page RAM Memory. Une fois que vous avez accédé à cette page, l'icône d'état d'alerte SYSLOG ne s'affiche plus. Pour afficher la page en l'absence de message SYSLOG actif, cliquez sur **État et statistiques** > **Afficher le journal** > **Mémoire RAM**.

Boutons de gestion

Le tableau suivant décrit les boutons couramment utilisés qui s'affichent sur différentes pages du système.

Nom du bouton	Description
	Servez-vous du menu déroulant pour configurer le nombre d'entrées par page.
	Indique un champ obligatoire.
Add	Cliquez sur ce bouton pour afficher la page Add correspondante et ajouter une entrée à une table. Saisissez les informations requises et cliquez sur **Appliquer** pour les enregistrer dans la Configuration d'exécution. Cliquez sur **Fermer** pour retourner à la page principale. Cliquez sur **Enregistrer** pour afficher la page Copier/enregistrer la configuration et enregistrer la Configuration d'exécution dans le type de fichier Configuration de démarrage du périphérique.
Apply	Cliquez sur ce lien pour appliquer les modifications à la Configuration d'exécution du périphérique. En cas de redémarrage du périphérique, la Configuration d'exécution est perdue, sauf si elle a été enregistrée dans le type de fichier de Configuration de démarrage ou dans un autre type de fichier. Cliquez sur **Enregistrer** pour afficher la page Copier/enregistrer la configuration et enregistrer la Configuration d'exécution dans le type de fichier Configuration de démarrage du périphérique.
Cancel	Cliquez sur réinitialiser les modifications apportées à la page.
Clear All Interfaces Counters	Cliquez sur ce bouton pour effacer les compteurs de statistiques de toutes les interfaces.
Clear Interface Counters	Cliquez sur ce bouton pour effacer les compteurs de statistiques de l'interface sélectionnée.
Clear Logs	Efface les fichiers journaux.
Clear Table	Efface les entrées de la table.

Nom du bouton	Description
Close	Permet de revenir à la page principale. Un message s'affiche si des modifications n'ont pas été appliquées à la configuration de fonctionnement.
Copy Settings	Une table comporte généralement une ou plusieurs entrées contenant des paramètres de configuration. Au lieu de modifier chaque entrée individuellement, il est possible de modifier une entrée, puis de la copier sur plusieurs autres, comme décrit ci-dessous : 1. Sélectionnez l'entrée à copier. Cliquez sur **Copier les paramètres** pour afficher la fenêtre contextuelle. 2. Saisissez les numéros des entrées de destination dans le champ **to**. 3. Cliquez sur **Appliquer** pour enregistrer les modifications et sur **Fermer** pour retourner à la page principale.
Delete	Après avoir sélectionné une entrée dans la table, cliquez sur **Supprimer** pour la supprimer.
Details	Cliquez sur ce bouton pour afficher les détails relatifs à l'entrée sélectionnée.
Edit	Sélectionnez l'entrée et cliquez sur **Edit**. La page Edit qui s'ouvre vous permet de modifier l'entrée. 1. Cliquez sur **Appliquer** pour enregistrer les modifications dans la Configuration d'exécution. 2. Cliquez sur **Fermer** pour retourner à la page principale.
Go	Saisissez les critères de filtrage et cliquez sur **Go**. Les résultats s'affichent sur la page.
Refresh	Cliquez sur **Actualiser** pour actualiser les valeurs de compteur.
Test	Cliquez sur **Tester** pour effectuer les tests liés.

3

État et statistiques

Cette section décrit comment afficher les statistiques de l'appareil.

Elle couvre les rubriques suivantes :

- **Récapitulatif système**
- **Interfaces Ethernet**
- **Statistiques Etherlike**
- **Statistiques EAP 802.1X**
- **Intégrité**
- **RMON**
- **Afficher le journal**

Récapitulatif système

Reportez-vous à la section **Paramètres système**.

Interfaces Ethernet

La page Interface affiche les statistiques de trafic pour chaque port. La fréquence d'actualisation des informations peut être sélectionnée.

Cette page est utile pour analyser le volume de trafic envoyé et reçu, ainsi que sa dispersion (destination unique, multidestination et diffusion).

Pour afficher les statistiques Ethernet et/ou définir la fréquence d'actualisation :

ÉTAPE 1 Cliquez sur **Status and Statistics** > **Interface**.

ÉTAPE 2 Saisissez les paramètres.

- **Interface** : sélectionnez le type d'interface et l'interface spécifique pour laquelle les statistiques Ethernet doivent être affichées.
- **Taux d'actualisation** : sélectionnez la durée qui s'écoule avant l'actualisation des statistiques Ethernet de l'interface.

La zone Statistiques de réception affiche les informations se rapportant aux paquets entrants.

- **Total Bytes (Octets)** : octets reçus, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **Unicast Packets** : paquets de destination unique corrects reçus.
- **Multicast Packets** : paquets de multidestination corrects reçus.
- **Broadcast Packets** : paquets de diffusion corrects reçus.
- **Packets with Errors** : paquets avec erreurs reçus.

La zone Statistiques de transmission affiche les informations se rapportant aux paquets sortants.

- **Total Bytes (Octets)** : octets transmis, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **Unicast Packets** : paquets de destination unique corrects transmis.
- **Multicast Packets** : paquets de multidestination corrects transmis.
- **Broadcast Packets** : paquets de diffusion corrects transmis.

Pour effacer ou afficher les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs de l'interface affichée.
- Cliquez sur **Voir les statistiques de toutes les interfaces** pour visualiser l'ensemble des ports sur une seule et même page.

Statistiques Etherlike

La page Etherlike affiche les statistiques par port sur la base de la définition standard MIB Etherlike. La fréquence d'actualisation des informations peut être sélectionnée. Cette page fournit des informations plus détaillées sur les erreurs au niveau de la couche physique (Couche 1), qui pourraient perturber le trafic.

Pour afficher les statistiques Etherlike et/ou définir la fréquence d'actualisation :

ÉTAPE 1 Cliquez sur **Status and Statistics** > **Etherlike**.

ÉTAPE 2 Saisissez les paramètres.

- **Interface** : sélectionnez le type d'interface et l'interface spécifique pour laquelle les statistiques Ethernet doivent être affichées.
- **Taux d'actualisation** : sélectionnez la durée qui s'écoule avant l'actualisation des statistiques Etherlike.

Les champs sont affichés pour l'interface sélectionnée.

- **Erreurs FCS (Frame Check Sequence)** : trames reçues ayant échoué aux contrôles de redondance cyclique (CRC).
- **Trames de collisions individuelles** : trames impliquées dans une collision individuelle, mais ayant été transmises avec succès.
- **Collisions tardives** : collisions ayant été détectées après les 512 premiers octets de données.
- **Collisions excessives** : transmissions rejetées dues à des collisions excessives.
- **Paquets de taille excessive** : paquets de plus de 2000 octets reçus.
- **Erreurs de réception MAC internes** : trames rejetées en raison d'erreurs de destination.
- **Trames de pause reçues** : trames de pause de contrôle de flux reçues.
- **Trames de pause transmises** : trames de pause de contrôle de flux transmises à partir de l'interface sélectionnée.

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs sélectionnés.
- Cliquez sur **Voir les statistiques de toutes les interfaces** pour visualiser l'ensemble des ports sur une seule et même page.

Statistiques EAP 802.1X

La page *802.1x EAP* affiche des informations détaillées sur les trames EAP (Extensible Authentication Protocol) qui ont été envoyées ou reçues. Pour configurer la fonction 802.1X, reportez-vous à la page Propriétés 802.1X.

Pour afficher les statistiques EAP et/ou définir la fréquence d'actualisation :

ÉTAPE 1 Cliquez sur **État et statistiques** > **802.1x EAP**.

ÉTAPE 2 Sélectionnez l'**Interface** interrogée pour les statistiques.

ÉTAPE 3 Sélectionnez la durée (**Fréq. d'actualisation**) qui s'écoule avant l'actualisation des statistiques EAP.

Les valeurs sont affichées pour l'interface sélectionnée.

- **Trames EAPOL reçues** : trames EAPOL valides reçues sur le port.
- **Trames EAPOL transmises** : trames EAPOL valides transmises par le port.
- **Trames EAPOL de début reçues** : affiche le nombre de trames EAPOL de début qui ont été reçues sur le port.
- **Trames EAPOL de déconnexion reçues** : affiche le nombre de trames EAPOL de déconnexion qui ont été reçues sur le port.
- **Trames ID/de réponse EAP reçues** : trames ID/de réponse EAP reçues sur le port.
- **Trames de réponse EAP reçues** : trames de réponse EAP reçues par le port (autres que les trames ID/de réponse).
- **Trames ID/de demande EAP transmises** : trames ID/de demande EAP transmises par le port.
- **Trames de demande EAP transmises** : trames de demande EAP transmises par le port.
- **Trames EAPOL non valides reçues** : affiche le nombre de trames EAPOL non reconnues qui ont été reçues sur ce port.
- **Trames d'erreur de longueur EAP reçues** : trames EAPOL avec une longueur de corps de paquet non valide reçues sur ce port.
- **Version de la dernière trame EAPOL** : numéro de version de protocole associé à la dernière trame EAPOL reçue.
- **Source de la dernière trame EAPOL** : adresse MAC source associée à la dernière trame EAPOL reçue.

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs sélectionnés.
- Cliquez sur **Actualiser** pour actualiser les compteurs d'interfaces sélectionnés.
- Cliquez sur **Voir les statistiques de toutes les interfaces** pour effacer les compteurs de l'ensemble des interfaces.

Intégrité

Reportez-vous à la section **Intégrité**.

RMON

RMON (Remote Networking Monitoring) permet à un agent SNMP sur le périphérique de surveiller de façon proactive les statistiques de trafic sur une période donnée et d'envoyer des interceptions à un gestionnaire SNMP. L'agent SNMP local compare les compteurs en temps réel par rapport à des seuils prédéfinis et génère des alarmes, sans qu'une plate-forme de gestion SNMP centrale n'ait à générer des interrogations. Il s'agit d'un mécanisme efficace en termes de gestion proactive, à condition que des seuils adaptés aient été définis par rapport à la ligne de base de votre réseau.

RMON réduit le trafic entre le gestionnaire et le périphérique. Le gestionnaire SNMP n'a en effet pas à interroger fréquemment le périphérique afin d'obtenir des informations. RMON permet en outre au gestionnaire d'obtenir des rapports d'état opportuns, le périphérique signalant les événements à mesure qu'ils se produisent.

Cette fonction vous permet de réaliser les actions suivantes :

- Afficher les statistiques actuelles (depuis le moment où les valeurs du compteur ont été effacées). Vous pouvez également collecter les valeurs de ces compteurs sur une période puis afficher la table des données collectées, chaque ensemble collecté représentant une ligne individuelle de l'onglet *Historique*.
- Définir des changements intéressants dans les valeurs des compteurs, comme « un certain nombre de collisions tardives a été atteint » (définissant l'alarme), puis définir l'action à mettre en œuvre lorsque cet événement se produit (journal et/ou message d'interception).

RMON Statistics

La page Statistiques affiche des informations détaillées sur la taille des paquets, ainsi que des informations sur les erreurs de couche physique. Les informations sont affichées conformément à la norme RMON. Un paquet surdimensionné est une trame Ethernet respectant les critères suivants :

- La longueur du paquet est supérieure à la taille en octets de la MRU.
- Un événement de collision n'a pas été détecté.
- Un événement de collision tardive n'a pas été détecté.
- Un événement d'erreur de réception (Rx) n'a pas été détecté.
- Le paquet a un CRC valide.

Pour afficher les statistiques RMON et/ou définir la fréquence d'actualisation :

ÉTAPE 1 Cliquez sur **État et statistiques > RMON > Statistiques**.

ÉTAPE 2 Sélectionnez l'**interface** pour laquelle les statistiques Ethernet doivent être affichées.

ÉTAPE 3 Sélectionnez la **fréquence d'actualisation**, autrement dit la durée qui s'écoule avant l'actualisation des statistiques de l'interface.

Les statistiques suivantes sont affichées pour l'interface sélectionnée.

- **Octets reçus** : octets reçus, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **Événements d'abandon** : paquets abandonnés.
- **Paquets reçus** : paquets corrects reçus, dont les paquets de multidiffusion et de diffusion.
- **Paquets de diffusion reçus** : paquets de diffusion corrects reçus. Ce nombre n'inclut pas les paquets de multidestination.
- **Paquets de multidiffusion reçus** : paquets de multidiffusion corrects reçus.
- **Erreurs d'alignement et CRC** : erreurs d'alignement et CRC qui se sont produites.
- **Paquets de taille insuffisante** : paquets de taille insuffisante (moins de 64 octets) reçus.
- **Paquets de taille excessive** : paquets de taille excessive (plus de 2 000 octets) reçus.
- **Fragments** : fragments (paquets de moins de 64 octets) reçus, à l'exception des bits de synchronisation, mais en incluant les octets FCS.

- **Jabbers** : paquets reçus ayant une longueur supérieure à 1 632 octets. Ce nombre exclut les bits de synchronisation, mais inclut les octets FCS qui comportaient une séquence FCS (Frame Check Sequence) erronée avec un nombre entier d'octets (erreur FCS) ou une séquence FCS erronée avec un nombre non entier d'octets (erreur d'alignement). Un paquet long est une trame Ethernet respectant les critères suivants :
  - La longueur des données du paquet est supérieure à la MRU.
  - Le paquet a un CRC non valide.
  - Un événement d'erreur de réception (Rx) n'a pas été détecté.
- **Collisions** : collisions reçues. Si les trames géantes sont activées, le seuil des trames Jabber est augmenté de façon à correspondre à la taille maximale des trames géantes.
- **Trames de 64 octets** : trames de 64 octets reçues.
- **Trames de 65 à 127 octets** : trames de 65 à 127 octets reçues.
- **Trames de 128 à 255 octets** : trames de 128 à 255 octets reçues.
- **Trames de 256 à 511 octets** : trames de 256 à 511 octets reçues.
- **Trames de 512 à 1 023 octets** : trames de 512 à 1 023 octets reçues.
- **Trames de 1 024 octets ou plus** : trames de 1 024 à 2 000 octets et trames géantes reçues.

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs sélectionnés.
- Cliquez sur **Voir les statistiques de toutes les interfaces** pour visualiser l'ensemble des ports sur une seule et même page.

Historique RMON

La fonction RMON vous permet de contrôler les statistiques de chaque interface.

Vous pouvez configurer la fréquence d'échantillonnage, la quantité d'échantillons à stocker, ainsi que le port à partir duquel recueillir les données via la page Table de contrôle de l'historique.

Une fois que les données ont été échantillonnées et stockées, elles apparaissent sur la page Table d'historique que vous pouvez consulter en cliquant sur **Table d'historique**.

Pour saisir des données de contrôle RMON :

ÉTAPE 1 Cliquez sur **État et statistiques > RMON > Historique**. Les champs de cette page sont définis dans la page Ajouter un historique RMON ci-dessous. Le seul champ de cette page qui n'est pas défini dans la page Ajouter est le suivant :

- **Nombre d'échantillons actuel** : de par la norme, RMON est autorisé à ne pas accepter tous les échantillons demandés et à limiter plutôt le nombre d'échantillons par demande. Ce champ représente donc le nombre d'échantillons réellement accordé à la demande, ce nombre étant égal ou inférieur à la valeur demandée.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez les paramètres.

- **Nouvelle entrée d'historique** : affiche le numéro de la nouvelle entrée de la table d'historique.
- **Interface source** : sélectionnez le type d'interface à partir de laquelle les échantillons d'historique doivent être recueillis.
- **Max No. of Samples to Keep** : saisissez le nombre d'échantillons à stocker.
- **Intervalle d'échantillonnage** : saisissez la durée (en secondes) pendant laquelle des échantillons sont collectés au niveau des ports. La plage du champ est comprise entre 1 et 3 600.
- **Owner** : saisissez l'utilisateur ou la station RMON ayant demandé les informations RMON.

ÉTAPE 4 Cliquez sur **Apply**. L'entrée est ajoutée à la page Table de contrôle de l'historique, et le fichier de Configuration d'exécution est mis à jour.

ÉTAPE 5 Cliquez sur **Table d'historique** (décrite ci-dessous) pour afficher les statistiques réelles.

Table de l'historique RMON

La page Table d'historique affiche les échantillonnages réseau statistiques propres à l'interface. Les échantillons ont été configurés dans la table de contrôle de l'historique décrite ci-dessus.

Pour afficher les statistiques de l'historique RMON :

ÉTAPE 1 Cliquez sur **Status and Statistics** > **RMON** > **History**.

ÉTAPE 2 Cliquez sur **History Table**.

ÉTAPE 3 Dans le menu déroulant **N° d'entrée d'historique**, sélectionnez éventuellement le numéro d'entrée de l'échantillon à afficher.

Les champs sont affichés pour l'échantillon sélectionné.

- **Propriétaire** : propriétaire de l'entrée dans la table d'historique.
- **Sample No.** : les statistiques ont été récupérées à partir de cet échantillon.
- **Événements d'abandon** : paquets abandonnés en raison d'un manque de ressources réseau lors de l'intervalle d'échantillonnage. Cela peut ne pas correspondre au nombre exact de paquets abandonnés, mais plutôt au nombre de détections de paquets de ce type.
- **Octets reçus** : octets reçus, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **Paquets reçus** : paquets reçus, y compris les paquets erronés, ainsi que les paquets multicast et broadcast.
- **Paquets de diffusion** : paquets de diffusion corrects reçus, à l'exception des paquets de multidiffusion.
- **Multicast Packets** : paquets de multidestination corrects reçus.
- **Erreurs d'alignement et CRC** : erreurs d'alignement et CRC qui se sont produites.
- **Paquets de taille insuffisante** : paquets de taille insuffisante (moins de 64 octets) reçus.
- **Paquets de taille excessive** : paquets de taille excessive (plus de 2 000 octets) reçus.
- **Fragments** : fragments (paquets de moins de 64 octets) reçus, à l'exception des bits de synchronisation, mais incluant les octets FCS.
- **Jabotages** : nombre total de paquets reçus dont la taille dépassait 2000 octets. Ce nombre exclut les bits de synchronisation, mais inclut les octets FCS qui comportaient une séquence FCS (Frame Check Sequence) erronée avec un nombre entier d'octets (erreur FCS) ou une séquence FCS erronée avec un nombre non entier d'octets (erreur d'alignement).
- **Collisions** : collisions reçues.
- **Utilisation** : pourcentage du trafic actuel de l'interface par rapport au trafic maximum pouvant être géré par cette dernière.

Contrôle des événements RMON

Vous pouvez contrôler les occurrences à l'origine du déclenchement d'une alarme et le type de notification envoyé. Pour ce faire, procédez comme suit :

- **Page Événements** : permet de configurer les conséquences liées au déclenchement d'une alarme. Ce peut être n'importe quelle combinaison de journaux et de messages d'interception.
- **Alarms Page** : permet de configurer les occurrences qui déclenchent une alarme.

Pour définir les événements RMON :

ÉTAPE 1 Cliquez sur **État et statistiques > RMON** > **Événements**.

Cette page affiche les événements précédemment définis.

Les champs de cette page sont définis par la boîte de dialogue *Ajouter des événements RMON*, à l'exception du champ Heure.

- **Heure** : affiche l'heure de l'événement. (Il s'agit d'une table en lecture seule dans la fenêtre parent qui ne peut pas être définie.)

  ÉTAPE 2 Cliquez sur **Ajouter**.

  ÉTAPE 3 Saisissez les paramètres.

- **Entrée d'événement** : affiche le numéro d'index d'entrée d'événement pour la nouvelle entrée.
- **Description** : saisissez un nom pour l'événement. Ce nom est utilisé sur la page Ajouter une alarme RMON pour associer une alarme à un événement.
- **Notification Type** : sélectionnez le type d'action résultant de cet événement. Les valeurs possibles sont :
  - *None* : aucune action ne se produit lorsque l'alarme se déclenche.
  - *Journal (Table journal d'événements)* : ajoutez une entrée de journal à la table du journal d'événements lorsque l'alarme se déclenche.
  - *Interception (gestionnaire SNMP et serveur SYSLOG)* : permet d'envoyer une interception au serveur de journalisation distant lorsque l'alarme se déclenche.
  - *Journal et interception* : ajoute une entrée de journal à la table du journal d'événements et envoie une interception au serveur de journalisation distant lorsque l'alarme se déclenche.
- **Owner** : saisissez le périphérique ou l'utilisateur ayant défini l'événement.

  ÉTAPE 4 Cliquez sur **Apply**. L'événement RMON est consigné dans le fichier de Configuration d'exécution.

  ÉTAPE 5 Cliquez sur **Table du journal d'événements** pour afficher le journal des alarmes déclenchées et consignées (voir description ci-dessous).

Journaux d'événements RMON

La page Event Log Table affiche le journal des événements (actions) qui se sont produits. Deux types d'événements peuvent être journalisés : *Journal* ou *Journal et interception*. L'action de l'événement est réalisée lorsque l'événement est associé à une alarme (reportez-vous à la page Alarmes) et que les conditions de déclenchement de l'alarme sont remplies.

ÉTAPE 1 Cliquez sur **État et statistiques > RMON** > **Événements**.

ÉTAPE 2 Cliquez sur **Event Log Table**.

Cette page affiche les champs suivants :

- **N° d'entrée d'événement** : numéro d'entrée dans le journal de l'événement.
- **Log No.** : numéro du journal (au sein de l'événement).
- **Log Time** : heure à laquelle l'entrée a été enregistrée dans le journal.
- **Description** : description de l'événement qui a déclenché l'alarme.

Alarmes RMON

Les alarmes RMON fournissent un mécanisme pour la définition de seuils et d'intervalles d'échantillonnage afin de générer des événements d'exception sur des compteurs ou sur tout autre compteur d'objets SNMP géré par l'agent. Les seuils supérieurs et inférieurs doivent tous deux être configurés dans l'alarme. Une fois qu'un seuil supérieur est franchi, aucun autre événement de hausse n'est généré jusqu'à ce que le seuil inférieur associé soit lui-même franchi. Lorsqu'une alarme de baisse est déclenchée, l'alarme suivante se déclenche dès qu'un seuil supérieur est franchi.

Une ou plusieurs alarmes sont liées à un événement, ce qui indique l'action à entreprendre lorsque l'alarme se déclenche.

Les compteurs d'alarme peuvent être contrôlés par des valeurs absolues ou par des changements (delta) dans les valeurs de ces compteurs.

Pour entrer des alarmes RMON :

ÉTAPE 1 Cliquez sur **État et statistiques > RMON** > **Alarmes**. Toutes les alarmes définies précédemment sont affichées. Les champs sont décrits dans la page Ajouter une alarme RMON ci-dessous. En plus de ces champs, le champ suivant apparaît :

- **Valeur du compteur** : affiche la valeur de la statistique lors de la dernière période d'échantillonnage.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **N° d'entrée d'alarme** : affiche le numéro d'entrée de l'alarme.
- **Interface** : sélectionnez le type d'interface pour lequel les statistiques RMON s'affichent.
- **Counter Name** : sélectionnez la variable MIB qui indique le type d'occurrence mesuré.
- **Valeur du compteur** : nombre d'occurrences.
- **Sample Type** : sélectionnez la méthode d'échantillonnage pour générer une alarme. Les options sont les suivantes :
  - *Absolu* : si le seuil est franchi, une alarme est générée.
  - *Delta* : soustrait la valeur du dernier échantillon de la valeur actuelle. La différence obtenue est comparée au seuil. Si le seuil est franchi, une alarme est générée.
- **Seuil supérieur** : saisissez la valeur qui déclenche l'alarme de seuil supérieur.
- **Événement de hausse** : sélectionnez l'événement qui doit se produire lorsqu'un événement de hausse se déclenche. Les événements sont créés sur la page Événements.
- **Seuil inférieur** : saisissez la valeur qui déclenche l'alarme de seuil inférieur.
- **Événement de baisse** : sélectionnez l'événement qui doit se produire lorsqu'un événement de baisse se déclenche.
- **Startup Alarm** : sélectionnez le premier événement à partir duquel lancer la génération d'alarmes. La hausse est définie en franchissant le seuil en partant d'un seuil de faible valeur vers un seuil de valeur plus importante.
  - *Alarme de hausse* : une valeur en hausse déclenche l'alarme de seuil supérieur.
  - *Alarme de baisse* : une valeur en baisse déclenche l'alarme de seuil inférieur.
  - *Hausse et baisse* : des valeurs en hausse et en baisse déclenchent l'alarme.
- **Interval** : saisissez l'intervalle (en secondes) entre les alarmes.
- **Owner** : saisissez le nom de l'utilisateur ou du système de gestion du réseau qui reçoit l'alarme.

ÉTAPE 4 Cliquez sur **Apply**. L'alarme RMON est consignée dans le fichier de Configuration d'exécution.

Afficher le journal

Reportez-vous à la section **Afficher les journaux de la mémoire**.

4

Administration : Journal système

Cette section décrit la fonction de journalisation système, qui permet à l'appareil de générer plusieurs journaux indépendants. Chaque journal correspond à un ensemble de messages décrivant les événements système.

L'appareil génère les journaux locaux suivants :

- journal envoyé à l'interface de la console ;
- journal enregistré dans une liste cyclique d'événements journalisés dans la mémoire RAM et effacé au redémarrage de l'appareil ;
- journal enregistré dans un fichier journal cyclique enregistré dans la mémoire Flash et conservé d'un redémarrage à l'autre.

Vous pouvez en outre envoyer des messages vers des serveurs SYSLOG distants sous la forme d'interceptions SNMP et de messages SYSLOG.

Cette section contient les rubriques suivantes :

- **Définition des paramètres de journalisation système**
- **Définition des paramètres de journalisation distante**
- **Afficher les journaux de la mémoire**

Définition des paramètres de journalisation système

Vous pouvez sélectionner les événements à journaliser en fonction de leur niveau de gravité. Chaque message de journal s'accompagne d'un niveau de sévérité. Il est marqué avec la première lettre de ce niveau concaténé avec un tiret (-) de chaque côté (à l'exception d'*Urgence*, indiquée par la lettre F). Par exemple, le message de journal « %INIT-I-InitCompleted: ... » a un niveau de sévérité correspondant à **I**, qui signifie *Informatif*.

Les niveaux de sévérité des événements sont répertoriés du niveau le plus élevé au plus faible, comme suit :

- *Emergency* : le système n'est pas utilisable.
- *Alerte* : une action est requise.
- *Critical* : le système est dans un état critique.

- *Error* : le système subit une condition d'erreur.
- *Warning* : un avertissement système a été généré.
- *Notice* : le système fonctionne correctement, mais une remarque système a été générée.
- *Informational* : informations sur le périphérique.
- *Débogage* : fournit des informations détaillées sur un événement.

Vous pouvez sélectionner des niveaux de sévérité différents pour les journaux de la mémoire RAM et Flash. Ces journaux s'affichent respectivement sur les pages Mémoire RAM et Mémoire Flash.

Si vous choisissez d'enregistrer un niveau de gravité spécifique dans un journal, tous les événements de sévérité plus élevée le seront également. Les événements de gravité plus faible ne seront pas enregistrés dans le journal.

Par exemple, si **Warning** est sélectionné, tous les niveaux de gravité de type **Warning** et plus élevés sont enregistrés dans le journal (Emergency, Alert, Critical, Error et Warning). Aucun événement dont le niveau de sévérité est inférieur à **Avertissement** n'est enregistré (Remarque, Informatif et Débogage).

Pour définir des paramètres de journalisation globaux :

ÉTAPE 1 Cliquez sur **Administration** > **System Log** > **Log Settings**.

ÉTAPE 2 Saisissez les paramètres.

- **Journalisation** : sélectionnez cette option pour activer la journalisation des messages.
- **Agrégateur Syslog** : sélectionnez cette option pour activer l'agrégation des interceptions et SYSLOG. Si elle est activée, les interceptions et les messages SYSLOG identiques et contigus sont agrégés pendant le temps d'agrégation max. spécifié et envoyés dans un même message. Les messages agrégés sont envoyés dans l'ordre de leur arrivée. Chaque message indique le nombre de fois où il a été agrégé.
- **Temps d'agrégation max.** : saisissez la période pendant laquelle les messages SYSLOG sont agrégés.
- **Identifiant d'initiateur** : permet d'ajouter un identifiant d'origine aux messages SYSLOG. Les options sont les suivantes :
  - *Aucun* : aucun identifiant d'origine n'est ajouté aux messages SYSLOG.
  - *Nom d'hôte* : inclut le nom d'hôte système aux messages SYSLOG.
  - *Adresse IPv4* : l'adresse IPv4 de l'interface expéditrice est ajoutée aux messages SYSLOG.
  - *Adresse IPv6* : l'adresse IPv6 de l'interface expéditrice est ajoutée aux messages SYSLOG.
  - *Défini par l'utilisateur* : permet de saisir la description à faire figurer dans les messages SYSLOG.

- **Journalisation de la mémoire RAM** : sélectionnez les niveaux de sévérité des messages à journaliser dans la RAM.
- **Journalisation de la mémoire Flash** : sélectionnez les niveaux de sévérité des messages à journaliser dans la mémoire Flash.

ÉTAPE 3 Cliquez sur **Apply**. Le fichier de configuration de fonctionnement est mis à jour.

Définition des paramètres de journalisation distante

La page Serveurs de journalisation distants permet de définir les serveurs SYSLOG distants où sont envoyés les messages de journalisation. Vous pouvez configurer la sévérité des messages que reçoit chaque serveur.

Pour définir les serveurs SYSLOG :

ÉTAPE 1 Cliquez sur **Administration** > **System Log** > **Remote Log Servers**.

ÉTAPE 2 Renseignez les champs suivants :

- **Interface source IPv4** : sélectionnez l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source des messages SYSLOG envoyés aux serveurs SYSLOG.
- **Interface source IPv6** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source des messages SYSLOG envoyés aux serveurs SYSLOG.

REMARQUE Si l'option Auto est sélectionnée, le système récupère l'adresse IP source de l'adresse IP définie dans l'interface sortante.

Les informations sont décrites pour chaque serveur de journalisation configuré précédemment. Les champs sont décrits ci-dessous sur la page **Ajouter**.

ÉTAPE 3 Cliquez sur **Ajouter.**

ÉTAPE 4 Saisissez les paramètres.

- **Server Definition** : indiquez si vous souhaitez identifier le serveur de journalisation distante par son adresse IP ou par son nom.
- **Version IP** : sélectionnez le format IP pris en charge.

- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée).
- **Adresse IP/Nom serveur de journalisation** : saisissez l'adresse IP ou le nom de domaine du serveur de journalisation.
- **UDP Port** : saisissez le numéro du port UDP auquel les messages de journal sont envoyés.
- **Équipement** : sélectionnez une valeur pour l'équipement à partir duquel les journaux système sont envoyés au serveur distant. Une seule valeur d'équipement peut être affectée à un serveur. Si un autre code d'équipement est affecté, la première valeur est remplacée.
- **Description** : saisissez une description pour le serveur.
- **Minimum Severity** : sélectionnez le niveau minimum de gravité des messages de journalisation système à envoyer au serveur.

ÉTAPE 5 Cliquez sur **Appliquer**. La page Ajouter serveur de journalisation distant se ferme ; le serveur SYSLOG est ajouté et le fichier de Configuration d'exécution est mis à jour.

Afficher les journaux de la mémoire

L'appareil peut enregistrer des informations dans les journaux suivants :

- Journal de la RAM (effacé lors du redémarrage).
- Journal de la mémoire Flash (uniquement effacé sur instruction de l'utilisateur)

Vous pouvez configurer les messages à enregistrer dans chaque journal en fonction de leur sévérité. Un message peut en outre être enregistré dans plusieurs journaux, y compris ceux qui résident sur des serveurs SYSLOG externes.

Mémoire RAM

La page Mémoire RAM affiche tous les messages enregistrés dans la RAM (cache) dans l'ordre chronologique. Les entrées sont enregistrées dans le journal de la RAM en fonction de la configuration définie sur la page Paramètres des journaux.

Pour afficher les entrées du journal, cliquez sur **État et statistiques** > **Afficher le journal** > **Mémoire RAM**.

En haut de la page se trouve un bouton qui vous permet de **désactiver le clignotement de l'icône d'alerte**. **Cliquez dessus.** Ce bouton permet d'activer ou de désactiver cette fonction.

Le **seuil de journalisation actuel** spécifie les niveaux de journalisation qui sont générés. Celui-ci peut être modifié en cliquant sur **Modifier** selon le nom du champ.

Cette page contient les champs suivants, pour chaque fichier journal :

- **Log Index** : numéro de l'entrée dans le journal.
- **Log Time** : heure à laquelle le message a été généré.
- **Severity** : niveau de sévérité de l'événement.
- **Description** : message texte décrivant l'événement.

Pour effacer les messages des journaux, cliquez sur **Effacer les journaux**. Les messages sont effacés.

Mémoire Flash

La page Mémoire Flash affiche, dans l'ordre chronologique, les messages enregistrés dans la mémoire Flash. Le niveau de gravité minimal de la journalisation peut être configuré sur la page Paramètres des journaux. Les journaux de la mémoire Flash sont conservés au redémarrage du commutateur. Vous pouvez effacer les journaux manuellement.

Pour afficher les journaux de la mémoire Flash, cliquez sur **État et statistiques** > **Afficher le journal** > **Mémoire Flash**.

Le **seuil de journalisation actuel** spécifie les niveaux de journalisation qui sont générés. Celui-ci peut être modifié en cliquant sur **Modifier** selon le nom du champ.

Cette page contient les champs suivants, pour chaque fichier journal :

- **Log Index** : numéro de l'entrée dans le journal.
- **Log Time** : heure à laquelle le message a été généré.
- **Severity** : niveau de sévérité de l'événement.
- **Description** : message texte décrivant l'événement.

Pour effacer les messages, cliquez sur **Effacer les journaux**. Les messages sont effacés.

5

Administration : Gestion de fichiers

Cette section se concentre sur la gestion des fichiers système.

Les sujets suivants sont traités :

- **Fichiers système**
- **Mettre à niveau/sauvegarder micrologiciel/langue**
- **Télécharger/sauvegarder configuration/journal**
- **Propriétés des fichiers de configuration**
- **Copier/enregistrer la configuration**
- **Configuration/Mise à jour automatique de l'image via DHCP**

Fichiers système

Les fichiers système contiennent des informations de configuration, des images du micrologiciel ou du code de démarrage.

Vous pouvez effectuer diverses actions avec ces fichiers, par exemple : sélectionner le fichier du micrologiciel à partir duquel l'appareil doit démarrer, copier différents types de fichiers de configuration en interne sur l'appareil ou copier des fichiers vers ou depuis un appareil externe, comme un serveur externe.

Les méthodes de transfert de fichiers disponibles sont les suivantes :

- copie interne ;
- HTTP/HTTPS qui utilise la structure fournie par le navigateur ;
- client TFTF/SCP, nécessitant un serveur TFTP/SCP.

Les fichiers de configuration de l'appareil sont définis en fonction de leur *type* et comportent les réglages et valeurs de paramètre de l'appareil.

Lorsqu'une configuration est référencée sur l'appareil, cette opération s'effectue en fonction de son *type de fichier de configuration (par exemple, Configuration de démarrage ou Configuration d'exécution)* et non en fonction d'un nom de fichier modifiable par l'utilisateur.

Le contenu peut être copié d'un type de fichier de configuration vers un autre, mais le nom des types de fichiers ne peut pas être modifié par l'utilisateur.

Les autres fichiers présents sur l'appareil incluent les fichiers de micrologiciel, de code de démarrage et journaux et sont appelés *fichiers opérationnels*.

Les fichiers de configuration sont des fichiers texte qui peuvent être modifiés dans un éditeur de texte tel que le Bloc-notes une fois copiés sur un appareil externe, un PC par exemple.

Fichiers et types de fichiers

Les fichiers de configuration et fichiers opérationnels correspondant aux types suivants sont présents sur l'appareil :

- **Configuration d'exécution** : paramètres de fonctionnement actuellement utilisés par l'appareil. C'est le seul type de fichier qui est modifié quand vous changez les valeurs des paramètres du périphérique.

  En cas de redémarrage de l'appareil, la Configuration d'exécution est perdue. La Configuration de démarrage, stockée dans la mémoire Flash, remplace la Configuration d'exécution, stockée dans la mémoire RAM.

  Pour conserver toutes les modifications apportées à l'appareil, vous devez enregistrer la Configuration d'exécution dans la Configuration de démarrage ou dans un autre type de fichier.

- **Configuration de démarrage** : valeurs de paramètres que vous avez enregistrées en copiant une autre configuration (généralement la Configuration d'exécution) dans la Configuration de démarrage.

  La Configuration de démarrage est conservée dans la mémoire Flash et préservée à chaque redémarrage de l'appareil. Lors du redémarrage, la configuration de démarrage est copiée dans la RAM et identifiée comme étant la configuration de fonctionnement.

- **Configuration miroir** : copie de la Configuration de démarrage, créée par l'appareil dans l'un des cas suivants :

  - l'appareil a fonctionné en continu pendant 24 heures ;
  - aucune modification n'a été apportée à la configuration de fonctionnement au cours des dernières 24 heures ;
  - la Configuration de démarrage est identique à la Configuration d'exécution.

  Seul le système peut copier la configuration de démarrage dans la configuration miroir. Vous pouvez toutefois copier la configuration miroir vers d'autres types de fichiers ou sur un autre périphérique.

L'option permettant de copier automatiquement la Configuration d'exécution dans la Configuration miroir peut être désactivée sur la page Propriétés des fichiers de configuration.

- **Configuration de secours** : copie manuelle d'un fichier de configuration servant à protéger le système en cas d'arrêt ou à maintenir un état de fonctionnement spécifique. Vous pouvez copier la Configuration miroir, la Configuration de démarrage ou la Configuration d'exécution dans un fichier de configuration de sauvegarde. La Configuration de secours est conservée dans la mémoire Flash et préservée en cas de redémarrage de l'appareil.
- **Micrologiciel** : programme qui contrôle les opérations et les fonctions de l'appareil. Plus communément appelé *image*.
- **Code de démarrage** : contrôle le démarrage de base du système et lance l'image du micrologiciel.
- **Fichier de langue** : dictionnaire qui permet d'afficher les fenêtres de l'utilitaire de configuration Web dans la langue sélectionnée.
- **Journal Flash** : messages SYSLOG stockés dans la mémoire Flash.

Actions des fichiers

Les actions suivantes peuvent être réalisées pour gérer le micrologiciel et les fichiers de configuration :

- Mettre à niveau le micrologiciel ou le code de démarrage, ou remplacer une langue, comme décrit dans la section **Mettre à niveau/sauvegarder micrologiciel/langue**.
- Enregistrer les fichiers de configuration de l'appareil dans un répertoire situé sur un autre appareil, comme décrit à la section **Télécharger/sauvegarder configuration/journal**.
- Effacer les types de fichiers de Configuration de démarrage ou de Configuration de sauvegarde, comme décrit dans la section **Propriétés des fichiers de configuration**.
- Copier un type de fichier de configuration dans un autre type de fichier de configuration, comme décrit dans la section **Copier/enregistrer la configuration**.
- Télécharger automatiquement un fichier de configuration depuis un serveur DHCP vers l'appareil, comme décrit à la section **Configuration/Mise à jour automatique de l'image via DHCP**.

Cette section aborde les points suivants :

- **Mettre à niveau/sauvegarder micrologiciel/langue**
- **Télécharger/sauvegarder configuration/journal**
- **Propriétés des fichiers de configuration**
- **Copier/enregistrer la configuration**
- **Configuration/Mise à jour automatique de l'image via DHCP**

Mettre à niveau/sauvegarder micrologiciel/langue

Le processus **Mettre à niveau/sauvegarder micrologiciel/langue** peut être utilisé pour :

- mettre à niveau ou sauvegarder l'image du micrologiciel ;
- mettre à niveau ou sauvegarder le code de démarrage ;
- importer ou mettre à niveau un autre fichier de langue ;

Les méthodes de transfert de fichiers suivantes sont prises en charge :

- HTTP/HTTPS qui utilise la structure fournie par le navigateur
- TFTP qui nécessite un serveur TFTP
- SCP (Secure Copy Protocol), nécessitant un serveur SCP

Lorsqu'un nouveau fichier de langue est chargé sur l'appareil, la langue y correspondant peut être sélectionnée dans le menu déroulant. Notez que redémarrer l'appareil n'est pas nécessaire.

Une seule image du micrologiciel est stockée sur l'appareil. Après le chargement d'un nouveau micrologiciel sur l'appareil, ce dernier doit être redémarré pour que le nouveau micrologiciel devienne actif. La page Récapitulatif continue d'afficher l'image précédente tant que l'appareil n'a pas été redémarré.

Mise à niveau et sauvegarde des fichiers de micrologiciel ou de langue

Pour télécharger ou sauvegarder une image logicielle ou un fichier de langue :

ÉTAPE 1 Cliquez sur **Administration** > **File Management** > **Upgrade/Backup Firmware/Language**.

ÉTAPE 2 Cliquez sur la Méthode de transfert. Procédez comme suit :

- Si vous avez sélectionné **TFTP**, passez à l'**ÉTAPE 3**.
- Si vous avez sélectionné **via HTTP/HTTPS**, passez à l'**ÉTAPE 4**.
- Si vous avez sélectionné **via SCP**, passez à l'**ÉTAPE 5**.

ÉTAPE 3 Si vous avez sélectionné **via TFTP**, saisissez les paramètres en suivant la procédure décrite dans cette étape. Sinon, passez à l'**ÉTAPE 4**.

Sélectionnez le **Mode d'enregistrement** parmi les options suivantes :

- **Mettre à niveau** : spécifie que le type de fichier présent sur l'appareil doit être remplacé par sa nouvelle version, laquelle version est située sur un serveur TFTP.
- **Sauvegarder** : spécifie qu'une copie du type de fichier doit être enregistrée dans un fichier situé sur un autre appareil.

Renseignez les champs suivants :

- **Type de fichier** : sélectionnez le type de fichier de destination. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)
- **Définition du serveur TFTP** : indiquez si vous souhaitez spécifier le serveur TFTP **Par adresse IP** ou **Par nom**.
- **Version IP** : indiquez si l'adresse utilisée est de type IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - **Liaison locale** : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe FE80, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - **Global** : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée).
- **Nom/Adresse IP du serveur TFTP** : saisissez l'adresse IP ou le nom du serveur TFTP.
- **(Pour une mise à niveau) Nom du fichier source** : saisissez le nom du fichier source.
- **(Pour une sauvegarde) Nom du fichier de destination** : saisissez le nom du fichier de sauvegarde.

ÉTAPE 4 Si vous avez sélectionné **via HTTP/HTTPS**, vous pouvez uniquement sélectionner le **Mode d'enregistrement** : **Mettre à niveau**. Saisissez les paramètres décrits dans cette étape.

- **Type du fichier** : sélectionnez l'un des types de fichiers suivants :
  - *Image du micrologiciel* : sélectionnez cette option pour mettre à niveau l'image du micrologiciel.
  - *Fichier de langue* : sélectionnez cette option pour mettre à niveau le fichier de langue.
- **Nom du fichier** : cliquez sur **Parcourir** pour sélectionner un fichier ou saisissez le chemin et le nom du fichier source à utiliser pour le transfert.

ÉTAPE 5 Si vous avez sélectionné via **SCP (sur SSH),** consultez la section **Authentification du client SSH** pour obtenir de plus amples instructions. Renseignez ensuite les champs suivants : Notez que seuls les champs uniques sont décrits, pour les autres, consultez les descriptions ci-dessus.

- **Authentification du serveur SSH distant** : pour activer l'authentification du serveur SSH (qui est désactivée par défaut), cliquez sur **Modifier**. Vous êtes redirigé vers la page **Authentification du serveur SSH**, où vous pourrez configurer le serveur SSH, puis vous reviendrez vers cette page. Utilisez la page **Authentification du serveur SSH** pour sélectionner une méthode d'authentification de l'utilisateur SSH (mot de passe ou clé privée/publique), définir un nom d'utilisateur et un mot de passe sur l'appareil (si vous avez choisi la méthode par mot de passe) et générer une clé RSA ou DSA, le cas échéant.

Authentification du client SSH : l'authentification du client peut être effectuée de l'une des manières suivantes :

- **Utiliser les informations d'identification système du client SSH** : définit les informations d'identification permanentes de l'utilisateur SSH. Cliquez sur **Informations d'identification système** pour accéder à la page Authentification de l'utilisateur SSH où vous pouvez définir le nom d'utilisateur et le mot de passe pour toutes les utilisations futures.
- **Utiliser les infos d'identification unique du client SSH** : saisissez les informations suivantes :
  - *Nom d'utilisateur* : saisissez un nom d'utilisateur pour ce mode de copie.
  - *Mot de passe* : saisissez un mot de passe pour cette copie.

  REMARQUE Le nom d'utilisateur et le mot de passe relatifs aux informations d'identification unique ne seront pas enregistrés dans le fichier de configuration.

Sélectionnez le **Mode d'enregistrement** parmi les options suivantes :

- **Mettre à niveau** : spécifie que le type de fichier présent sur l'appareil doit être remplacé par sa nouvelle version, laquelle version est située sur un serveur TFTP.
- **Sauvegarder** : spécifie qu'une copie du type de fichier doit être enregistrée dans un fichier situé sur un autre appareil.

Renseignez les champs suivants :

- **Type de fichier** : sélectionnez le type de fichier de destination. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)
- **Définition du serveur SCP** : indiquez si vous souhaitez spécifier le serveur SCP par son adresse IP ou son nom de domaine.
- **Version IP** : indiquez si l'adresse utilisée est de type IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (si IPv6 est utilisé). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut être routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.

- **Interface de liaison locale** : sélectionnez l'interface de liaison locale dans la liste.
- **Adresse IP/Nom serveur SCP** : saisissez l'adresse IP ou le nom de domaine du serveur SCP.
- **(Pour une mise à niveau) Nom du fichier source** : saisissez le nom du fichier source.
- **(Pour une sauvegarde) Nom du fichier de destination** : saisissez le nom du fichier de sauvegarde.

ÉTAPE 6 Cliquez sur **Apply**. Si les fichiers, les mots de passe et les adresses du serveur sont corrects, l'une des actions suivantes peut se produire :

- Si l'authentification du serveur SSH est activée (dans la page Authentification du serveur SSH) et si le serveur SCP est sécurisé, l'opération aboutit. Si le serveur SCP n'est pas sécurisé, l'opération échoue et une erreur s'affiche.
- Si l'authentification du serveur SSH n'est pas activée, l'opération aboutit pour n'importe quel serveur SCP.

Télécharger/sauvegarder configuration/journal

La page Download/Backup Configuration/Log permet :

- La sauvegarde de fichiers de configuration ou de journaux depuis l'appareil vers un périphérique externe.
- La restauration de fichiers de configuration depuis un périphérique externe vers l'appareil.

Lorsque vous restaurez un fichier de configuration vers la Configuration d'exécution, le fichier importé *ajoute* toute commande de configuration qui n'existait pas dans l'ancien fichier et *remplace* toute valeur de paramètre dans les commandes de configuration existantes.

Lorsque vous restaurez un fichier de configuration vers la Configuration de démarrage ou un fichier de configuration de secours, le nouveau fichier *remplace* le fichier précédent.

Lorsque vous procédez à une restauration vers la Configuration de démarrage, l'appareil doit être redémarré pour que cette Configuration puisse être utilisée en tant que Configuration d'exécution. Notez que vous pouvez redémarrer l'appareil en suivant la procédure présentée à la section **Interface de gestion**.

Compatibilité descendante du fichier de configuration

Lors de la restauration des fichiers de configuration depuis un périphérique externe vers l'appareil, le problème de compatibilité peut survenir si les modes système ne sont pas identiques sur l'appareil et dans le nouveau fichier de configuration. Dans ce cas :

- Lorsque le téléchargement du fichier de configuration sur l'appareil s'effectue à l'aide de la page Télécharger/sauvegarder configuration/journal, cette opération est annulée et un message s'affiche indiquant que le mode système doit être modifié sur la page Paramètres système.
- Lorsque le téléchargement du fichier de configuration fait partie d'un processus de configuration automatique, le fichier de configuration de démarrage est supprimé et l'appareil redémarre automatiquement en utilisant le nouveau mode système. Lorsqu'un fichier de configuration vide est utilisé pour la configuration de l'appareil,

Téléchargement ou sauvegarde d'un fichier de configuration ou d'un journal

Pour sauvegarder ou restaurer le fichier de configuration système :

ÉTAPE 1 Cliquez sur **Administration** > **File Management** > **Download/Backup Configuration/Log**.

ÉTAPE 2 Sélectionnez la **Méthode de transfert**.

ÉTAPE 3 Si vous avez sélectionné **via TFTP**, saisissez les paramètres. Sinon, passez à l'**ÉTAPE 4**.

Sélectionnez **Télécharger** ou **Sauvegarde** comme **Mode d'enregistrement**.

Télécharger : indique que le type de fichier de l'appareil est remplacé par le type de fichier d'un autre appareil. Renseignez les champs suivants :

a. **Définition du serveur TFTP** : indiquez si vous souhaitez spécifier le serveur TFTP par adresse IP ou par nom de domaine.

b. **Version IP** : indiquez si l'adresse utilisée est de type IPv4 ou IPv6.

REMARQUE Si le serveur est sélectionné par son nom dans la définition de serveur, il est inutile de sélectionner les options relatives à la version IP.

c. **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (si IPv6 est utilisé). Les options sont les suivantes :

- *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
- *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.

d. **Interface de liaison locale** : sélectionnez l'interface de liaison locale dans la liste.

e. **Nom/Adresse IP du serveur TFTP** : saisissez l'adresse IP ou le nom du serveur TFTP.

f. **Source File Name** : saisissez le nom du fichier source. Les noms de fichiers ne peuvent pas comporter de barres obliques (\ ou /), ne doivent pas débuter par un point (.) et ne peuvent dépasser 160 caractères. (Caractères valides : A-Z, a-z, 0-9, « . », « - », « _ »).

g. **Type du fichier de destination** : saisissez le type du fichier de configuration de destination. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)

Sauvegarde : spécifie qu'un type de fichier doit être copié dans un fichier situé sur un autre appareil. Renseignez les champs suivants :

a. **Définition du serveur TFTP** : indiquez si vous souhaitez spécifier le serveur TFTP par adresse IP ou par nom de domaine.

b. **Version IP** : indiquez si l'adresse utilisée est de type IPv4 ou IPv6.

c. **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (si IPv6 est utilisé). Les options sont les suivantes :

- *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
- *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.

d. **Interface de liaison locale** : sélectionnez l'interface de liaison locale dans la liste.

e. **Nom/Adresse IP du serveur TFTP** : saisissez l'adresse IP ou le nom du serveur TFTP.

f. **Type du fichier source** : saisissez le type du fichier de configuration source. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)

g. **Données confidentielles** : choisissez comment les données sensibles doivent être incluses dans le fichier de sauvegarde. Les options suivantes sont disponibles :

- *Exclure* : ne pas inclure les données sensibles à la sauvegarde.
- *Chiffré* : inclure les données sensibles dans la sauvegarde, mais en les cryptant.
- *Texte en clair* : inclure les données sensibles dans la sauvegarde sous forme de texte en clair.

REMARQUE Les options disponibles relatives aux données confidentielles sont déterminées par les règles SSD de l'utilisateur actuel. Pour en savoir plus, consultez la page Gestion sécurisée des données confidentielles > Règles SSD.

h. **Nom du fichier de destination** : saisissez le nom du fichier de destination. Les noms de fichiers ne peuvent pas comporter de barres obliques (\ ou /), ils doivent comprendre de 1 à 160 caractères et leur première lettre ne doit pas être un point (.). (Caractères valides : A-Z, a-z, 0-9, « . », « - », « _ »).

i. Cliquez sur **Apply**. Le fichier est mis à niveau ou sauvegardé.

ÉTAPE 4 Si vous avez sélectionné **via HTTP/HTTPS**, saisissez les paramètres en suivant la procédure décrite dans cette étape.

Sélectionnez l'**Enregistrement**.

Si le **Mode d'enregistrement** est défini sur *Télécharger* (remplacement du fichier de l'appareil par une nouvelle version provenant d'un autre périphérique), procédez comme suit. Sinon, passez à la procédure suivante de cette étape.

a. **Nom du fichier source** : cliquez sur **Parcourir** pour sélectionner un fichier ou saisissez le chemin et le nom du fichier source à utiliser pour le transfert.

b. **Type du fichier de destination** : sélectionnez le type du fichier de configuration. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)

c. Cliquez sur **Apply**. Le fichier est transféré de l'autre périphérique vers l'appareil.

Si le **Mode d'enregistrement** est défini sur *Sauvegarder* (copie d'un fichier vers un autre périphérique), procédez comme suit :

a. **Type du fichier source** : sélectionnez le type de fichier de configuration. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)

b. **Données confidentielles** : choisissez comment les données sensibles doivent être incluses dans le fichier de sauvegarde. Les options suivantes sont disponibles :

- *Exclure* : ne pas inclure les données sensibles à la sauvegarde.
- *Chiffré* : inclure les données sensibles dans la sauvegarde, mais en les cryptant.
- *Texte en clair* : inclure les données sensibles dans la sauvegarde sous forme de texte en clair.

REMARQUE Les options disponibles relatives aux données confidentielles sont déterminées par les règles SSD de l'utilisateur actuel. Pour en savoir plus, consultez la page Gestion sécurisée des données confidentielles > Règles SSD.

c. Cliquez sur **Apply**. Le fichier est mis à niveau ou sauvegardé.

ÉTAPE 5 Si vous avez sélectionné **via SCP (sur SSH)**, reportez-vous à la section **Configuration du client SSH via l'interface utilisateur graphique (GUI)** pour plus d'instructions. Renseignez ensuite les champs suivants :

- **Authentification du serveur SSH distant** : pour activer l'authentification du serveur SSH (qui est désactivée par défaut), cliquez sur **Modifier**. Vous serez dirigé vers la page **Authentification du serveur SSH** pour procéder à la configuration, puis vous reviendrez sur cette page. Utilisez la page **Authentification du serveur SSH** pour sélectionner une méthode d'authentification de l'utilisateur SSH (mot de passe ou clé privée/publique), définir un nom d'utilisateur et un mot de passe sur l'appareil (si vous avez choisi la méthode par mot de passe) et générer une clé RSA ou DSA, le cas échéant.

Authentification du client SSH : l'authentification du client peut être effectuée de l'une des manières suivantes :

- **Utiliser les informations d'identification système du client SSH** : définit les informations d'identification permanentes de l'utilisateur SSH. Cliquez sur **Informations d'identification système** pour accéder à la page Authentification de l'utilisateur SSH où vous pouvez définir le nom d'utilisateur et le mot de passe pour toutes les utilisations futures.
- **Utiliser les infos d'identification unique du client SSH** : saisissez les informations suivantes :
  - *Nom d'utilisateur* : saisissez un nom d'utilisateur pour ce mode de copie.
  - *Mot de passe* : saisissez un mot de passe pour cette copie.
- **Mode d'enregistrement** : choisissez de sauvegarder ou de restaurer le fichier de configuration système.
- **Définition du serveur SCP** : indiquez si vous souhaitez spécifier le serveur SCP par **adresse IP** ou par **nom** de domaine.
- **Version IP** : indiquez si l'adresse utilisée est de type IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (si IPv6 est utilisé). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut être routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez l'interface de liaison locale dans la liste.
- **Nom/Adresse IP du serveur SCP** : saisissez l'adresse IP ou le nom du serveur SCP.

Si le **Mode d'enregistrement** est défini sur *Télécharger* (remplacement du fichier de l'appareil par une nouvelle version provenant d'un autre périphérique), renseignez les champs suivants :

- **Nom du fichier source** : saisissez le nom du fichier source.
- **Type du fichier de destination** : sélectionnez le type du fichier de configuration. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)

Si le **Mode d'enregistrement** est défini sur *Sauvegarder* (copie d'un fichier vers un autre périphérique), renseignez les champs suivants (en plus de ceux répertoriés ci-dessus) :

- **Type du fichier source** : sélectionnez le type de fichier de configuration. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)
- **Données confidentielles** : choisissez comment les données sensibles doivent être incluses dans le fichier de sauvegarde. Les options suivantes sont disponibles :
  - *Exclure* : ne pas inclure les données sensibles à la sauvegarde.
  - *Chiffré* : inclure les données sensibles dans la sauvegarde, mais en les cryptant.
  - *Texte en clair* : inclure les données sensibles dans la sauvegarde sous forme de texte en clair.

  REMARQUE Les options disponibles relatives aux données confidentielles sont déterminées par les règles SSD de l'utilisateur actuel. Pour en savoir plus, consultez la page Gestion sécurisée des données confidentielles > Règles SSD.
- **Nom du fichier de destination** : nom du fichier vers lequel vous copiez des données.

ÉTAPE 6 Cliquez sur **Apply**. Le fichier est mis à niveau ou sauvegardé.

Propriétés des fichiers de configuration

La page Propriétés des fichiers de configuration indique quand les différents fichiers de configuration du système ont été créés. Elle permet également de supprimer les fichiers de la configuration de démarrage et de la configuration de secours. En revanche, vous ne pouvez pas supprimer les autres types de fichiers de configuration.

Pour définir si des fichiers de configuration miroir seront créés, effacez les fichiers de configuration et vérifiez quand les fichiers de configuration ont été créés :

ÉTAPE 1 Cliquez sur **Administration** > **File Management** > **Configuration Files Properties**.

Cette page affiche les champs suivants :

- **Nom du fichier de configuration** : type de fichier système.
- **Heure de création** : date et heure de modification du fichier.

ÉTAPE 2 Si nécessaire, désactivez la **Configuration miroir automatique**. Des fichiers de configuration miroir ne seront donc pas créés automatiquement. En désactivant cette option, le fichier de configuration miroir est supprimé si vous en aviez créé un. Consultez la section **Fichiers système** pour obtenir une description des fichiers miroir et pour connaître les raisons qui peuvent vous pousser à éviter la création automatique de fichiers de configuration miroir.

ÉTAPE 3 Si nécessaire, choisissez Configuration de démarrage et/ou Configuration de secours, et cliquez sur **Effacer les fichiers** pour supprimer ces fichiers.

Copier/enregistrer la configuration

Lorsque vous cliquez sur **Appliquer** dans une quelconque fenêtre, les modifications que vous avez apportées aux paramètres de configuration de l'appareil sont stockées *uniquement* dans la Configuration d'exécution. Pour conserver les paramètres de la Configuration d'exécution, celle-ci doit être copiée sur un autre type de configuration ou enregistrée sur un autre appareil.

ATTENTION À moins que la Configuration d'exécution ne soit copiée sur la Configuration de démarrage ou sur un autre fichier de configuration, toutes les modifications apportées depuis la dernière copie du fichier seront perdues au redémarrage de l'appareil.

Les combinaisons suivantes de copie de types de fichiers internes sont autorisées :

- De la Configuration d'exécution sur la Configuration de démarrage ou la Configuration de secours
- De la Configuration de démarrage sur la Configuration d'exécution, Configuration de démarrage ou Configuration de secours
- De la Configuration de secours sur la Configuration d'exécution, Configuration de démarrage ou Configuration de secours
- De la Configuration miroir sur la Configuration d'exécution, Configuration de démarrage ou Configuration de secours

Pour copier un type de fichier de configuration dans un autre type de fichier de configuration :

ÉTAPE 1 Cliquez sur **Administration** > **File Management** > **Copy/Save Configuration**.

ÉTAPE 2 Sélectionnez le **Nom du fichier source** à copier. Seuls les types de fichiers valides sont affichés (description dans la section **Fichiers et types de fichiers**).

ÉTAPE 3 Sélectionnez le **Nom du fichier de destination** à remplacer par le fichier source.

ÉTAPE 4 Sélectionnez l'option **Données confidentielles** si vous sauvegardez un fichier de configuration, puis sélectionnez un des formats suivants.

- **Exclure** : ne pas inclure les données sensibles à la sauvegarde.
- **Chiffré** : inclure les données sensibles dans la sauvegarde, mais en les cryptant.
- **Texte en clair** : inclure les données sensibles dans la sauvegarde sous forme de texte en clair.

REMARQUE Les options disponibles relatives aux données confidentielles sont déterminées par les règles SSD de l'utilisateur actuel. Pour en savoir plus, consultez la page Gestion sécurisée des données confidentielles > Règles SSD.

ÉTAPE 5 Le champ **Save Icon Blinking** indique si une icône clignote lorsque certaines données ne sont pas enregistrées. Pour activer/désactiver cette fonctionnalité, cliquez sur **Désactiver/Activer clignotement icône d'enr.**

ÉTAPE 6 Cliquez sur **Apply**. Le fichier est copié.

Configuration/Mise à jour automatique de l'image via DHCP

La fonctionnalité de configuration/mise à jour automatique de l'image constitue un moyen pratique de configurer automatiquement des commutateurs Cisco Small Business 200, 300 et 500 dans un réseau et de mettre à jour leur micrologiciel. Ce processus permet à l'administrateur de vérifier à distance que la configuration et le micrologiciel de ces périphériques du réseau sont à jour.

Cette fonctionnalité comporte les étapes suivantes :

- **Mise à jour automatique de l'image** : téléchargement automatique d'une image du micrologiciel depuis un serveur TFTP/SCP distant. À l'issue du processus de configuration/mise à jour automatique de l'image, le périphérique redémarre avec la nouvelle image du micrologiciel.
- **Configuration automatique** : téléchargement automatique d'un fichier de configuration depuis un serveur TFTP/SCP distant. À l'issue du processus de configuration/mise à jour automatique de l'image, le périphérique redémarre avec le nouveau fichier de configuration.

REMARQUE Si à la fois la mise à jour automatique de l'image et la configuration automatique sont demandées, la mise à jour automatique de l'image est effectuée en premier. Après le redémarrage du périphérique, la configuration automatique a lieu à son tour, laquelle est également suivie d'un redémarrage final.

Pour utiliser cette fonctionnalité, configurez un serveur DHCP dans le réseau en fonction de l'emplacement et du nom du fichier de configuration et de l'image du micrologiciel de vos périphériques. Les périphériques du réseau sont configurés en tant que clients DHCP par défaut. Lorsqu'une adresse IP a été attribuée par le serveur DHCP aux périphériques, ces derniers reçoivent également des informations sur le fichier de configuration et l'image du micrologiciel. Si le fichier de configuration et/ou l'image du micrologiciel diffèrent de ceux utilisés actuellement sur le périphérique, ce dernier redémarre après avoir téléchargé le fichier et/ou l'image. La présente section décrit ces processus.

Outre la possibilité de garder les périphériques du réseau à jour avec les derniers fichiers de configuration et image du micrologiciel disponibles, la fonctionnalité de configuration/mise à jour automatique permet une installation rapide des nouveaux périphériques sur le réseau. En effet, tout nouveau périphérique prêt à l'emploi est configuré de manière à extraire son fichier de configuration et l'image du logiciel depuis le réseau, sans intervention manuelle de l'administrateur système. Lorsqu'il demande une adresse IP auprès du serveur DHCP pour la première fois, le périphérique télécharge le fichier de configuration et/ou l'image du micrologiciel spécifiés par le serveur DHCP et redémarre automatiquement.

Le processus de configuration automatique prend en charge le téléchargement de fichiers de configuration contenant des informations sensibles telles que des clés de serveur RADIUS et clés SSH/SSL, via l'utilisation du protocole de sécurité SCP (Secured Copy Protocol) et de la fonctionnalité de sécurisation SSD (Secure Sensitive Data). Pour en savoir plus à ce sujet, reportez-vous aux sections **Authentification du client SSH** et **Sécurité : Gestion sécurisée des données confidentielles**.

Protocoles de téléchargement (TFTP ou SCP)

Les fichiers de configuration et les images du micrologiciel peuvent être téléchargés depuis un serveur TFTP ou SCP.

L'utilisateur configure le protocole à utiliser, comme suit :

- **Automatique par extension de fichier** (option par défaut) : lorsque vous sélectionnez cette option, l'extension de fichier définie par l'utilisateur indique que les fichiers présentant cette extension doivent être téléchargés à l'aide du protocole SCP (sur SSH) tandis que les fichiers pourvus d'une extension autre doivent être téléchargés à l'aide du protocole TFTP. Par exemple, si vous avez défini l'extension *.xyz*, les fichiers portant cette extension sont téléchargés via SCP, tandis que les fichiers aux extensions différentes sont téléchargés via TFTP. L'extension par défaut est .scp.
- **TFTP uniquement** : le téléchargement est effectué via TFTP quelle que soit l'extension de fichier du nom du fichier de configuration.
- **SCP uniquement** : le téléchargement est effectué via SCP (sur SSH) quelle que soit l'extension de fichier du nom du fichier de configuration.

Authentification du client SSH

SCP est basé sur le protocole SSH. Par défaut, l'authentification du serveur SSH distant est désactivée ; l'appareil accepte donc n'importe quel serveur SSH distant prêt à l'emploi. Vous pouvez activer l'authentification du serveur SSH distant pour que seuls les serveurs répertoriés dans la liste des serveurs sécurisés puissent être utilisés.

Les paramètres d'authentification du client SSH sont obligatoires pour que le client (autrement dit l'appareil) puisse accéder au serveur SSH. Voici les paramètres par défaut d'authentification du client SSH :

- Méthode d'authentification SSH : par nom d'utilisateur/mot de passe
- Nom d'utilisateur SSH : anonyme
- Mot de passe SSH : anonyme

REMARQUE Notez que les paramètres d'authentification du client SSH peuvent également être utilisés lors du téléchargement manuel d'un fichier (c.-à-d., téléchargement effectué sans exploiter la fonctionnalité de configuration/mise à jour automatique de l'image DHCP).

Processus de configuration/Mise à jour automatique de l'image

La configuration automatique DHCP utilise le nom/l'adresse du serveur de configuration et le nom/chemin du fichier de configuration, le cas échéant, dans les messages DHCP reçus. Par ailleurs, la fonctionnalité de mise à jour de l'image DHCP utilise le nom de fichier indirect du micrologiciel, le cas échéant, dans les messages. Ces informations sont spécifiées sous forme d'options DHCP dans le message d'**offre** provenant des serveurs DHCPv4 et dans les messages de **réponse informative** provenant des serveurs DHCPv6.

Si ces informations sont introuvables dans les messages des serveurs DHCP, ce sont les informations de secours qui ont été configurées sur la page DHCP de configuration/mise à jour automatique de l'image qui sont utilisées.

Lorsque le processus de configuration/mise à jour automatique de l'image est déclenché (reportez-vous à la section **Déclenchement de la configuration/mise à jour automatique de l'image**), la séquence d'événements décrite ci-dessous se produit.

Démarrage de la mise à jour automatique de l'image :

- Le commutateur utilise le nom de fichier indirect de l'option 125 (DHCPv4) et de l'option 60 (DHCPv6), le cas échéant, dans le message DHCP reçu.
- Si le serveur DHCP n'a pas envoyé le nom du fichier indirect du fichier image du micrologiciel, c'est le nom du fichier image indirect de sauvegarde (indiqué sur la page de configuration/mise à jour automatique de l'image DHCP) qui est utilisé.
- Le commutateur télécharge le fichier image indirect, puis en extrait le nom du fichier image du serveur TFTP/SCP.

- Le commutateur compare la version du fichier image du serveur TFTP à la version de l'image active du commutateur.
- Si les deux versions sont différentes, la nouvelle version est chargée dans l'image non active, un redémarrage a lieu et l'image non active devient l'image active.
- Lors de l'utilisation du protocole SCP, un message SYSLOG est généré pour indiquer qu'un redémarrage va avoir lieu.
- Lors de l'utilisation du protocole SCP, un message SYSLOG est généré pour confirmer que le processus de mise à jour automatique a eu lieu.
- Lors de l'utilisation du protocole TFTP, des messages SYSLOG sont générés par le processus de copie.

Démarrage de la configuration automatique :

- Le périphérique utilise le nom/l'adresse du serveur TFTP/SCP ainsi que le nom/chemin du fichier de configuration (options DHCPv4 : 66, 150 et 67, options DHCPv6 : 59 et 60), le cas échéant, dans le message DHCP reçu.
- Si ces informations ne sont pas envoyées par le serveur DHCP, c'est le nom/l'adresse IP du serveur de secours et le nom du fichier de configuration de secours (de la page de configuration/mise à jour automatique de l'image DHCP) qui sont utilisés.
- Le nouveau fichier de configuration est utilisé si son nom est différent de celui du fichier de configuration précédemment utilisé sur le périphérique ou si ce dernier n'a jamais été configuré.
- Le périphérique redémarre avec le nouveau fichier de configuration à l'issue du processus de configuration/mise à jour automatique de l'image.
- Des messages SYSLOG sont générés par le processus de copie.

Options manquantes

- Si le serveur DHCP n'a pas envoyé l'adresse du serveur TFTP/SCP dans une option DHCP et que le paramètre d'adresse du serveur TFTP/SCP de secours n'a pas été configuré, voici ce qui se passe :
  - **SCP** : le processus de configuration automatique est interrompu.
  - **TFTP** : l'appareil envoie des messages de requête TFTP à une adresse de diffusion limitée (pour IPv4) ou à l'adresse de TOUS LES NŒUDS (pour IPv6) présents sur ses interfaces IP et se sert ensuite du premier serveur dont il parvient à obtenir une réponse pour poursuivre le processus de configuration/mise à jour automatique de l'image.

Sélection du protocole de téléchargement

- Le protocole de copie (SCP/TFTP) est sélectionné, comme décrit à la section **Protocoles de téléchargement (TFTP ou SCP)**.

SCP

- Dans le cas d'un téléchargement via SCP, l'appareil accepte n'importe quel serveur SCP/SSH spécifié (sans authentification), si l'un des cas suivants se présente :
  - L'authentification du serveur SSH est désactivée. Par défaut, l'authentification du serveur SSH est désactivée pour permettre le téléchargement d'un fichier de configuration pour les périphériques disposant d'une configuration d'origine (par exemple, des appareils prêts à l'emploi).
  - Le serveur SSH est configuré dans la liste des serveurs SSH sécurisés.

  Si le processus d'authentification du serveur SSH est activé et si le serveur SSH ne figure pas dans la liste des serveurs SSH sécurisés, le processus de configuration automatique est interrompu.
- Si cette information est en revanche disponible, le téléchargement du fichier de configuration ou de l'image s'effectue à partir du serveur SCP.

Déclenchement de la configuration/mise à jour automatique de l'image

La configuration/mise à jour automatique de l'image via DHCPv4 se déclenche lorsque les conditions suivantes sont remplies :

- L'adresse IP du périphérique est affectée/renouvelée de manière dynamique au redémarrage, renouvelée de manière explicite par une opération administrative ou renouvelée automatiquement en raison de l'expiration d'un bail. Le renouvellement explicité peut être activé dans la page de l'interface IPv4.
- Si la mise à jour automatique de l'image est activée, le processus correspondant est déclenché lorsqu'un nom de fichier image indirect est reçu d'un serveur DHCP ou qu'un nom de fichier image indirect de sauvegarde a été configuré. Le terme "indirect" signifie qu'il ne s'agit pas de l'image proprement dite, mais d'un fichier qui contient le nom du chemin d'accès à l'image.
- Si la configuration automatique est activée, le processus correspondant est déclenché lorsque le nom du fichier de configuration est reçu d'un serveur DHCP ou qu'un nom de fichier de fichier de configuration de secours a été configuré.

La configuration/mise à jour automatique de l'image via DHCPv6 se déclenche lorsque les conditions suivantes sont remplies :

- Lorsqu'un serveur DHCPv6 envoie des informations à l'appareil. Cet envoi se produit dans les cas suivants :
  - Lorsqu'une interface compatible IPv6 est définie comme client de configuration DHCPv6 sans état.
  - Lorsque des messages DHCPv6 sont reçus du serveur (p. ex., lorsque vous appuyez sur le bouton de **redémarrage** d'une page d'interfaces IPv6.
  - Lorsque des informations DHCPv6 sont actualisées par l'appareil.
  - Lorsque le client DHCPv6 sans état est activé après redémarrage de l'appareil.
- Lorsque les paquets du serveur DHCPv6 contiennent l'option de nom de fichier de configuration.

- Le processus de mise à jour automatique de l'image est déclenché lorsqu'un nom de fichier image indirect est fourni par le serveur DHCP ou qu'un nom de fichier image indirect de sauvegarde a été configuré. Le terme "indirect" signifie qu'il ne s'agit pas de l'image proprement dite, mais d'un fichier qui contient le nom du chemin d'accès à l'image.

Contrôle des performances

Pour vous assurer que la fonctionnalité de configuration/mise à jour automatique de l'image fonctionne correctement, notez les points suivants :

- Un fichier de configuration placé sur le serveur TFTP/SCP doit correspondre aux exigences en termes de forme et de format du fichier de configuration pris en charge. La forme et le format du fichier sont vérifiés mais la validité des *paramètres* de configuration n'est pas contrôlée avant son chargement dans la Configuration de démarrage.
- Dans IPv4, pour s'assurer qu'un périphérique télécharge les fichiers images et de configuration comme prévu lors du processus de configuration/mise à jour automatique de l'image, il est recommandé de toujours attribuer la même adresse IP au périphérique. Ainsi, le périphérique dispose toujours de la même adresse IP et obtient les mêmes informations que celles utilisées dans le processus de configuration/mise à jour automatique de l'image.

Configuration/mise à jour automatique de l'image DHCP

Les pages d'interface utilisateur graphique suivantes permettent de configurer le périphérique :

- Administration > Gestion de fichiers > DHCP Auto Configuration/Image Update (Configuration automatique DHCP/Mise à jour automatique de l'image DHCP) : pour configurer le périphérique en tant que client DHCP.
- Administration > Interface de gestion > Interface IPv4 (dans L2) ou Configuration IP > Interfaces et gestion IPv4 > Interfaces IPv4 (dans L3) : pour renouveler l'adresse IP via DHCP lors le périphérique fonctionne en mode système Couche 2.

Configuration et paramètres par défaut

Les valeurs par défaut suivantes existent sur le système :

- La configuration automatique est activée.
- La mise à jour automatique de l'image est activée.
- Le périphérique est activé en tant que client DHCP.
- L'authentification du serveur SSH distant est désactivée.

Avant de lancer le processus de configuration/mise à jour automatique de l'image

Pour utiliser cette fonctionnalité, le périphérique doit être configuré comme client DHCPv4 ou DHCPv6. Le type de client DHCP défini sur le périphérique doit être en adéquation avec le type d'interfaces défini sur le périphérique.

Préparatifs en vue de la configuration automatique sur le serveur

Pour préparer les serveurs DHCP et TFTP/SCP, procédez comme suit :

Serveur TFTP/SCP

- Placez un fichier de configuration dans le répertoire de travail. Ce fichier peut être créé en copiant un fichier de configuration depuis un périphérique. Au démarrage du périphérique, ce fichier devient le fichier Configuration d'exécution.

Serveur DHCP

Configurez le serveur DHCP avec les options suivantes :

- DHCPv4 :
  - 66 (adresse de serveur unique) ou 150 (liste d'adresses de serveur)
  - 67 (nom du fichier de configuration)
- DHCPv6
  - Option 59 (adresse du serveur)
  - Options 60 (nom du fichier de configuration, ainsi que le nom du fichier image indirect, séparés par une virgule)

Préparatifs en vue de la mise à jour automatique de l'image

Pour préparer les serveurs DHCP et TFTP/SCP, procédez comme suit :

Serveur TFTP/SCP

1. Créez un sous-répertoire dans le répertoire principal. Placez un fichier image du logiciel dans ce sous-répertoire.
2. Créez un fichier indirect contenant un chemin d'accès, ainsi que le nom de la version du micrologiciel (indirect-cisco.txt, par exemple, qui contient cisco\cisco-version.ros).
3. Copiez ce fichier indirect dans le répertoire principal du serveur TFTP/SCP

Serveur DHCP

Configurez le serveur DHCP avec les options suivantes

- DHCPv4 : option 125 (nom de fichier indirect)
- DHCPv6 : options 60 (nom du fichier de configuration, ainsi que le nom du fichier image indirect, séparés par une virgule)

Workflow du client DHCP

ÉTAPE 1 Configurez les paramètres de configuration automatique et/ou de mise à jour automatique de l'image sur la page Administration > Gestion de fichiers > DHCP Auto Configuration/Image Update (Configuration automatique DHCP/Mise à jour automatique de l'image DHCP).

ÉTAPE 2 Définissez le type d'adresse IP sur Dynamique sur la page Administration > Interface de gestion > Interface IPv4.

Configuration Web

Pour configurer la fonctionnalité de configuration automatique et/ou de mise à jour automatique :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion de fichiers** > **DHCP Auto Configuration/ Image Update (Configuration automatique DHCP/Mise à jour automatique de l'image DHCP)**.

ÉTAPE 2 Saisissez les valeurs appropriées.

- **Configuration automatique via DHCP** : sélectionnez cette option pour activer la configuration automatique DHCP. Cette fonctionnalité est activée par défaut, mais peut être désactivée ici.
- **Protocole de téléchargement** : sélectionnez une des options suivantes :
  - *Automatique par extension de fichier* : sélectionnez cette option pour indiquer que la configuration automatique utilise le protocole TFTP ou SCP en fonction de l'extension du fichier de configuration. Si cette option est sélectionnée, l'extension du fichier de configuration n'a pas besoin d'être spécifiée. Si vous ne spécifiez rien, l'extension par défaut est utilisée (comme indiqué ci-dessous).
  - *Extension de fichier pour SCP* : si l'option **Automatique par extension de fichier** est sélectionnée, vous pouvez indiquer une extension de fichier ici. Tout fichier portant cette extension est téléchargé via SCP. Si aucune extension n'est saisie, l'extension par défaut **.scp** est utilisée.
  - *TFTP uniquement* : choisissez cette option pour indiquer que seul le protocole TFTP doit être utilisé pour la configuration automatique.
  - *SCP uniquement* : choisissez cette option pour indiquer que seul le protocole SCP doit être utilisé pour la configuration automatique.

- **Image Auto Update Via DHCP (Mise à jour automatique de l'image via DHCP)** : sélectionnez ce champ pour activer la mise à jour de l'image du micrologiciel depuis le serveur DHCP. Cette fonctionnalité est activée par défaut, mais peut être désactivée ici.
- **Protocole de téléchargement** : sélectionnez une des options suivantes :
  - *Automatique par extension de fichier* : sélectionnez cette option pour indiquer que la mise à jour automatique utilise le protocole TFTP ou SCP en fonction de l'extension du fichier image. Si cette option est sélectionnée, l'extension du fichier du fichier image n'a pas besoin d'être spécifiée. Si vous ne spécifiez rien, l'extension par défaut est utilisée (comme indiqué ci-dessous).
  - *Extension de fichier pour SCP* : si l'option **Automatique par extension de fichier** est sélectionnée, vous pouvez indiquer une extension de fichier ici. Tout fichier portant cette extension est téléchargé via SCP. Si aucune extension n'est saisie, l'extension par défaut **.scp** est utilisée.
  - *TFTP uniquement* : choisissez cette option pour indiquer que seul le protocole TFTP doit être utilisé pour la mise à jour automatique.
  - *SCP uniquement* : choisissez cette option pour indiquer que seul le protocole SCP doit être utilisé pour la mise à jour automatique.
- **Paramètres SSH pour SCP** : lorsque vous utilisez le protocole SCP pour télécharger les fichiers de configuration, sélectionnez l'une des options suivantes :
- **Authentification du serveur SSH distant** : cliquez sur le lien **Activer/désactiver** pour accéder à la page Authentification du serveur SSH. Vous pouvez y activer l'authentification du serveur SSH à utiliser pour le téléchargement et saisir le serveur SSH sécurisé si nécessaire.
- **Authentification du client SSH** : cliquez sur le lien Informations d'identification système pour saisir les informations d'identification utilisateur sur la page Authentification des utilisateurs SSH.
- **Définition du serveur de secours** : indiquez si le serveur de secours sera configuré **Par adresse IP** ou **Par nom**.
- **Version IP** : indiquez si l'adresse utilisée est de type IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - **Liaison locale** : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe FE80, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - **Global** : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée)

ÉTAPE 3 Entrez les informations facultatives suivantes qui seront utilisées si le serveur DHCP ne fournit pas les informations requises.

- **Nom/Adresse IP du serveur de secours** : saisissez l'adresse IP ou le nom du serveur de secours.
- **Nom du fichier de configuration de secours** : entrez le nom du fichier de configuration de secours.
- **Backup Indirect Image File Name (Nom du fichier image indirect de sauvegarde)** : entrez le nom du fichier image indirect à utiliser. Il s'agit d'un fichier qui contient le chemin d'accès à l'image. Exemple de nom de fichier image indirect : indirect-cisco.scp. Ce fichier contient le chemin d'accès et le nom de l'image du micrologiciel.

Les champs suivants s'affichent :

- **Last Auto Configuration/Image Server IP Address (Adresse IP du dernier serveur pour configuration automatique/mise à jour automatique de l'image)** : adresse du dernier serveur de secours.
- **Dernier nom du fichier de configuration automatique** : dernier nom du fichier de configuration.

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres sont copiés dans le fichier de Configuration d'exécution.

6

Administration

Cette section décrit comment afficher les informations relatives au système et configurer différentes options sur le périphérique.

Elle couvre les rubriques suivantes :

- **Modèles de périphériques**
- **Paramètres système**
- **Interface de gestion**
- **Comptes d'utilisateur**
- **Définition du délai d'expiration en cas de session inactive**
- **Paramètres de l'heure**
- **Journal système**
- **Gestion de fichiers**
- **Redémarrage du périphérique**
- **Intégrité**
- **Diagnostic**
- **Détection - Bonjour**
- **Détection - LLDP**
- **Détection - CDP**
- **Ping**

Modèles de périphériques

Tous les modèles peuvent être entièrement gérés via l'utilitaire Web de configuration du commutateur.

REMARQUE Reportez-vous à la section **Conventions de nommage de l'interface** pour connaître les conventions d'affectation de noms aux ports.

Le tableau suivant décrit les différents modèles, le nombre et le type de ports qu'ils contiennent, ainsi que leurs informations PoE.

Nom du modèle	ID du produit (PID)	Description des ports de l'appareil	Puissance dédiée au PoE	Nbre de ports gérant PoE
SG200-18	SLM2016T	16 ports GE + 2 ports GE combinés spécifiques	N/A	N/A
SG200-26	SLM2024T	24 ports GE + 2 ports GE combinés spécifiques	N/A	N/A
SG200-26P	SLM2024PT	24 ports GE + 2 ports GE combinés spécifiques	100 W	12 ports FE1-FE6, FE13 - FE18
SG200-50	SLM2048T	48 ports GE + 2 ports GE combinés spécifiques	N/A	N/A
SG200-50P	SLM2048PT	48 ports GE + 2 ports GE combinés spécifiques	180 W	24 ports FE1-FE12, FE25 - FE36
SF200-24	SLM224GT	24 ports FE + 2 ports GE combinés spécifiques	N/A	N/A
SF200-24P	SLM224PT	24 ports FE + 2 ports GE combinés spécifiques	100 W	12 ports FE1-FE6, FE13 - FE18
SF200-48	SLM248GT	48 ports FE + 2 ports GE combinés spécifiques	N/A	N/A
SF200-48P	SLM248PT V.0	48 ports FE + 2 ports GE combinés spécifiques	180 W	24 ports PoE

Nom du modèle	ID du produit (PID)	Description des ports de l'appareil	Puissance dédiée au PoE	Nbre de ports gérant PoE
SG200-10FP	SG200-10FP V.0	Commutateur intelligent PoE Gigabit à 10 ports	62 W	8
SF200-24FP	SF200-24FP V.0	Commutateur intelligent PoE 24 ports 10/100	180 W	24
SG200-26FP	SG200-26FP V.0	Commutateur intelligent PoE Gigabit à 26 ports	180 W	24
SG200-50FP	SG200-50FP V.0	Commutateur intelligent PoE Gigabit à 50 ports	375 W	48

Paramètres système

La page Récapitulatif du système fournit une vue graphique du périphérique et affiche l'état du périphérique, des informations sur le matériel, des informations sur le micrologiciel, l'état PoE (Power-over-Ethernet) général, etc.

Affichage du récapitulatif du système

Pour afficher les informations système :

ÉTAPE 1 Cliquez sur **État et statistiques** > **Récapitulatif du système**.

Informations système :

- **Description du système** : affiche une description du système.
- **Emplacement du système** : indique l'emplacement physique du périphérique. Cliquez sur **Modifier** pour accéder à la page Paramètres système, afin d'entrer cette information.
- **System Contact** : nom de la personne à contacter. Cliquez sur **Modifier** pour accéder à la page Paramètres système, afin d'entrer cette information.
- **Nom d'hôte** : nom du périphérique. Cliquez sur **Modifier** pour accéder à la page Paramètres système, afin d'entrer cette information. Par défaut, le nom d'hôte du périphérique se compose du mot *périphérique* concaténé avec les trois octets les moins significatifs de l'adresse MAC du périphérique (les six chiffres hexadécimaux les plus à droite).

- **ID de l'objet système** : identification unique du fournisseur du sous-système de gestion du réseau contenu dans l'entité (utilisée dans SNMP).
- **System Uptime** : temps qui s'est écoulé depuis le dernier redémarrage.
- **Current Time** : heure actuelle du système.
- **Adresse MAC de base** : indique l'adresse MAC du périphérique.
- **Jumbo Frames** : état de prise en charge des cadres géants. Cette prise en charge peut être activée ou désactivée sur la page Paramètres des ports du menu Gestion des ports.

  REMARQUE La prise en charge des trames Jumbo est effective une fois qu'elle a été activée et que le périphérique a été redémarré.

Informations sur le logiciel :

- **Version du micrologiciel** : affiche le numéro de version du micrologiciel de l'image active.
- **Total de contrôle MD5 du micrologiciel** : affiche le total de contrôle MD5 de l'image active.
- **Version de démarrage** : numéro de version de démarrage.
- **Total de contrôle MD5 de démarrage** : total de contrôle MD5 de la version de démarrage.
- **Locale** : paramètres régionaux de la première langue. (toujours définis sur Anglais).
- **Version de langue** : version du module linguistique de la première langue ou de la langue anglaise.
- **Total de contrôle MD5 de langue** : total de contrôle MD5 du fichier de langue.

État des services TCP/UDP :

- **Service HTTP** : indique si HTTP est activé ou désactivé.
- **Service HTTPS** : indique si HTTPS est activé ou désactivé.
- **Service SNMP** : indique si SNMP est activé ou désactivé.

Informations d'alimentation PoE : (sur les périphériques prenant en charge PoE)

- **Puissance PoE maximale disponible (W)** : puissance maximale disponible pouvant être fournie par le PoE.
- **Consommation totale de la puissance PoE (W)** : puissance PoE totale fournie aux périphériques PoE connectés.
- **Mode d'alimentation PoE** : limite du port ou de la classe.

Paramètres système

Pour accéder aux paramètres système :

ÉTAPE 1 Cliquez sur **Administration** > **System Settings**.

ÉTAPE 2 Permet d'afficher ou de modifier les paramètres système.

- **Description du système** : affiche une description du périphérique.
- **Emplacement du système** : entrez l'emplacement physique du périphérique.
- **System Contact** : saisissez le nom de la personne à contacter.
- **Nom d'hôte** : sélectionnez le nom d'hôte de ce périphérique. Voici ce qui est utilisé dans l'invite de l'interface de ligne de commande :
  - *Valeurs par défaut* : le nom d'hôte par défaut (Nom du système) de ces commutateurs est *périphérique123456*, où 123456 représente les trois derniers octets de l'adresse MAC du périphérique au format hexadécimal.
  - *Défini par l'utilisateur* : saisissez le nom d'hôte. Utilisez uniquement des lettres, des chiffres et des tirets. Les noms d'hôte ne peuvent pas être précédés ni suivis d'un tiret. Les autres symboles, les signes de ponctuation et les espaces ne sont pas autorisés (comme cela est spécifié dans les normes RFC1033, 1034 et 1035).
- **Paramètres de bannière personnalisée** : les bannières suivantes peuvent être définies :
  - **Bannière de connexion** : saisissez le texte à afficher sur la page de connexion avant la connexion. Cliquez sur **Aperçu** pour afficher les résultats.
  - **Bannière de bienvenue** : saisissez le texte à afficher sur la page de connexion après la connexion. Cliquez sur **Aperçu** pour afficher les résultats.

REMARQUE Lorsque vous définissez une bannière de connexion à partir de l'utilitaire de configuration Web, celle-ci est également activée pour les interfaces de ligne de commande (Console, Telnet et SSH).

ÉTAPE 3 Cliquez sur **Appliquer** pour enregistrer les valeurs dans le fichier de Configuration d'exécution.

Interface de gestion

Reportez-vous à la section **IPv4 Management and Interfaces (Interfaces et gestion IPv4)**.

Comptes d'utilisateur

Reportez-vous à la section **Définition d'utilisateurs**.

Définition du délai d'expiration en cas de session inactive

L'option *Expiration de la session inactive* permet de configurer l'intervalle de temps pendant lequel la session HTTP peut rester inactive avant qu'elle n'expire et que l'utilisateur doive se reconnecter pour rétablir la session.

- **Délai d'expiration de session HTTP**
- **Délai d'expiration de session HTTPS**

Pour définir le délai d'expiration d'une session HTTP ou HTTPS :

ÉTAPE 1 Cliquez sur **Administration** > **Expiration de la session inactive**.

ÉTAPE 2 Sélectionnez le délai d'expiration de chaque session dans la liste correspondante. La valeur d'expiration par défaut est de 10 minutes.

ÉTAPE 3 Cliquez sur **Appliquer** pour enregistrer les paramètres de configuration sur le périphérique.

Paramètres de l'heure

Reportez-vous à la section **Administration : Paramètres d'heure**.

Journal système

Reportez-vous à la section **Administration : Journal système**.

Gestion de fichiers

Reportez-vous à la section **Administration : Gestion de fichiers**.

Redémarrage du périphérique

Certaines modifications apportées à la configuration, telles que l'activation de la prise en charge des trames Jumbo, nécessitent le redémarrage du système pour être effectives. Le redémarrage du périphérique supprime toutefois la Configuration d'exécution. Il est donc indispensable de l'enregistrer dans la Configuration de démarrage avant de procéder à un redémarrage. Cliquer sur **Apply** n'a pas pour effet d'enregistrer la configuration dans la configuration de démarrage. Pour plus d'informations sur les fichiers et les types de fichiers, reportez-vous à la section **Fichiers système**.

Vous pouvez sauvegarder la configuration du périphérique en utilisant *Administration > Gestion de fichiers > Copier/enregistrer la configuration* ou en cliquant sur **Enreg.** en haut de la fenêtre. Vous pouvez également charger la configuration depuis un périphérique distant. Reportez-vous à la section **Télécharger/sauvegarder configuration/journal**.

Vous préférerez peut-être régler le redémarrage à une heure ultérieure. Cela peut notamment se produire dans l'un des cas suivants :

- Vous effectuez des actions sur un périphérique distant et ces actions peuvent provoquer une perte de connexion à ce périphérique distant. La pré-planification d'un redémarrage restaure la configuration fonctionnant et permet la restauration de la connexion au périphérique distant. Si ces actions sont réussies, le redémarrage retardé peut être annulé.
- Le rechargement du périphérique provoque la perte de connexion dans le réseau, en raison du redémarrage retardé, vous pouvez planifier le redémarrage à une heure plus propice pour les utilisateurs (par exemple tard dans la nuit).

Pour redémarrer le périphérique :

ÉTAPE 1 Cliquez sur **Administration** > **Reboot**.

ÉTAPE 2 Cliquez sur le bouton **Redémarrer** pour redémarrer le périphérique.

- **Redémarrer** : permet de redémarrer le périphérique. Les informations non enregistrées de la Configuration d'exécution étant ignorées lors du redémarrage du périphérique, vous devez cliquer sur **Enregistrer** en haut à droite de n'importe quelle fenêtre afin de conserver la configuration actuelle lors du processus de démarrage. Si l'option Enregistrer ne s'affiche pas, cela signifie que la Configuration d'exécution est identique à la Configuration de démarrage et qu'aucune action n'est nécessaire.
- **Annuler le redémarrage** : annule un redémarrage qui a été programmé pour plus tard.

Les options suivantes sont disponibles :

- *Immédiat* : permet de redémarrer immédiatement.
- *Date* : saisissez la date (mois/jour) et l'heure (heure et minutes) du redémarrage planifié. Vous planifiez ainsi un rechargement du logiciel à l'heure spécifiée (utilisation du mode 24 heures). Si vous spécifiez le mois et le jour, le rechargement est planifié et sera effectué à l'heure et à la date spécifiées. Si vous ne spécifiez pas le mois et le jour, le rechargement aura lieu à l'heure spécifiée du jour actuel (si l'heure spécifiée est ultérieure à l'heure actuelle) ou le jour suivant (si l'heure spécifiée est antérieure à l'heure actuelle). La spécification 00:00 planifie le rechargement à minuit. Le rechargement doit avoir lieu dans les 24 jours.

  REMARQUE Vous pouvez uniquement utiliser cette option si l'heure du système a été réglée manuellement ou via SNTP.
- *In* : redémarre dans le nombre d'heures et de minutes spécifié. La durée maximale pouvant s'écouler est de 24 jours.

- **Redémarrer avec les paramètres d'origine** : redémarre le périphérique en utilisant sa configuration d'origine. Ce processus efface le fichier de Configuration de démarrage et le fichier de configuration de sauvegarde. Le fichier de configuration miroir n'est pas supprimé lorsque vous restaurez les paramètres d'origine.
- **Effacer le fichier de configuration de démarrage** : choisissez cette option pour effacer la configuration du périphérique la prochaine fois qu'il démarrera.

  REMARQUE Effacer le fichier de Configuration de démarrage et redémarrer est une procédure différente d'un redémarrage avec les paramètres d'origine. Ce dernier est beaucoup plus intrusif.

Intégrité

La page Intégrité affiche l'état du ventilateur sur tous les périphériques équipés de ventilateurs. Selon le modèle, un périphérique possède un ou plusieurs ventilateurs. Certains modèles ne possèdent aucun ventilateur.

Certains périphériques comportent un capteur de température permettant de protéger le matériel d'une surchauffe éventuelle. Dans ce cas, les actions suivantes sont effectuées par le périphérique en cas de surchauffe et pendant la période de refroidissement après une surchauffe :

Événement	Action
Au moins un capteur de température dépasse le seuil d'avertissement	Les actions suivantes sont générées : ▪ Message SYSLOG ▪ Message « trap » SNMP
Au moins un capteur de température dépasse le seuil critique	Les actions suivantes sont générées : ▪ Message SYSLOG ▪ Message « trap » SNMP Les actions suivantes sont générées : ▪ La LED système s'allume en orange fixe (si le matériel la prend en charge). ▪ Les ports sont désactivés : lorsque la température critique dépasse deux minutes, tous les ports sont arrêtés. ▪ (Sur les périphériques qui prennent PoE en charge), les circuits PoE sont désactivés pour abaisser la consommation d'énergie et diminuer la chaleur émise.
La période de refroidissement qui suit le seuil critique a été dépassée (tous les capteurs indiquent une valeur inférieure de 2 °C au seuil d'avertissement)	Lorsque tous les capteurs ont atteint une valeur inférieure de 2 °C au seuil d'avertissement, le PHY est réactivé et tous les ports sont rétablis. Si l'état du VENTILATEUR est OK, les ports sont activés. (Sur les périphériques qui prennent PoE en charge) les circuits PoE sont activés.

Pour afficher les paramètres d'intégrité du périphérique, cliquez sur **État et statistiques** > **Santé**.

La page Intégrité affiche les champs suivants :

- **État du ventilateur** : état du ventilateur. Les valeurs suivantes sont possibles :
  - *OK* : le ventilateur fonctionne normalement.
  - *Échec* : le ventilateur ne fonctionne pas correctement.
  - *S/O* : l'ID du ventilateur n'est pas applicable au modèle en question.
- **Direction du ventilateur** : (sur les périphériques concernés) la direction du fonctionnement des ventilateurs est (par exemple : de l'avant vers l'arrière).
- **Température** : les options sont les suivantes :
  - *OK* : la température est inférieure au seuil d'avertissement.
  - *Avertissement* : la température est comprise entre le seuil d'avertissement et le seuil critique.
  - *Critique* : la température est supérieure au seuil critique

Diagnostic

Reportez-vous à la section **Administration : Diagnostics**.

Détection - Bonjour

Reportez-vous à la section **Bonjour**.

Détection - LLDP

Reportez-vous à la section **Configuration de LLDP**.

Détection - CDP

Reportez-vous à la section **Configuration de CDP**.

Ping

L'utilitaire Ping sert à déterminer si un hôte distant peut être joint et mesure la durée aller-retour de transfert des paquets entre le périphérique et un périphérique de destination.

Ping envoie des paquets de demande d'écho ICMP (protocole de message de contrôle Internet) à destination de l'hôte cible et attend une réponse ICMP, parfois appelée « pong ». Il mesure le temps de parcours de la transmission et enregistre toute perte de paquets.

Pour envoyer une requête Ping à un hôte :

ÉTAPE 1 Cliquez sur **Administration > Ping**.

ÉTAPE 2 Configurez les opérations Ping en renseignant les champs suivants :

- **Définition de l'hôte** : indiquez si vous souhaitez spécifier l'interface source par son adresse IP ou son nom. Ce champ a une influence sur les interfaces affichées dans le champ IP source, comme décrit ci-après.
- **Version IP** : si l'interface source est identifiée par son adresse IP, sélectionnez IPv4 ou IPv6 pour indiquer qu'elle sera entrée au format sélectionné.
- **IP source** : sélectionnez l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source pour la communication avec la cible. Si le champ Définition de l'hôte a été défini sur Par nom, toutes les adresses IPv4 et IPv6 seront affichées dans ce champ déroulant. Si le champ Définition de l'hôte a été défini sur Par adresse IP, seules les adresses IP existantes du type spécifié dans le champ Version IP seront affichées.

  REMARQUE Si l'option Auto est sélectionnée, le système génère l'adresse source en fonction de l'adresse de destination.
- **Type d'adresse IPv6 de destination** : sélectionnez Liaison locale ou Global comme type d'adresse IPv6 à saisir en tant qu'adresse IP de destination.
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, sélectionnez son lieu de réception.
- **Nom/adresse IP de destination** : adresse ou nom d'hôte du périphérique auquel la requête Ping est envoyée. C'est la définition de l'hôte qui détermine s'il s'agit d'une adresse IP ou d'un nom d'hôte.

- **Intervalle de Ping** : durée d'attente du système entre les paquets Ping. La requête Ping est réitérée autant de fois que configurée dans le champ **Nombre de Pings**, que la requête aboutisse ou non. Sélectionnez l'intervalle par défaut ou spécifiez votre propre valeur.
- **Nombre de Pings** : nombre de fois que l'opération Ping sera effectuée. Sélectionnez la valeur par défaut ou spécifiez votre propre valeur.
- **État** : indique si la requête Ping a réussi ou échoué.

ÉTAPE 3 Cliquez sur **Activer Ping** pour envoyer une requête Ping à l'hôte. L'état de la requête Ping apparaît et un message est ajouté à la liste des messages, indiquant le résultat de l'opération Ping.

ÉTAPE 4 Vous pouvez consulter le résultat de l'opération Ping au sein de la section **Compteurs et état du Ping** de cette page.

7

Administration : Paramètres d'heure

Les horloges système synchronisées constituent un cadre de référence pour tous les périphériques du réseau. La synchronisation de l'heure du réseau est cruciale, car chaque aspect de la gestion, de la sécurité, de la planification et du débogage d'un réseau implique de déterminer le moment où se produit l'événement. Sans synchronisation des horloges, la corrélation précise des fichiers journaux entre périphériques est impossible pour la détection des failles de sécurité ou le suivi de l'utilisation du réseau.

La synchronisation de l'heure réduit également la confusion dans les systèmes de fichiers partagés, car il est essentiel que les heures de modification soient cohérentes, quelle que soit la machine sur laquelle se trouvent les systèmes de fichiers.

C'est pour ces raisons que l'heure configurée sur tous les périphériques du réseau doit être précise.

REMARQUE Le périphérique prend en charge le protocole SNTP (Simple Network Time Protocol). Lorsque ce dernier est activé, le périphérique synchronise son heure de manière dynamique à partir d'un serveur SNTP. Le périphérique fonctionne uniquement en tant que client SNTP et ne peut pas fournir de services d'heure à d'autres périphériques.

Cette section décrit les options permettant de configurer l'heure système, le fuseau horaire et l'heure d'été (DST). Elle couvre les rubriques suivantes :

- **Options d'heure système**
- **Modes SNTP**
- **Configuration de l'heure système**

Options d'heure système

L'heure système peut être réglée manuellement par l'utilisateur, définie dynamiquement à partir d'un serveur SNTP ou synchronisée à partir de l'ordinateur qui exécute l'interface utilisateur graphique (GUI). Si un serveur SNTP est choisi, les paramètres d'heure manuels sont écrasés lorsque des communications avec le serveur sont établies.

Dans le cadre du processus de démarrage, le périphérique configure toujours l'heure, le fuseau horaire et l'heure d'été. Ces paramètres sont obtenus à partir de l'ordinateur qui exécute la GUI, du SNTP, des valeurs définies manuellement ou, si ces éléments échouent, des valeurs d'usine.

Time (Heure)

Les méthodes suivantes permettent de définir l'heure système sur le périphérique :

- **Manuel** : l'utilisateur doit définir l'heure manuellement.
- **À partir de votre ordinateur** : l'heure peut être reçue à partir de l'ordinateur, à l'aide des informations du navigateur.

  La configuration de l'heure à partir de l'ordinateur est enregistrée dans le fichier de Configuration d'exécution. Vous devez copier la Configuration d'exécution vers la Configuration de démarrage pour permettre au périphérique d'utiliser l'heure de l'ordinateur après le redémarrage. L'heure après le redémarrage est définie lors de la première connexion WEB au périphérique.

  Lorsque vous configurez cette fonction pour la première fois, si l'heure n'a pas encore été réglée, le périphérique définit l'heure à partir de l'ordinateur.

  Cette méthode de réglage de l'heure fonctionne avec les connexions HTTP et HTTPS.
- **SNTP** : l'heure peut être reçue à partir de serveurs de temps SNTP. SNTP garantit une synchronisation précise de l'heure réseau du périphérique, à la milliseconde près, en utilisant un serveur SNTP comme source d'horloge. Lors de la spécification d'un serveur SNTP, si vous choisissez de l'identifier par son nom d'hôte, trois suggestions sont données dans l'interface utilisateur graphique :
  - time-a.timefreq.bldrdoc.gov
  - time-b.timefreq.bldrdoc.gov
  - time-c.timefreq.bldrdoc.gov

Une fois que l'heure a été définie par l'une des sources ci-dessus, elle n'est pas redéfinie par le navigateur.

REMARQUE SNTP est la méthode recommandée pour le réglage de l'heure.

Fuseau horaire et heure d'été

Le fuseau horaire et l'heure d'été peuvent être définis sur le périphérique comme suit :

- Configuration dynamique du périphérique via un serveur DHCP, où :
  - L'heure d'été dynamique, lorsqu'elle est activée et disponible, a toujours la priorité sur la configuration manuelle de l'heure d'été.
  - Les paramètres manuels sont utilisés si le serveur fournissant les paramètres de source échoue ou si la configuration dynamique est désactivée par l'utilisateur.
  - La configuration dynamique du fuseau horaire et de l'heure d'été se poursuit après l'expiration de l'heure de bail IP.
- La configuration manuelle du fuseau horaire et de l'heure d'été devient la configuration de fuseau horaire et d'heure d'été opérationnelle seulement si la configuration dynamique est désactivée ou échoue.

  REMARQUE Le serveur DHCP doit fournir l'option 100 DHCP pour que la configuration dynamique du fuseau horaire puisse avoir lieu.

Modes SNTP

Le périphérique peut recevoir l'heure système à partir d'un serveur SNTP de l'une des manières suivantes :

- **Réception de diffusion client (mode passif) :** les serveurs SNTP diffusent l'heure et le périphérique écoute ces diffusions. Lorsque le périphérique se trouve dans ce mode, il n'est pas nécessaire de définir un serveur SNTP monodiffusion.
- **Transmission de diffusion client (mode actif)** : le commutateur, en tant que client SNTP, demande périodiquement des mises à jour de l'heure SNTP. Ce mode fonctionne de l'une des manières suivantes :
  - **Mode client pluridiffusion SNTP** : le périphérique diffuse des paquets de requêtes d'heure à tous les serveurs SNTP du sous-réseau et attend une réponse.
  - **Mode Serveur SNTP monodiffusion** : le périphérique envoie des requêtes de monodiffusion à une liste de serveurs SNTP configurés manuellement et attend une réponse.

Le périphérique prend en charge tous les modes mentionnés ci-dessus et actifs en même temps, et sélectionne la meilleure heure système reçue d'un serveur SNTP, conformément à un algorithme basé sur la strate la plus proche (distance par rapport à l'horloge de référence).

Configuration de l'heure système

Sélection de la source d'heure système

Utilisez la page Heure système pour sélectionner la source d'heure système. Si la source est manuelle, vous pouvez saisir l'heure à cet endroit.

ATTENTION Si l'heure système est définie manuellement et que le périphérique est redémarré, saisissez à nouveau les paramètres d'heure entrés manuellement.

Pour définir l'heure système :

ÉTAPE 1 Cliquez sur **Administration** > **Time Settings** > **System Time**.

Les champs suivants s'affichent :

- **Heure actuelle (statique)** : heure système sur le périphérique. Indique le fuseau horaire du serveur DHCP ou l'acronyme correspondant au fuseau horaire défini par l'utilisateur, le cas échéant.
- **Dernier serveur synchronisé** : adresse, strate et type du serveur SNTP à partir duquel l'heure système a été extraite pour la dernière fois.

ÉTAPE 2 Saisissez les paramètres suivants :

Paramètres de source d'horloge : sélectionnez la source utilisée pour définir l'horloge système.

- **Source d'horloge principale (serveurs SNTP)** : si cette option est activée, l'heure système est obtenue à partir d'un serveur SNTP. Pour utiliser cette fonctionnalité, vous devez également configurer une connexion à un serveur SNTP sur la page Paramètres d'interface SNTP. Vous pouvez également appliquer l'authentification des sessions SNTP via la page Authentification SNTP.
- **Source d'horloge alternative (ordinateur via des sessions HTTP/HTTPS actives)** : sélectionnez cette option pour définir la date et l'heure depuis l'ordinateur effectuant la configuration via le protocole HTTP.

REMARQUE Le paramètre de source d'horloge doit être défini à l'une des valeurs ci-dessus pour que l'authentification MD5 RIP fonctionne.

Paramètres manuels : définissez la date et l'heure manuellement. L'heure locale est utilisée lorsqu'aucune source d'horloge alternative, telle qu'un serveur SNTP, n'est disponible :

- **Date** : saisissez la date du système.
- **Local Time** : saisissez l'heure système.

Paramètres de fuseau horaire : l'heure locale est utilisée via le serveur DHCP ou l'option Décalage du fuseau horaire.

- **Obtenir le fuseau horaire de DHCP** : sélectionnez cette option pour activer la configuration dynamique du fuseau horaire et l'heure d'été à partir du serveur DHCP. Un seul ou les deux paramètres peuvent être configurés selon les informations trouvées dans le paquet DHCP. Si cette option est activée, *le client DHCP doit être activé sur le périphérique*.

  REMARQUE Le client DHCP prend en charge l'option 100 permettant le réglage dynamique du fuseau horaire.

- **Fuseau horaire de DHCP** : affiche l'acronyme du fuseau horaire configuré à partir du serveur DHCP. L'acronyme s'affiche dans le champ **Heure actuelle**.

- **Décalage du fuseau horaire** : sélectionnez la différence en heures entre le *temps du méridien de Greenwich* (GMT) et l'heure locale. Par exemple, le décalage de fuseau horaire pour Paris et GMT+1 et celui pour New York est GMT- 5.

- **Acronyme du fuseau horaire** : saisissez un nom qui représente ce fuseau horaire. L'acronyme s'affiche dans le champ **Actual Time**.

Paramètres d'heure d'été : sélectionnez le mode de définition de l'heure d'été :

- **Heure d'été** : sélectionnez cette option pour activer l'heure d'été.

- **Compensation d'heure définie** : entrez le nombre de minutes de décalage par rapport à l'heure GMT (entre 1 et 1 440). La valeur par défaut est 60.

- **Type d'heure d'été** : cliquez sur l'un des éléments suivants :

  - *États-Unis* : l'heure d'été est définie selon les dates utilisées aux États-Unis.

  - *Europe* : l'heure d'été est définie selon les dates utilisées par l'Union Européenne et d'autres pays qui appliquent cette norme.

  - *Par dates* : l'heure d'été est définie manuellement, généralement pour un autre pays que les États-Unis ou un pays européen. Saisissez les paramètres décrits ci-après.

  - *Recurring* : l'heure d'été entre en vigueur à la même date chaque année.

  Sélectionnez *By Dates* pour personnaliser le début et la fin de l'heure d'été :

  - **De** : jour et heure de début de l'heure d'été.

  - **À** : jour et heure de fin de l'heure d'été.

  Sélectionnez *Récurrent* pour personnaliser différemment le début et la fin de l'heure d'été :

- **De** : date à laquelle l'heure d'été commence chaque année.

  - *Jour* : jour de la semaine au cours duquel l'heure d'été débute chaque année.

  - *Semaine* : semaine du mois au cours de laquelle l'heure d'été débute chaque année.

- *Mois* : mois de l'année au cours duquel l'heure d'été débute chaque année.
- *Heure* : heure à laquelle l'heure d'été débute chaque année.

- **À** : date à laquelle l'heure d'été prend fin chaque année. Par exemple, l'heure d'été prend localement fin le quatrième vendredi du mois d'octobre à 05 h 00. Les paramètres sont les suivants :
  - *Jour* : jour de la semaine au cours duquel l'heure d'été prend fin chaque année.
  - *Semaine* : semaine du mois au cours de laquelle l'heure d'été prend fin chaque année.
  - *Mois* : mois de l'année au cours duquel l'heure d'été prend fin chaque année.
  - *Heure* : heure à laquelle l'heure d'été prend fin chaque année.

ÉTAPE 3 Cliquez sur **Apply**. Les valeurs d'heure système sont écrites dans le fichier de Configuration d'exécution.

Ajout d'un serveur de monodiffusion SNTP

Seize serveurs de monodiffusion SNTP maximum peuvent être configurés.

REMARQUE Pour spécifier un serveur de monodiffusion SNTP par son nom, vous devez d'abord configurer le ou les serveurs DNS sur le périphérique (reportez-vous à la section **Paramètres DNS**).

Pour ajouter un serveur de monodiffusion SNTP :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres d'heure** > **Monodiffusion SNTP**.

ÉTAPE 2 Renseignez les champs suivants :

- **Client SNTP monodiffusion** : sélectionnez cette option pour permettre au périphérique d'utiliser des clients monodiffusion SNTP prédéfinis avec des serveurs SNTP monodiffusion.
- **Interface source IPv4** : sélectionnez l'interface IPv4 dont l'adresse IPv4 sera utilisée comme adresse IPv4 source dans les messages utilisés pour les communications avec le serveur SNTP.
- **Interface source IPv6** : sélectionnez l'interface IPv6 dont l'adresse IPv6 sera utilisée comme adresse IPv6 source dans les messages utilisés pour les communications avec le serveur SNTP.

  REMARQUE Si l'option Auto est sélectionnée, le système récupère l'adresse IP source de l'adresse IP définie dans l'interface sortante.

La page suivante affiche ces informations pour chaque serveur SNTP monodiffusion :

- **Serveur SNTP** : adresse IP du serveur SNTP. Le serveur ou nom d'hôte préféré est choisi selon son niveau de strate.
- **Intervalle d'interrogation** : indique si l'interrogation est activée ou désactivée.
- **ID de clé d'authentification** : l'identification de clé sert à communiquer entre le serveur SNTP et le périphérique.
- **Niveau de strate** : distance par rapport à l'horloge de référence, exprimée sous la forme d'une valeur numérique. Un serveur SNTP ne peut pas être le serveur principal (niveau de strate 1), sauf si l'intervalle d'interrogation est activé.
- **État** : état du serveur SNTP. Ce champ peut prendre les valeurs suivantes :
  - *Actif* : le serveur SNTP fonctionne actuellement normalement.
  - *Inactif* : le serveur SNTP n'est actuellement pas disponible.
  - *Inconnu* : le serveur SNTP est actuellement recherché par le périphérique.
  - *En cours* : se produit lorsque le serveur SNTP n'a pas entièrement approuvé son propre serveur de temps (c'est-à-dire lors du premier démarrage du serveur SNTP).
- **Dernière réponse** : date et heure auxquelles une réponse a été reçue de la part de ce serveur SNTP pour la dernière fois.
- **Décalage** : décalage estimé entre l'horloge du serveur et l'horloge locale, en millisecondes. L'hôte détermine la valeur de ce décalage à l'aide de l'algorithme décrit au sein de la RFC 2030.
- **Délai** : temps estimé d'un aller-retour de transmission entre l'horloge du serveur et l'horloge locale sur le chemin du réseau, en millisecondes. L'hôte détermine la valeur de cet écart à l'aide de l'algorithme décrit au sein de la RFC 2030.
- **Source** : configuration du serveur SNTP, par exemple : manuelle ou à partir du serveur DHCPv6.
- **Interface** : interface sur laquelle les paquets sont reçus.

ÉTAPE 3 Pour ajouter un serveur de monodiffusion SNTP, activez **Client SNTP monodiffusion**.

ÉTAPE 4 Cliquez sur **Add**.

ÉTAPE 5 Saisissez les paramètres suivants :

- **Définition du serveur** : sélectionnez cette option si le serveur SNTP est identifié par son adresse IP ou si vous allez sélectionner un serveur SNTP connu par son nom dans la liste.

REMARQUE Pour spécifier un serveur SNTP connu, le périphérique doit être connecté à Internet et configuré avec un serveur DNS, ou configuré de manière à ce qu'un serveur DNS soit identifié en utilisant le serveur DHCP. (Voir **Paramètres DNS**.)

- **Version IP** : sélectionnez la version de l'adresse IP : **Version 6** ou **Version 4**.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée).
- **Adresse IP du serveur SNTP** : saisissez l'adresse IP du serveur SNTP. Le format dépend du type d'adresse sélectionné.
- **Serveur SNTP** : sélectionnez le nom du serveur SNTP à partir d'une liste de serveurs NTP connus. Si vous avez choisi **autres**, saisissez le nom d'un serveur SNTP dans le champ adjacent.
- **Intervalle d'interrogation** : sélectionnez cette option afin d'activer l'interrogation du serveur SNTP pour les informations d'heure système. Tous les serveurs NTP enregistrés pour l'interrogation sont interrogés et l'horloge est sélectionnée à partir du serveur accessible qui dispose du niveau de strate le plus faible (distance par rapport à l'horloge de référence). Le serveur disposant de la strate la plus faible est considéré comme étant le serveur principal. Le serveur disposant de la strate la deuxième plus faible est un serveur secondaire et ainsi de suite. Si le serveur principal est inactif, le périphérique interroge tous les serveurs ayant leur paramètre d'interrogation activé et sélectionne celui disposant de la strate la plus faible comme le nouveau serveur principal.
- **Authentification** : cochez la case pour activer l'authentification.
- **ID de clé d'authentification** : si l'authentification est activée, sélectionnez la valeur de l'ID de clé (Vous pouvez créer des clés d'authentification sur la page Authentification SNTP.)

ÉTAPE 6 Cliquez sur **Apply**. Le serveur SNTP est ajouté et vous retournez à la page principale.

Configuration du mode SNTP

Le périphérique peut être en mode actif et/ou passif (Consultez la rubrique **Modes SNTP** pour plus d'informations.)

Pour activer la réception de paquets SNTP à partir de tous les serveurs du sous-réseau et/ou la transmission de demandes d'heure aux serveurs SNTP :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres d'heure** > **SNTP multidiffusion/ pluridiffusion**.

ÉTAPE 2 Sélectionnez l'une des options suivantes :

- **Mode client multidiffusion IPv4 SNTP (réception de diffusion client)** : sélectionnez cette option pour recevoir les transmissions de multidiffusion IPv4 de l'heure système à partir de l'un des serveurs SNTP du sous-réseau.
- **Mode client multidiffusion IPv6 SNTP (réception de diffusion client)** : sélectionnez cette option pour recevoir les transmissions de multidiffusion IPv6 de l'heure système à partir de l'un des serveurs SNTP du sous-réseau.
- **Mode client pluridiffusion IPv4 SNTP (transmission de diffusion client)** : sélectionnez cette option pour transmettre des paquets de synchronisation IPv4 SNTP demandant des informations relatives à l'heure système. Les paquets sont transmis à tous les serveurs SNTP du sous-réseau.
- **Mode client pluridiffusion IPv6 SNTP (transmission de diffusion client)** : sélectionnez cette option pour transmettre des paquets de synchronisation IPv6 SNTP demandant des informations relatives à l'heure système. Les paquets sont transmis à tous les serveurs SNTP du sous-réseau.

ÉTAPE 3 Cliquez sur **Appliquer** pour enregistrer les paramètres dans le fichier de Configuration d'exécution.

Définition de l'authentification SNTP

Les clients SNTP peuvent authentifier les réponses à l'aide de HMAC-MD5. Un serveur SNTP est associé à une clé, qui est utilisée en guise d'entrée de la fonction MD5 avec la réponse elle-même, le résultat de la fonction MD5 étant également inclus dans le paquet de réponse.

La page Authentification SNTP permet de configurer des clés d'authentification utilisées pour communiquer avec un serveur SNTP qui requiert une authentification.

La clé d'authentification est créée sur le serveur SNTP dans un processus distinct qui varie selon le type de serveur SNTP que vous utilisez. Pour plus d'informations à ce sujet, contactez l'administrateur système du serveur SNTP.

Flux de travail

ÉTAPE 1 Activez l'authentification sur la page Authentification SNTP.

ÉTAPE 2 Créez une clé sur la page Authentification SNTP.

ÉTAPE 3 Associez cette clé à un serveur SNTP sur la page SNTP monodiffusion.

Pour activer l'authentification SNTP et définir des clés :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres d'heure** > **Authentification SNTP**.

ÉTAPE 2 Sélectionnez **Authentification SNTP** pour prendre en charge l'authentification d'une session SNTP entre le périphérique et un serveur SNTP.

ÉTAPE 3 Cliquez sur **Appliquer** pour mettre le périphérique à jour.

ÉTAPE 4 Cliquez sur **Ajouter**.

ÉTAPE 5 Saisissez les paramètres suivants :

- **ID de clé d'authentification** : saisissez le numéro utilisé pour identifier cette clé d'authentification SNTP en interne.
- **Clé d'authentification** : saisissez la clé utilisée pour l'authentification (huit caractères maximum). Le serveur SNTP doit envoyer cette clé pour que le périphérique se synchronise dessus.
- **Clé de confiance** : sélectionnez cette option pour recevoir les informations de synchronisation uniquement à partir d'un serveur SNTP utilisant cette clé d'authentification.

ÉTAPE 6 Cliquez sur **Apply**. Les paramètres d'authentification SNTP sont écrits dans le fichier de Configuration d'exécution.

8

Administration : Diagnostics

Cette section comporte des informations relatives à la configuration de la mise en miroir des ports, à l'exécution de tests de câbles et à l'affichage des informations opérationnelles se rapportant à l'appareil.

Elle couvre les rubriques suivantes :

- **Tests des ports en cuivre**
- **Affichage de l'état des modules optiques**
- **Configuration de la mise en miroir des ports et de VLAN**
- **Affichage de l'utilisation du CPU et fonction Secure Core Technology (SCT)**

Tests des ports en cuivre

La page Test cuivre affiche les résultats des tests de câbles intégrés effectués sur les câbles en cuivre par le VCT (Virtual Cable Tester, testeur de câble virtuel).

VCT réalise deux types de tests :

- La technologie de réflectométrie à dimension temporelle (TDR, Time Domain Reflectometry) teste la qualité et les caractéristiques d'un câble en cuivre relié à un port. Il est possible de tester des câbles faisant jusqu'à 140 mètres de long. Ces résultats apparaissent dans le bloc Résultats de test de la page Test cuivre.
- Les tests s'appuyant sur la technologie DSP sont effectués sur des liaisons GE actives pour en mesurer la longueur de câble. Ces résultats apparaissent dans le bloc Informations avancées de la page Test cuivre.

Conditions préalables à l'exécution du test des ports cuivre

Avant d'exécuter le test, procédez comme suit :

- (Obligatoire) Désactivez le mode Courte portée (reportez-vous à la page Gestion des ports > Green Ethernet > Propriétés)
- (Facultatif) Désactivez EEE (reportez-vous à la page Gestion des ports > Green Ethernet > Propriétés)

Utilisez un câble de données CAT5 pour exécuter le test de tous les câbles (VCT).

Les résultats de test peuvent avoir une marge d'erreur de +/- 10 pour le test avancé et de +/- 2 pour le test de base.

ATTENTION Lorsqu'un port est testé, il est mis en l'état inactif (Down) et les communications sont interrompues. Une fois le test terminé, le port revient à l'état actif (Up). Il est déconseillé d'exécuter un test de port cuivre sur un port que vous utilisez pour exécuter l'utilitaire Web de configuration du commutateur, les communications avec cet appareil étant interrompues.

Pour tester les câbles en cuivre reliés aux ports :

ÉTAPE 1 Cliquez sur **Administration** > **Diagnostics** > **Copper Test**.

ÉTAPE 2 Sélectionnez le port sur lequel vous souhaitez exécuter le test.

ÉTAPE 3 Cliquez sur **Copper Test**.

ÉTAPE 4 Une fois le message affiché, cliquez sur **OK** pour confirmer que la liaison peut passer à l'état inactif ou sur **Annuler** pour arrêter le test.

Les champs suivants s'affichent dans le bloc Résultats de test :

- **Dernière mise à jour** : heure à laquelle a été effectué le dernier test sur le port.
- **Résultats de test** : résultats du test de câbles. Les valeurs possibles sont les suivantes :
  - *OK* : le câble a réussi le test.
  - *Aucun câble* : le câble n'est pas connecté au port.
  - *Câble ouvert* : le câble n'est connecté que d'un côté.
  - *Câble court-circuité* : un court-circuit s'est produit au niveau du câble.
  - *Résultat de test inconnu* : une erreur s'est produite.
- **Distance au défaut** : distance entre le port et l'emplacement du câble où le problème a été détecté.
- **État du port opérationnel** : indique si le port est actif ou inactif.

Si le port testé est un port Giga, le bloc **Informations avancées** affiche les informations suivantes (il est actualisé à chaque fois que vous accédez à la page) :

- **Longueur de câble** : propose une estimation de longueur.
- **Paire** : paire de fils de câble testée.
- **État** : état de la paire de fils. Rouge indique un défaut et Vert indique l'état OK.

- **Canal** : canal de câble indiquant si les fils sont droits ou croisés.
- **Polarité** : indique si la détection et la correction automatiques de la polarité ont été activées pour la paire de fils.
- **Déphasage entre paires** : différence de phase entre les paires de fils.

REMARQUE Les tests TDR ne peuvent pas être effectués lorsque le débit du port atteint 10 Mbit/s.

Affichage de l'état des modules optiques

La page État des modules optiques affiche les conditions de fonctionnement signalées par l'émetteur-récepteur SFP (Small Form-factor Pluggable). Certaines informations pourraient ne pas être disponibles pour les SFP qui ne prennent pas en charge la norme de surveillance diagnostique numérique SFF-8472.

SFP compatibles MSA

Les émetteurs-récepteurs SFP FE (100 Mbit/s) suivants sont pris en charge :

- MFEBX1 : émetteur-récepteur SFP 100BASE-BX-20U pour la fibre monomode, longueur d'onde de 1 310 nm, jusqu'à 20 km.
- MFEFX1 : émetteur-récepteur SFP 100BASE-FX pour la fibre multimode, longueur d'onde de 1 310 nm, jusqu'à 2 km.
- MFELX1 : émetteur-récepteur SFP 100BASE-LX pour la fibre monomode, longueur d'onde de 1 310 nm, jusqu'à 10 km.

Les émetteurs-récepteurs SFP GE (1 000 Mbit/s) suivants sont pris en charge :

- MGBBX1 : émetteur-récepteur SFP 1000BASE-BX-20U pour la fibre monomode, longueur d'onde de 1 310 nm, jusqu'à 40 km.
- MGBLH1 : émetteur-récepteur SFP 1000BASE-LH pour la fibre monomode, longueur d'onde de 1 310 nm, jusqu'à 40 km.
- MGBLX1 : émetteur-récepteur SFP 1000BASE-LX pour la fibre monomode, longueur d'onde de 1 310 nm, jusqu'à 10 km.
- MGBSX1 : émetteur-récepteur SFP 1000BASE-SX pour la fibre multimode, longueur d'onde de 850 nm, jusqu'à 550 m.
- MGBT1 : émetteur-récepteur SFP 1000BASE-T pour le fil cuivre de catégorie 5, jusqu'à 100 m.

Pour afficher les résultats des tests optiques, cliquez sur **Administration** > **Diagnostics** > **État des modules optiques**.

Cette page affiche les champs suivants :

- **Port** : numéro du port sur lequel le SFP est connecté.
- **Description** : description de l'émetteur-récepteur optique.
- **Numéro de série** : numéro de série de l'émetteur-récepteur optique.
- **PID** : ID du VLAN.
- **VID** : ID de l'émetteur-récepteur optique.
- **Température** : température en degrés Celsius à laquelle le SFP fonctionne.
- **Tension** : tension de fonctionnement du SFP.
- **Intensité** : consommation de courant du SFP.
- **Output Power** : puissance optique transmise.
- **Input Power** : puissance optique reçue.
- **Défaillance du transmetteur** : le SFP distant indique une perte de signal. Les valeurs sont Vrai, Faux et A/S (Aucun signal).
- **Loss of Signal** : le SFP local indique une perte de signal. Les valeurs sont True (vrai) et False (faux).
- **Données prêtes** : le SFP est opérationnel. Les valeurs sont Vrai et Faux.

Configuration de la mise en miroir des ports et de VLAN

La mise en miroir des ports est utilisée sur un appareil réseau pour envoyer une copie des paquets réseau détectés sur un port d'appareil unique, sur plusieurs ports d'appareil ou sur l'intégralité d'un VLAN vers une connexion de surveillance réseau située sur un autre port de l'appareil. Cette opération est souvent utilisée sur les équipements réseau qui nécessitent une surveillance du trafic réseau, par exemple un système de détection des intrusions. Un analyseur de réseau connecté au port de surveillance traite les paquets de données à des fins de diagnostic, de débogage et de contrôle des performances.

Quatre sources maximum peuvent être mises en miroir. Il peut s'agir de n'importe quelle combinaison de quatre ports et/ou VLAN individuels.

Un paquet reçu sur un port réseau affecté à un VLAN soumis à une mise en miroir est mis en miroir sur le port de l'analyseur même si le paquet a été intercepté ou abandonné. Les paquets envoyés par l'appareil sont mis en miroir lorsque la mise en miroir des émissions est activée.

La mise en miroir ne garantit pas que l'ensemble du trafic en provenance du ou des ports source sera reçu sur le port de l'analyseur (de destination). Si le port de l'analyseur reçoit plus de données qu'il ne peut en gérer, une partie de ces données risque d'être perdue.

Une seule instance de mise en miroir est prise en charge sur l'ensemble du système. Le port de l'analyseur (ou le port cible pour la mise en miroir des VLAN ou des ports) est le même pour l'ensemble des VLAN et des ports mis en miroir.

Pour activer la mise en miroir :

ÉTAPE 1 Cliquez sur **Administration** > **Diagnostics** > **Port and VLAN Mirroring**.

Les champs suivants s'affichent :

- **Port de destination** : port sur lequel le trafic doit être copié ; port de l'analyseur.
- **Interface source** : interface, port ou VLAN à partir duquel le trafic est envoyé au port de l'analyseur.
- **Type** : type de surveillance ; entrant sur le port (réception), sortant du port (émission) ou les deux.
- **État** : affiche l'une des valeurs suivantes :
  - *Actif* : les interfaces source et de destination sont actives et transfèrent le trafic.
  - *Pas prêt* : la source ou la destination est inactive (ou les deux) et ne transfère pas le trafic pour une raison quelconque.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un port ou un VLAN à mettre en miroir.

ÉTAPE 3 Configurez les paramètres suivants :

- **Destination Port** : sélectionnez le port de l'analyseur sur lequel les paquets sont copiés. Un analyseur de réseau, par exemple un PC exécutant Wireshark, est connecté à ce port. Si un port est identifié en tant que port de destination de l'analyseur, il conserve cette fonction jusqu'à ce que toutes les entrées aient été supprimées.
- **Interface source** : sélectionnez un port ou VLAN source à partir duquel le trafic doit être mis en miroir.
- **Type** : indiquez si le trafic entrant, le trafic sortant ou les deux sont mis en miroir sur le port de l'analyseur. Si vous sélectionnez **Port**, les options disponibles sont :
  - *Rx Only* : mise en miroir des ports sur les paquets entrants.
  - *Tx Only* : mise en miroir des ports sur les paquets sortants.
  - *Tx and Rx* : mise en miroir des ports sur les paquets entrants et sortants.

ÉTAPE 4 Cliquez sur **Apply**. La mise en miroir des ports est ajoutée à la Configuration d'exécution.

Affichage de l'utilisation du CPU et fonction Secure Core Technology (SCT)

L'appareil gère les types de trafic suivants en plus du trafic de l'utilisateur final :

- Trafic de gestion
- Trafic de protocole
- Trafic de surveillance

Un trafic excessif encombre le CPU et peut empêcher l'appareil de fonctionner normalement. L'appareil utilise la fonction Secure Core Technology (SCT) qui lui garantit de recevoir et traiter le trafic de gestion et de protocole, quel que soit le volume de trafic total reçu. La fonction SCT est activée par défaut sur l'appareil et ne peut pas être désactivée.

Il n'y a pas d'interactions avec les autres fonctions.

Pour afficher l'utilisation du CPU :

ÉTAPE 1 Cliquez sur **Administration > Diagnostics > Utilisation des CPU**.

La page Utilisation du CPU s'affiche.

Le champ Niveau d'entrée CPU affiche le débit de trames d'entrée dans le CPU par seconde.

La fenêtre affiche un graphique de l'utilisation du CPU. L'axe des Y représente le pourcentage d'utilisation et l'axe des X le numéro de l'échantillon.

ÉTAPE 2 Assurez-vous que la case Utilisation du processeur est activée.

ÉTAPE 3 Sélectionnez le **Fréquence d'actualisation**, à savoir la durée en secondes qui s'écoule avant l'actualisation des statistiques. Un nouvel échantillon est créé pour chaque période.

ÉTAPE 4 Cliquez sur **Appliquer**.

9

Administration : Détection

Cette section fournit des informations sur la configuration de la détection.

Elle couvre les rubriques suivantes :

- **Bonjour**
- **LLDP et CDP**
- **Configuration de LLDP**
- **Configuration de CDP**

Bonjour

En tant que client Bonjour, le périphérique diffuse périodiquement des paquets de protocole de détection Bonjour vers un ou plusieurs sous-réseaux IP à connexion directe, annonçant ainsi sa propre existence et les services qu'il offre, par exemple HTTP ou HTTPS. (Utilisez la page Sécurité > Services TCP/UDP pour activer ou désactiver les services de périphérique.) Le périphérique peut être *détecté* par un système de gestion réseau ou autre application tierce. Par défaut, Bonjour est activé et s'exécute sur le VLAN de gestion. La console Bonjour détecte automatiquement le périphérique et l'affiche.

Bonjour en mode système Layer 2

La détection Bonjour peut uniquement être activée globalement, et non séparément pour chaque port ou chaque VLAN. Le périphérique annonce les services qui ont été activés par l'administrateur.

Lorsque vous activez à la fois la découverte Bonjour et IGMP, l'adresse IP de multidiffusion de Bonjour apparaît sur la page Ajout d'adresses IP de groupe de multidiffusion.

Si la détection Bonjour est désactivée, le périphérique cesse les annonces de type de service et ne répond à aucune demande de service émanant des applications de gestion réseau.

Par défaut, Bonjour est activé sur toutes les interfaces membres du VLAN de gestion.

Pour activer Bonjour globalement :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - Bonjour**.

ÉTAPE 2 Sélectionnez **Activer** pour activer globalement la **détection** Bonjour sur le périphérique.

ÉTAPE 3 Cliquez sur **Apply**. Bonjour est activé ou désactivé sur le périphérique, en fonction des options sélectionnées.

LLDP et CDP

LLDP (Link Layer Discovery Protocol) et CDP (Cisco Discovery Protocol) sont des protocoles de couche de liaison permettant aux voisins LLDP et CDP à connexion directe de s'annoncer et de notifier leurs fonctionnalités. Par défaut, le périphérique envoie régulièrement une annonce LLDP/CDP à toutes ses interfaces, puis traite les paquets LLDP et CDP entrants conformément aux exigences des protocoles. Dans LLDP et CDP, les annonces sont codées en TLV (Type, Longueur, Valeur) dans le paquet.

Les remarques de configuration CDP/LLDP suivantes s'appliquent :

- CDP/LLDP peut être activé ou désactivé globalement, ou pour chaque port. La fonctionnalité CDP/LLDP d'un port ne s'applique que si CDP/LLDP est globalement activé.
- Si CDP/LLDP est globalement activé, le périphérique élimine les paquets CDP/LLDP entrants provenant des ports où CDP/LLDP est désactivé.
- Si CDP/LLDP est globalement désactivé, le périphérique peut être configuré pour ignorer l'inondation tenant compte du VLAN, ou l'inondation ne tenant pas compte du VLAN, de tous les paquets CDP/LLDP entrants. L'inondation tenant compte du VLAN transmet un paquet CDP/LLDP entrant au VLAN où le paquet est reçu, mais pas au port d'entrée. L'inondation ne tenant pas compte du VLAN transmet un paquet CDP/LLDP entrant à tous les ports, sauf au port d'entrée. Par défaut, le système élimine les paquets CDP/LLDP lorsque CDP/LLDP est désactivé au niveau global. Vous pouvez configurer l'élimination/inondation des paquets CDP et LLDP entrants respectivement sur les pages Propriétés CDP et Propriétés LLDP.
- La fonction Port intelligent automatique requiert l'activation de CDP et/ou LLDP. La fonction Port intelligent automatique configure automatiquement une interface basée sur l'annonce CDP/LLDP reçue de l'interface.

- Les périphériques d'extrémité CDP et LLDP, tels que les téléphones IP, apprennent la configuration VLAN voix des annonces CDP et LLDP. Par défaut, le périphérique est activé pour envoyer une annonce CDP et LLDP basée sur le VLAN voix qui est configuré sur le périphérique. Pour plus d'informations, reportez-vous à la section **VLAN voix**.

  REMARQUE CDP/LLDP ne peut pas détecter si un port se trouve dans un LAG. Si un LAG contient plusieurs ports, CDP/LLDP transmet les paquets sur chaque port sans tenir compte de l'appartenance des ports à un LAG.

Le fonctionnement du CDP/LLDP est indépendant de l'état STP d'une interface.

Si le contrôle d'accès au port 802.1x est activé sur une interface, le périphérique transmet les paquets CDP/LLDP à l'interface, et les reçoit de cette dernière, uniquement si l'interface est authentifiée et autorisée.

Si un port est la cible de la mise en miroir, CDP/LLDP le considère inactif.

REMARQUE CDP et LLDP sont des protocoles de couche de liaison permettant aux périphériques CDP/LLDP à connexion directe de s'annoncer et de notifier mutuellement leurs fonctionnalités. Dans les déploiements où les périphériques prenant en charge CDP/LLDP ne sont pas directement connectés et sont séparés des périphériques ne prenant pas en charge CDP/LLDP, les périphériques prenant en charge CDP/LLDP ne peuvent recevoir l'annonce des autres périphériques que si les périphériques ne prenant pas en charge CDP/LLDP transmettent les paquets CDP/LLDP qu'ils reçoivent. Si les périphériques ne prenant pas en charge CDP/LLDP effectuent une inondation tenant compte du VLAN, les périphériques prenant en charge CDP/LLDP ne peuvent s'entendre mutuellement que s'ils se trouvent sur le même VLAN. Un périphérique prenant en charge CDP/LLDP peut recevoir une annonce de plusieurs périphériques si les périphériques ne prenant pas en charge CDP/LLDP transmettent les paquets CDP/LLDP.

Configuration de LLDP

Cette section explique comment configurer LLDP. Elle couvre les rubriques suivantes :

- **Présentation de LLDP**
- **Propriétés LLDP**
- **Paramètres de port LLDP**
- **LLDP MED Network Policy (stratégie réseau LLDP MED)**
- **Paramètres des ports LLDP MED**
- **État des ports LLDP**

- **Informations locales LLDP**
- **Informations de voisinage LLDP**
- **Statistiques LLDP**
- **Surcharge LLDP**

Présentation de LLDP

Le protocole LLDP permet aux gestionnaires de réseaux d'effectuer des dépannages et d'améliorer la gestion du réseau dans des environnements multifournisseurs. LLDP normalise les méthodes permettant aux périphériques réseau de s'annoncer auprès des autres systèmes et de stocker les informations détectées.

LLDP permet à un périphérique d'annoncer son identificateur, sa configuration et ses fonctions auprès de périphériques voisins qui peuvent alors stocker ces données dans un fichier MIB (Management Information Base, base d'informations de gestion). Le système de gestion réseau modélise la topologie du réseau en interrogeant ces bases de données MIB.

LLDP est un protocole de couche de liaison. Par défaut, le périphérique arrête et traite tous les paquets LLDP entrants conformément aux exigences du protocole.

Le protocole LLDP possède une extension appelée LLDP Media Endpoint Discovery (LLDP MED, détection d'extrémité de média), qui fournit et accepte des informations émanant de périphériques d'extrémité de média, tels que les téléphones VoIP et les téléphones vidéo. Pour plus d'informations sur LLDP-MED, reportez-vous à **LLDP MED Network Policy (stratégie réseau LLDP MED)**.

Flux de travail de configuration de LLDP

Voici des exemples d'actions qu'il est possible de réaliser avec la fonction LLDP, dans l'ordre suggéré : Pour obtenir des instructions supplémentaires sur la configuration de LLDP, reportez-vous à la section LLDP/CDP. Les pages de configuration de LLDP sont accessibles sous le menu **Administration > Détection - LLDP**.

1. Saisissez les paramètres globaux LLDP, tels que l'intervalle de temps pour l'envoi des mises à jour LLDP, via la page Propriétés LLDP.
2. Configurez LLDP pour chaque port à l'aide de la page Paramètres des ports. Sur cette page, vous pouvez configurer les interfaces pour recevoir/transmettre des PDU LLDP, envoyer des notifications SNMP, spécifier les TLV à annoncer, mais aussi annoncer l'adresse de gestion du périphérique.
3. Créez des stratégies réseau LLDP MED à l'aide de la page Stratégie réseau LLDP MED.
4. Associez les stratégies réseau LLDP MED et les TLV LLDP-MED facultatives aux interfaces souhaitées, à l'aide de la page Paramètres des ports LLDP-MED.
5. Si la fonction Port intelligent automatique doit détecter les fonctionnalités des périphériques LLDP, activez LLDP sur la page Propriétés des ports intelligents.
6. Affichez les informations de surcharge à l'aide de la page Surcharge LLDP.

Propriétés LLDP

La page Propriétés permet de saisir les paramètres LLDP généraux, comme l'activation/la désactivation globale de cette fonction et la définition d'horloges.

Pour saisir des propriétés LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Propriétés**.

ÉTAPE 2 Saisissez les paramètres.

- **État LLDP** : sélectionnez cette option pour activer LLDP sur le périphérique (activée par défaut).
- **Traitement des trames LLDP** : si LLDP n'est pas activé, sélectionnez l'action à réaliser en cas de réception d'un paquet correspondant aux critères sélectionnés :
  - *Filtrage* : supprime le paquet.
  - *Inondation* : transfère le paquet à tous les membres du VLAN.
- **Intervalle d'annonce TLV** : définissez, en nombre de secondes, la fréquence d'envoi des mises à jour des annonces LLDP ou utilisez la valeur par défaut.
- **Intervalle de notification SNMP de changement de topologie** : saisissez le délai minimal entre deux notifications SNMP.
- **Multiplicateur de conservation** : saisissez la durée de conservation des paquets LLDP avant leur élimination, en multiples de l'intervalle d'annonce TLV. Par exemple, si l'intervalle d'annonce TLV est de 30 secondes et que le multiplicateur de conservation (Hold Multiplier) est 4, les paquets LLDP seront supprimés après 120 secondes.
- **Délai de réinitialisation** : saisissez l'intervalle en secondes qui sépare la désactivation et la réactivation de LLDP, suite à un cycle d'activation ou de désactivation de LLDP.
- **Délai de transmission** : saisissez le délai en secondes qui séparera deux transmissions de trames LLDP successives en cas de modification dans la MIB de systèmes locaux LLDP.
- **Notification d'ID de châssis** : sélectionnez l'une des options suivantes pour une notification dans les messages LLDP :
  - *Adresse MAC* : spécifiez l'adresse MAC du périphérique.
  - *Nom d'hôte* : spécifiez le nom d'hôte de ce périphérique.

ÉTAPE 3 Dans le champ **Nombre de répétitions pour le démarrage rapide**, saisissez le nombre d'envois de paquets LLDP lors de l'initialisation du mécanisme de démarrage rapide LLDP MED. Cela se produit lorsqu'un nouveau périphérique d'extrémité établit une liaison au périphérique. Pour consulter la description de LLDP MED, reportez-vous à la section Stratégie réseau LLDP MED.

ÉTAPE 4 Cliquez sur **Apply**. Les propriétés LLDP sont ajoutées au fichier de Configuration d'exécution.

Paramètres de port LLDP

La page Paramètres des ports vous permet d'activer LLDP et la notification SNMP pour chaque port, et de saisir les TLV envoyées dans la PDU LLDP.

Vous pouvez sélectionner les TLV LLDP-MED à annoncer sur la page Paramètres des ports LLDP-MED et configurer la TLV d'adresse de gestion du périphérique.

Pour définir les paramètres des ports LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Paramètres des ports**.

Cette page affiche les informations LLDP des ports.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier**.

Cette page contient les champs suivants :

- **Interface** : sélectionnez le port à modifier.
- **Administrative Status** : sélectionnez l'option de publication LLDP pour le port. Les valeurs disponibles sont les suivantes :
  - *Émission uniquement* : publication uniquement, pas de détection.
  - *Rx Only* : détection uniquement, pas de publication.
  - *Tx & Rx* : publication et détection.
  - *Désactiver* : indique que LLDP est désactivé sur le port.
- **Notification SNMP** : sélectionnez **Activer** pour envoyer des notifications aux destinataires de notifications SNMP (système de gestion SNMP, par exemple) en cas de modification de la topologie.

  L'intervalle entre deux notifications est défini dans le champ Intervalle de notification SNMP de changement de topologie de la page Propriétés LLDP. Définissez les destinataires des notifications SNMP à l'aide de la page SNMP > Destinataire de notification v1,2 et/ou SNMP > Destinataire de notification v3.
- **TLV facultatives sélectionnées** : sélectionnez les informations que le périphérique doit publier en déplaçant la TLV voulue depuis la liste **TLV facultatives disponibles**. Les TLV disponibles contiennent les informations suivantes :
  - *Description du port* : informations sur le port, notamment son fabricant, son nom de produit et la version du matériel/logiciel.
  - *Nom du système* : nom attribué au système, au format alphanumérique. Cette valeur est identique à l'objet sysName.
  - *Description du système* : description de l'entité réseau, au format alphanumérique. Inclut le nom du système et la version du matériel, le système d'exploitation et les logiciels réseau pris en charge par le périphérique. Cette valeur est identique à l'objet sysDescr.

- *Fonctionnalités du système* : fonctions principales du périphérique. L'écran indique aussi si ces fonctions sont activées sur le périphérique. Les fonctionnalités sont indiquées par deux octets. Les bits 0 à 7 indiquent respectivement Autres, Répéteur, Pont, Point d'accès WLAN, Routeur, Téléphone, Système de câble DOCSIS et Station. Les bits 8 à 15 sont réservés.
- *802.3 MAC-PHY* : fonction duplex et débit, avec les paramètres duplex et de débit actuels du périphérique d'envoi. L'écran indique également si les paramètres actuels sont obtenus par négociation automatique ou par configuration manuelle.
- *802.3 Link Aggregation* : indique s'il est possible d'agréger la liaison (associée au port sur lequel la PDU LLDP est transmise). L'écran indique également si la liaison est actuellement agrégée et, le cas échéant, précise l'ID du port agrégé.
- *802.3 Maximum Frame Size* : capacité de taille maximale de trame de l'implémentation MAC/PHY.

TLV facultative d'adresse de gestion :

- **Mode d'annonce** : sélectionnez l'une des méthodes suivantes pour l'annonce de l'adresse IP de gestion au périphérique :
  - *Annonce automatique* : spécifie que le logiciel choisit automatiquement une adresse de gestion à annoncer parmi toutes les adresses IP du périphérique. En cas d'adresses IP multiples, le logiciel choisit l'adresse IP la plus basse parmi les adresses IP dynamiques. S'il n'y a pas d'adresses dynamiques, le logiciel choisit l'adresse IP la plus basse parmi les adresses IP statiques.
  - *Aucune* : aucune annonce de l'adresse IP de gestion.
  - *Annonce manuelle* : sélectionnez cette option et l'adresse IP de gestion à annoncer.
- **Adresse IP** : si vous avez sélectionné Annonce manuelle, sélectionnez l'adresse de gestion voulue dans la liste d'adresses IP fournie.

Les champs suivants concernent **VLAN et protocole 802.1** :

- **PVID** : sélectionnez cette option pour annoncer le PVID dans la TLV.
- **ID VLAN de port et de protocole** : sélectionnez ces options pour annoncer l'ID VLAN de port et de protocole.
- **ID VLAN** : sélectionnez les VLAN qui feront l'objet d'une annonce.
- **ID de protocole** : sélectionnez les protocoles qui feront l'objet d'une annonce.
- **ID des protocoles sélectionnés** : affiche les protocoles sélectionnés.

ÉTAPE 3 Saisissez les informations voulues et cliquez sur **Appliquer**. Les paramètres des ports sont écrits dans le fichier de Configuration d'exécution.

LLDP MED Network Policy (stratégie réseau LLDP MED)

LLDP Media Endpoint Discovery (LLDP MED) est une extension de LLDP qui fournit les fonctionnalités supplémentaires suivantes pour la prise en charge des périphériques d'extrémité de média.

- Permet l'annonce et la découverte des stratégies réseau pour les applications en temps réel telles que la voix et/ou la vidéo.
- Elle détecte l'emplacement des périphériques afin de permettre la création de bases de données d'emplacements. Dans le cas du protocole VoIP (voix sur IP), elle permet également l'accès aux services d'urgence (E-911 aux États-Unis) à l'aide des informations de géolocalisation du téléphone IP.
- Informations de dépannage. LLDP MED envoie des alertes aux gestionnaires de réseaux concernant les éléments ci-dessous :
  - Conflits de débit de port et de mode duplex
  - Erreurs de configuration des stratégies QoS

Configuration d'une stratégie réseau LLDP MED

Une stratégie réseau LLDP MED est un ensemble de paramètres de configuration apparentés, destiné à une application en temps réel, telle que la voix ou la vidéo. Une stratégie réseau (si elle est configurée) est incluse dans les paquets LLDP sortants qui sont envoyés vers le périphérique d'extrémité de média LLDP associé. Le périphérique d'extrémité de média doit envoyer son trafic comme spécifié dans la stratégie réseau qu'il reçoit. Par exemple, vous pouvez créer une stratégie pour le trafic VoIP qui demande au téléphone VoIP d'effectuer les tâches suivantes :

- Envoyer du trafic voix sur le VLAN 10 en tant que paquet balisé et avec 802.1p priorité 5
- Envoyer du trafic voix avec DSCP 46

Vous pouvez associer des stratégies réseau à des ports à l'aide de la page Paramètres des ports LLDP-MED. Un administrateur peut configurer manuellement une ou plusieurs stratégies réseau, ainsi que les interfaces où les stratégies doivent être envoyées. Il est de la responsabilité de l'administrateur de créer manuellement les VLAN et leurs appartenances de port conformément aux stratégies réseau et à leurs interfaces associées.

En outre, l'administrateur peut demander au périphérique de générer et d'annoncer automatiquement une stratégie réseau pour l'application vocale qui est basée sur le VLAN voix géré par le périphérique. Pour plus d'informations sur la façon dont le périphérique gère son VLAN voix, reportez-vous à la section VLAN voix automatique.

Pour définir une stratégie réseau LLDP MED :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Stratégie réseau LLDP MED**.

Cette page contient les stratégies réseau précédemment créées.

ÉTAPE 2 Sélectionnez **Auto** pour la stratégie réseau LLDP MED de l'application vocale si le périphérique doit générer et annoncer automatiquement une stratégie réseau pour l'application vocale qui est basée sur le VLAN voix géré par le périphérique.

REMARQUE Si cette case est cochée, vous ne pouvez pas configurer manuellement une stratégie réseau de voix.

ÉTAPE 3 Cliquez sur **Appliquer** pour ajouter ce paramètre au fichier de Configuration d'exécution.

ÉTAPE 4 Pour définir une nouvelle stratégie, cliquez sur **Ajouter**.

ÉTAPE 5 Saisissez les valeurs appropriées :

- **Network Policy Number** : sélectionnez le numéro de la stratégie à créer.
- **Application** : sélectionnez le type d'application (type de trafic) pour lequel vous définissez la stratégie réseau.
- **ID VLAN** : saisissez l'ID du VLAN auquel le trafic doit être envoyé.
- **Type VLAN** : indiquez si le trafic doit être balisé ou non.
- **User Priority** : sélectionnez le niveau de priorité qui sera accordé au trafic défini par cette stratégie réseau. Il s'agit de la valeur CoS.
- **DSCP Value** : sélectionnez la valeur DSCP à associer aux données d'application envoyées par les voisins. Cela leur indique la façon dont ils doivent marquer le trafic d'application qu'ils envoient au périphérique.

ÉTAPE 6 Cliquez sur **Apply**. La stratégie réseau est définie.

REMARQUE Vous devez configurer manuellement les interfaces, afin d'inclure les stratégies réseau définies manuellement pour les paquets LLDP sortants, via la page Paramètres des ports LLDP-MED.

Paramètres des ports LLDP MED

La page Paramètres des ports LLDP-MED permet de sélectionner les TLV LLDP-MED et/ou les stratégies réseau à inclure dans l'annonce LLDP sortante pour les interfaces souhaitées. Vous pouvez configurer les stratégies réseau sur la page Stratégie réseau LLDP MED.

REMARQUE Si la stratégie réseau LLDP-MED pour l'application vocale (page Stratégie réseau LLDP MED) est Automatique et que le VLAN voix automatique fonctionne, le périphérique génère automatiquement une stratégie réseau LLDP MED pour l'application vocale, pour tous les ports qui sont activés pour LLDP-MED et membres du VLAN voix.

Pour configurer LLDP MED sur chaque port :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Paramètres des ports LLDP MED**.

Cette page affiche les paramètres LLDP MED suivants pour tous les ports (seuls les champs qui ne sont pas décrits sur la page **Modifier** sont répertoriés) :

- **Lieu** : indique si la TLV de lieu est transmise.
- **PoE** : indique si la TLV POE-PSE est transmise.
- **Inventaire** : indique si la TLV d'inventaire est transmise.

ÉTAPE 2 Le message affiché en haut de la page indique si la génération de la stratégie réseau LLDP MED pour l'application vocale est automatique (reportez-vous à **Présentation de LLDP**). Cliquez sur le lien pour changer de mode.

ÉTAPE 3 Pour associer une TLV LLDP MED supplémentaire et/ou une ou plusieurs stratégies réseau LLDP MED définies par l'utilisateur à un port, sélectionnez-la, puis cliquez sur **Modifier**.

ÉTAPE 4 Configurez les paramètres suivants :

- **Interface** : sélectionnez l'interface à configurer.
- **État LLDP MED** : activez/désactivez LLDP MED sur ce port.
- **Notification SNMP** : indiquez si la notification SNMP doit être envoyée, port par port, lorsqu'une station de travail prenant en charge MED est détectée (un système de gestion SNMP, par exemple), lors d'un changement de topologie.
- **TLV facultatives sélectionnées** : sélectionnez les TLV que le périphérique peut publier en les déplaçant de la liste **TLV facultatives disponibles** vers la liste TLV facultatives sélectionnées.

- **Stratégies réseau disponibles** : sélectionnez les stratégies LLPD MED que LLDP va publier en les déplaçant de la liste **Stratégies réseau disponibles** vers la liste Stratégies réseau sélectionnées. Elles ont été créées sur la page Stratégie réseau LLDP MED. Pour inclure une ou plusieurs stratégies réseau définies par l'utilisateur dans l'annonce, vous devez aussi sélectionner **Stratégie réseau** dans les **TLV facultatives disponibles**.

  REMARQUE Vous devez remplir les champs suivants, au format hexadécimal, en respectant exactement le format de données défini dans la norme LLDP MED (ANSI-TIA-1057_final_for_publication.pdf) :

  - **Location Coordinate** : saisissez les coordonnées de l'emplacement que LLDP devra publier.
  - **Adresse physique de l'emplacement** : saisissez l'adresse de l'emplacement que LLDP devra publier.
  - **Emplacement ECS ELIN** : saisissez l'emplacement ECS (Emergency Call Service, service d'appel d'urgence) ELIN que LLDP devra publier.

ÉTAPE 5 Cliquez sur **Apply.** Les paramètres des ports LLDP MED sont écrits dans le fichier de Configuration d'exécution.

État des ports LLDP

La page Table d'état des ports LLDP contient des informations globales LLDP pour chaque port.

ÉTAPE 1 Pour afficher l'état des ports LLDP, cliquez sur **Administration** > **Détection - LLDP** > **État des ports LLDP**.

ÉTAPE 2 Cliquez sur **Détails sur les informations locales LLDP** pour consulter le détail des TLV LLDP et LLDP MED envoyées au voisin.

ÉTAPE 3 Cliquez sur **Détails des informations du voisin LLDP** pour consulter le détail des TLV LLDP et LLDP MED reçues du voisin.

Informations globales d'état des ports LLDP

- **Chassis ID Subtype** : type d'ID de châssis (adresse MAC, par exemple).
- **Chassis ID** : identificateur du châssis. Si vous avez choisi l'adresse MAC comme sous-type d'ID de châssis, l'adresse MAC du périphérique s'affiche.
- **Nom du système** : nom du périphérique.
- **Description du système** : description du périphérique, au format alphanumérique.
- **Supported System Capabilities** : fonctions principales du périphérique telles que Bridge (pont), WLAN AP (point d'accès WLAN) ou Router (routeur).
- **Fonctionnalités système activées** : fonctions principales activées sur le périphérique.
- **Port ID Subtype** : type d'ID de port affiché.

Table d'état des ports LLDP

- **Interface** : identificateur de port.
- **LLDP Status** : option de publication LLDP.
- **État LLDP MED** : indique si la fonction est activée ou désactivée.
- **PoE local** : informations PoE locales annoncées.
- **PoE distant** : informations PoE annoncées par le voisin.
- **# of neighbors** : nombre de voisins détectés.
- **Fonctionnalités de voisinage du 1er périphérique** : affiche les fonctions principales du voisin ; par exemple : pont ou routeur.

Informations locales LLDP

Pour afficher l'état LLDP de port local annoncé sur un port :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Informations locales LLDP**.

ÉTAPE 2 Sélectionnez l'interface pour laquelle les informations locales LLDP doivent être affichées.

Cette page contient les champs suivants pour l'interface sélectionnée :

Global

- **Sous-type de l'ID du châssis** : type d'ID de châssis (adresse MAC, par exemple).
- **Chassis ID** : identificateur du châssis. Si vous avez choisi l'adresse MAC comme sous-type d'ID de châssis, l'adresse MAC du périphérique s'affiche.
- **Nom du système** : nom du périphérique.
- **Description du système** : description du périphérique, au format alphanumérique.
- **Supported System Capabilities** : fonctions principales du périphérique telles que Bridge (pont), WLAN AP (point d'accès WLAN) ou Router (routeur).
- **Fonctionnalités système activées** : fonctions principales activées sur le périphérique.
- **Port ID Subtype** : type d'ID de port affiché.
- **Port ID** : identificateur du port.
- **Description du port** : informations sur le port, notamment son fabricant, son nom de produit et la version du matériel/logiciel.

Management Address (adresse de gestion)

Affiche la table d'adresses de l'agent LLDP local. D'autres gestionnaires distants peuvent utiliser cette adresse pour obtenir des informations sur le périphérique local. Cette adresse est constituée des éléments suivants :

- **Sous-type de l'adresse** : type de l'adresse IP de gestion affichée dans le champ Adresse de gestion. Par exemple, IPv4.
- **Adresse** : adresse renvoyée qui convient le mieux pour la gestion.
- **Interface Subtype** : méthode de numérotation servant à définir le numéro de l'interface.
- **Numéro de l'interface** : interface spécifique associée à cette adresse de gestion.

MAC/PHY Details (informations MAC/PHY)

- **Auto-Negotiation Supported** : état de prise en charge de la négociation automatique du débit de port.
- **Auto-Negotiation Enabled** : état d'activation de la négociation automatique du débit de port.
- **Fonctionnalités annoncées de négociation automatique** : fonctions de négociation automatique du débit de port. Exemples : mode half-duplex 1000BASE-T ou mode full duplex 100BASE-TX.
- **Operational MAU Type** : type de MAU (unité de raccordement de supports). La MAU gère les fonctions de couche physique, notamment la conversion des données numériques à partir de la détection de collision des interfaces Ethernet et l'injection de bits dans le réseau. Exemple : mode full duplex 100BASE-TX.

802.3 Details (informations relatives à 802.3)

- **802.3 Maximum Frame Size** : taille maximale de trame IEEE 802.3 prise en charge.

802.3 Link Aggregation (agrégation de liaisons 802.3)

- **Aggregation Capability** : indique si l'interface peut faire l'objet d'une agrégation.
- **Aggregation Status** : indique si l'interface est agrégée.
- **ID du port d'agrégation** : ID d'interface agrégée annoncé.

802.3 Energy Efficient Ethernet (EEE) (si le périphérique prend en charge EEE)

- **Émission locale** : durée (en microsecondes) pendant laquelle le partenaire de liaison effectuant la transmission attend avant de commencer la transmission des données après avoir quitté le mode LPI (Low Power Idle).
- **Réception locale** : durée (en microsecondes) pendant laquelle le partenaire de liaison effectuant la réception demande au partenaire de liaison effectuant la transmission d'attendre avant de transmettre les données après avoir quitté le mode LPI (Low Power Idle).

- **Écho d'émission à distance** : indique la réflexion du partenaire de liaison locale pour la valeur d'émission du partenaire de liaison distante.
- **Écho de réception à distance** : indique la réflexion du partenaire de liaison locale pour la valeur de réception du partenaire de liaison distante.

MED Details (informations MED)

- **Capabilities Supported** : fonctions MED prises en charge sur le port.
- **Current Capabilities** : fonctions MED activées sur le port.
- **Classe de périphérique** : classe du périphérique d'extrémité LLDP MED. Les classes disponibles sont les suivantes :
  - *Classe d'extrémité 1*: classe d'extrémité générique offrant des services LLDP de base.
  - *Classe d'extrémité 2*: classe d'extrémité de média offrant des services de lecture multimédia en continu, en plus des services de classe 1.
  - *Classe d'extrémité 3*: classe de périphérique de communications offrant tous les services de classe 1 et de classe 2 ainsi que des fonctions de reconnaissance de l'emplacement, d'appel d'urgence, de prise en charge des périphériques de Couche 2 et de gestion des informations de périphérique.
- **Type de périphérique PoE** : type PoE du port. Exemple : alimenté.
- **Source d'alimentation PoE** : source d'alimentation du port.
- **Priorité d'alimentation PoE** : priorité d'alimentation du port.
- **Valeur d'alimentation PoE** : valeur d'alimentation du port.
- **Hardware Revision** : version du matériel.
- **Firmware Revision** : version du microprogramme.
- **Software Revision** : version du logiciel.
- **Serial Number** : numéro de série du périphérique.
- **Manufacturer Name** : nom du fabricant du périphérique.
- **Model Name** : nom du modèle de périphérique.
- **Asset ID** : ID de la ressource.

Location Information (informations sur l'emplacement)

- **Physique** : adresse postale.
- **Coordinates** : coordonnées géographiques : latitude, longitude et altitude.
- **ECS ELIN** : numéro ELIN (Emergency Location Identification Number, numéro d'identification de l'emplacement en cas d'urgence) pour l'ECS (Emergency Call Service, service d'appel d'urgence).

Network Policy Table (table des stratégies réseau)

- **Type d'application** : type d'application de la stratégie réseau. Exemple : Voix.
- **VLAN ID** : ID du VLAN pour lequel la stratégie réseau est définie.
- **VLAN Type** : type de VLAN pour lequel la stratégie réseau est définie. Ce champ peut prendre les valeurs suivantes :
  - *Tagged* : indique que la stratégie réseau est définie pour les VLAN balisés.
  - *Untagged* : indique que la stratégie réseau est définie pour les VLAN non balisés.
- **User Priority** : priorité d'utilisateur de la stratégie réseau.
- **DSCP** : DSCP de la stratégie réseau.

ÉTAPE 3 En bas de la page, cliquez sur **Table d'état des ports LLDP** pour voir les détails dans la **Table d'état des ports LLDP**.

Informations de voisinage LLDP

La page Informations de voisinage LLDP contient les informations reçues des périphériques voisins.

Après une temporisation (basée sur la valeur reçue du paramètre de durée de vie du voisin, durée au cours de laquelle aucune PDU LLDP n'a été reçue d'un voisin), les informations sont supprimées.

Pour afficher les informations LLDP des voisins :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Informations de voisinage LLDP**.

ÉTAPE 2 Sélectionnez l'interface pour laquelle les informations de voisinage LLDP doivent être affichées.

Cette page contient les champs suivants pour l'interface sélectionnée :

- **Local Port** : numéro du port local auquel le voisin est connecté.
- **Chassis ID Subtype** : type d'ID de châssis (adresse MAC, par exemple).
- **Chassis ID** : identificateur du châssis du périphérique de voisinage réseau (LAN) 802.
- **Port ID Subtype** : type d'ID de port affiché.
- **Port ID** : identificateur du port.
- **Nom du système** : nom publié du périphérique.
- **Time to Live** : durée en secondes à l'issue de laquelle les informations concernant ce voisin sont supprimées.

ÉTAPE 3 Sélectionnez un port local puis cliquez sur **Détails**.

La page Informations de voisinage LLDP comporte les champs suivants :

Détails du port

- **Port local** : numéro du port.
- **Entrée MSAP** : numéro d'entrée MSAP (Media Service Access Point, point d'accès de service multimédia) du périphérique.

Détails de base

- **Chassis ID Subtype** : type d'ID de châssis (adresse MAC, par exemple).
- **ID du châssis** : identificateur du châssis du périphérique de voisinage réseau (LAN) 802.
- **Port ID Subtype** : type d'ID de port affiché.
- **Port ID** : identificateur du port.
- **Description du port** : informations sur le port, notamment son fabricant, son nom de produit et la version du matériel/logiciel.
- **Nom du système** : nom du système publié.
- **Description du système** : description de l'entité réseau, au format alphanumérique. Inclut le nom du système et la version du matériel, le système d'exploitation et les logiciels réseau pris en charge par le périphérique. Cette valeur est identique à l'objet sysDescr.
- **Fonctionnalités système prises en charge** : fonctions principales du périphérique. Les fonctionnalités sont indiquées par deux octets. Les bits 0 à 7 indiquent respectivement Autres, Répéteur, Pont, Point d'accès WLAN, Routeur, Téléphone, Système de câble DOCSIS et Station. Les bits 8 à 15 sont réservés.
- **Fonctionnalités système activées** : fonctions principales activées sur le périphérique.

Table des adresses de gestion

- **Sous-type de l'adresse** : sous-type d'adresse gérée. Exemple : MAC ou IPv4.
- **Adresse** : adresse gérée.
- **Sous-type de l'interface** : sous-type de port.
- **Numéro de l'interface** : numéro de port.

MAC/PHY Details (informations MAC/PHY)

- **Auto-Negotiation Supported** : état de prise en charge de la négociation automatique du débit de port. Les valeurs admises sont Vrai et Faux.
- **Auto-Negotiation Enabled** : état d'activation de la négociation automatique du débit de port. Les valeurs admises sont Vrai et Faux.
- **Fonctionnalités annoncées de négociation automatique** : fonctions de négociation automatique du débit de port. Exemples : mode half-duplex 1000BASE-T ou mode full duplex 100BASE-TX.
- **Operational MAU Type** : type de MAU (unité de raccordement de supports). La MAU gère les fonctions de couche physique, notamment la conversion des données numériques à partir de la détection de collision des interfaces Ethernet et l'injection de bits dans le réseau. Exemple : mode full duplex 100BASE-TX.

Alimentation 802.3 via MDI

- **Classe de port de prise en charge de l'alimentation MDI** : classe de port annoncée pour la prise en charge de l'alimentation.
- **Prise en charge de l'alimentation MDI PSE** : indique si l'alimentation MDI est prise en charge sur le port.
- **État de l'alimentation MDI PSE** : indique si l'alimentation MDI est activée sur le port.
- **Capacité de contrôle des paires d'alimentation PSE** : indique si le contrôle des paires d'alimentation est pris en charge sur le port.
- **Paire d'alimentation PSE** : type de contrôle des paires d'alimentation pris en charge sur le port.
- **Classe d'alimentation PSE** : classe de port annoncée pour l'alimentation.

802.3 Details (informations relatives à 802.3)

- **Taille de trame maximale 802.3** : taille maximale de trame annoncée comme possible sur le port.

802.3 Link Aggregation (agrégation de liaisons 802.3)

- **Capacité d'agrégation** : indique si le port peut faire l'objet d'une agrégation.
- **État de l'agrégation** : indique si le port est actuellement agrégé.
- **ID du port d'agrégation** : ID du port agrégé annoncé.

802.3 Energy Efficient Ethernet (EEE)

- **Émission à distance** : durée (en microsecondes) pendant laquelle le partenaire de liaison effectuant la transmission attend avant de commencer la transmission des données après avoir quitté le mode LPI (Low Power Idle).
- **Réception à distance** : durée (en microsecondes) pendant laquelle le partenaire de liaison effectuant la réception demande au partenaire de liaison effectuant la transmission d'attendre avant de transmettre les données après avoir quitté le mode LPI (Low Power Idle).
- **Écho d'émission local** : indique la réflexion du partenaire de liaison locale pour la valeur d'émission du partenaire de liaison distante.
- **Écho de réception local** : indique la réflexion du partenaire de liaison locale pour la valeur de réception du partenaire de liaison distante.

MED Details (informations MED)

- **Fonctionnalités prises en charge** : fonctions MED activées sur le port.
- **Fonctionnalités actuelles** : TLV MED annoncées par le port.
- **Classe de périphérique** : classe du périphérique d'extrémité LLDP MED. Les classes disponibles sont les suivantes :
  - *Classe de point de terminaison 1* : indique une classe de point de terminaison générique offrant des services LLDP de base.
  - *Classe de point de terminaison 2* : indique une classe de point de terminaison de média offrant des services de lecture multimédia en continu, en plus des services de classe 1.
  - *Classe de point de terminaison 3* : indique une classe de périphérique de communications offrant tous les services de classe 1 et de classe 2, ainsi que des fonctions de reconnaissance de l'emplacement, d'appel d'urgence, de prise en charge des commutateurs Layer 2 et de gestion des informations de périphérique.
- **Type de périphérique PoE** : type PoE du port. Exemple : alimenté.
- **Source d'alimentation PoE** : source d'alimentation du port.
- **Priorité d'alimentation PoE** : priorité d'alimentation du port.

- **Valeur d'alimentation PoE** : valeur d'alimentation du port.
- **Révision du matériel** : version du matériel.
- **Firmware Revision** : version du microprogramme.
- **Software Revision** : version du logiciel.
- **Serial Number** : numéro de série du périphérique.
- **Manufacturer Name** : nom du fabricant du périphérique.
- **Model Name** : nom du modèle de périphérique.
- **Asset ID** : ID de la ressource.

VLAN et protocole 802.1

- **PVID** : ID VLAN annoncé pour le port.

PPVID

Table PPVID

- **VID** : ID VLAN du protocole.
- **Pris en charge** : ID VLAN de port et de protocole pris en charge.
- **Activés** : ID VLAN de port et de protocole activés.

ID VLAN

Table des ID VLAN

- **VID** : ID VLAN du port et du protocole.
- **Nom du VLAN** : noms des VLAN annoncés.

ID de protocole

- **ID du protocole** : ID de protocole annoncés.

Location Information (informations sur l'emplacement)

Saisissez les structures de données suivantes au format hexadécimal, conformément à la section 10.2.4 de la norme ANSI-TIA-1057 :

- **Physique** : adresse physique ou postale.
- **Coordonnées** : coordonnées géographiques de l'emplacement : latitude, longitude et altitude.

- **ECS ELIN** : numéro ELIN (Emergency Location Identification Number, numéro d'identification de l'emplacement en cas d'urgence) du périphérique pour l'ECS (Emergency Call Service, service d'appel d'urgence).
- **Inconnu** : informations d'emplacement inconnues.

Stratégies réseau

Network Policy Table (table des stratégies réseau)

- **Type d'application** : type d'application de la stratégie réseau. Exemple : Voix.
- **VLAN ID** : ID du VLAN pour lequel la stratégie réseau est définie.
- **Type VLAN** : type de VLAN pour lequel la stratégie réseau est définie, à savoir avec ou sans balise.
- **User Priority** : priorité d'utilisateur de la stratégie réseau.
- **DSCP** : DSCP de la stratégie réseau.

ÉTAPE 4 Sélectionnez un port et cliquez sur **Table d'état des ports LLDP** pour voir les détails dans la Table d'état des ports LLDP.

Statistiques LLDP

La page Statistiques LLDP affiche des informations statistiques concernant LLDP pour chaque port.

Pour afficher les statistiques LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Statistiques LLDP**.

Pour chaque port, les champs suivants sont affichés :

- **Interface** : identificateur d'interface.
- **Trames émises (total)** : nombre de trames transmises.
- **Trames reçues**
  - *Total* : nombre des trames reçues.
  - *Éliminé* : nombre des trames reçues qui ont été éliminées.
  - *Erreurs* : nombre total des trames reçues comportant des erreurs.

- **TLV reçues**
  - *Éliminé* : nombre total de TLV reçues qui ont été éliminées.
  - *Non reconnu* : nombre total de TLV reçues non reconnues.
- **Nombre de suppressions d'informations du voisin** : nombre d'expirations du délai maximal du voisin sur l'interface.

ÉTAPE 2 Cliquez sur **Actualiser** pour afficher les statistiques les plus récentes.

Surcharge LLDP

LLDP ajoute des informations telles que des TLV LLDP et LLDP MED dans les paquets LLDP. La surcharge LLDP se produit lorsque la quantité totale d'informations à inclure dans un paquet LLDP dépasse la taille PDU maximale prise en charge par une interface.

La page Surcharge LLDP affiche le nombre d'octets d'informations LLDP/LLDP-MED, le nombre d'octets disponibles pour les informations LLDP supplémentaires, ainsi que l'état de surcharge de chaque interface.

Pour afficher les informations de surcharge LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Surcharge LLDP**.

Cette page contient les champs suivants, pour chaque port :

- **Interface** : identificateur de port.
- **Octets totaux utilisés** : nombre total d'octets d'informations LLDP dans chaque paquet.
- **Available Bytes Left** : nombre total d'octets disponibles restants pour des informations LLDP supplémentaires dans chaque paquet.
- **État** : indique si des TLV sont en cours de transmission ou si une surcharge est intervenue.

ÉTAPE 2 Pour afficher les détails de surcharge d'un port, sélectionnez-le et cliquez sur **Détails**.

Cette page contient les informations suivantes pour chaque TLV envoyée sur le port :

- **LLDP Mandatory TLVs (TLV LLDP obligatoires)**
  - *Taille (octets)* : taille totale des TLV obligatoires, en octets.
  - *État* : indique si un groupe de TLV obligatoires est en cours de transmission ou si une surcharge est intervenue.

- **LLDP MED Capabilities (fonctionnalités LLDP MED)**
  - *Taille (octets)* : taille totale des paquets de fonctionnalités LLDP MED, en octets.
  - *État* : indique si les paquets de fonctionnalités LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **LLDP MED Location (emplacement LLDP MED)**
  - *Taille (octets)* : taille totale des paquets d'emplacement LLDP MED, en octets.
  - *État* : indique si les paquets d'emplacement LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **LLDP MED Network Policy (stratégie réseau LLDP MED)**
  - *Taille (octets)* : taille totale des paquets de stratégie réseau LLDP MED, en octets.
  - *État* : indique si les paquets de stratégie réseau LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **Alimentation LLDP MED étendue via MDI**
  - *Taille (octets)* : taille totale des paquets d'alimentation LLDP MED étendue via MDI, en octets.
  - *État* : indique si les paquets d'alimentation LLDP MED étendue via MDI ont été envoyés ou si une surcharge est intervenue.
- **802.3 TLVs (TLV 802.1)**
  - *Taille (octets)* : taille totale des paquets de TLV 802.3 LLDP MED, en octets.
  - *État* : indique si les paquets de TLV 802.3 LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **LLDP Optional TLVs (TLV LLDP facultatives)**
  - *Taille (octets)* : taille totale des paquets de TLV LLDP MED facultatives, en octets.
  - *État* : indique si les paquets de TLV LLDP MED facultatives ont été envoyés ou si une surcharge est intervenue.
- **LLDP MED Inventory (inventaire LLDP MED)**
  - *Taille (octets)* : taille totale des paquets de TLV d'inventaire LLDP MED, en octets.
  - *État* : indique si les paquets de TLV d'inventaire LLDP MED ont été envoyés ou si une surcharge est intervenue.

- **Total**
  - *Total (octets)* : nombre total d'octets d'informations LLDP dans chaque paquet.
  - *Octets restants disponibles* : nombre total d'octets disponibles restants pour envoyer des informations LLDP supplémentaires dans chaque paquet.

Configuration de CDP

Cette section explique comment configurer CDP.

Elle couvre les rubriques suivantes :

- **Propriétés CDP**
- **Paramètres d'interface CDP**
- **Informations locales CDP**
- **Informations de voisinage CDP**
- **Statistiques CDP**

Propriétés CDP

Comme LLDP, CDP (Cisco Discovery Protocol) est un protocole de couche de liaison permettant aux voisins à connexion directe de s'annoncer et de notifier mutuellement leurs fonctionnalités. Contrairement à LLDP, CDP est un protocole appartenant à Cisco.

Flux de travail de configuration de CDP

Vous trouverez ci-après un exemple de workflow pour la configuration de CDP sur le périphérique. Vous trouverez également des instructions de configuration de CDP supplémentaires à la section LLDP/CDP.

ÉTAPE 1 Entrez les paramètres globaux CDP sur la page Propriétés CDP.

ÉTAPE 2 Configurez CDP sur chaque interface via la page Paramètres d'interface.

ÉTAPE 3 Si la fonction Port intelligent automatique est utilisée pour détecter les fonctionnalités des périphériques CDP, activez CDP sur la page Propriétés des ports intelligents.

Reportez-vous à **Identification du Type de port intelligent** afin d'obtenir une description de la façon dont CDP est utilisé pour identifier les périphériques pour la fonction Port intelligent.

Pour saisir les paramètres généraux CDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - CDP** > **Propriétés**.

ÉTAPE 2 Saisissez les paramètres.

- **État CDP** : sélectionnez cette option pour activer CDP sur le périphérique.
- **Traitement des trames CDP** : si CDP n'est pas activé, sélectionnez l'action à réaliser en cas de réception d'un paquet correspondant aux critères sélectionnés :
  - *Pontage* : transfère le paquet basé sur le VLAN.
  - *Filtrage* : supprime le paquet.
  - *Inondation* : inondation ne tenant pas compte du VLAN qui transmet les paquets CDP entrants à tous les ports, sauf aux ports d'entrée.
- **Annonce VLAN voix CDP** : sélectionnez cette option pour permettre au périphérique d'annoncer le VLAN voix dans CDP sur tous les ports activés pour CDP et membres du VLAN voix. Vous pouvez configurer le VLAN voix sur la page Propriétés du VLAN voix.
- **Validation CDP des TLV obligatoires** : si cette option est sélectionnée, les paquets CDP entrants qui ne contiennent pas de TLV obligatoires sont éliminés et le compteur d'erreurs non valides est incrémenté.
- **CDP Version** : sélectionnez la version du protocole CDP à utiliser.
- **Délai d'attente CDP** : durée de conservation des paquets CDP avant leur élimination, en multiples de l'intervalle d'annonce TLV. Par exemple, si l'intervalle d'annonce TLV est de 30 secondes et que le multiplicateur de conservation (Hold Multiplier) est 4, les paquets LLDP seront supprimés après 120 secondes. Les options suivantes sont disponibles :
  - *Valeurs par défaut* : utilisez la durée par défaut (180 secondes).
  - *Défini par l'utilisateur* : saisissez la durée en secondes.
- **Niveau de transmission CDP** : fréquence (en secondes) d'envoi des mises à jour d'annonces CDP. Les options suivantes sont disponibles :
  - *Valeurs par défaut* : utilisez la fréquence par défaut (60 secondes).
  - *Défini par l'utilisateur* : saisissez la fréquence en secondes.

- **Format d'ID de périphérique** : sélectionnez le format de l'ID de périphérique (adresse MAC ou numéro de série). Les options suivantes sont disponibles :
  - *Adresse MAC* : utilisez l'adresse MAC du périphérique comme ID de périphérique.
  - *Numéro de série* : utilisez le numéro de série du périphérique comme ID de périphérique.
  - *Nom d'hôte* : utilisez le nom d'hôte du périphérique comme ID de périphérique.
- **Interface source** : adresse IP à utiliser dans la TLV des trames. Les options suivantes sont disponibles :
  - *Valeurs par défaut* : utilisez l'adresse IP de l'interface sortante.
  - *Défini par l'utilisateur* : utilisez l'adresse IP de l'interface (dans le champ **Interface**) dans la TLV d'adresse.
- **Interface** : si vous avez sélectionné *Défini par l'utilisateur* pour **Interface source**, sélectionnez l'interface.
- **Non-concordance VLAN voix Syslog** : cochez cette option pour envoyer un message SYSLOG lorsqu'une non-concordance VLAN voix est détectée. Cela signifie que les informations de VLAN voix dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.
- **Non-concordance VLAN natif Syslog** : cochez cette option pour envoyer un message SYSLOG lorsqu'une non-concordance VLAN natif est détectée. Cela signifie que les informations de VLAN natif dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.
- **Non-concordance duplex Syslog** : cochez cette option pour envoyer un message SYSLOG lorsque les informations duplex ne correspondent pas. Cela signifie que les informations duplex dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.

ÉTAPE 3 Cliquez sur **Apply**. Les propriétés LLDP sont définies.

Paramètres d'interface CDP

Utilisez la page Paramètres d'interface pour activer LLDP et la notification de serveur de journalisation distant par port et pour sélectionner les TLV incluses dans les PDU LLDP.

En définissant ces propriétés, il est possible de sélectionner les types d'informations à fournir aux périphériques qui prennent en charge le protocole LLDP.

Vous pouvez sélectionner les TLV LLDP MED à annoncer sur la page Paramètres d'interface LLDP MED.

Pour définir les paramètres d'interface CDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - CDP** > **Paramètres d'interface**.

Cette page affiche les informations CDP suivantes pour chaque interface.

- **CDP Status** : option de publication CDP pour le port.
- **Signalisation des conflits avec les voisins CDP** : état des options de rapport qui sont activées/désactivées sur la page **Modifier** (VLAN voix/VLAN natif/Duplex).
- **No. of Neighbors** : nombre de voisins détectés.

Quatre boutons sont disponibles en bas de la page :

- **Copier les paramètres** : sélectionnez ce bouton pour copier une configuration d'un port vers un autre.
- **Modifier** : les différents champs sont décrits à l'étape 2 ci-dessous.
- **Détails des informations locales CDP** : ouvre la page Administration > Détection - CDP > Informations locales CDP.
- **Détails des informations de voisinage CDP** : ouvre la page Administration > Détection - CDP > Informations de voisinage CDP.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier**.

Cette page contient les champs suivants :

- **Interface** : sélectionnez l'interface à définir.
- **État CDP** : sélectionnez cette option pour activer/désactiver l'option de publication CDP pour le port.

  REMARQUE Les trois champs suivants sont opérationnels si le périphérique a été configuré pour envoyer des interceptions à la station de gestion.

- **Non-concordance VLAN voix Syslog** : cochez cette option pour permettre l'envoi d'un message SYSLOG lorsqu'une non-concordance VLAN voix est détectée. Cela signifie que les informations de VLAN voix dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.
- **Non-concordance VLAN natif Syslog** : cochez cette option pour permettre l'envoi d'un message SYSLOG lorsqu'une non-concordance VLAN natif est détectée. Cela signifie que les informations de VLAN natif dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.
- **Non-concordance duplex Syslog** : cochez cette option pour permettre l'envoi d'un message SYSLOG lors de la détection d'informations duplex ne correspondant pas. Cela signifie que les informations duplex dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.

ÉTAPE 3 Saisissez les informations voulues et cliquez sur **Appliquer**. Les paramètres des ports sont écrits dans le fichier de Configuration d'exécution.

Informations locales CDP

Pour afficher les informations qui sont annoncées par le protocole CDP à propos du périphérique local :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - CDP** > **Informations locales CDP**.

ÉTAPE 2 Sélectionnez un port local ; les champs suivants s'affichent :

- **Interface** : numéro du port local.
- **État CDP** : indique si CDP est activé.
- **Device ID TLV (TLV d'ID de périphérique)**
  - **Type d'ID de périphérique** : type d'ID de périphérique annoncé dans la TLV d'ID de périphérique.
  - **ID de périphérique** : ID de périphérique annoncé dans la TLV d'ID de périphérique.
- **Durée de vie du nom du système**
  - **Nom du système** : nom système de l'appareil.
- **Address TLV (TLV de l'adresse)**
  - **Adresses 1-3** : adresses IP (annoncées dans la TLV d'adresse de périphérique).
- **Port TLV (TLV du port)**
  - **ID du port** : identificateur du port annoncé dans la TLV de port.
- **Capabilities TLV (TLV des fonctionnalités)**
  - **Fonctionnalités** : fonctionnalités annoncées dans la TLV de port.
- **Version TLV (TLV de la version)**
  - **Version** : informations sur la version logicielle sous laquelle le périphérique fonctionne.
- **Platform TLV (TLV de la plateforme)**
  - **Plate-forme** : identificateur de la plate-forme annoncée dans la TLV de plate-forme.
- **Native VLAN TLV (TLV du VLAN natif)**
  - **VLAN natif** : identificateur du VLAN natif annoncé dans la TLV de VLAN natif.
- **Full/Half Duplex TLV (TLV duplex intégral/semi-duplex)**
  - **Duplex** : port semi-duplex ou duplex intégral annoncé dans la TLV semi-duplex ou duplex intégral.

- **Appliance TLV (TLV du dispositif)**
  - **ID du dispositif** : type de périphérique associé au port annoncé dans la TLV de dispositif.
  - **ID du VLAN du dispositif** : VLAN du périphérique utilisé par le dispositif ; par exemple, si le dispositif est un téléphone IP, il s'agit du VLAN voix.
- **Extended Trust TLV (TLV de confiance étendue)**
  - **Confiance étendue** : l'activation de cette option indique que le port est sécurisé. L'hôte/serveur à partir duquel le paquet est reçu est ainsi sécurisé pour le marquage des paquets. Dans ce cas, les paquets reçus sur ce port ne sont pas marqués à nouveau. La désactivation de cette option indique que le port n'est pas validé, auquel cas le champ suivant peut être défini.
- **CoS for Untrusted Ports TLV (CoS pour le TLV des ports non validés)**
  - **CoS pour les ports non sécurisés** : si l'option Confiance étendue est désactivée sur le port, ce champ affiche la valeur CoS Layer 2, à savoir une valeur de priorité 802.1D/802.1p. Il s'agit de la valeur COS par l'intermédiaire de laquelle tous les paquets reçus sur un port non validé sont à nouveau marqués par le périphérique.
- **TLV de l'alimentation**
  - **ID de demande** : l'ID de dernière demande d'alimentation reçu correspond au dernier champ ID de demande reçu dans une TLV de demande d'alimentation. Sa valeur est 0 si aucune TLV de demande d'alimentation n'a été reçue depuis le dernier passage de l'interface vers l'état activé (Up).
  - **ID de gestion de l'alimentation** : valeur incrémentée de 1 (ou 2 pour éviter 0) à chaque fois que l'un des événements suivants se produit :

    La valeur des champs Puissance disponible ou Niveau de gestion d'alimentation change.

    Une TLV de demande d'alimentation est reçue avec un champ ID de demande différent du dernier ensemble reçu (ou à la réception de la première valeur).

    L'interface passe à l'état Désactivé.
  - **Puissance disponible** : puissance consommée par le port.
  - **Niveau de gestion d'alimentation** : affiche la demande du fournisseur au périphérique alimenté pour connaître sa TLV de consommation électrique. Le périphérique affiche toujours « Aucune préférence » dans ce champ.

Informations de voisinage CDP

La page Informations de voisinage CDP affiche les informations CDP reçues des périphériques voisins.

Après une temporisation (basée sur la valeur reçue du paramètre de durée de vie du voisin, durée au cours de laquelle aucune PDU CDP n'a été reçue d'un voisin), les informations sont supprimées.

Pour afficher les informations de voisinage CDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - CDP** > **Informations de voisinage CDP**.

ÉTAPE 2 Pour sélectionner un filtre, cochez la case **Filtre**, sélectionnez une interface locale et cliquez sur **OK**.

Le filtre est défini et la case **Effacer le filtre** est activée.

ÉTAPE 3 Cliquez sur **Effacer le filtre** pour supprimer le filtre.

La page Informations de voisinage CDP contient les champs suivants pour le partenaire de liaison (voisin) :

- **ID de périphérique** : ID de périphérique des voisins.
- **Nom du système** : nom du système des voisins.
- **Local Interface** : numéro du port local auquel le voisin est connecté.
- **Advertisement Version** : version du protocole CDP.
- **Durée de vie (sec.)** : durée en secondes à l'issue de laquelle les informations concernant ce voisin sont supprimées.
- **Capabilities** : fonctionnalités annoncées par le voisin.
- **Platform** : informations issues de la TLV de plate-forme du voisin.
- **Neighbor Interface** : interface sortante du voisin.

ÉTAPE 4 Sélectionnez un périphérique, puis cliquez sur **Détails**.

Cette page contient les champs suivants relatifs au voisin :

- **Device ID** : ID du périphérique de voisinage.
- **Nom du système** : nom de l'ID de périphérique de voisinage.
- **Local Interface** : numéro d'interface du port via lequel la trame a été reçue.
- **Advertisement Version** : version du protocole CDP.
- **Time to Live** : durée en secondes à l'issue de laquelle les informations concernant ce voisin sont supprimées.

- **Capabilities** : fonctions principales du périphérique. Les fonctionnalités sont indiquées par deux octets. Les bits 0 à 7 indiquent respectivement Autres, Répéteur, Pont, Point d'accès WLAN, Routeur, Téléphone, Système de câble DOCSIS et Station. Les bits 8 à 15 sont réservés.
- **Plate-forme** : identificateur de la plate-forme des voisins.
- **Neighbor Interface** : numéro d'interface du voisin via lequel la trame a été reçue.
- **VLAN natif** : VLAN natif du voisin.
- **Application** : nom de l'application qui s'exécute sur le voisin.
- **Duplex** : indique si l'interface de voisinage est semi-duplex ou duplex intégral.
- **Adresses** : adresses des voisins.
- **Alimentation prélevée** : puissance consommée par le voisin sur l'interface.
- **Version** : version logicielle des voisins.

REMARQUE En cliquant sur le bouton **Effacer la table**, vous déconnectez tous les périphériques connectés du CDP. Si la fonction Port intelligent automatique est activée, le système rétablit la valeur par défaut de tous les types de port.

Statistiques CDP

La page Statistiques CDP affiche des informations sur les trames CDP qui ont été envoyées ou reçues depuis un port. Les paquets CDP sont reçus des périphériques associés aux interfaces de commutateur et sont utilisés pour la fonction Port intelligent. Pour plus d'informations, reportez-vous à la section **Configuration de CDP**.

Les statistiques CDP d'un port ne s'affichent que si CDP est activé globalement et sur le port. Cette opération s'effectue sur les pages Propriétés CDP et Paramètres d'interface CDP.

Pour afficher les statistiques CDP :

ÉTAPE 1 Cliquez sur **Administration > Détection - CDP > Statistiques CDP**.

Les champs suivants sont affichés pour chaque interface :

Paquets reçus/transmis :

- **Version 1** : nombre de paquets CDP de version 1 reçus/transmis.
- **Version 2** : nombre de paquets CDP de version 2 reçus/transmis.
- **Total** : nombre total de paquets CDP reçus/transmis.

La section Statistiques d'erreurs CDP affiche les compteurs d'erreurs CDP.

- **Somme de contrôle incorrecte** : nombre de paquets reçus ayant une valeur de somme de contrôle incorrecte.
- **Autres erreurs** : nombre de paquets reçus comportant d'autres erreurs que des sommes de contrôle incorrectes.
- **Voisinages supérieurs au maximum** : nombre de fois que les informations de paquet n'ont pas pu être stockées dans le cache en raison d'un manque d'espace disponible.

Pour effacer tous les compteurs sur toutes les interfaces, cliquez sur **Effacer tous les compteurs de l'interface**. Pour effacer tous les compteurs sur une interface, sélectionnez-la et cliquez sur **Effacer les compteurs de l'interface**.

10

Gestion des ports

Cette section décrit la configuration des ports, l'agrégation de liaisons et la fonction Green Ethernet.

Elle couvre les rubriques suivantes :

- **Configuration des ports**
- **Détection de bouclage**
- **Agrégation de liaison**
- **UDLD**
- **Configuration de Green Ethernet**

Configuration des ports

Flux de travail

Pour configurer les ports, procédez comme suit :

1. Configurez le port sur la page Paramètres des ports.
2. Activez/désactivez le protocole LACP (Link Aggregation Control Protocol), puis configurez les ports membres potentiels sur les LAG souhaités via la page Gestion des LAG. Par défaut, tous les LAG sont vides.
3. Configurez les paramètres Ethernet, comme le débit et la négociation automatique pour les LAG, via la page Paramètres des LAG.
4. Configurez les paramètres LACP des ports membres d'un LAG ou candidats à l'adhésion à un LAG dynamique, via la page LACP.
5. Configurez Green Ethernet et 802.3 Energy Efficient Ethernet par l'intermédiaire de la page Propriétés.
6. Configurez le mode d'économie d'énergie Green Ethernet et 802.3 Energy Efficient Ethernet pour chaque port, via la page Paramètres des ports.
7. Si la PoE (Power on Ethernet, alimentation sur Ethernet) est prise en charge pour le périphérique concerné, configurez ce dernier en suivant les instructions de la rubrique **Gestion des ports : PoE**.

Configuration de port

Les ports peuvent être configurés dans les pages suivantes.

Paramètres des ports

La page Paramètres des ports affiche les paramètres globaux de tous les ports ainsi que ceux de chaque port. Cette page vous permet de sélectionner et de configurer les ports souhaités sur la page Modifier les paramètres de port.

Pour configurer les paramètres des ports :

ÉTAPE 1 Cliquez sur **Port Management** > **Port Settings**.

ÉTAPE 2 Sélectionnez **Trames Jumbo** pour prendre en charge les paquets dont les tailles sont inférieures ou égales à 10 Ko. Si l'option **Trames Jumbo** n'est pas activée (par défaut), le système prend en charge les tailles de paquets allant jusqu'à 2 000 octets. Pour que les trames Jumbo soient appliquées, vous devez redémarrer le périphérique une fois la fonction activée.

ÉTAPE 3 Cliquez sur **Appliquer** pour mettre à jour le paramètre global.

Les modifications apportées à la configuration des trames Jumbo sont *uniquement* appliquées après l'enregistrement explicite de la configuration d'exécution dans le fichier de Configuration de démarrage sur la page Copier/enregistrer la configuration et après le redémarrage du périphérique.

ÉTAPE 4 Pour mettre à jour les paramètres des ports, sélectionnez le port voulu et cliquez sur **Modifier**.

ÉTAPE 5 Modifiez les paramètres suivants :

- **Interface** : sélectionnez le numéro du port.
- **Port Description** : saisissez le nom défini par l'utilisateur pour ce port ou un commentaire.
- **Type de port** : affiche le type et le débit du port. Les options possibles sont les suivantes :
  - *Ports cuivre* : les ports standard, non mixtes, prennent en charge les valeurs suivantes : 10M, 100M et 1000M (type : Cuivre).
  - *Ports cuivre Combo* : un port Combo connecté à un câble cuivre CAT5 prend en charge les valeurs suivantes : 10M, 100M et 1000M (type : ComboC).
  - *Fibre Combo* : *un port GBIC (Gigabit Interface Converter*, convertisseur d'interface Gigabit) fibre SFP prend en charge les valeurs suivantes : 100M et 1000M (type : ComboF).
  - Fibre optique 10G : ports avec vitesse de 1G ou 10G.

REMARQUE La fibre SFP est prioritaire dans les ports mixtes lorsque les deux ports sont utilisés.

- **État administratif** : sélectionnez si le port doit être démarré ou arrêté au redémarrage du périphérique.
- **État opérationnel** : indique si le port est actuellement actif ou inactif. Si le port est fermé en raison d'une erreur, la description de cette erreur s'affiche.
- **Interceptions SNMP d'état de lien** : sélectionnez cette option pour activer la génération des interceptions SNMP notifiant que l'état du lien du port a subi des modifications.
- **Négociation automatique** : sélectionnez cette option pour activer la négociation automatique sur le port. La négociation automatique permet à un port d'annoncer sa vitesse de transmission, son mode duplex et ses fonctions de contrôle de flux à son partenaire de liaison.
- **Operational Auto Negotiation** : affiche l'état actuel de la négociation automatique sur le port.
- **Vitesse du port administratif** : sélectionnez la vitesse du port. Le type de port détermine les vitesses disponibles. Vous ne pouvez choisir *Vitesse administrative* que si la négociation automatique est désactivée pour le port.
- **Operational Port Speed** : affiche le débit actuel du port, obtenu par négociation.
- **Mode duplex administratif** : sélectionnez le mode duplex du port. Ce champ ne peut être configuré que lorsque la négociation automatique est désactivée et que le débit du port est réglé sur 10M ou 100M. Lorsque le port a un débit de 1G, le mode est toujours Duplex intégral. Les options possibles sont les suivantes :
  - *Semi-duplex* : l'interface prend en charge la transmission entre le périphérique et le client dans une seule direction à la fois.
  - *Duplex intégral* : l'interface prend en charge la transmission entre le périphérique et le client dans les deux directions simultanément.
- **Mode duplex opérationnel** : affiche le mode duplex actuel des ports.
- **Annonce automatique** : sélectionnez les fonctionnalités annoncées par la négociation automatique lorsqu'elle est activée. Les options sont les suivantes :
  - *Capacité maximale* : tous les débits de port et paramètres de mode duplex sont acceptés.
  - *10 Semi-duplex* : débit de 10 Mbits/s et mode Semi-duplex.
  - *10 Duplex intégral* : débit de 10 Mbits/s et mode Duplex intégral.
  - *100 Semi-duplex* : débit de 100 Mbits/s et mode Semi-duplex.
  - *100 Duplex intégral* : débit de 100 Mbits/s et mode Duplex intégral.
  - *1 000 Duplex intégral* : débit de 1 000 Mbits/s et mode Duplex intégral.
- **Annonce opérationnelle** : affiche les fonctionnalités actuellement publiées à l'attention du voisin des ports. Les options disponibles sont celles spécifiées dans le champ *Annonce administrative*.

- **Mode Préférence** : sélectionnez le mode unité principale/asservie de l'interface pour l'opération de négociation automatique. Sélectionnez une des options suivantes :
  - *Unité asservie* : commencez la négociation avec la préférence selon laquelle le port du périphérique est l'esclave dans le processus de négociation automatique.
  - *Unité principale* : commencez la négociation avec la préférence selon laquelle le port du périphérique est le maître dans le processus de négociation automatique.
- **Annonce de voisin** : affiche les fonctionnalités publiées par le périphérique de voisinage réseau (partenaire de liaison).
- **Contre-pression** : sélectionnez le mode de contre-pression du port (utilisé en mode Semi-duplex) à appliquer pour ralentir la vitesse de réception des paquets en cas de surcharge du périphérique. Cela désactive le port distant, ce qui l'empêche d'envoyer des paquets en brouillant le signal.
- **Contrôle de flux** : activez ou désactivez le contrôle de flux 802.3x ou activez la négociation automatique du contrôle de flux sur le port (uniquement en mode Duplex intégral).
- **MDI/MDIX** : *état MDI (Media Dependent Interface*, interface dépendant du support)/*MDIX (Media Dependent Interface with Crossover*, interface dépendant du support avec croisement) sur le port.

  Les options sont les suivantes :
  - *MDIX* : sélectionnez cette option pour permuter les paires d'émission et de réception du port.
  - *MDI* : sélectionnez cette option pour relier ce périphérique à une station de travail via un câble droit.
  - *Auto* : sélectionnez cette option pour configurer le périphérique afin qu'il détecte automatiquement le brochage correct pour la connexion à un autre périphérique.
- **MDI/MDIX opérationnel** : affiche le paramètre MDI/MDIX actuel.
- **Membre dans LAG** : indique si le port est membre d'un LAG.

ÉTAPE 6 Cliquez sur **Appliquer**. Les paramètres des ports sont écrits dans le fichier de Configuration d'exécution.

Paramètres de récupération d'erreur

Cette page permet de réactiver automatiquement un port qui a été fermé en raison d'une condition d'erreur à l'issue de l'intervalle de récupération automatique.

Pour configurer les paramètres de reprise sur erreur :

ÉTAPE 1 Cliquez sur **Port Management** > **Error Recovery Settings**.

ÉTAPE 2 Renseignez les champs suivants :

- **Intervalle de récupération automatique** : spécifie le délai de la récupération d'erreur automatique, si elle est activée, après la fermeture d'un port

Récupération ErrDisable automatique

- **Sécurité des ports** : sélectionnez cette option pour activer la récupération d'erreur automatique lorsque le port a été fermé en raison d'une violation de la sécurité des ports.
- **Violation d'hôte unique 802.1x** : sélectionnez cette option pour activer la récupération d'erreur automatique lorsque le port a été fermé par 802.1x.
- **Protection de bouclage STP** : activez la récupération automatique lorsque le port a été fermé par une protection de bouclage STP.
- **Détection de bouclage** : sélectionnez cette option pour activer le mécanisme de récupération d'erreur pour les ports fermés par la détection de bouclage.

ÉTAPE 3 Cliquez sur **Appliquer** pour mettre à jour le paramètre global.

Pour réactiver manuellement un port :

ÉTAPE 1 Cliquez sur **Port Management** > **Error Recovery Settings**.

La liste des interfaces désactivées et leur **Motif de la suspension** s'affichent.

ÉTAPE 2 Sélectionnez l'interface que vous souhaitez réactiver.

ÉTAPE 3 Cliquez sur **Réactiver**.

Détection de bouclage

La détection de bouclage (LBD) empêche la formation de boucles en transmettant les paquets de protocole de bouclage vers les ports sur lesquels la protection de bouclage a été activée. Lorsque le commutateur envoie un paquet de protocole de bouclage, puis reçoit le même paquet, il ferme le port qui a reçu le paquet.

La détection de bouclage fonctionne indépendamment de STP. Une fois qu'une boucle a été détectée, le port qui l'a reçue est placé dans l'état Arrêter (fermé). Une interception est envoyée et l'événement est consigné. Les gestionnaires de réseau peuvent définir un intervalle de détection qui définit l'intervalle de temps entre les paquets LBD.

Les cas de boucle suivants peuvent être détectés à l'aide du protocole de détection de bouclage :

- **Câble court-circuité** : port qui renvoie en boucle tout le trafic reçu.

- **Direct multi-ports loop (Diriger la boucle multi-ports)** : le commutateur est connecté à un autre commutateur avec plusieurs ports et STP est désactivé.
- **LAN segment loop (Boucle de segment LAN)** : le commutateur est connecté avec un ou plusieurs ports à un segment LAN qui comporte des boucles.

Fonctionnement de LBD

Le protocole LBD diffuse régulièrement des paquets de détection de bouclage. Un commutateur détecte une boucle lorsqu'il reçoit ses propres paquets LBD.

Les conditions suivantes doivent être remplies pour que la fonctionnalité LBD d'un port soit active :

- La fonction LBD est activée globalement.
- La fonction LBD est activée sur le port.
- L'état opérationnel du port est actif.
- Le port se trouve dans l'état STP de redirection ou désactivé (état de redirection d'instance MSTP, instance 0).

Les trames LBD sont transmises sur la file d'attente de priorité la plus élevée sur les ports LBD actifs (avec les LAG, le paquet LBD est transmis sur chaque membre de port actif dans le LAG).

Lorsqu'une boucle est détectée, le commutateur effectue les actions suivantes :

- Il définit les LAG ou les ports de réception sur l'état de désactivation d'erreur.
- Il émet une interception SNMP appropriée.
- Il génère un message SYLOG approprié.

Configuration de la détection de bouclage

Configuration et paramètres par défaut

La détection de bouclage n'est pas activée par défaut.

Interactions avec les autres fonctions

Si STP est activé sur un port sur lequel la détection de bouclage est activée, ce port doit se trouver dans l'état de redirection STP.

Configuration du workflow LBD

Pour activer et configurer LBD :

ÉTAPE 1 Activez la détection de bouclage à l'échelle du système sur la page des paramètres de détection du bouclage.

ÉTAPE 2 Activez la détection de bouclage sur les ports d'accès sur la page des paramètres de détection du bouclage.

ÉTAPE 3 Activez la récupération automatique pour la détection du bouclage sur la page Paramètres de récupération d'erreur.

Pour configurer la détection du bouclage :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Paramètres de détection du bouclage**.

ÉTAPE 2 Sélectionnez **Activer** dans le champ global **Détection de bouclage** afin d'activer cette fonction.

ÉTAPE 3 Entrez l'**intervalle de détection**. Il s'agit de l'intervalle entre les transmissions de paquets LBD.

ÉTAPE 4 Cliquez sur **Appliquer** pour enregistrer la configuration dans le fichier de Configuration d'exécution.

Les champs suivants s'affichent pour chaque interface pour indiquer l'**état de détection du bouclage** :

- **Administratif** : la détection du bouclage est activée.
- **Opérationnel** : la détection du bouclage est activée, mais elle n'est pas active sur l'interface.

ÉTAPE 5 Choisissez s'il faut activer LBD sur les ports ou les LAG dans le champ **Interface Type equals (Type d'interface égal à)**.

ÉTAPE 6 Sélectionnez les ports ou les LAG sur lesquels LBD doit être activé, puis cliquez sur **Modifier**.

ÉTAPE 7 Sélectionnez **Activer** dans le champ d'état de détection du bouclage pour le port ou le LAG sélectionné.

ÉTAPE 8 Cliquez sur **Appliquer** pour enregistrer la configuration dans le fichier de Configuration d'exécution.

Agrégation de liaison

Cette section explique comment configurer les LAG. Elle couvre les rubriques suivantes :

- **Présentation de l'agrégation de liaisons**
- **Configuration et paramètres par défaut**
- **Flux de travail des LAG statiques et dynamiques**
- **Définition de la gestion des LAG**
- **Configuration des paramètres des LAG**
- **Configuration de LACP**

Présentation de l'agrégation de liaisons

Le protocole LACP (Link Aggregation Control Protocol, protocole de contrôle de l'agrégation de liaisons) fait partie de la spécification IEEE (802.3az) qui vous permet de regrouper plusieurs ports physiques en un seul canal logique (LAG). Les LAG multiplient la bande passante, augmentent la souplesse des ports et établissent une redondance de liaisons entre deux périphériques.

Deux types de LAG sont pris en charge :

- **Statique** : un LAG est statique si le protocole LACP (Link Aggregation Control Protocol) est désactivé sur celui-ci. Les ports attribués à un LAG statique sont toujours des membres actifs. Une fois qu'un LAG a été créé manuellement, l'option LACP ne peut pas être ajoutée ni supprimée tant que le LAG n'a pas été modifié et qu'un membre n'a pas été supprimé (celui-ci pouvant être ajouté avant l'application). Le bouton LACP devient alors disponible pour la modification.
- **Dynamic** : un LAG est dynamique si le protocole LACP est activé sur celui-ci. Les ports attribués à un LAG dynamique sont des ports candidats. Le protocole LACP détermine les ports candidats qui sont des ports membres actifs. Les ports candidats non actifs sont des ports *de réserve* prêts à remplacer n'importe quel port membre actif défaillant.

Équilibrage de charge

La charge du trafic transféré à un LAG est équilibrée entre les divers ports qui sont des membres actifs. Ceci permet d'obtenir une bande passante effective proche du total cumulé des bandes passantes de tous les membres actifs du LAG.

L'équilibrage de charge du trafic sur les ports membres actifs d'un LAG est géré par une fonction de distribution par hachage, qui répartit le trafic de diffusion et de multidiffusion sur la base des informations d'en-tête de paquet Couche 2 ou Couche 3.

Le périphérique prend en charge deux modes d'équilibrage de charge :

- **Selon les adresses MAC** : traitement basé sur les adresses MAC source et cible de tous les paquets.
- **Par les adresses IP et MAC** : traitement basé sur les adresses IP source et cible pour les paquets IP. Pour les paquets non-IP, traitement basé sur les adresses MAC source et cible.

Gestion des LAG

En général, un LAG est traité par le système comme étant un seul port logique. En particulier, le LAG comporte des attributs semblables à ceux d'un port unique, notamment son état et son débit.

Le périphérique peut prendre huit LAG en charge.

Chaque LAG possède les caractéristiques suivantes :

- Tous les ports d'un LAG doivent disposer du même type de support.
- Pour que vous puissiez ajouter un port au LAG, il ne doit appartenir à aucun autre VLAN que le VLAN par défaut.
- Les ports d'un LAG ne doivent être affectés à aucun autre LAG.
- Il est impossible d'affecter plus de huit ports à un LAG statique. Il est également impossible de définir plus de 16 ports comme candidats à un LAG dynamique.
- Bien que cette fonction puisse être activée sur le LAG, vous devez désactiver la négociation automatique sur tous les ports d'un LAG.
- Lorsqu'un port est ajouté à un LAG, la configuration du LAG est appliquée au port. Lorsque vous retirez ce port du LAG, il reprend sa configuration d'origine.
- Les divers protocoles, tels que le protocole d'arbre recouvrant (STP, Spanning Tree Protocol), considèrent tous les ports d'un LAG comme étant un port unique.

Configuration et paramètres par défaut

Par défaut, les ports ne sont pas membres d'un LAG et ne sont pas candidats pour l'appartenance à un LAG.

Flux de travail des LAG statiques et dynamiques

Une fois qu'un LAG a été manuellement créé, le protocole LACP ne peut être ni ajouté ni supprimé tant que le LAG n'est pas modifié et qu'aucun membre n'est supprimé. C'est seulement à cette condition que le bouton LACP deviendra disponible pour la modification.

Pour configurer un LAG **statique**, procédez comme suit :

1. Désactivez LACP sur le LAG pour le rendre statique. Attribuez jusqu'à huit ports membres au LAG statique. Pour ce faire, sélectionnez les ports et déplacez-les de la **Liste des ports** vers la liste **Membres de LAG**. Sélectionnez l'algorithme d'équilibrage de charge pour le LAG. Effectuez ces actions sur la page Gestion des LAG.
2. Configurez les divers aspects du LAG, comme la vitesse et le contrôle de flux, via la page Paramètres des LAG.

Pour configurer un LAG **dynamique**, procédez comme suit :

1. Activez le protocole LACP sur le LAG. Attribuez jusqu'à 16 ports candidats au LAG dynamique. Pour ce faire, sélectionnez les ports et déplacez-les de la **Liste des ports** vers la liste **Membres de LAG**, sur la page Gestion des LAG.
2. Configurez les divers aspects du LAG, comme la vitesse et le contrôle de flux, via la page Paramètres des LAG.
3. Configurez la priorité et le délai LACP des ports du LAG, via la page LACP.

Définition de la gestion des LAG

La page Gestion des LAG affiche les paramètres globaux ainsi que ceux de chaque LAG. Cette page vous permet également de configurer les paramètres globaux, mais aussi de sélectionner et de modifier le LAG souhaité sur la page Modifier l'appartenance du LAG.

Pour sélectionner l'algorithme d'équilibrage de charge du LAG :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Agrégation de liaisons** > **Gestion des LAG**.

ÉTAPE 2 Sélectionnez l'un des **algorithmes d'équilibrage de charge** suivants :

- *Adresse MAC* : équilibrage de charge basé sur les adresses MAC source et cible de tous les paquets.
- *Adresse IP/MAC* : équilibrage de charge basé sur les adresses IP source et cible pour les paquets IP. Pour les paquets non-IP, traitement basé sur les adresses MAC source et cible.

ÉTAPE 3 Cliquez sur **Apply**. L'algorithme d'équilibrage de charge est enregistré dans le fichier de Configuration d'exécution.

Pour définir les ports membres ou candidats dans un LAG :

ÉTAPE 1 Sélectionnez le LAG à configurer et cliquez sur **Modifier**.

Les champs suivants sont affichés pour chaque LAG (seuls les champs ne figurant pas sur la page Modifier font l'objet d'une description) :

- **État des liaisons** : indique si le port est actif ou inactif.
- **Membre actif** : ports actifs dans le LAG.
- **Membre de réserve** : ports candidats pour ce LAG.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **LAG** : sélectionnez le numéro du LAG.
- **Nom du LAG** : saisissez le nom du LAG ou un commentaire.
- **LACP** : sélectionnez cette option pour activer LACP sur le LAG sélectionné. Ceci en fait un LAG dynamique. Vous ne pouvez activer ce champ qu'après avoir déplacé un port vers le LAG dans le champ suivant.
- **Liste des ports** : déplacez les ports à attribuer au LAG de la **Liste des ports** vers la liste **Membres de LAG**. Vous pouvez affecter jusqu'à huit ports à un LAG statique et jusqu'à 16 ports à un LAG dynamique. Il s'agit de ports candidats.

ÉTAPE 3 Cliquez sur **Apply**. L'appartenance LAG est enregistrée dans le fichier de Configuration d'exécution.

Configuration des paramètres des LAG

La page Paramètres des LAG affiche une table des paramètres actuels de tous les LAG. Vous pouvez configurer les paramètres des LAG sélectionnés et réactiver les LAG suspendus sur la page Modifier les paramètres des LAG.

Pour configurer les paramètres des LAG ou réactiver un LAG suspendu :

ÉTAPE 1 Cliquez sur **Port Management** > **Link Aggregation** > **LAG Settings**.

ÉTAPE 2 Sélectionnez un LAG et cliquez sur **Edit**.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **LAG** : sélectionnez l'ID du LAG.
- **LAG Type** : affiche le type de port inclus dans le LAG.
- **Description** : saisissez le nom du LAG ou un commentaire.

- **État administratif** : définissez le LAG sélectionné comme étant démarré ou arrêté.
- **Operational Status** : indique si le LAG est actuellement opérationnel.
- **Interceptions SNMP d'état de lien** : sélectionnez cette option pour activer la génération des interceptions SNMP notifiant que l'état du lien des ports a subi des modifications dans le LAG.
- **Réactiver le LAG suspendu** : sélectionnez cette option pour réactiver un port si le LAG a été désactivé via l'option de sécurité de verrouillage des ports <300-500>ou via des configurations ACL.
- **Négociation automatique administrative** : permet d'activer ou de désactiver la négociation automatique sur le LAG. La négociation automatique est un protocole établi entre deux partenaires de liaison qui permet à un LAG d'annoncer sa vitesse de transmission et son contrôle de flux à son partenaire (la valeur par défaut pour le contrôle de flux est *Désactivé*). Il est recommandé de maintenir la négociation automatique activée des deux côtés d'une liaison agrégée (ou de la désactiver des deux côtés), tout en s'assurant que les débits de liaison sont identiques.
- **Négociation automatique opérationnelle** : affiche le paramètre de négociation automatique.
- **Débit administratif** : sélectionnez le débit du LAG.
- **Operational LAG Speed** : affiche le débit actuel de fonctionnement du LAG.
- **Annonce administrative** : sélectionnez les fonctionnalités que le LAG doit annoncer. Les options sont les suivantes :
  - *Capacité maximale* : tous les débits de LAG et modes duplex sont acceptés.
  - *10 Duplex intégral* : le LAG annonce un débit de 10 Mbits/s et le mode est Duplex intégral.
  - *100 Duplex intégral* : le LAG annonce un débit de 100 Mbits/s et le mode est Duplex intégral.
  - *1 000 Duplex intégral* : le LAG annonce un débit de 1 000 Mbits/s et le mode est Duplex intégral.
  - *10000 Duplex intégral* : le LAG annonce un débit de 10000 Mbits/s et le mode est Duplex intégral.
- **Annonce opérationnelle** : affiche l'état d'annonce administrative. Le LAG annonce ses capacités à son LAG voisin pour lancer le processus de négociation. Les options disponibles sont celles spécifiées dans le champ *Annonce administrative*.
- **Contrôle de flux administratif** : définissez le contrôle de flux à **Activer** ou **Désactiver**, ou activez la **négociation automatique** du contrôle de flux sur le LAG.
- **Contrôle de flux opérationnel** : affiche le paramètre de contrôle de flux actuel.

ÉTAPE 4 Cliquez sur **Appliquer**. Le fichier de configuration de fonctionnement est mis à jour.

Configuration de LACP

Un LAG dynamique est un LAG où LACP est activé ; le protocole LACP (Link Aggregation Control Protocol, protocole de contrôle de l'agrégation de liaisons) est exécuté sur chaque port candidat défini dans le LAG.

Priorité et règles LACP

Les options Priorité du système LACP et Priorité des ports LACP déterminent les ports candidats qui deviennent des ports membres actifs d'un LAG dynamique configuré avec plus de huit ports candidats.

Les ports candidats sélectionnés pour le LAG sont tous connectés au même périphérique distant. Les commutateurs locaux et distants sont associés à une priorité du système LACP.

L'algorithme suivant permet de déterminer si les priorités des ports LACP doivent être obtenues du périphérique local ou du périphérique distant : la priorité du système LACP du périphérique local est comparée à la priorité du système LACP du périphérique distant. Le périphérique ayant la priorité la plus basse contrôle la sélection de ports candidats pour le LAG. Si les deux priorités sont identiques, les adresses MAC locale et distante sont comparées. La priorité du périphérique ayant l'adresse MAC la plus basse contrôle la sélection de ports candidats pour le LAG.

Un LAG dynamique peut comporter jusqu'à 16 ports Ethernet du même type. Huit ports au maximum peuvent être actifs et huit ports au maximum peuvent être en mode de réserve. Si un LAG dynamique comprend plus de huit ports, le périphérique situé du côté qui contrôle la liaison applique les priorités de port pour déterminer les ports agrégés dans le LAG et ceux qui restent en mode de réserve à chaud. Les priorités des ports de l'autre périphérique (du côté de la liaison qui n'a pas le contrôle) sont ignorées.

Les règles supplémentaires permettant de sélectionner des ports actifs ou de réserve dans un LACP dynamique sont les suivantes :

- Toute liaison fonctionnant avec un débit différent de celui du membre actif ayant le débit le plus élevé ou fonctionnant en mode semi-duplex est désignée comme étant celle de réserve. Tous les ports actifs d'un LAG dynamique fonctionnent avec le même débit en bauds.
- Si la priorité LACP du port de la liaison est inférieure à celle des membres de liaison actuellement actifs et si le nombre maximal de membres actifs a déjà été atteint, la liaison devient inactive et est placée en mode de réserve.

LACP sans membre de liaison

Pour que le protocole LACP puisse créer un LAG, vous devez configurer les ports situés aux deux extrémités du lien pour LACP, ce qui signifie que les ports envoient des PDU LACP et gèrent les PDU reçues.

Toutefois, un partenaire de liaison peut être temporairement non configuré pour LACP. Par exemple, lorsque le partenaire de liaison est sur un périphérique qui est en cours de réception de sa configuration via le protocole de configuration automatique. Les ports de ce périphérique ne sont pas encore configurés pour LACP. Si la liaison LAG ne s'établit pas, le périphérique ne peut pas être configuré. Un cas similaire se produit avec les ordinateurs à amorçage réseau par double carte (PXE par exemple), qui reçoivent leur configuration LAG uniquement après leur démarrage.

Lorsque vous configurez plusieurs ports LACP et que la liaison est activée sur un ou plusieurs ports, mais que ces derniers restent sans réponse LACP de la part du partenaire de liaison, le premier port dont la liaison a été activée est ajouté au LAG LACP et devient actif (les autres ports deviennent non-candidats). Ainsi, le périphérique voisin peut, par exemple, obtenir son adresse IP via DHCP et obtenir sa configuration via la configuration automatique.

Configuration des paramètres LACP

Utilisez la page LACP pour configurer les ports candidats au LAG et pour configurer les paramètres LACP pour chaque port.

Lorsque tous les facteurs sont égaux, si le LAG est configuré avec davantage de ports candidats que le maximum de ports actifs autorisé (8), le périphérique sélectionne des ports et les marque comme actifs à partir du LAG dynamique dont la priorité est la plus élevée sur le périphérique.

REMARQUE Le paramètre LACP ne s'applique pas aux ports qui ne sont pas membres d'un LAG dynamique.

Pour définir les paramètres LACP :

ÉTAPE 1 Cliquez sur **Port Management** > **Link Aggregation** > **LACP**.

ÉTAPE 2 Saisissez la priorité du système LACP. Reportez-vous à la section **Priorité et règles LACP**.

ÉTAPE 3 Sélectionnez un port et cliquez sur **Modifier**.

ÉTAPE 4 Saisissez les valeurs pour les champs suivants :

- **Port** : sélectionnez le numéro du port auquel s'appliquent les valeurs de délai et de priorité.
- **Priorité des ports LACP** : saisissez la valeur de priorité LACP du port. Reportez-vous à la section **Configuration des paramètres LACP**.
- **Délai LACP** : intervalle qui sépare l'envoi et la réception de deux PDU LACP consécutives. Sélectionnez les transmissions périodiques des PDU LACP, qui s'effectuent à une vitesse de transmission **longue** ou **courte**, selon la préférence de délai LACP définie.

ÉTAPE 5 Cliquez sur **Apply**. Le fichier de configuration de fonctionnement est mis à jour.

UDLD

Reportez-vous à la section **Gestion des ports : Unidirectional Link Detection**.

PoE

Reportez-vous à la section **Gestion des ports : PoE**.

Configuration de Green Ethernet

Cette section décrit la fonction Green Ethernet qui est conçue pour réduire la consommation d'énergie du périphérique.

Elle contient les sections suivantes :

- **Présentation de la fonction Green Ethernet**
- **Propriétés Green Ethernet globales**
- **Propriétés Green Ethernet des ports**

Présentation de la fonction Green Ethernet

Green Ethernet est le nom d'usage d'un ensemble de fonctions conçues pour respecter l'environnement et réduire la consommation électrique d'un périphérique. La fonction Green Ethernet est différente de EEE, puisque la détection d'énergie Green Ethernet est activée sur tous les périphériques alors qu'avec EEE, seuls les ports Giga-octets sont activés.

La fonction Green Ethernet réduit la consommation énergétique globale comme suit :

- **Mode Détection d'énergie** : sur une liaison inactive, le port passe en mode inactif, ce qui permet d'économiser l'énergie tout en maintenant le port à l'état administratif Démarré. La sortie de ce mode et le retour au mode entièrement opérationnel sont rapides, transparents et sans aucune perte de trame. Ce mode est pris en charge sur les ports GE comme sur les ports FE.
- **Mode Courte portée** : cette fonction permet d'économiser de l'énergie sur une courte longueur de câble. Une fois que la longueur du câble a été analysée, la consommation d'énergie est ajustée en fonction de cette longueur. Si la longueur de câble est inférieure à 50 mètres, le périphérique a besoin de moins de puissance pour envoyer des trames sur ce câble, ce qui représente une économie d'énergie. Ce mode n'est pris en charge que sur les ports GE RJ45 ; il ne s'applique pas aux ports mixtes.

Par défaut, ce mode est désactivé au niveau global. Il ne peut pas être activé si le mode EEE est activé (voir ci-dessous).

Outre les fonctions Green Ethernet ci-dessus, la fonction **802.3az Energy Efficient Ethernet (EEE)** est disponible sur les périphériques prenant en charge les ports GE. EEE réduit la consommation électrique lorsqu'il n'y a pas de trafic sur le port. Pour plus d'informations, reportez-vous à **Fonction 802.3az Energy Efficient Ethernet** (uniquement sur les modèles GE).

EEE est activé par défaut au niveau global. Sur un port donné, si EEE est activé, le mode Courte portée est désactivé. Si le mode Courte portée est activé, EEE apparaît en grisé.

Ces modes peuvent être configurés pour chaque port, sans tenir compte de l'appartenance au LAG des ports.

Les LED des périphériques consomment de l'énergie. Étant donné que les périphériques se situent la plupart du temps dans une pièce inoccupée, le fait de maintenir ces LED allumées est un gaspillage d'énergie. La fonction Green Ethernet permet de désactiver les LED des ports (liaison, vitesse et PoE) lorsqu'elles ne sont pas nécessaires et de les activer lorsqu'elles le sont (débogage, raccordement de périphériques supplémentaires, etc.).

Sur la page Récapitulatif système, les LED qui sont représentées sur les illustrations des cartes des périphériques ne sont pas affectées par la désactivation des LED.

Il est possible de contrôler les économies d'énergie, la consommation électrique actuelle et l'énergie totale économisée. La quantité totale d'énergie économisée est affichée sous la forme d'un pourcentage de l'énergie qu'auraient consommé les interfaces physiques sans le mode Green Ethernet.

L'énergie économisée s'affiche uniquement si elle est liée à la fonction Green Ethernet. La quantité d'énergie économisée par EEE n'apparaît pas.

Économie d'énergie par la désactivation des LED de port

La fonctionnalité de désactivation des LED des ports permet d'économiser l'énergie consommée par les LED des périphériques. Étant donné que les périphériques se trouvent souvent dans une pièce inoccupée, le fait de maintenir ces LED allumées est un gaspillage d'énergie. La fonction Green Ethernet permet de désactiver les LED des ports (liaison, vitesse et PoE) lorsqu'elles ne sont pas nécessaires et de les activer lorsqu'elles le sont (débogage, raccordement de périphériques supplémentaires, etc.).

Sur la page Récapitulatif système, les LED qui sont représentées sur les illustrations des cartes des périphériques ne sont pas affectées par la désactivation des LED.

Les LED des ports peuvent être désactivées sur la page Green Ethernet -> Propriétés.

Fonction 802.3az Energy Efficient Ethernet

Cette section décrit la fonction 802.3az Energy Efficient Ethernet (EEE).

Elle couvre les rubriques suivantes :

- **Présentation de 802.3az EEE**
- **Négociation des fonctionnalités d'annonce**
- **Détection du niveau de liaison pour 802.3az EEE**
- **Disponibilité de 802.3az EEE**
- **Configuration par défaut**
- **Interactions entre les fonctions**
- **Flux de travail de configuration de 802.3az EEE**

Présentation de 802.3az EEE

802.3az EEE est conçue pour réduire la consommation énergétique lorsqu'il n'y a pas de trafic sur la liaison. Dans Green Ethernet, la consommation est réduite lorsque le port est inactif. Avec 802.3az EEE, la consommation est réduite lorsque le port est actif, mais qu'il n'y a pas de trafic sur celui-ci.

La fonction 802.3az EEE est uniquement prise en charge sur les périphériques utilisant des ports GE.

Lorsque vous utilisez la fonction 802.3az EEE, les systèmes situés aux deux extrémités de la liaison peuvent désactiver une partie de leurs fonctionnalités et économiser de l'énergie au cours des périodes sans trafic.

802.3az EEE prend en charge le fonctionnement IEEE 802.3 MAC à 100 Mbits/s et 1 000 Mbits/s :

LLDP permet de sélectionner un ensemble optimal de paramètres pour les deux périphériques. Si LLDP n'est pas pris en charge par le partenaire de liaison ou s'il est désactivé, la fonction 802.3az EEE reste opérationnelle, mais n'utilise peut-être pas le mode opérationnel optimal.

La fonction 802.3az EEE est implémentée via le mode de port LPI (Low Power Idle). Lorsqu'il n'y a pas de trafic et que cette fonction est activée sur le port, ce dernier passe en mode LPI, ce qui réduit de manière importante la consommation énergétique.

Les deux extrémités d'une connexion (le port du périphérique et le périphérique en cours de connexion) doivent prendre en charge 802.3az EEE pour qu'elle fonctionne. Lorsqu'il n'y a aucun trafic, les deux extrémités envoient des signaux indiquant que la consommation va être réduite. Lorsque les signaux provenant des deux extrémités sont reçus, le signal Maintenir actif indique que les ports ont l'état LPI (et non l'état Inactif) et que la consommation est réduite.

Pour que les ports restent en mode LPI, le signal Maintenir actif doit être reçu en continu des deux extrémités.

Négociation des fonctionnalités d'annonce

La prise en charge de la fonction 802.3az EEE est annoncée lors de le phase de négociation automatique. La négociation automatique permet au périphérique lié de détecter les fonctionnalités (modes de fonctionnement) prises en charge par le périphérique situé à l'autre extrémité de la liaison, de déterminer les fonctionnalités communes et de se configurer lui-même pour un fonctionnement conjoint. La négociation automatique s'effectue au moment de la connexion, lors d'une commande exécutée par le système de gestion ou lors de la détection d'une erreur de liaison. Au cours du processus d'établissement de la liaison, les deux partenaires de liaison échangent leurs fonctionnalités 802.3az EEE. La négociation automatique fonctionne automatiquement sans interaction de l'utilisateur lorsqu'elle est activée sur le périphérique.

REMARQUE Si la négociation automatique n'est pas activée sur un port, la fonction EEE est désactivée. La seule exception est que si la vitesse de la liaison est de 1 Go ; la fonction EEE est toujours activée même si la négociation automatique est désactivée.

Détection du niveau de liaison pour 802.3az EEE

Outre les fonctionnalités décrites ci-dessus, les fonctionnalités et paramètres 802.3az EEE sont également annoncés par le biais de trames qui sont basées sur les TLV spécifiques à l'organisation et définies dans l'annexe G du protocole IEEE Std 802.1AB (LLDP). LLDP permet d'optimiser encore davantage le fonctionnement de 802.3az EEE une fois que la négociation automatique est terminée. La TLV 802.3az EEE permet de définir précisément le réveil et les durées d'actualisation du système.

Disponibilité de 802.3az EEE

Reportez-vous aux notes de version pour obtenir la liste complète des produits qui prennent en charge EEE.

Configuration par défaut

Par défaut, les fonctions 802.3az EEE et EEE LLDP sont activées au niveau global et pour chaque port.

Interactions entre les fonctions

Les interactions de 802.3az EEE avec les autres fonctions sont décrites ci-après :

- Si la négociation automatique n'est pas activée sur le port, l'état opérationnel de la fonction 802.3az EEE est désactivé. L'exception à cette règle est que si la vitesse de la liaison est de 1 Go, la fonction EEE est toujours activée même si la négociation automatique est désactivée.
- Si la fonction 802.3az EEE est activée et que le port est actif, elle commence à fonctionner immédiatement conformément à la valeur de réveil maximale du port.
- Sur l'interface utilisateur graphique (GUI), le champ EEE du port n'est pas disponible lorsque l'option Mode Courte portée est cochée.
- Si la vitesse du port sur le port GE passe à 10 Mbit, la fonction 802.3az EEE est désactivée. Cette fonctionnalité est uniquement prise en charge sur les modèles GE.

Flux de travail de configuration de 802.3az EEE

Cette section explique comment configurer la fonction 802.3az EEE et afficher ses compteurs.

ÉTAPE 1 Assurez-vous que la négociation automatique est activée sur le port en ouvrant la page **Gestion des ports > Paramètres des ports**.

a. Sélectionnez un port et ouvrez la page Modifier le paramètre de port.

b. Sélectionnez le champ **Négociation automatique** pour vérifier qu'elle est bien activée.

ÉTAPE 2 Assurez-vous que la fonction **802.3 Energy Efficient Ethernet (EEE)** est activée au niveau global sur la page Gestion des ports > Green Ethernet > Propriétés (elle est activée par défaut). Cette page indique également la quantité d'énergie qui a été économisée.

ÉTAPE 3 Assurez-vous que la fonction 802.3az EEE est activée sur un port en ouvrant la page Green Ethernet > Paramètres des ports.

a. Sélectionnez un port et ouvrez la page Modifier le paramètre de port.

b. Activez le mode **802.3 Efficient Energy Ethernet (EEE)** sur le port (il est activé par défaut).

c. Indiquez si vous souhaitez activer ou désactiver l'annonce des fonctionnalités 802.3az EEE via LLDP dans **LLDP 802.3 Energy Efficient Ethernet (EEE)** (elle est activée par défaut).

ÉTAPE 4 Pour consulter les informations relatives à 802.3 EEE sur le périphérique local, ouvrez la page Administration > Détection LLDP > Informations locales LLDP, puis affichez les informations disponibles dans le bloc 802.3 Energy Efficient Ethernet (EEE).

ÉTAPE 5 Pour consulter les informations associées à 802.3az EEE sur le périphérique distant, ouvrez les pages > Administration > Détection - LLDP > Informations de voisinage LLDP, puis affichez les informations contenues dans le bloc 802.3 Energy Efficient Ethernet (EEE).

Propriétés Green Ethernet globales

La page Propriétés affiche et active la configuration du mode Green Ethernet pour le périphérique. Les économies d'énergie actuelles sont également affichées.

Pour activer Green Ethernet et EEE, et afficher les économies d'énergie :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Green Ethernet** > **Propriétés**.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **Mode Détection d'énergie** : désactivé par défaut. Activez la case à cocher.
- **Courte portée** : permet d'activer ou de désactiver globalement le mode Courte portée s'il existe des ports GE sur le périphérique.

  REMARQUE Si le mode Courte portée est activé, EEE doit être désactivé.
- **LED des ports** : sélectionnez cette option pour activer les LED des ports. Lorsque les LED des ports sont désactivés, ils n'affichent pas l'état des liaisons, l'activité, etc.
- **Économies d'énergie** : affiche le pourcentage d'énergie économisé grâce aux modes Green Ethernet et Courte portée. Les économies d'énergie affichées ne concernent que l'énergie économisée grâce aux modes Courte portée et Détection d'énergie. Les économies d'énergie EEE sont de nature dynamique, étant donné qu'elles sont basées sur l'utilisation des ports et qu'elles ne sont par conséquent pas prises en compte. Le calcul d'économie d'énergie est effectué en comparant la consommation maximale sans économies d'énergie à la consommation actuelle.
- **Énergie totale économisée** : affiche la quantité d'énergie économisée depuis le dernier redémarrage du périphérique. Cette valeur est mise à jour à chaque événement qui affecte l'économie d'énergie.
- **802.3 Energy Efficient Ethernet (EEE)** : permet d'activer ou de désactiver globalement le mode EEE.

ÉTAPE 3 Cliquez sur **Reset Energy Saving Counter (Réinitialiser le compte d'économie d'énergie)** pour réinitialiser les informations sur les économies d'énergie réalisées.

ÉTAPE 4 Cliquez sur **Apply.** Les propriétés Green Ethernet sont écrites dans le fichier de Configuration d'exécution.

Propriétés Green Ethernet des ports

La page Paramètres des ports affiche les modes Green Ethernet et EEE actuels de chaque port, et permet de configurer la fonction Green Ethernet sur un port par l'intermédiaire de la page Modifier le paramètre de port. Pour que les modes Green Ethernet fonctionnent sur un port, vous devez avoir activé ces modes globalement sur la page Propriétés.

Les paramètres EEE s'affichent uniquement pour les périphériques qui disposent de ports GE. EEE fonctionne uniquement lorsque les ports sont activés pour la négociation automatique. Seule exception : EEE fonctionne encore même si la négociation automatique est désactivée, mais que le port a un débit de 1 Go minimum.

Pour définir les paramètres Green Ethernet de chaque port :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Green Ethernet** > **Paramètres des ports**.

La page Paramètres des ports affiche les éléments suivants :

- **État des paramètres globaux** : décrit les fonctionnalités activées.

Pour chaque port, les champs suivants sont décrits :

- **Port** : numéro du port.
- **Détection d'énergie** : état du mode Détection d'énergie sur le port :
  - *Administratif* : indique si le mode Détection d'énergie est activé.
  - *Opérationnel* : indique si le mode Détection d'énergie est actuellement opérationnel.
  - *Motif* : si le mode Détection d'énergie n'est pas opérationnel, indique le motif.
- **Courte portée** : état du mode Courte portée sur le port :
  - *Administratif* : indique si le mode Courte portée est activé.
  - *Opérationnel* : indique si le mode Courte portée est actuellement opérationnel.
  - *Motif* : si le mode Courte portée n'est pas opérationnel, indique le motif.
  - *Longueur de câble* : indique la longueur de câble détectée par VCT, en mètres.

  REMARQUE Le mode Courte portée n'est pris en charge que sur les ports GE RJ45 ; il ne s'applique pas aux ports mixtes.
- **802.3 Energy Efficient Ethernet (EEE)** : état du port concernant la fonction EEE :
  - *Administratif* : indique si la fonction EEE est activée.
  - *Opérationnel* : indique si la fonction EEE est actuellement opérationnelle sur le port local. Vous savez ainsi si elle a été activée (État administratif), si elle a été activée sur le port local et si elle est opérationnelle sur le port local.
  - *LLDP administratif* : indique si l'annonce des compteurs EEE via LLDP est activée.
  - *LLDP opérationnel* : indique si l'annonce des compteurs EEE via LLDP est actuellement opérationnelle.
  - *Support EEE sur la distance* : indique si la fonction EEE est prise en charge sur le partenaire de liaison. La fonction EEE doit être prise en charge sur les partenaires de liaison local et distant.

  REMARQUE Cette fenêtre affiche les paramètres Courte portée, Détection d'énergie et EEE de chaque port. Pour autant, vous ne pouvez pas les activer sur un port s'ils ne sont pas aussi activés globalement via la page Propriétés. Pour activer globalement les modes Courte portée et EEE, consultez **Propriétés Green Ethernet globales**.

ÉTAPE 2 Sélectionnez un **port** puis cliquez sur **Modifier**.

ÉTAPE 3 Choisissez d'activer ou de désactiver le mode **Détection d'énergie** pour le port.

ÉTAPE 4 Activez ou désactivez le mode **Courte portée** sur le port si le périphérique comporte des ports GE.

ÉTAPE 5 Activez ou désactivez le mode **802.3 Energy Efficient Ethernet (EEE)** sur le port si le périphérique comporte des ports GE.

ÉTAPE 6 Activez ou désactivez le mode LLDP **802.3 Energy Efficient Ethernet (EEE)** sur le port (annonce des fonctionnalités EEE via LLDP) si le périphérique comporte des ports GE.

ÉTAPE 7 Cliquez sur **Apply.** Les paramètres des ports Green Ethernet sont écrits dans le fichier de Configuration d'exécution.

11

Gestion des ports : Unidirectional Link Detection

Cette section décrit la fonction Unidirectional Link Detection (UDLD).

Elle couvre les rubriques suivantes :

- **Présentation de la fonction UDLD**
- **Fonctionnement de UDLD**
- **Instructions d'utilisation**
- **Dépendances envers les autres fonctions**
- **Configuration et paramètres par défaut**
- **Avant de commencer**
- **Tâches UDLD courantes**
- **Configuration de UDLD**

Présentation de la fonction UDLD

UDLD est un protocole de couche 2 qui permet aux périphériques connectés par des câbles Ethernet à fibre optique ou à paire torsadée de détecter des liaisons unidirectionnelles. Une liaison unidirectionnelle est établie lorsque le trafic provenant d'un périphérique de voisinage est reçu par le périphérique local, mais que le trafic issu du périphérique local n'est pas reçu par le voisin.

L'objectif du protocole UDLD est de détecter les ports sur lesquels le voisin ne reçoit pas de trafic du périphérique local (liaison unidirectionnelle) et de fermer ces ports.

Tous les périphériques connectés doivent prendre en charge UDLD pour que le protocole puisse détecter les liaisons unidirectionnelles. Si seul le périphérique local prend en charge UDLD, le périphérique ne pourra pas détecter l'état de la liaison. Dans ce cas, l'état de la liaison est défini sur indéterminé. L'utilisateur peut spécifier si les ports ayant l'état indéterminé sont fermés ou déclenchent simplement des notifications.

Fonctionnement de UDLD

États et modes de UDLD

Sous le protocole UDLD, les ports se voient attribuer les états suivants :

- **Détection** : le système tente de déterminer si la liaison est bidirectionnelle ou unidirectionnelle. Il s'agit d'un état temporaire.
- **Bidirectionnel** : le trafic envoyé par un périphérique local est reçu par son voisin et le trafic envoyé par le voisin est reçu par le périphérique local.
- **Fermer** : la liaison est unidirectionnelle. Le trafic envoyé par un périphérique local est reçu par son voisin, mais le trafic envoyé par le voisin n'est pas reçu par le périphérique local.
- **Indéterminé** : le système ne peut pas déterminer l'état du port, car l'une des situations suivantes se produit :
  - Le voisin ne prend pas en charge UDLD.

    Ou

  - Le voisin ne reçoit pas de trafic du périphérique local.

  Dans ce cas, l'action UDLD dépend du mode UDLD du périphérique, comme expliqué ci-après.

UDLD prend en charge les modes de fonctionnement suivants :

- **Normal**

  Si l'état de liaison du port est déterminé être bidirectionnel et que les informations UDLD expirent alors que la liaison sur le port fonctionne toujours, UDLD tente de rétablir l'état du port.

- **Agressif**

  Si l'état de liaison du port est déterminé être bidirectionnel et que les informations UDLD expirent, UDLD arrête le port au bout d'une période prolongée, lorsqu'il peut déterminer que la liaison est défectueuse. L'état du port pour UDLD est marqué comme Indéterminé.

UDLD est activé sur un port lorsque l'une des situations suivantes se produit :

- Le port est un port fibre et UDLD est activé globalement.
- Le port est un port cuivre et vous activez spécifiquement UDLD sur celui-ci.

Fonctionnement de UDLD

Lorsque UDLD est activé sur un port, les actions suivantes sont réalisées :

- UDLD initie l'état de détection sur le port.

  Dans cet état, UDLD envoie régulièrement des messages sur chaque interface active vers tous les voisins. Ces messages contiennent l'ID de périphérique de tous les voisins connus. Il envoie ces messages en fonction du délai de message défini par l'utilisateur.

- UDLD reçoit les messages UDLD des périphériques de voisinage. Il met en cache ces messages jusqu'à ce que le délai d'expiration soit atteint (3 fois le délai de message). Si un nouveau message est reçu avant l'heure d'expiration, les informations contenues dans ce message remplacent les précédentes.

- Lorsque le délai d'expiration est atteint, le périphérique procède comme suit avec les informations reçues :

  - **Si le message du voisin contient l'ID du périphérique local** : l'état de liaison du port est défini sur bidirectionnel.

  - **Si le message du voisin ne contient pas l'ID du périphérique local** : l'état de liaison du port est défini sur unidirectionnel et le port est fermé.

- Si les messages UDLD ne sont pas reçus d'un périphérique voisin avant l'expiration du délai, l'état de liaison du port est défini sur indéterminé et le système procède comme suit :

  - **Le périphérique est en mode UDLD normal :** Une notification est émise.

  - **Le périphérique est en mode UDLD agressif.** Le port est fermé.

Si l'interface a l'état bidirectionnel ou indéterminé, le périphérique envoie régulièrement un message à chaque seconde du délai de message. Les étapes suivantes sont effectuées à maintes reprises.

Un port qui a été fermé peut être réactivé manuellement sur la page Gestion des ports > Paramètres de récupération d'erreur. Pour obtenir plus d'informations, reportez-vous à la section **Réactivation d'un port fermé**.

Si une interface est arrêtée et que UDLD est activé, le périphérique supprime toutes les informations de voisinage et envoie au moins un message ULDL aux voisins pour leur indiquer que le port est fermé. Lorsque le port est réactivé, l'état UDLD devient Détection.

UDLD non pris en charge ou désactivé sur un voisin

Si UDLD n'est pas pris en charge ou désactivé sur un voisin, aucun message UDLD n'est reçu de ce voisin. Dans ce cas, le périphérique ne peut pas déterminer si la liaison est unidirectionnelle ou bidirectionnelle. L'état de l'interface est alors définie sur indéterminé.

Réactivation d'un port fermé

Vous pouvez réactiver un port qui a été fermé par UDLD en procédant de l'une des manières suivantes :

- **Automatiquement** : vous pouvez configurer le système pour qu'il réactive automatiquement les ports fermés par UDLD sur la page Gestion des ports > Paramètres de récupération d'erreur. Dans ce cas, lorsqu'un port est fermé par UDLD, il est automatiquement réactivé à l'expiration de l'intervalle de récupération automatique. UDLD est alors de nouveau exécuté sur le port. Si la liaison est toujours unidirectionnelle, UDLD la ferme à nouveau, par exemple à l'issue du délai d'expiration de UDLD.
- **Manuellement** : vous pouvez réactiver un port sur la page Gestion des ports > Paramètres de récupération d'erreur.

Instructions d'utilisation

Cisco vous recommande de ne pas activer UDLD sur les ports connectés aux périphériques sur lesquels UDLD n'est pas pris en charge ou désactivé. L'envoi de paquets UDLD sur un port connecté à un périphérique qui ne prend pas en charge UDLD génère davantage de trafic sur le port sans offrir d'avantages.

En outre, tenez compte des éléments suivants lorsque vous configurez UDLD :

- Définissez le délai du message selon l'urgence qu'il y a de fermer les ports avec une liaison unidirectionnelle. Plus le délai de message est petit, plus les paquets UDLD envoyés et analysés sont nombreux, mais plus le port est fermé rapidement si la liaison est unidirectionnelle.
- Si vous souhaitez activer UDLD sur un port cuivre, vous devez l'activer sur chaque port. Si vous activez UDLD globalement, il est uniquement activé sur les ports fibre.
- Définissez le mode UDLD sur normal si vous ne souhaitez pas fermer les ports sauf s'il est certain que la liaison est unidirectionnelle.
- Définissez le mode UDLD sur Agressif quand vous voulez une perte de liaison à la fois unidirectionnelle et bidirectionnelle.

Dépendances envers les autres fonctions

- UDLD et Couche 1.

  Lorsque UDLD est activé sur un port, UDLD s'exécute activement sur ce port tant que le port est actif. Lorsque le port est fermé, UDLD passe à l'état de fermeture UDLD. Dans cet état, UDLD supprime tous les voisins appris. Lorsque le port repasse de fermé à ouvert, UDLD est de nouveau exécuté activement.

- UDLD et protocoles de couche 2

  UDLD s'exécute sur un port indépendamment des autres protocoles de couche 2 exécutés sur le même port, tels que STP ou LACP. Par exemple, UDLD attribue un état au port quel que soit l'état STP du port ou peu importe si le port appartient à un LAG ou pas.

Configuration et paramètres par défaut

Les valeurs par défaut suivantes sont disponibles pour cette fonction :

- UDLD est désactivé par défaut sur tous les ports du périphérique.
- Le délai de message par défaut est de 15 secondes.
- Le délai d'expiration par défaut est de 45 secondes (3 fois le délai de message).
- État UDLD du port par défaut :
  - Les interfaces fibre ont l'état UDLD global.
  - Les interfaces non fibre ont l'état désactivé.

Avant de commencer

Aucune tâche préalable n'est requise.

Tâches UDLD courantes

Cette section décrit quelques tâches courantes permettant de configurer UDLD.

Flux de travail 1 : *pour activer globalement UDLD sur les ports fibre, procédez comme suit :*

ÉTAPE 1 Ouvrez la page **Gestion des ports** > **Paramètres globaux UDLD**.

a. Saisissez le **Délai de message**.

b. Dans le champ État UDLD par défaut du port fibre, entrez **Désactivé**, **Normal** ou **Agressif** comme état UDLD global.

ÉTAPE 2 Cliquez sur **Appliquer**.

Flux de travail 2 : *pour changer la configuration UDLD d'un port fibre ou pour activer UDLD sur un port cuivre, procédez comme suit :*

ÉTAPE 1 Ouvrez la page **Gestion des ports > Paramètres globaux UDLD**.

a. Sélectionnez un port.

b. Sélectionnez l'état UDLD du port **Par défaut**, **Désactivé**, **Normal** ou **Agressif**. Si vous sélectionnez Par défaut, le port se voit appliquer le paramètre global.

ÉTAPE 2 Cliquez sur **Appliquer**.

Flux de travail 3 : *pour réactiver un port après sa fermeture par UDLD si la réactivation automatique n'a pas été configurée :*

ÉTAPE 1 Ouvrez la page **Gestion des ports** > **Paramètres de récupération d'erreur**.

a. Sélectionnez un port.

b. Cliquez sur **Réactiver**.

Configuration de UDLD

La fonction UDLD peut être configurée pour tous les ports fibre à la fois (sur la page Paramètres globaux UDLD) ou pour chaque port (sur la page Paramètres d'interface UDLD).

Paramètres globaux UDLD

L'État UDLD par défaut du port fibre s'applique uniquement aux ports fibre.

Le champ Délai de message s'applique aux ports cuivre et fibre.

Pour configurer UDLD globalement :

ÉTAPE 1 Cliquez sur **Gestion des ports > UDLD** > **Paramètres globaux UDLD**.

ÉTAPE 2 Renseignez les champs suivants :

- **Délai de message** : entrez l'intervalle entre deux messages UDLD envoyés. Ce champ est destiné aux ports fibre et cuivre.
- **État UDLD par défaut du port fibre** : ce champ est uniquement destiné aux ports **fibre**. L'état UDLD des ports cuivre doit être défini individuellement sur la page Paramètres d'interface UDLD. Les états possibles sont :
  - *Désactivé* : UDLD est désactivé sur tous les ports du périphérique.
  - *Normal* : le périphérique arrête une interface si la liaison est unidirectionnelle. Si la liaison est indéterminée, une notification est émise.
  - *Agressif* : le périphérique arrête une interface si la liaison est unidirectionnelle. Si la liaison est bidirectionnelle, le périphérique s'arrête après expiration des informations UDLD. L'état du port est marqué comme Indéterminé.

ÉTAPE 3 Cliquez sur **Appliquer** pour enregistrer les paramètres dans le fichier de configuration d'exécution.

Paramètres d'interface UDLD

Utilisez la page Paramètres d'interface UDLD pour changer l'état UDLD d'un port spécifique. Vous pouvez ici définir l'état pour les ports cuivre et fibre.

Pour copier un ensemble de valeurs spécifique vers plusieurs ports, définissez la valeur pour un port, puis utilisez le bouton **Copier** pour la copier sur les autres ports.

Pour configurer UDLD sur une interface :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **UDLD** > **Paramètres d'interface UDLD**.

Les informations sont affichées pour tous les ports sur lesquels UDLD est activé. Toutefois, si vous avez effectué un filtrage sur un groupe de ports spécifique, les informations sont affichées pour ce groupe de ports uniquement.

- **Port** : l'identifiant du port.
- **État UDLD** : les états possibles sont :
  - *Désactivé* : UDLD est désactivé sur tous les ports fibre du périphérique.
  - *Normal* : le périphérique arrête une interface s'il détecte que la liaison est unidirectionnelle. Si la liaison est indéterminée, il émet une notification.
  - *Agressif* : le périphérique arrête une interface si la liaison est unidirectionnelle. Si la liaison est bidirectionnelle, le périphérique s'arrête après expiration des informations UDLD. L'état du port est marqué comme Indéterminé.
- **État bidirectionnel** : sélectionnez la valeur de ce champ pour le port sélectionné. Les états possibles sont :
  - *Détection* : le dernier état UDLD du port est en cours de détermination. Le délai d'expiration n'a pas encore été atteint depuis la dernière détermination (le cas échéant) ou depuis le début de l'exécution de UDLD sur le port ; l'état n'a donc pas encore été déterminé.
  - *Bidirectionnel* : le trafic envoyé par le périphérique local est reçu par son voisin et le trafic envoyé par le voisin est reçu par le périphérique local.
  - *Indéterminé* : l'état de la liaison entre le port et son port connecté ne peut pas être déterminé, car aucun message UDLD n'a été reçu ou le message UDLD ne contenait pas l'ID du périphérique local.
  - *Désactivé* : UDLD a été désactivé sur ce port.
  - *Fermer* : le port a été fermé car sa liaison avec le périphérique connecté est indéterminée en mode agressif.
- **Nombre de voisins** : nombre de périphériques connectés détectés.

ÉTAPE 2 Pour modifier l'état UDLD d'un port spécifique, sélectionnez-le et cliquez sur **Modifier**.

ÉTAPE 3 Modifiez la valeur de l'état UDLD. Si vous sélectionnez **Par défaut**, le port reçoit la valeur de l'**État UDLD par défaut du port fibre** défini sur la page Paramètres globaux UDLD.

ÉTAPE 4 Cliquez sur **Appliquer** pour enregistrer les paramètres dans le fichier de Configuration d'exécution.

Voisins UDLD

Pour afficher tous les périphériques connectés au périphérique local :

ÉTAPE 1 Cliquez sur **Gestion des ports > UDLD** > **Voisins UDLD**.

Les champs suivants sont affichés pour tous les ports sur lesquels UDLD est activé.

- **Nom de l'interface** : nom du port UDLD local.
- **Informations de voisinage :**
  - *ID du périphérique* : ID du périphérique distant.
  - *MAC du périphérique* : adresse MAC du périphérique distant.
  - *Nom du périphérique* : nom du périphérique distant.
  - *ID du port* : nom du port distant.
- **État** : état de la liaison entre le périphérique local et le périphérique voisin sur le port local. Les valeurs suivantes sont possibles :
  - *Détection* : le dernier état UDLD du port est en cours de détermination. Le délai d'expiration n'a pas encore été atteint depuis la dernière détermination (le cas échéant) ou depuis le début de l'exécution de UDLD sur le port ; l'état n'a donc pas encore été déterminé.
  - *Bidirectionnel* : le trafic envoyé par le périphérique local est reçu par son voisin et le trafic envoyé par le voisin est reçu par le périphérique local.
  - *Indéterminé* : l'état de la liaison entre le port et son port connecté ne peut pas être déterminé, car aucun message UDLD n'a été reçu ou le message UDLD ne contenait pas l'ID du périphérique local.
  - *Désactivé* : UDLD a été désactivé sur ce port.
  - *Fermer* : le port a été fermé car sa liaison avec le périphérique connecté est indéterminée en mode agressif.
- **Délai d'expiration du voisin (s)** : indique le délai à respecter avant que le périphérique tente de déterminer l'état UDLD du port. Il correspond à trois fois le délai de message.
- **Heure du message du voisin (s)** : indique le délai entre les messages UDLD.

12

Port intelligent

Ce document décrit la fonction Port intelligent.

Il contient les rubriques suivantes :

- **Présentation**
- **Qu'est-ce qu'un port intelligent ?**
- **Types de port intelligent**
- **Macros Port intelligent**
- **Échec de la macro et opération de réinitialisation**
- **Fonctionnement de la fonction Port intelligent**
- **Port intelligent automatique**
- **Gestion des erreurs**
- **Configuration par défaut**
- **Relations avec les autres fonctions et compatibilité descendante**
- **Tâches courantes de port intelligent**
- **Configuration de port intelligent à l'aide de l'interface Web**
- **Macros Port intelligent intégrées**

Présentation

La fonction Port intelligent constitue un moyen pratique d'enregistrer et de partager des configurations communes. En appliquant la même macro Port intelligent à plusieurs interfaces, ces dernières partagent un ensemble commun de configurations. .

Il est possible d'appliquer une macro Port intelligent à une interface par type de port intelligent associé à la macro.

Il y a deux façons d'appliquer une macro Port intelligent par type de port intelligent à une interface :

- **Port intelligent statique** : vous attribuez manuellement un type de port intelligent à une interface. La macro Port intelligent correspondante est alors appliquée à l'interface.
- **Port intelligent automatique** : l'option Port intelligent automatique attend qu'un appareil soit associé à l'interface avant d'appliquer une configuration. Lorsqu'un appareil est détecté à partir d'une interface, la macro Port intelligent (si elle est attribuée) qui correspond au Type de port intelligent de l'appareil en cours d'association est automatiquement appliquée.

La fonction Port intelligent est constituée de plusieurs composants et opère conjointement avec d'autres fonctions de l'appareil. Ces composants et fonctions sont décrits dans les sections suivantes :

- Port intelligent, Types de port intelligent et Macros Port intelligent, décrits dans cette section.
- VLAN vocal et Port intelligent, décrits dans la section **VLAN voix**.
- LLDP/CDP pour port intelligent, décrits respectivement dans les sections **Configuration de LLDP** et **Configuration de CDP**.

Les flux de travail classiques sont également décrits dans la section **Tâches courantes de port intelligent**.

Qu'est-ce qu'un port intelligent ?

Un port intelligent est une interface à laquelle une macro intégrée peut être appliquée. Ces macros sont conçues pour permettre de configurer rapidement l'appareil, afin de répondre aux exigences de communication et d'utiliser les fonctions des différents types de périphériques réseau. Les exigences d'accès réseau et de qualité de service (QoS) varient si l'interface est connectée à un téléphone IP, une imprimante ou un routeur et/ou un point d'accès (AP).

Types de port intelligent

Les Types de port intelligent se réfèrent aux types des appareils associés ou devant être associés aux ports intelligents. L'appareil prend en charge les types de port intelligent suivants :

- Imprimante
- Bureau
- Invité
- Serveur

- Hôte
- Caméra IP
- Téléphone IP
- Téléphone IP+Bureau
- Commutateur
- Routeur
- Point d'accès sans fil

Les Types de port intelligent sont nommés pour décrire le type d'appareil connecté à une interface. Chaque Type de port intelligent est associé à deux macros Port intelligent. La première, appelée « la macro », permet d'appliquer la configuration souhaitée. La deuxième, appelée « l'anti-macro », permet d'annuler toute configuration effectuée par « la macro » lorsque cette interface change de type de port intelligent.

Le tableau suivant décrit la relation entre les Types de port intelligent et le Port intelligent automatique.

Type de port intelligent	Pris en charge par le Port intelligent automatique	Pris en charge par le Port intelligent automatique par défaut
Inconnu	Non	Non
Par défaut	Non	Non
Imprimante	Non	Non
Bureau	Non	Non
Invité	Non	Non
Serveur	Non	Non
Hôte	Oui	Non
Caméra IP	Non	Non
Téléphone IP	Oui	Oui
Téléphone IP de bureau	Oui	Oui
Commutateur	Oui	Oui
Routeur	Oui	Non
Point d'accès sans fil	Oui	Oui

Types de port intelligent spéciaux

Il existe deux types de port intelligent spéciaux : *Par défaut* et *Inconnu*. Ces deux types ne sont pas associés à des macros, mais servent à indiquer l'état de l'interface par rapport au port intelligent.

Les types de port intelligent spéciaux sont décrits ci-dessous :

- **Par défaut**

  Une interface à laquelle un Type de port intelligent n'est pas (encore) attribué a l'état Port intelligent par défaut.

  Si l'option Port intelligent automatique attribue un type de port intelligent à une interface et que l'interface n'est pas configurée pour être Port intelligent automatique persistant, alors son type de port intelligent est réinitialisé à la valeur par défaut dans les cas suivants :

  - Une opération de désactivation/activation de la liaison est effectuée sur l'interface.
  - L'appareil est redémarré.
  - Tous les appareils associés à l'interface ont vu leur délai expirer, ce qui est défini par l'absence d'annonce CDP et/ou LLDP en provenance de l'appareil pendant une durée spécifiée.

- **Inconnu**

  Si une macro Port intelligent est appliquée à une interface et qu'une erreur se produit, l'état Inconnu est attribué à l'interface. Dans ce cas, les fonctions Port intelligent et Port intelligent automatique ne sont pas actives sur l'interface tant que vous n'avez pas corrigé l'erreur et appliqué l'action Réinitialiser (sur les pages Paramètres d'interface) qui réinitialise l'état Port intelligent.

  Pour obtenir des conseils de dépannage, reportez-vous à la partie flux de travail dans **Tâches courantes de port intelligent**.

  REMARQUE Dans cette section, l'expression « délai expiré » sert à décrire les messages LLDP et CDP via leur TTL. Si la fonction Port intelligent automatique est activée, que l'État persistant est désactivé et qu'aucun message CDP ou LLDP n'est plus reçu sur l'interface avant que les deux TTL des paquets CDP et LLDP les plus récents ne diminuent à 0, l'anti-macro est exécutée et le Type de port intelligent est réinitialisé à ses valeurs par défaut.

Macros Port intelligent

Une macro Port intelligent est un script qui configure une interface de manière appropriée pour un appareil réseau spécifique.

Ne confondez pas les macros Port intelligent avec les macros globales. Les macros globales configurent l'appareil de manière globale, alors que l'étendue d'une macro Port intelligent est limitée à l'interface à laquelle elle s'applique.

Le code source de la macro peut être trouvé en cliquant sur le bouton **Afficher la source de la macro** de la page Paramètres de type de port intelligent.

Une macro et l'anti-macro correspondante sont couplées en association avec chaque Type de port intelligent. La macro applique la configuration et l'anti-macro la supprime.

Deux macros Port intelligent sont couplées par leurs noms de la manière suivante :

- nom_macro (par exemple : printer)
- no_nom_macro (par exemple : no_printer, l'anti macro Port intelligent de la macro Port intelligent printer)

Pour afficher la liste des macros Port intelligent intégrées pour chaque type d'appareil, reportez-vous à la section **Macros Port intelligent intégrées**.

Application d'un Type de port intelligent à une interface

Lorsque des Types de port intelligent sont appliqués aux interfaces, les Types de port intelligent et la configuration dans les macros Port intelligent associées sont enregistrés dans le fichier de Configuration d'exécution. Si l'administrateur enregistre le fichier de Configuration d'exécution dans le fichier de Configuration de démarrage, l'appareil applique les Types de port intelligent et les macros Port intelligent aux interfaces après le redémarrage du système, comme suit:

- Si le fichier de Configuration de démarrage ne spécifie pas de Type de port intelligent pour une interface, son Type de port intelligent est défini sur Par défaut.
- Si le fichier de Configuration de démarrage spécifie un Type de port intelligent statique, le Type de port intelligent de l'interface est défini sur ce type statique.
- Si le fichier de Configuration de démarrage spécifie un Type de port intelligent qui a été dynamiquement attribué par la fonction Port intelligent automatique.
  - Si l'état Auto Smartport Global Operational (Port intelligent automatique global opérationnel), l'état Port intelligent automatique de l'interface et l'état Persistant sont tous **activés**, le type de port intelligent est défini sur ce type dynamique.
  - Sinon, l'anti-macro correspondante est appliquée et l'état de l'interface est défini sur Par défaut.

Échec de la macro et opération de réinitialisation

Une macro Port intelligent peut échouer s'il y a un conflit entre la configuration existante de l'interface et une macro Port intelligent.

Lorsqu'une macro Port intelligent échoue, un message SYSLOG contenant les paramètres suivants est envoyé :

- Numéro de port
- Type de port intelligent
- Numéro de ligne de la commande CLI ayant échoué dans la macro

Lorsqu'une macro Port intelligent échoue sur une interface, l'état de l'interface est défini sur *Inconnu*. La raison de l'échec peut être affichée sur la page Paramètres d'interface, dans la fenêtre contextuelle **Afficher les diagnostics**.

Une fois que la source du problème a été identifiée et que la configuration existante ou la macro Port intelligent a été corrigée, vous devez effectuer une opération de réinitialisation pour réinitialiser l'interface avant de pouvoir la réappliquer avec un Type de port intelligent (sur les pages Paramètres d'interface). Pour obtenir des conseils de dépannage, reportez-vous à la partie flux de travail dans **Tâches courantes de port intelligent**.

Fonctionnement de la fonction Port intelligent

Il est possible d'appliquer une macro Port intelligent à une interface par le type de port intelligent associé à la macro.

Puisque le système prend en charge les Types de port intelligent correspondant aux appareils qui ne peuvent pas être découverts via CDP et/ou LLDP, ces Types de port intelligent doivent être attribués de manière statique aux interfaces souhaitées. Pour ce faire, accédez à la page Paramètres d'interface de port intelligent, sélectionnez la case d'option correspondant à l'interface souhaitée, puis cliquez sur **Modifier**. Sélectionnez ensuite le Type de port intelligent que vous souhaitez attribuer, puis réglez les paramètres si nécessaire avant de cliquer sur **Appliquer**.

Il y a deux façons d'appliquer une macro Port intelligent par type de port intelligent à une interface :

- **Port intelligent statique**

  Vous attribuez manuellement un Type de port intelligent à une interface. La macro Port intelligent correspondante est appliquée à l'interface. Sur la page Paramètres d'interface de port intelligent, vous pouvez attribuer manuellement un Type de port intelligent à une interface.

- **Port intelligent automatique**

  Lorsqu'un appareil est détecté à partir d'une interface, la macro Port intelligent (si elle est présente) qui correspond au Type de port intelligent de l'appareil en cours d'association est automatiquement appliquée. La fonction Port intelligent automatique est activée par défaut au niveau global et au niveau de l'interface.

Dans les deux cas, l'anti-macro associée est exécutée lorsque le Type de port intelligent est supprimé de l'interface, et l'anti-macro est exécutée exactement de la même manière, supprimant ainsi toute la configuration de l'interface.

Port intelligent automatique

Pour que le Port intelligent automatique attribue automatiquement des Types de port intelligent aux interfaces, la fonction Port intelligent automatique doit être activée au niveau global et sur les interfaces pertinentes que le port intelligent automatique doit être autorisé à configurer. Par défaut, le Port intelligent automatique est activé et autorisé à configurer toutes les interfaces. Le type de port intelligent attribué à chaque interface est déterminé par les paquets CDP et LLDP reçus respectivement sur chaque interface.

- Si plusieurs appareils sont associés à une interface, un profil de configuration adapté à tous les appareils est si possible appliqué à l'interface.
- Si un appareil est arrivé à expiration (ne reçoit plus d'annonces des autres appareils), la configuration de l'interface est modifiée conformément à son État persistant. Si l'État persistant est activé, la configuration de l'interface est conservée. Sinon, le Type de port intelligent revient à ses valeurs par défaut.

Activation du Port intelligent automatique

L'option Port intelligent automatique peut être activée globalement sur la page Propriétés en procédant comme suit :

- **Activé** : active manuellement le Port intelligent automatique et le rend opérationnel immédiatement.
- **Activer par VLAN voix automatique** : permet au Port intelligent automatique de fonctionner si la fonction VLAN voix automatique est activée et opérationnelle. Activer par VLAN voix automatique est la valeur par défaut.

  REMARQUE Outre l'activation du Port intelligent automatique au niveau global, vous devez aussi activer le Port intelligent automatique sur l'interface souhaitée. Par défaut, le Port intelligent automatique est activé sur toutes les interfaces.

Pour plus d'informations sur l'activation du VLAN voix automatique, reportez-vous à la section **VLAN voix**.

Identification du Type de port intelligent

Si le Port intelligent automatique est activé au niveau global (sur la page Propriétés) et sur une interface (sur la page Paramètres d'interface), l'appareil applique une macro Port intelligent à l'interface conformément au Type de port intelligent de l'appareil en cours d'association. Le Port intelligent automatique détecte les Types de port intelligent des appareils en cours d'association, sur la base des fonctionnalités CDP et/ou LLDP notifiées par les appareils.

Par exemple, si un téléphone IP est associé à un port, il transmet des paquets CDP ou LLDP qui annoncent ses fonctionnalités. Après réception de ces paquets CDP et/ou LLDP, l'appareil détecte le Type de port intelligent approprié au téléphone et applique la macro Port intelligent correspondante à l'interface à laquelle le téléphone IP est associé.

Excepté si le Port intelligent automatique persistant est activé sur une interface, le Type de port intelligent et la configuration générée qui est appliquée par le Port intelligent automatique sont supprimés si le ou les appareils en cours d'association arrivent à expiration, passent en liaison inactive, redémarrent, ou si des fonctionnalités conflictuelles sont reçues. Les délais d'expiration sont déterminés par l'absence d'annonces CDP et/ou LLDP en provenance de l'appareil pendant une durée spécifiée.

Utilisation des informations CDP/LLDP pour identifier les Types de port intelligent

L'appareil détecte le type d'appareil associé au port, sur la base des fonctionnalités CDP/LLDP.

Ce mappage est présenté dans les tableaux suivants :

Mappage des fonctionnalités CDP au type de port intelligent

Nom de la fonctionnalité	Bit CDP	Type de port intelligent
Routeur	0x01	Routeur
Pont TB	0x02	Point d'accès sans fil
Pont SR	0x04	Ignorer
Commutateur	0x08	Commutateur
Hôte	0x10	Hôte
Filtrage conditionnel IGMP	0x20	Ignorer
Répéteur	0x40	Ignorer
Téléphone VoIP	0x80	ip_phone
Appareil géré à distance	0x100	Ignorer
Port de téléphone CAST	0x200	Ignorer
Relais MAC à deux ports	0x400	Ignorer

Mappage des fonctionnalités LLDP au type de port intelligent

Nom de la fonctionnalité	Bit LLDP	Type de port intelligent
Autre	1	Ignorer
Répéteur IETF RFC 2108	2	Ignorer
Pont MAC IEEE Std. 802.1D	3	Commutateur
Point d'accès WLAN IEEE Std. 802.11 MIB	4	Point d'accès sans fil
Routeur IETF RFC 1812	5	Routeur
Téléphone IETF RFC 4293	6	ip_phone
Système de câble DOCSIS IETF RFC 4639 et IETF RFC 4546	7	Ignorer
Station uniquement IETF RFC 4293	8	Hôte
Composant C-VLAN d'un pont VLAN IEEE Std. 802.1Q	9	Commutateur
Composant S-VLAN d'un pont VLAN IEEE Std. 802.1Q	10	Commutateur
Relais MAC à deux ports (TPMR) IEEE Std. 802.1Q	11	Ignorer
Réservé	12-16	Ignorer

REMARQUE Si seul le téléphone IP et les bits hôtes sont définis, le type de port intelligent est ip_phone_desktop.

Plusieurs appareils associés au port

L'appareil détecte le Type de port intelligent d'un appareil connecté via les fonctionnalités que l'appareil annonce dans ses paquets CDP et/ou LLDP.

Si plusieurs appareils sont connectés à l'appareil par le biais d'une seule interface, le Port intelligent automatique utilise chaque annonce de fonctionnalité qu'il reçoit via cette interface pour attribuer le Type de port intelligent correct. L'attribution est basée sur l'algorithme suivant :

- Si tous les appareils présents sur une interface annoncent la même fonctionnalité (il n'y a pas de conflit), le Type de port intelligent correspondant est appliqué à l'interface.
- Si l'un des appareils est un commutateur, le Type de port intelligent *Commutateur* est utilisé.

- Si l'un des appareils est un point d'accès, le Type de port intelligent *Point d'accès sans fil* est utilisé.
- Si l'un des appareils est un téléphone IP et qu'un autre appareil est un hôte, le type de port intelligent *ip_phone_desktop* est utilisé.
- Si l'un des appareils est un téléphone IP de bureau et que l'autre est un téléphone IP ou un hôte, le type de port intelligent *ip_phone_desktop* est utilisé.
- Dans tous les autres cas, le Type de port intelligent par défaut est utilisé.

Pour plus d'informations sur LLDP/CDP, reportez-vous respectivement aux sections **Configuration de LLDP** et **Configuration de CDP**.

Interface du Port intelligent automatique persistant

Si l'État persistant d'une interface est activé, son Type de port intelligent et la configuration qui est déjà appliquée dynamiquement par le Port intelligent automatique sont conservés sur l'interface, même si l'appareil en cours d'association est arrivé à expiration, l'interface a été désactivée et l'appareil a été redémarré (si l'on part du principe que la configuration a été enregistrée). Le Type de port intelligent et la configuration de l'interface ne sont pas modifiés, sauf si le Port intelligent automatique détecte un appareil en cours d'association avec un autre Type de port intelligent. Si l'État persistant d'une interface est désactivé, l'interface rétablit le Type de port intelligent par défaut lorsque l'appareil en cours d'association arrive à expiration, l'interface est désactivée ou l'appareil est redémarré. L'activation de l'État persistant sur une interface élimine le retard de détection de l'appareil.

REMARQUE La persistance des Types de port intelligent appliqués aux interfaces est effective entre les redémarrages uniquement si la configuration d'exécution avec le Type de port intelligent appliqué aux interfaces est enregistrée dans le fichier de Configuration de démarrage.

Gestion des erreurs

Lorsque l'application d'une macro Port intelligent à une interface échoue, vous pouvez examiner le point d'échec sur la page Paramètres d'interface, réinitialiser le port et réappliquer la macro une fois que l'erreur a été corrigée à partir des pages Paramètres d'interface et Modifier les paramètres d'interface.

Configuration par défaut

Le port intelligent est toujours disponible. Par défaut, le Port intelligent automatique est activé par le VLAN voix automatique, se base sur CDP et LLDP pour détecter le type de port intelligent de l'appareil en cours d'association, et détecte le type de port intelligent Téléphone IP, Téléphone IP+Bureau, Commutateur ou Point d'accès sans fil.

Pour obtenir une description des valeurs de voix par défaut, reportez-vous à la section **VLAN voix**.

Relations avec les autres fonctions et compatibilité descendante

La fonction Port intelligent automatique est activée par défaut. Vous avez la possibilité de la désactiver. Les OUI de téléphonie ne peuvent actuellement pas fonctionner avec les fonctions Port intelligent automatique et VLAN voix automatique. Le Port intelligent automatique doit être désactivé avant d'activer le OUI de téléphonie.

Tâches courantes de port intelligent

Cette section décrit quelques tâches courantes permettant de configurer le Port intelligent et le Port intelligent automatique.

Flux de travail 1 : pour activer globalement le Port intelligent automatique sur l'appareil et configurer un port avec la fonction Port intelligent automatique, procédez comme suit :

ÉTAPE 1 Pour activer la fonction Port intelligent automatique sur l'appareil, ouvrez la page Port intelligent > Propriétés. Définissez **Port intelligent automatique administratif** sur **Activer** ou **Activer par VLAN voix**.

ÉTAPE 2 Spécifiez si l'appareil doit traiter les annonces CDP et/ou LLDP des appareils connectés.

ÉTAPE 3 Sélectionnez le type des appareils à détecter dans le champ **Détection périphérique de port intelligent auto**.

ÉTAPE 4 Cliquez sur **Appliquer.**

ÉTAPE 5 Pour activer la fonction Port intelligent automatique sur une ou plusieurs interfaces, ouvrez la page Port intelligent > Paramètres d'interface.

ÉTAPE 6 Sélectionnez l'interface et cliquez sur **Modifier.**

ÉTAPE 7 Sélectionnez Port intelligent automatique dans le champ **Application de port intelligent**.

ÉTAPE 8 Cochez ou décochez **État persistant**.

ÉTAPE 9 Cliquez sur **Appliquer**.

Flux de travail 2 : pour configurer une interface en tant que port intelligent statique, procédez comme suit:

ÉTAPE 1 Pour activer la fonction Port intelligent sur l'interface, ouvrez la page Port intelligent > Paramètres d'interface.

ÉTAPE 2 Sélectionnez l'interface et cliquez sur **Modifier**.

ÉTAPE 3 Sélectionnez le type de port intelligent que vous souhaitez attribuer à l'interface dans le champ **Application de port intelligent**.

ÉTAPE 4 Définissez les paramètres de macro souhaités.

ÉTAPE 5 Cliquez sur **Appliquer**.

Flux de travail 3 : *pour définir les valeurs par défaut des paramètres de macro Port intelligent, procédez comme suit :*

Cette procédure vous permet d'effectuer les opérations suivantes :

- Afficher la source de la macro.
- Modifier les valeurs par défaut des paramètres.
- Restaurer les paramètres d'usine.

1. Ouvrez la page Port intelligent > Paramètres de type de port intelligent.
2. Sélectionnez le Type de port intelligent.
3. Cliquez sur **Afficher la source de la macro** pour afficher la macro Port intelligent actuelle qui est associée au Type de port intelligent sélectionné.
4. Cliquez sur **Modifier** pour ouvrir une nouvelle fenêtre dans laquelle vous pouvez modifier les valeurs par défaut des paramètres dans les macros qui sont liées à ce type de port intelligent. Les valeurs par défaut de ces paramètres sont utilisées lorsque le Port intelligent automatique applique le Type de port intelligent sélectionné (le cas échéant) à une interface.
5. Sur la page Modifier, modifiez les champs.

6. Cliquez sur **Appliquer** pour réexécuter la macro si les paramètres ont été modifiés ou sur **Restaurer les valeurs par défaut** pour restaurer si nécessaire les valeurs par défaut des paramètres dans les macros intégrées.

Flux de travail 4 : pour réexécuter une macro Port intelligent si celle-ci a échoué, procédez comme suit :

ÉTAPE 1 Sur la page Paramètres d'interface, sélectionnez une interface avec le Type de port intelligent Inconnu.

ÉTAPE 2 Cliquez sur **Afficher les diagnostics** pour visualiser le problème.

ÉTAPE 3 Lancez la procédure de dépannage, puis corrigez le problème. Reportez-vous au conseil de dépannage ci-dessous.

ÉTAPE 4 Cliquez sur **Modifier**. Une nouvelle fenêtre s'ouvre. Cliquez sur **Réinitialiser** pour réinitialiser l'interface.

ÉTAPE 5 Revenez à la page principale et réappliquez la macro en utilisant **Réappliquer** (pour les appareils qui ne sont ni des commutateurs, ni des routeurs ni des points d'accès) ou **Réappliquer la macro de port intelligent** (pour les commutateurs, routeurs ou points d'accès) afin d'exécuter la macro Port intelligent sur l'interface.

Il existe une deuxième méthode de réinitialisation d'une ou plusieurs interfaces inconnues :

ÉTAPE 1 Sur la page Paramètres d'interface, activez la case à cocher Type de port est égal à.

ÉTAPE 2 Sélectionnez *Inconnu* et cliquez sur **OK**.

ÉTAPE 3 Cliquez sur **Réinitialiser tous les ports intelligents inconnus**. Réappliquez ensuite la macro comme indiqué ci-dessus.

CONSEIL L'échec de la macro peut être dû à un conflit avec une configuration de l'interface qui a été effectuée avant l'application de la macro (le plus souvent rencontré dans les paramètres de sécurité et de contrôle des tempêtes), un type de port incorrect, une typo ou une commande incorrecte dans la macro définie par l'utilisateur ou encore une valeur de paramètre non valide. Les paramètres sont contrôlés, sans prise en compte du type ou de la limite, avant la tentative d'application de la macro. Par conséquent, une entrée incorrecte ou non valide pour une valeur de paramètre se soldera presque assurément par un échec lors de l'application de la macro.

Configuration de port intelligent à l'aide de l'interface Web

Vous pouvez configurer la fonction Port intelligent sur les pages Port intelligent > Propriétés, Paramètres de type de port intelligent et Paramètres d'interface.

Pour la configuration du VLAN vocal, reportez-vous à la section **VLAN voix**.

Pour la configuration de LLDP/CDP, reportez-vous respectivement aux sections **Configuration de LLDP** et **Configuration de CDP**.

Propriétés de port intelligent

Pour configurer la fonction Port intelligent globalement :

ÉTAPE 1 Cliquez sur **Port intelligent > Propriétés**.

ÉTAPE 2 Saisissez les paramètres.

- **Port intelligent automatique administratif** : sélectionnez cette option pour activer ou désactiver globalement le Port intelligent automatique. Les options suivantes sont disponibles :
  - *Désactiver* : sélectionnez cette option pour désactiver le Port intelligent automatique sur l'appareil.
  - *Activer* : sélectionnez cette option pour activer le Port intelligent automatique sur l'appareil.
  - *Activer par VLAN voix automatique* : cette option active le Port intelligent automatique, mais ne le rend opérationnel que lorsque le VLAN voix automatique est aussi activé et opérationnel. Activer par VLAN voix automatique est la valeur par défaut.
- **Port intelligent automatique opérationnel** : affiche l'état de la fonction Port intelligent automatique.
- **Méthode de détection périphérique de port intelligent auto.** : indiquez si les types de paquets entrants CDP et/ou LLDP doivent être utilisés pour détecter le type de port intelligent des appareils en cours d'association. Vous devez cocher au moins un type pour que le Port intelligent automatique puisse identifier les appareils.
- **État CDP opérationnel** : affiche l'état opérationnel de CDP. Activez CDP si le Port intelligent automatique doit détecter le type de port intelligent à partir de l'annonce CDP.
- **État LLDP opérationnel** : affiche l'état opérationnel de LLDP. Activez LLDP si le Port intelligent automatique doit détecter le type de port intelligent à partir de l'annonce LLDP/LLDP-MED.
- **Détection périphérique de port intelligent auto.** : sélectionnez chaque type d'appareil pour lequel le Port intelligent automatique peut attribuer des types de port intelligent aux interfaces. Si vous ne cochez pas cette option, le Port intelligent automatique n'attribue ce Type de port intelligent à aucune interface.

ÉTAPE 3 Cliquez sur **Appliquer**. Vous appliquez ainsi les paramètres de Port intelligent globaux sur l'appareil.

Paramètres de type de port intelligent

Utilisez la page Paramètres de type de port intelligent pour modifier les paramètres de type de port intelligent et afficher la source de la macro.

Par défaut, chaque Type de port intelligent est associé à une paire de macros Port intelligent intégrées. Pour plus d'informations sur la macro et l'anti-macro, reportez-vous à la section **Types de port intelligent**. Les macros intégrées ou définies par l'utilisateur peuvent comporter des paramètres. Les macros intégrées peuvent intégrer jusqu'à trois paramètres.

La modification de ces paramètres pour les Types de port intelligent qui sont appliqués par le Port intelligent automatique sur la page Paramètres de type de port intelligent configure les valeurs par défaut de ces paramètres. Ces valeurs par défaut sont utilisées par le Port intelligent automatique.

REMARQUE Une fois les modifications apportées aux types Port intelligent automatique, les nouveaux paramètres sont appliqués aux interfaces auxquelles le Port intelligent automatique a déjà attribué ce type. Dans ce cas, si vous liez une macro non valide ou définissez une valeur par défaut non valide pour un paramètre, tous les ports de ce Type de port intelligent deviennent inconnus.

ÉTAPE 1 Cliquez sur **Port intelligent > Paramètres de type de port intelligent**.

ÉTAPE 2 Pour afficher la macro Port intelligent associée à un Type de port intelligent, sélectionnez un Type de port intelligent, puis cliquez sur **Afficher la source de la macro**.

ÉTAPE 3 Pour modifier les paramètres d'une macro, sélectionnez un Type de port intelligent, puis cliquez sur **Modifier**.

ÉTAPE 4 Renseignez les champs.

- **Type de port** : sélectionnez un type de port intelligent.
- **Nom de la macro** : affiche le nom de la macro Port intelligent actuellement associée au type de port intelligent.
- **Paramètres de macro** : affiche les champs suivants pour trois paramètres dans la macro :
  - *Nom du paramètre* : nom du paramètre dans la macro.
  - *Valeur du paramètre* : valeur actuelle du paramètre dans la macro. Vous pouvez la modifier ici.
  - *Description du paramètre* : description du paramètre.

Vous pouvez restaurer les valeurs par défaut des paramètres en cliquant sur **Restaurer les valeurs par défaut**.

ÉTAPE 5 Cliquez sur **Appliquer** pour enregistrer les modifications dans la configuration d'exécution. Si la macro Port intelligent et/ou ses valeurs de paramètre associées au Type de port intelligent sont modifiées, le Port intelligent automatique réapplique automatiquement la macro aux interfaces qui sont actuellement attribuées avec le Type de port intelligent par le Port intelligent automatique. Le Port intelligent automatique n'applique pas les modifications aux interfaces auxquelles un Type de port intelligent a été attribué de façon statique.

REMARQUE Il n'existe aucune méthode permettant de valider les paramètres de macro, car ils n'ont aucune association de type. Toutefois, n'importe quelle entrée est valide à ce stade. Néanmoins, des valeurs de paramètre non valides peuvent entraîner des erreurs lorsque le Type de port intelligent est attribué à une interface appliquant la macro associée.

Paramètres d'interface de port intelligent

Utilisez la page Paramètres d'interface pour effectuer les tâches suivantes :

- Appliquez de manière statique un Type de port intelligent spécifique à une interface, avec des valeurs spécifiques à l'interface pour les paramètres de macro.
- Activez le Port intelligent automatique sur une interface.
- Diagnostiquez une macro Port intelligent dont l'application a échoué et a généré l'état Inconnu du Type de port intelligent.
- Réappliquez une macro Port intelligent après son échec pour l'un des types d'interface suivants : commutateur, routeur et point d'accès. Vous devez avoir effectué les corrections nécessaires avant de cliquer sur **Réappliquer**. Pour obtenir des conseils de dépannage, reportez-vous à la partie flux de travail dans **Tâches courantes de port intelligent**.
- Réappliquez une macro Port intelligent à une interface. Dans certaines circonstances, il se peut que vous souhaitiez réappliquer une macro Port intelligent pour mettre à jour la configuration sur une interface. Par exemple, en réappliquant une macro Port intelligent d'appareil sur une interface de commutateur, l'interface devient membre des VLAN qui ont été créés depuis la dernière application de la macro. Vous devez connaître les configurations actuelles de l'appareil et la définition de la macro pour déterminer si une réapplication aura un impact sur l'interface.
- Réinitialisez les interfaces inconnues. Le mode des interfaces inconnues est ainsi défini sur Par défaut.

Pour appliquer une macro Port intelligent :

ÉTAPE 1 Cliquez sur **Port intelligent > Paramètres d'interface**.

Réappliquez la macro Port intelligent associée comme suit :

- Sélectionnez un groupe de Types de port intelligent (commutateurs, routeurs ou points d'accès) et cliquez sur **Réappliquer la macro de port intelligent.** Les macros sont appliquées à tous les types d'interface sélectionnés.
- Sélectionnez une interface UP et cliquez sur **Réappliquer** pour réappliquer la dernière macro appliquée à l'interface.

  L'action **Réappliquer** ajoute aussi l'interface à tous les VLAN nouvellement créés.

ÉTAPE 2 Diagnostic de port intelligent.

Si une macro Port intelligent échoue, le Type de port intelligent de l'interface est Inconnu. Sélectionnez une interface dont le type est inconnu, puis cliquez sur **Afficher les diagnostics**. Le système affiche la commande où l'application de la macro a échoué. Pour obtenir des conseils de dépannage, reportez-vous à la partie flux de travail dans **Tâches courantes de port intelligent**. Corrigez le problème et réappliquez la macro.

ÉTAPE 3 Réinitialisation de toutes les interfaces inconnues au type Par défaut.

- Activez la case à cocher *Type de port est égal à*.
- Sélectionnez *Inconnu* et cliquez sur **OK**.
- Cliquez sur **Réinitialiser tous les ports intelligents inconnus**. Réappliquez ensuite la macro comme indiqué ci-dessus. Cette opération réinitialise l'ensemble des interfaces de type Inconnu, ce qui signifie que le type Par défaut est réattribué à toutes les interfaces. Une fois que vous avez corrigé l'erreur dans la macro et/ou dans la configuration d'interface actuelle, vous pouvez appliquer une nouvelle macro.

REMARQUE La réinitialisation de l'interface de type inconnu ne réinitialise pas la configuration effectuée par la macro qui a échoué. Ce nettoyage doit être réalisé manuellement.

Pour attribuer un type de port intelligent à une interface ou activer la fonction Port intelligent automatique sur l'interface :

ÉTAPE 1 Sélectionnez une interface et cliquez sur **Modifier**.

ÉTAPE 2 Renseignez les champs.

- **Interface** : sélectionnez le port ou LAG.
- **Type de port intelligent** : affiche le type de port intelligent actuellement attribué au port/LAG.

- **Application de port intelligent** : sélectionnez le type de port intelligent dans le menu déroulant Application de port intelligent.
- **Méthode d'application de port intelligent** : si Port intelligent automatique est sélectionné, le type de port intelligent est automatiquement attribué en fonction de l'annonce CDP et/ou LLDP reçue des appareils en cours de connexion, et la macro Port intelligent correspondante est appliquée. Pour attribuer un Type de port intelligent de manière statique et appliquer la macro Port intelligent correspondante à l'interface, sélectionnez le Type de port intelligent souhaité.
- **État persistant** : sélectionnez cette option pour activer l'état persistant. S'il est activé, l'association d'un Type de port intelligent à une interface est conservée même si l'interface est désactivée ou que l'appareil est redémarré. L'État persistant s'applique uniquement si l'Application de port intelligent de l'interface est Port intelligent automatique. L'activation de l'État persistant sur une interface élimine le retard de détection de l'appareil.
- **Paramètres de macro** : affiche les champs suivants pour un maximum de trois paramètres dans la macro :
  - *Nom du paramètre* : nom du paramètre dans la macro.
  - *Valeur du paramètre* : valeur actuelle du paramètre dans la macro. Vous pouvez la modifier ici.
  - *Description du paramètre* : description du paramètre.

ÉTAPE 3 Cliquez sur **Réinitialiser** pour définir une interface sur Par défaut si son état est Inconnu (en raison d'un échec d'application de macro). La macro peut être réappliquée sur la page principale.

ÉTAPE 4 Cliquez sur **Appliquer** pour mettre à jour les modifications et attribuer le Type de port intelligent à l'interface.

Macros Port intelligent intégrées

Vous trouverez ci-dessous une description de la paire de macros intégrées pour chaque Type de port intelligent. Pour chaque Type de port intelligent, une macro permet de configurer l'interface et une anti-macro permet de supprimer la configuration.

Le code de macro des types de port intelligent suivants est indiqué ci-après :

- **desktop**
- **printer**
- **guest**
- **server**

- **host**
- **ip_camera**
- **ip_phone**
- **ip_phone_desktop**
- **switch**
- **router**
- **ap**

desktop

```
[desktop]
#interface configuration, for increased network security and reliability when connecting a desktop
device, such as a PC, to a switch port. (configuration d'interface pour une sécurité et une fiabilité
réseau accrues au moment de connecter un périphérique de bureau, tel qu'un PC à un port de
commutateur.)
#macro description Desktop
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré sur le port
#                         $max_hosts: Nombre maximum de périphériques autorisés sur le port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_desktop

```
[no_desktop]
#macro description No Desktop
#
```

```
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

printer

```
[printer]
#macro description printer
#macro keywords $native_vlan
#
#macro key description: $native_vlan: VLAN sans balise qui sera configuré sur le port
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_printer

```
[no_printer]
#macro description No printer
#
no switchport access vlan
no switchport mode
#
```

```
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

guest

```
[guest]
#macro description guest
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré sur le port
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_guest]]

```
[no_guest]
#macro description No guest
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
```

```
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

server

```
[server]
#macro description server
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré sur le port
#                         $max_hosts: Nombre maximum de périphériques autorisés sur le port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_server

```
[no_server]
#macro description No server
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
spanning-tree portfast auto
```

```
#
@
```

host

```
[host]
#macro description host
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré sur le port
#                         $max_hosts: Nombre maximum de périphériques autorisés sur le port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_host

```
[no_host]
#macro description No host
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_camera

```
[ip_camera]
#macro description ip_camera
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré sur le port
#Default Values are
#$native_vlan = Default VLAN
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_camera

```
[no_ip_camera]
#macro description No ip_camera
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone

```
[ip_phone]
#macro description ip_phone
#macro keywords $native_vlan $voice_vlan $max_hosts
#
```

```
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré sur le port
#                         $voice_vlan: ID du VLAN voix
#                         $max_hosts: Nombre maximum de périphériques autorisés sur le port
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone

```
[no_ip_phone]
#macro description no ip_phone
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: ID du VLAN voix
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone_desktop

```
[ip_phone_desktop]
#macro description ip_phone_desktop
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré sur le port
#                         $voice_vlan: ID du VLAN voix
#                         $max_hosts: Nombre maximum de périphériques autorisés sur le port
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone_desktop

```
[no_ip_phone_desktop]
#macro description no ip_phone_desktop
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: ID du VLAN voix
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
```

```
spanning-tree portfast auto
#
@
```

switch

```
[switch]
#macro description switch
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré sur le port
#                        $voice_vlan: ID du VLAN voix
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
#
@
```

no_switch

```
[no_switch]
#macro description No switch
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: ID du VLAN voix
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

router

```
[router]
#macro description router
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré sur le port
#                        $voice_vlan: ID du VLAN voix
#
```

```
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree link-type point-to-point
#
@
```

no_router

```
[no_router]

#macro description No router

#macro keywords $voice_vlan

#

#macro key description:   $voice_vlan: ID du VLAN voix

#

no smartport switchport trunk native vlan

smartport switchport trunk allowed vlan remove all

#

no smartport storm-control broadcast enable

no smartport storm-control broadcast level

#

no spanning-tree link-type

#

@
```

ap

```
[ap]
#macro description ap
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré sur le port
```

13

Gestion des ports : PoE

La fonctionnalité PoE (Power over Ethernet) n'est disponible que sur les appareils basés sur PoE. Une liste de ces appareils vous est présentée à la section **Modèles de périphériques**.

Cette section décrit comment utiliser la fonctionnalité PoE.

Elle couvre les rubriques suivantes :

- **PoE sur l'appareil**
- **Propriétés PoE**
- **Paramètres PoE**

PoE sur l'appareil

Un appareil PoE est un PSE (Power Sourcing Equipment) qui assure l'alimentation électrique des appareils alimentés (PD, Powered Devices) connectés par les câbles cuivre existants, sans interférence avec le trafic réseau, la mise à jour du réseau physique ou la modification de l'infrastructure réseau.

Consultez la section **Modèles de périphériques** pour en savoir plus sur la prise en charge PoE sur les différents modèles.

Fonctions PoE

PoE offre les fonctions suivantes :

- Elle élimine le besoin d'assurer l'alimentation 110/220 V (CA) de tous les appareils connectés à un réseau local (LAN) filaire.
- Elle supprime la nécessité de placer tous les appareils réseau à proximité de sources d'alimentation.
- Elle élimine le besoin de déployer des systèmes à double câblage dans une entreprise et permet ainsi de réduire de façon significative les coûts d'installation.

PoE peut être utilisé dans tout réseau d'entreprise déployant des appareils de puissance relativement faible connectés au LAN Ethernet et notamment :

- les téléphones IP ;
- les points d'accès sans fil ;
- les passerelles IP ;
- les appareils de surveillance audio et vidéo à distance.

Fonctionnement de PoE

Le processus de mise en œuvre de PoE comprend les étapes suivantes :

- **Détection** : envoie des impulsions spéciales sur le câble cuivre. Lorsqu'un appareil PoE est situé à l'autre extrémité, cet appareil répond à ces impulsions.
- **Classification** : la négociation entre le PSE (Power Sourcing Equipment) et l'appareil alimenté (PD, Powered Device) débute après l'étape de détection. Au cours de la négociation, l'appareil alimenté spécifie sa classe, qui correspond à la quantité maximale d'énergie qu'il consomme.
- **Consommation électrique** : une fois l'étape de classification terminée, le PSE assure l'alimentation de l'appareil alimenté (PD). Si l'appareil alimenté prend en charge la technologie PoE, mais sans classification, il est supposé être de classe 0 (le maximum). Si un appareil alimenté essaie de consommer plus d'énergie que ne l'autorise la norme, le PSE arrête d'alimenter le port.

Le PoE prend en charge deux modes :

- **Limite du port** : la puissance maximale que l'appareil accepte de fournir est limitée à la valeur configurée par l'administrateur système, indépendamment du résultat de la classification.
- **Limite de classe** : la puissance maximale que l'appareil accepte de fournir est déterminée par les résultats obtenus à l'étape de classification. Cela signifie qu'elle est définie conformément à la demande du client.

Considérations relatives à la configuration de PoE

Deux facteurs sont à prendre en considération dans la fonctionnalité PoE :

- la quantité d'énergie que le PSE peut fournir ;
- la quantité d'énergie que l'appareil alimenté essaie vraiment de consommer.

Les options suivantes peuvent être configurées :

- puissance maximale qu'un PSE est autorisé à fournir à un PD ;
- alors que l'appareil fonctionne, de changer le mode de Limite de classe en Limite du port et vice versa. Les valeurs de puissance par port qui ont été configurées pour le mode Port Limit sont conservées.

  REMARQUE Remplacer le mode Limite de classe par Limite de port et inversement tandis que l'appareil PSE fonctionne provoque le redémarrage forcé de l'appareil alimenté.
- De la limite de port maximale autorisée en tant que limite numérique par port en mW (mode Port Limit).
- De générer un filtre lorsqu'un appareil alimenté essaie de consommer trop d'énergie et à quel pourcentage de la puissance maximale ce filtre est généré.

Le matériel PoE spécifique détecte automatiquement la classe du PD et sa limite de puissance en fonction de la classe de l'appareil connecté à chaque port spécifique (mode Limite de classe).

Si, à tout moment au cours de la connexion, un PD relié nécessite plus de puissance de la part du PSE que l'allocation configurée ne le permet (que le PSE soit en mode Limite de classe ou Limite du port), le PSE en question :

- maintient l'état actif/inactif de la liaison du port PoE ;
- désactive l'alimentation du port PoE ;
- consigne le motif de l'arrêt de l'alimentation ;
- génère un filtre SNMP.

ATTENTION Lorsque vous connectez un commutateur capable d'alimenter des appareils PoE, tenez compte des éléments suivants :

Les modèles de commutateurs PoE des séries Sx200, Sx300 et SF500 sont des PSE pouvant fournir une alimentation CC aux appareils PD qui y sont reliés. Ces derniers englobent notamment des téléphones VoIP, des caméras IP et des points d'accès sans fil. Les commutateurs PoE peuvent détecter et alimenter des appareils alimentés préalablement standard PoE hérités. En raison de la prise en charge de l'ancien PoE, un appareil PoE agissant en tant que PSE peut détecter et alimenter à tort un appareil PSE connecté, y compris d'autres commutateurs PoE, en tant qu'ancien appareil alimenté.

Même si les commutateurs PoE Sx200/300/500 sont des appareils PSE qui doivent être alimentés en courant alternatif, ils peuvent être alimentés en tant qu'appareil alimenté hérité par un autre PSE suite à une erreur de détection. Dans cette situation, l'appareil PoE risque de ne pas fonctionner correctement et peut également ne pas alimenter convenablement ses PD connectés.

Pour éviter toute erreur de détection, vous devez désactiver le PoE au niveau des ports des commutateurs PoE que vous utilisez pour vous connecter à des appareils PSE. Vous devez également d'abord alimenter un appareil PSE avant de le connecter à un appareil PoE. Lorsqu'un appareil est considéré à tort comme un appareil alimenté, vous devez le déconnecter du port PoE, puis l'alimenter avec du courant alternatif avant de reconnecter ses ports PoE.

Propriétés PoE

La page Propriétés PoE permet de sélectionner le mode PoE Limite du port ou Limite de classe, et de spécifier les interceptions PoE à générer.

Ces paramètres sont saisis à l'avance. Lorsque l'appareil alimenté se connecte et consomme de l'énergie, il peut consommer beaucoup moins que la puissance maximale autorisée.

La puissance de sortie est désactivée lors du redémarrage, de l'initialisation et de la configuration système pour veiller à ne pas endommager les PD.

Pour configurer PoE sur l'appareil et surveiller la puissance consommée :

ÉTAPE 1 Cliquez sur **Gestion des ports > PoE > Propriétés**.

ÉTAPE 2 Entrez les valeurs des champs suivants :

- **Mode d'alimentation** : sélectionnez l'une des options suivantes :
  - *Limite du port* : la limite maximale de puissance de chaque port est configurée par l'utilisateur.
  - *Limite de classe* : la limite maximale de puissance par port est déterminée par la classe de l'appareil, elle-même résultant de l'étape de classification.

  REMARQUE Lorsque vous modifiez le mode de Limite de port à Limite de classe ou inversement, vous devez d'abord désactiver les ports PoE, puis les réactiver après avoir modifié les options de configuration de l'alimentation.
- **Interceptions** : permet d'activer ou de désactiver les interceptions. Si les interceptions sont activées, vous devez également activer SNMP et configurer au moins un destinataire de notification SNMP.
- **Seuil des interceptions d'alimentation** : saisissez le seuil d'utilisation sous la forme d'un pourcentage de la limite de puissance. Une alarme se déclenche si la puissance dépasse cette valeur.

Les compteurs suivants s'affichent :

- **Puissance nominale** : quantité totale de puissance que l'appareil peut fournir à l'ensemble des appareils alimentés connectés.

- **Consommation** : puissance actuellement consommée par les ports PoE.
- **Puissance disponible** : puissance nominale moins la quantité de puissance consommée.

ÉTAPE 3 Cliquez sur **Appliquer** pour enregistrer les propriétés PoE.

Paramètres PoE

La page Paramètres PoE affiche les informations PoE système sur l'activation de PoE sur les interfaces, la surveillance de la consommation actuelle et la limite maximale de puissance par port.

Cette page permet de limiter la puissance par port de deux façons différentes, ceci en fonction du mode d'alimentation :

- **Limite du port** : la puissance est limitée à une consommation en watts spécifique. Pour que ces paramètres soient actifs, le système doit être en mode Limite du port PoE. Vous pouvez configurer ce mode sur la page Propriétés PoE.

  Lorsque l'énergie consommée sur le port dépasse la limite du port, l'alimentation du port est désactivée.

- **Limite de classe** : la puissance est limitée en fonction de la classe de l'appareil alimenté connecté. Pour que ces paramètres soient actifs, le système doit être en mode Limite de classe PoE. Vous pouvez configurer ce mode sur la page Propriétés PoE.

  Lorsque l'énergie consommée sur le port dépasse la limite de classe, l'alimentation du port est désactivée.

Exemple de priorité PoE :

Supposition : un appareil doté de 48 ports fournit un total de 375 watts.

L'administrateur configure tous les ports pour qu'ils allouent jusqu'à 30 watts. Au final, si les 48 ports allouent 30 watts chacun, on obtient 1440 watts, ce qui est beaucoup trop. L'appareil ne peut pas fournir suffisamment de puissance à chaque port, il suit donc certaines priorités.

L'administrateur définit la priorité de chaque port, en lui allouant autant de puissance que possible.

Vous devez entrer ces priorités sur la page Paramètres PoE.

Reportez-vous à la section **Modèles de périphériques** pour obtenir une description des modèles d'appareils qui prennent en charge la fonctionnalité PoE et connaître la puissance maximale pouvant être allouée aux ports PoE.

Pour configurer les paramètres de port PoE :

ÉTAPE 1 Cliquez sur **Gestion des ports > PoE > Paramètres**. La liste des champs ci-dessous correspond au mode d'alimentation Limite du port. Les champs peuvent légèrement différer si le mode d'alimentation est Limite de classe.

ÉTAPE 2 Sélectionnez un port puis cliquez sur **Modifier.**

ÉTAPE 3 Renseignez le champ suivant :

- **Interface** : sélectionnez le port à configurer.
- **État administratif PoE** : permet d'activer ou de désactiver PoE sur le port.
- **Niveau de priorité d'alimentation** : sélectionnez la priorité du port (faible, élevée ou critique) à utiliser lorsque l'alimentation est faible. Par exemple, si 99 % de la puissance disponible est consommée, et que le port 1 a une priorité élevée et le port 3 une priorité faible, le port 1 sera alimenté, contrairement au port 3.
- **Affectation de puissance administrative** : ce champ s'affiche uniquement si le mode d'alimentation Limite du port est défini sur la page Propriétés PoE. Si le mode d'alimentation Limite du port est sélectionné, saisissez la puissance affectée au port (en milliwatts).
- **Affectation de puissance maximale** : ce champ s'affiche uniquement si le mode d'alimentation Limite de puissance est défini sur la page Propriétés PoE. Affiche la puissance maximale autorisée sur ce port.
- **Consommation électrique** : affiche la puissance (en milliwatts) affectée à l'appareil alimenté connecté à l'interface sélectionnée.
- **Classe** : ce champ n'est modifiable que si le mode d'alimentation Limite de classe est défini sur la page Propriétés PoE. La classe détermine le niveau de puissance :

Classe	Puissance maximale fournie par le port de l'appareil
0	15,4 watts
1	4,0 watts
2	7,0 W
3	15,4 watts
4	30,0 watts

- **Nombre de surcharges** : affiche le nombre total d'occurrences de surcharges de courant.
- **Nombre de courts-circuits** : affiche le nombre total d'occurrences de courts-circuits électriques.
- **Nombre de refus** : affiche le nombre de fois où l'alimentation a été refusée pour l'appareil alimenté.
- **Nombre d'absences** : affiche le nombre de fois où l'alimentation de l'appareil alimenté a été arrêtée, l'appareil n'étant plus détecté.
- **Nombre de signatures non valides** : affiche le nombre de fois où une signature non valide a été reçue. L'appareil alimenté utilise des signatures pour s'identifier auprès du PSE. Ces signatures sont générées lors de la détection, la classification ou la maintenance de l'appareil alimenté.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres PoE du port sont consignés dans le fichier de Configuration d'exécution.

14

Gestion des VLAN

Cette section aborde les points suivants :

- **Présentation**
- **VLAN standard**
- **VLAN voix**

Présentation

Un VLAN (Virtual LAN, réseau local virtuel) est un groupe logique de ports qui permet aux périphériques qui lui sont associés de communiquer entre eux sur une couche MAC Ethernet, quel que soit le segment LAN physique du réseau ponté auquel ils sont connectés.

Description des VLAN

Chaque VLAN est configuré avec un ID de VLAN unique (VID) ayant une valeur comprise entre 1 et 4094. Un port sur un périphérique d'un réseau raccordé est membre d'un VLAN s'il peut échanger (envoyer/recevoir) des données avec le VLAN. Un port est un membre non balisé d'un VLAN si aucun des paquets qui lui sont destinés ne dispose d'une balise VLAN. Un port est un membre balisé d'un VLAN si tous les paquets qui lui sont destinés disposent d'une balise VLAN. Un port peut être membre d'un seul VLAN non balisé ou de plusieurs VLAN balisés.

Un port en mode Accès VLAN ne peut faire partie que d'un seul VLAN. S'il est en mode General (Général) ou Trunk (Liaison), le port peut faire partie d'un ou de plusieurs VLAN.

Les VLAN permettent de faire face aux problèmes de sécurité et d'évolutivité. Le trafic d'un VLAN reste à l'intérieur du VLAN et se termine au niveau de ses périphériques. Le VLAN facilite également la configuration réseau en connectant logiquement les périphériques sans les transférer physiquement.

Si une trame est balisée VLAN, une balise VLAN à quatre octets est ajoutée à chaque trame Ethernet. La balise contient un ID de VLAN compris entre 1 et 4094 et une balise de priorité VLAN (VPT, VLAN Priority Tag) comprise entre 0 et 7. Pour plus d'informations sur la balise de priorité VLAN, reportez-vous à la section **Qualité de service**.

Lorsqu'une trame entre dans un périphérique tenant compte du VLAN, elle est classée comme appartenant à un VLAN, en vertu de la balise VLAN à quatre octets qu'elle contient.

S'il n'existe aucune balise VLAN dans la trame ou si la trame comporte une balise de priorité, elle est catégorisée dans le VLAN selon le PVID (identificateur de port VLAN) configuré au port de réception de la trame.

La trame est désactivée au niveau du port d'entrée si le filtrage d'entrée est activé et si le port d'entrée n'est pas membre du VLAN auquel appartient le paquet. Une trame est considérée comme balisée d'une priorité uniquement si le VID présent dans sa balise VLAN est 0.

Les trames appartenant à un VLAN restent dans le VLAN. Ce principe est appliqué par l'envoi ou le réacheminement d'une trame uniquement aux ports de sortie membres du VLAN cible. Un port de sortie peut être un membre balisé ou non balisé d'un VLAN.

Le port de sortie :

- Ajoute une balise VLAN à la trame si le port de sortie est un membre balisé du VLAN cible et si la trame d'origine n'a pas de balise VLAN.
- Supprime la balise VLAN de la trame si le port de sortie est un membre non balisé du VLAN cible et si la trame d'origine a une balise VLAN.

Rôles du VLAN

Tout le trafic VLAN (monodiffusion/diffusion/multidiffusion) demeure au sein du VLAN. Les périphériques reliés à différents VLAN n'ont pas de connectivité directe entre eux sur la couche MAC Ethernet.

Les réseaux VLAN d'un périphérique peuvent être créés uniquement de manière statique.

Certains VLAN peuvent avoir des rôles supplémentaires, notamment :

- VLAN voix : pour plus d'informations, reportez-vous à la section VLAN voix.
- VLAN invité : défini sur la page Modifier l'authentification VLAN.
- VLAN par défaut : pour plus d'informations, reportez-vous à la section Configuration des paramètres VLAN par défaut.
- VLAN de gestion : pour plus d'informations, reportez-vous à la section Configuration des informations IP.

QinQ

QinQ fournit l'isolation entre les réseaux de fournisseur de services et les réseaux de client. Le périphérique est un pont fournisseur qui prend en charge l'interface de service « c-tagged » basée sur les ports.

Avec QinQ, le périphérique ajoute une balise ID appelée ServiceTag (S-tag) qui permet de transférer le trafic sur le réseau. La balise S-tag permet de répartir le trafic entre plusieurs clients, tout en conservant les balises VLAN du client.

Le trafic du client est encapsulé avec une balise S-tag avec TPID 0x8100, indépendamment du fait qu'il soit au départ balisé « c-tagged » ou non balisé. La balise S-tag permet à ce trafic d'être traité comme un agrégat au sein d'un réseau de pont fournisseur, dans lequel le pontage est uniquement basé sur le VID S-tag (S-VID).

La balise S-Tag est conservée lorsque le trafic est transféré par le biais de l'infrastructure du fournisseur de services réseau ; elle est ensuite supprimée par un périphérique de sortie.

Un autre avantage de QinQ est qu'il n'est pas nécessaire de configurer les dispositifs de bordure du client.

Vous pouvez activer QinQ sur la page Gestion des VLAN > Paramètres d'interface.

VLAN standard

Cette section décrit les pages de l'interface utilisateur permettant de configurer les différents types de VLAN. Cette section décrit les processus suivants :

- **Charge de travail de la configuration VLAN**
- **Paramètres VLAN par défaut**
- **Paramètres VLAN - Création de VLAN**
- **Paramètres d'interface**
- **Appartenance VLAN**
- **Port vers VLAN**
- **Appartenance VLAN des ports**

Charge de travail de la configuration VLAN

Pour configurer les VLAN :

1. Le cas échéant, modifiez le VLAN par défaut en suivant les instructions de la section **Paramètres VLAN par défaut**.
2. Créez les VLAN requis en suivant les instructions de la section **Paramètres VLAN - Création de VLAN**.
3. Définissez la configuration VLAN souhaitée pour les ports et activez QinQ sur une interface comme décrit dans la section **Paramètres d'interface**.

4. Assignez des interfaces aux VLAN comme décrit dans la section **Port vers VLAN** ou la section **Appartenance VLAN des ports**.
5. Affichez l'appartenance actuelle des ports au VLAN pour toutes les interfaces, comme décrit dans la section **Appartenance VLAN des ports**.

Paramètres VLAN par défaut

Si les paramètres d'usine par défaut sont utilisés, le périphérique crée automatiquement un VLAN 1 en tant que VLAN par défaut. L'état de l'interface par défaut de tous les ports est défini sur Liaison et tous les ports sont configurés en tant que membres non balisés du VLAN par défaut.

Le VLAN par défaut présente les caractéristiques suivantes :

- Il est distinct, non statique/non dynamique et tous les ports sont des membres non balisés par défaut.
- Il peut être supprimé.
- Il ne peut recevoir d'étiquette.
- Il ne peut pas être utilisé pour un rôle spécial tel qu'un VLAN non authentifié ou un VLAN voix. Cette option ne concerne que les VLAN voix avec le mode OUI activé.
- Si un port n'est plus membre d'un VLAN, le périphérique le configure automatiquement en tant que membre non balisé du VLAN par défaut. Un port n'est plus membre d'un VLAN si le VLAN est supprimé ou si le port est supprimé du VLAN.

Lorsque le VID du VLAN par défaut est modifié, le périphérique exécute les opérations suivantes sur tous les ports du VLAN après avoir enregistré la configuration et redémarré :

- Supprime l'appartenance des ports au VLAN par défaut d'origine (prend effet après redémarrage).
- Remplace le PVID (identificateur de port VLAN) des ports par le VID du nouveau VLAN par défaut.
- L'ID du réseau VLAN par défaut d'origine est supprimé du périphérique. Il doit être recréé pour pouvoir être utilisé.
- Il ajoute les ports en tant que membres VLAN non balisés du nouveau VLAN par défaut.

Pour changer le VLAN par défaut :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres VLAN par défaut**.

ÉTAPE 2 Renseignez le champ suivant :

- **ID VLAN par défaut actuel** : affiche l'ID du VLAN par défaut actuel.
- **ID VLAN par défaut après redémarrage** : saisissez un nouvel ID de VLAN pour remplacer l'ID de VLAN par défaut après le redémarrage.

ÉTAPE 3 Cliquez sur **Appliquer**.

ÉTAPE 4 Cliquez sur **Enregistrer** (dans le coin supérieur droit de la fenêtre) et enregistrez la Configuration d'exécution dans la Configuration de démarrage.

L'**ID VLAN par défaut après réinitialisation** devient l'**ID VLAN par défaut actuel** après le redémarrage du périphérique.

Paramètres VLAN - Création de VLAN

Vous pouvez créer un VLAN, mais cela n'a aucun effet tant que le VLAN n'est pas manuellement ou dynamiquement lié à un port au moins. Les ports doivent toujours appartenir à un ou plusieurs VLAN.

Le périphérique de la série 200 prend en charge jusqu'à 256 VLAN, y compris le VLAN par défaut.

Chaque VLAN doit être configuré avec un ID unique ayant une valeur comprise entre 1 et 4094. Le périphérique se réserve le VID 4095 comme VLAN d'abandon. Tous les paquets classés comme VLAN d'abandon sont abandonnés à l'entrée et ne sont pas transférés vers un port.

Pour créer un VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres VLAN**.

Les informations s'affichent pour tous les VLAN définis. Les champs ci-dessous sont définis sur la page **Ajouter**. Le champ suivant n'est pas sur la page **Ajouter**.

- **Initiateurs** : façon dont le VLAN a été créé :
  - *Statique* : le VLAN a été défini par l'utilisateur.
  - *Par défaut* : c'est le VLAN par défaut.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un ou plusieurs nouveaux VLAN.

La page permet la création d'un VLAN unique ou d'une plage de VLAN.

ÉTAPE 3 Pour créer un seul VLAN, sélectionnez le bouton **VLAN**, saisissez l'**ID de VLAN** et le **Nom du VLAN** (facultatif).

Pour créer une plage de VLAN, sélectionnez le bouton **Plage** et spécifiez la plage de VLAN à créer en saisissant le VID de départ et le VID de fin (ces valeurs sont comprises). Si vous utilisez la fonction **Plage**, le nombre maximal de VLAN que vous pouvez créer en une seule fois est 100.

ÉTAPE 4 Ajoutez les champs suivants pour les nouveaux VLAN.

- **État de l'interface VLAN** : sélectionnez cette option pour arrêter le VLAN. Dans cet état, le VLAN ne transmet/reçoit pas de messages.

- en provenance/vers des niveaux plus élevés. Par exemple, si vous arrêtez un VLAN, sur lequel une interface IP est configurée,
- le pontage dans le VLAN continue, mais le commutateur ne peut pas transmettre ni recevoir le trafic IP sur le VLAN
- **Interceptions SNMP d'état de lien** : sélectionnez cette option pour activer la génération des interceptions SNMP relatives à l'état de la liaison.

ÉTAPE 5 Cliquez sur **Appliquer** pour créer le ou les VLAN.

Paramètres d'interface

La page *Paramètres d'interface* affiche et active la configuration des paramètres du VLAN pour toutes les interfaces.

Pour configurer les paramètres du VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres d'interface**.

ÉTAPE 2 Sélectionnez un type d'interface (Port ou LAG) et cliquez sur **OK**. Les ports ou LAG et leurs paramètres VLAN s'affichent.

ÉTAPE 3 Pour configurer un port ou LAG, sélectionnez-le puis cliquez sur **Modifier**.

ÉTAPE 4 Entrez les valeurs des champs suivants :

- **Interface** : sélectionnez un port/LAG.
- **Mode d'interface VLAN** : sélectionnez le mode d'interface du VLAN. Les options sont les suivantes :
  - *Général* : l'interface peut prendre en charge toutes les fonctions telles qu'elles sont définies dans la spécification IEEE 802.1q. Elle peut être un membre balisé ou non balisé d'un ou de plusieurs VLAN.
  - *Accès* : l'interface est un membre non balisé d'un VLAN unique. Un port configuré dans ce mode est appelé un port d'accès.
  - *Liaison* : l'interface est membre non balisé d'un VLAN au maximum, ainsi que membre balisé de zéro ou plusieurs VLAN. Un port configuré dans ce mode est appelé un port de liaison.
  - *Client* : sélectionnez cette option pour mettre l'interface en mode QinQ. Vous pouvez ainsi appliquer votre propre agencement VLAN (PVID) sur le réseau du fournisseur. Le périphérique est en mode Q-in-Q lorsqu'il comporte un ou plusieurs ports client. Reportez-vous à la section **QinQ**.

- **PVID administratif** : saisissez l'ID VLAN du port (PVID) du VLAN pour lequel les trames non balisées entrantes et les trames balisées de priorité sont classées. Les valeurs possibles sont comprises entre 1 et 4094.
- **Type de trame** : sélectionnez le type de trame que l'interface peut recevoir. Les trames qui ne sont pas du type configuré sont abandonnées à l'entrée. Ces types de trames sont uniquement disponibles en mode General. Les valeurs possibles sont les suivantes :
  - *Tout admettre* : l'interface accepte tous les types de trames, non balisées, balisées et balisées de priorité.
  - *Admettre balisées uniquement* : l'interface accepte uniquement les trames balisées.
  - *Admettre non balisées uniquement* : l'interface accepte uniquement les trames de priorité et les trames non balisées.
- **Filtrage d'entrée** : (uniquement disponible en mode Général) sélectionnez cette option pour activer le filtrage en entrée. Lorsqu'une interface est en mode de filtrage d'entrée, elle abandonne toutes les trames entrantes classées comme appartenant aux VLAN dont elle n'est pas membre. Le filtrage d'entrée peut être désactivé ou activé sur les ports généraux. Il est toujours activé sur les ports d'accès et les ports de liaison.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres sont écrits dans le fichier de Configuration d'exécution.

Appartenance VLAN

Les pages Port vers VLAN et Appartenance VLAN des ports affichent les appartenances VLAN des ports dans diverses présentations. Vous pouvez les utiliser pour ajouter des appartenances aux VLAN ou en supprimer de ces derniers.

Lorsque l'appartenance au VLAN par défaut est interdite pour un port, celui-ci ne peut appartenir à aucun autre VLAN. Le VID interne 4095 est affecté au port.

Pour transférer correctement les paquets, les périphériques intermédiaires tenant compte du VLAN qui acheminent le trafic VLAN entre les nœuds d'extrémité doivent être configurés manuellement.

Les ports non balisés de deux périphériques prenant en compte le VLAN sans aucune intervention des périphériques doivent disposer de la même appartenance VLAN. En d'autres termes, le PVID sur les ports entre les deux périphériques doit être le même si les ports doivent échanger (envoyer/recevoir) des paquets non balisés avec le VLAN. Dans le cas contraire, le trafic peut fuir d'un VLAN vers un autre.

Les trames balisées VLAN peuvent traverser d'autres périphériques réseau tenant compte ou non du VLAN. Si un nœud d'extrémité de destination ne tient pas compte du VLAN, mais doit recevoir du trafic d'un VLAN, alors le dernier périphérique tenant compte du VLAN (s'il en existe un) doit envoyer les trames du VLAN de destination au nœud d'extrémité sous forme non balisée.

Port vers VLAN

Utilisez la page Port vers VLAN pour afficher et configurer les ports dans un VLAN spécifique.

Pour mapper des ports ou des LAG à un VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Port vers VLAN**.

ÉTAPE 2 Sélectionnez un VLAN et le type d'interface (Port ou LAG), puis cliquez sur **OK** pour afficher ou modifier la caractéristique du port relative au VLAN.

Le mode actuel de chaque port ou LAG s'affiche (Accès, Liaison, Général ou Client). Vous pouvez configurer ce mode sur la page Paramètres d'interface.

Chaque port ou LAG s'affiche avec son enregistrement actuel sur le VLAN.

ÉTAPE 3 Modifiez l'enregistrement d'une interface sur le VLAN en sélectionnant le **Nom de l'interface** et l'option souhaitée dans la liste suivante :

- **Mode VLAN** : type des ports dans le VLAN.
- **Type d'appartenance** :
  - *Interdit* : l'interface n'est pas autorisée à rejoindre le VLAN. Lorsqu'un port n'est pas membre d'un autre VLAN, l'activation de cette option sur le port l'intègre au VLAN interne 4095 (VID réservé).
  - Exclu : l'interface n'est actuellement pas membre du VLAN. Ceci est le paramètre par défaut pour tous les ports et LAG lorsqu'un nouveau VLAN vient d'être créé.
  - *Balisé* : l'interface est un membre balisé du VLAN.
  - *Non balisé* : l'interface est un membre non balisé du VLAN. Les trames du VLAN sont envoyées non balisées à l'interface VLAN.
  - **PVID** : sélectionnez cette option pour définir le PVID de l'interface avec le VID du VLAN. Le PVID est un paramètre propre à chaque port.

ÉTAPE 4 Cliquez sur **Appliquer**. Les interfaces sont attribuées au VLAN et écrites dans le fichier de Configuration d'exécution.

Vous pouvez continuer d'afficher et/ou de configurer l'appartenance de port à un autre VLAN en sélectionnant l'ID d'un autre VLAN.

Appartenance VLAN des ports

La page Appartenance VLAN des ports affiche tous les ports du périphérique, ainsi qu'une liste des VLAN auxquels chaque port appartient.

Si la méthode d'authentification basée sur les ports pour une interface est 802.1x et que le Contrôle de port administratif est Auto, alors :

- Tant que le port n'est pas authentifié, il est exclu de tous les VLAN, à l'exception des VLAN invités et non authentifiés. Sur la page VLAN vers port, le port est marqué d'un « P » majuscule.
- Lorsque le port est authentifié, il reçoit l'appartenance dans le VLAN où il a été configuré.

Pour attribuer un port à un ou plusieurs VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Appartenance VLAN des ports**.

ÉTAPE 2 Sélectionnez un type d'interface (Port ou LAG), puis cliquez sur **OK**. Les champs suivants s'affichent pour toutes les interfaces du type sélectionné :

- **Interface** : ID du port/LAG.
- **Mode** : mode VLAN d'interface qui a été sélectionné sur la page Paramètres d'interface.
- **VLAN administratifs** : liste déroulante qui affiche tous les VLAN dont l'interface peut être membre.
- **VLAN opérationnels** : liste déroulante qui affiche tous les VLAN dont l'interface est actuellement membre.
- **LAG** : si l'interface sélectionnée est Port, affiche le LAG dont elle est membre.

ÉTAPE 3 Sélectionnez un port et cliquez sur le bouton **Connecter le VLAN**.

ÉTAPE 4 Entrez les valeurs des champs suivants :

- **Interface** : sélectionnez un port/LAG.
- **Mode** : affiche le mode VLAN du port qui a été sélectionné sur la page Paramètres d'interface.
- **Sélectionner le VLAN** : pour associer un port à un ou plusieurs VLAN, déplacez le ou les ID de VLAN de la liste de gauche vers la liste de droite à l'aide des flèches. Le VLAN par défaut peut apparaître dans la liste de droite s'il est balisé. Il ne peut cependant pas être sélectionné.
- **Balisage** : sélectionnez une des options de PVID/balisage suivantes :
  - **Interdit** : l'interface n'est pas autorisée à rejoindre le VLAN même à partir de l'enregistrement GVRP. Lorsqu'un port n'est pas membre d'un autre VLAN, l'activation de cette option sur le port l'intègre au VLAN interne 4095 (VID réservé).
  - **Balisé** : permet d'indiquer si le port est balisé.

- **Non balisé** : sélectionnez cette option pour que le port soit non balisé. Cette option ne concerne pas les ports d'accès.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres sont modifiés et écrits dans le fichier de Configuration d'exécution.

Pour afficher les VLAN administratifs et opérationnels sur une interface, cliquez sur **Détails**.

VLAN voix

Dans un LAN, les périphériques vocaux tels que les téléphones IP, les points d'extrémité VoIP et les systèmes vocaux sont placés dans le même VLAN. On appelle ce VLAN un VLAN voix. Si les périphériques vocaux se trouvent dans d'autres VLAN voix, des routeurs IP (couche 3) sont requis pour établir la communication.

Cette section aborde les points suivants :

- **Présentation du VLAN voix**
- **Configuration de VLAN voix**
- **OUI de téléphonie**

Présentation du VLAN voix

Cette section aborde les points suivants :

- **Modes VLAN voix dynamiques**
- **VLAN voix automatique, Port intelligent automatique, CDP et LLDP**
- **QoS VLAN voix**
- **Contraintes du VLAN voix**
- **Flux de travail de VLAN voix**

Vous trouverez ci-après des exemples de déploiement vocal classiques, accompagnés des configurations appropriées :

- **UC3xx/UC5xx hébergé** : tous les téléphones et points d'extrémité VoIP Cisco prennent en charge ce modèle de déploiement. Pour ce modèle (UC3xx/UC5xx), les téléphones et points d'extrémité VoIP Cisco résident sur le même VLAN voix. Par défaut, le VLAN voix de UC3xx/UC5xx est le VLAN 100.

- **PBX IP tiers hébergé** : les téléphones SBTG CP-79xx et SPA5xx ainsi que les points d'extrémité SPA8800 Cisco prennent en charge ce modèle de déploiement. Dans ce modèle, le VLAN utilisé par les téléphones est déterminé par la configuration réseau. Il peut éventuellement y avoir des VLAN voix et données séparés. Les téléphones et points d'extrémité VoIP s'inscrivent avec un PBX IP sur site.
- **Centrex IP/ITSP hébergé** : les téléphones CP-79xx et SPA5xx ainsi que les points d'extrémité SPA8800 Cisco prennent en charge ce modèle de déploiement. Dans ce modèle, le VLAN utilisé par les téléphones est déterminé par la configuration réseau. Il peut éventuellement y avoir des VLAN voix et données séparés. Les téléphones et points d'extrémité VoIP s'inscrivent sur un proxy SIP hors site dans le cloud.

En ce qui concerne le VLAN, les modèles ci-dessus fonctionnent dans des environnements tenant compte du VLAN et ne tenant pas compte du VLAN. Dans l'environnement tenant compte du VLAN, le VLAN voix fait partie des nombreux VLAN configurés dans une installation. L'exemple ne tenant pas compte du VLAN est équivalent à un environnement tenant compte du VLAN avec un seul VLAN.

Le périphérique fonctionne toujours en tant que commutateur tenant compte du VLAN.

Le périphérique prend en charge un seul VLAN voix. Par défaut, le VLAN voix est le VLAN 1. Par défaut, le VLAN voix est le VLAN 1. Un autre VLAN voix peuvent être configuré manuellement. Il peut aussi être appris dynamiquement lorsque la fonction VLAN voix automatique est activée.

Vous pouvez ajouter manuellement des ports au VLAN voix à l'aide de la configuration VLAN de base décrite à la section Configuration des paramètres d'interface VLAN, ou en appliquant manuellement aux ports la macro Port intelligent relative à la voix. Vous avez aussi la possibilité de les ajouter dynamiquement si le périphérique est en mode OUI de téléphonie ou que la fonction Ports intelligents automatiques est activée pour celui-ci.

Modes VLAN voix dynamiques

Le périphérique prend en charge deux modes VLAN voix dynamiques : OUI de téléphonie (Organization Unique Identifier) et VLAN voix automatique. Les deux modes influencent la façon dont le VLAN voix et/ou les appartenances de ports du VLAN voix sont configurés. Les deux modes s'excluent mutuellement.

- **OUI de téléphonie**

  En mode OUI de téléphonie, le VLAN voix doit être un VLAN configuré manuellement et ne peut pas être le VLAN par défaut.

  Lorsque le périphérique est en mode OUI de téléphonie et qu'un port est configuré manuellement comme candidat au VLAN voix, le périphérique ajoute dynamiquement le port au VLAN voix s'il reçoit un paquet dont l'adresse MAC source correspond à celle des OUI de téléphonie configurés. Un OUI correspond aux trois premiers octets d'une adresse MAC Ethernet. Pour plus d'informations sur le mode OUI de téléphonie, reportez-vous à la section **OUI de téléphonie**.

- **VLAN voix automatique**

  En mode VLAN voix automatique, le VLAN voix peut être le VLAN voix par défaut manuellement configuré ou peut être appris à partir de périphériques externes comme UC3xx/5xx et de commutateurs qui annoncent le VLAN voix dans CDP ou VSDP. VSDP est un protocole défini par Cisco pour la détection des services vocaux.

  À la différence du mode OUI de téléphonie qui détecte les périphériques vocaux basés sur le mode OUI de téléphonie, le mode VLAN voix automatique dépend de la fonction Port intelligent automatique pour ajouter dynamiquement les ports au VLAN voix. Si elle est activée, la fonction Port intelligent automatique ajoute un port au VLAN voix lorsqu'elle détecte sur le port un périphérique en cours d'association qui s'annonce en tant que téléphone ou points d'extrémité de média, par l'intermédiaire de CDP et/ou LLDP-MED.

Points d'extrémité vocaux

Pour qu'un VLAN voix fonctionne correctement, les périphériques vocaux tels que les téléphones et points d'extrémité VoIP Cisco doivent être attribués au VLAN pouvant envoyer et recevoir leur trafic vocal. Voici quelques exemples possibles :

- Un téléphone/point d'extrémité peut être configuré de manière statique avec le VLAN voix.
- Un téléphone/point d'extrémité peut obtenir le VLAN voix dans le fichier d'amorçage qu'il télécharge à partir d'un serveur TFTP. Un serveur DHCP peut spécifier le fichier d'amorçage et le serveur TFTP lorsqu'il attribue une adresse IP au téléphone.
- Un téléphone/point d'extrémité peut obtenir les informations VLAN voix à partir des annonces CDP et LLDP-MED qu'il reçoit de ses systèmes vocaux et commutateurs voisins.

Le périphérique attend des périphériques vocaux en cours de raccordement qu'ils envoient des paquets VLAN balisés. Sur les ports où le VLAN voix est également le VLAN natif, les paquets VLAN voix non balisés sont possibles.

VLAN voix automatique, Port intelligent automatique, CDP et LLDP

Valeurs par défaut

Par défaut (paramètres d'usine), CDP, LLDP et LLDP-MED, le mode Port intelligent automatique et le mode de base de QoS avec DSCP de confiance sont activés sur le périphérique, et tous les ports sont membres du VLAN 1 par défaut, qui est aussi le VLAN voix par défaut.

En outre, le mode VLAN voix dynamique est la valeur par défaut du VLAN voix automatique avec activation basée sur le déclenchement, et la fonction Port intelligent automatique est la valeur par défaut à activer en fonction du VLAN voix automatique.

Déclenchements de VLAN voix

Lorsque le mode VLAN voix dynamique est activé sur VLAN voix automatique, cela signifie que le VLAN voix automatique ne devient opérationnel que si un ou plusieurs déclenchements se produisent. Les déclenchements possibles sont la configuration de VLAN voix statique, la réception d'informations VLAN voix dans une annonce de voisinage CDP et la réception d'informations VLAN voix dans le protocole VSDP (Voice VLAN Discovery Protocol). Si vous le souhaitez, vous pouvez rendre le mode VLAN voix automatique immédiatement opérationnel sans attendre de déclenchement.

Si la fonction Port intelligent automatique est activée en fonction du mode VLAN voix automatique, la fonction Port intelligent automatique est activée lorsque le mode VLAN voix automatique devient opérationnel. Si vous le souhaitez, vous pouvez activer la fonction Port intelligent automatique indépendamment du mode VLAN voix automatique.

REMARQUE La liste de configuration par défaut s'applique ici aux commutateurs dont la version du micrologiciel prend directement en charge le mode VLAN voix automatique. Elle s'applique également aux commutateurs non configurés qui ont été mis à niveau vers la version du micrologiciel prenant en charge le mode VLAN voix automatique.

REMARQUE Les déclenchements par défaut et de VLAN voix sont conçus pour n'avoir aucun effet sur les installations ne comportant pas de VLAN voix, ainsi que sur les commutateurs qui ont déjà été configurés. Vous pouvez désactiver et activer manuellement le mode VLAN voix automatique et/ou Port intelligent automatique en fonction de votre déploiement.

VLAN voix automatique

Le mode VLAN voix automatique permet de gérer le VLAN voix, mais dépend de la fonction Port intelligent automatique pour gérer l'appartenance des ports VLAN voix. Le mode VLAN voix automatique offre les fonctions suivantes lorsqu'il est opérationnel :

- Il détecte les informations VLAN voix dans les annonces CDP provenant des périphériques voisins directement connectés.
- Si plusieurs commutateurs et/ou routeurs voisins, tels que des périphériques Cisco Unified Communication (UC), annoncent leur VLAN voix, le VLAN voix du périphérique ayant l'adresse MAC la plus basse est utilisé.

  REMARQUE En cas de connexion du périphérique à un périphérique UC Cisco, vous devrez peut-être configurer le port sur le périphérique UC à l'aide de la commande `switchport voice vlan` afin de vous assurer que le périphérique UC annonce son VLAN voix dans CDP sur le port.
- Il synchronise les paramètres VLAN voix avec les autres commutateurs activés pour le mode VLAN voix automatique, par l'intermédiaire du protocole VSDP (Voice Service Discovery Protocol). Le périphérique se configure toujours lui-même avec le VLAN voix provenant de la source de priorité la plus élevée qu'il détecte. La priorité est basée sur le type de source et l'adresse MAC de la source qui fournit les informations de VLAN voix. Les priorités du type de source, de la plus haute à la plus

basse, sont la configuration VLAN statique, l'annonce CDP et la configuration par défaut basée sur le VLAN par défaut modifié, ainsi que le VLAN voix par défaut. Une adresse MAC numériquement basse a une priorité plus élevée qu'une adresse MAC numériquement haute.

- Il conserve le VLAN voix jusqu'à ce qu'un nouveau VLAN voix provenant d'une source de priorité plus élevée soit détecté ou jusqu'à ce que le mode VLAN voix automatique soit redémarré par l'utilisateur. Après le redémarrage, le périphérique rétablit le VLAN voix par défaut et relance la détection VLAN voix automatique.
- Lorsqu'un nouveau VLAN voix est configuré ou détecté, le périphérique le crée automatiquement et remplace toutes les appartenances de port du VLAN voix existant par celles du nouveau VLAN voix. Cette opération est susceptible d'interrompre ou de terminer des sessions vocales existantes, notamment lorsque la topologie réseau a été modifiée.

L'option Port intelligent automatique fonctionne avec CDP/LLDP pour gérer les appartenances de port du VLAN voix lorsque des points d'extrémité vocaux sont détectés à partir des ports :

- Lorsque CDP et LLDP sont activés, le périphérique envoie périodiquement des paquets CDP et LLDP pour annoncer au VLAN voix les points d'extrémité vocaux à utiliser.
- Lorsqu'un périphérique en cours d'association à un port s'annonce lui-même en tant que point d'extrémité vocal, par l'intermédiaire de CDP et/ou LLDP, la fonction Port intelligent automatique ajoute automatiquement le port au VLAN voix en appliquant au port la macro Port intelligent correspondante (si aucun autre périphérique provenant du port n'annonce une fonctionnalité conflictuelle ou supérieure). Si un périphérique s'annonce lui-même en tant que téléphone, la macro Port intelligent par défaut est le téléphone. Si un périphérique s'annonce lui-même en tant que téléphone et hôte, ou téléphone et pont, la macro Port intelligent par défaut est le téléphone+ bureau.

QoS VLAN voix

Le VLAN voix peut propager les paramètres CoS/802.1p et DSCP à l'aide des stratégies réseau LLDP-MED. Par défaut, le protocole LLDP-MED est défini pour répondre avec le paramètre QoS voix lorsqu'un dispositif envoie des paquets LLDP-MED. Les périphériques prenant en charge MED doivent envoyer leur trafic vocal avec les mêmes valeurs CoS/802.1p et DSCP que celles reçues avec la réponse LLDP-MED.

Vous pouvez désactiver la mise à jour automatique entre le VLAN voix et LLDP-MED, et utiliser vos propres stratégies réseau.

S'il utilise le mode OUI, le périphérique peut en outre configurer le mappage et le re-marquage (CoS/802.1p) du trafic vocal basé sur le OUI.

Par défaut, toutes les interfaces sont approuvées pour CoS/802.1p. Le périphérique applique la qualité de service basée sur la valeur CoS/802.1p qui a été trouvée dans le flux vocal. Pour les flux vocaux OUI de téléphonie, vous pouvez remplacer la qualité de service et éventuellement re-marquer la valeur 802.1p des flux vocaux en spécifiant les valeurs CoS/802.1p souhaitées et en utilisant l'option de re-marquage sous OUI de téléphonie.

Contraintes du VLAN voix

Les contraintes suivantes doivent être prises en compte :

- Seul un VLAN voix est pris en charge.
- Un VLAN défini en tant que VLAN voix ne peut pas être supprimé.

En outre, les contraintes suivantes s'appliquent au OUI de téléphonie :

- Le VLAN voix ne peut pas être le VLAN1 (VLAN par défaut).
- Le VLAN voix ne peut pas être activé pour le mode Port intelligent.
- À l'exception de la décision QoS relative à la stratégie, la décision QoS du VLAN voix est prioritaire sur toute autre décision QoS.
- Un nouvel ID VLAN peut être configuré pour le VLAN voix uniquement si le VLAN voix actuel n'a pas de ports candidats.
- L'interface VLAN d'un port candidat doit être en mode Général ou Liaison.
- La QoS du VLAN voix est appliquée aux ports statiques ainsi qu'aux ports candidats qui ont rejoint le VLAN voix.
- Le flux vocal est accepté si l'adresse MAC peut être apprise par la base de données de transfert (FDB, Forwarding Database). (s'il n'existe aucun espace disponible dans la FDB, aucune action ne se produit).

Flux de travail de VLAN voix

La configuration par défaut du périphérique sur VLAN voix automatique, Ports intelligents automatiques, CDP et LLDP regroupe la plupart des exemples de déploiement vocal courants. Cette section décrit la façon de déployer un VLAN voix lorsque la configuration par défaut ne peut pas être utilisée.

Flux de travail 1 : pour configurer le VLAN voix automatique :

ÉTAPE 1 Ouvrez la page Gestion des VLAN > VLAN voix > Propriétés.

ÉTAPE 2 Sélectionnez l'ID du VLAN voix. Il ne peut pas être défini sur l'ID de VLAN 1 (cette étape n'est pas obligatoire pour un VLAN voix dynamique).

ÉTAPE 3 Sélectionnez **VLAN voix dynamique** pour activer le mode VLAN voix automatique.

ÉTAPE 4 Sélectionnez la méthode **Activation du VLAN voix automatique**.

REMARQUE Si le périphérique est actuellement en mode OUI de téléphonie, vous devez le désactiver pour pouvoir configurer le mode VLAN voix automatique.

ÉTAPE 5 Cliquez sur **Appliquer**.

ÉTAPE 6 Configurez les ports intelligents comme décrit dans la section **Tâches courantes de port intelligent**.

ÉTAPE 7 Configurez LLDP/CDP comme décrit respectivement dans les sections **Configuration de LLDP** et **Configuration de CDP**.

ÉTAPE 8 Activez la fonction Port intelligent sur les ports appropriés par l'intermédiaire de la page Port intelligent > Paramètres d'interface.

REMARQUE Les étapes 7 et 8 sont facultatives, car elles sont activées par défaut.

Flux de travail 2 : pour configurer la méthode OUI de téléphonie :

ÉTAPE 1 Ouvrez la page Gestion des VLAN > VLAN voix > Propriétés. Sélectionnez **VLAN voix dynamique** pour activer le mode OUI de téléphonie.

REMARQUE Si le périphérique est actuellement en mode VLAN voix automatique, vous devez le désactiver pour pouvoir activer le mode OUI de téléphonie.

ÉTAPE 2 Configurez le mode OUI de téléphonie sur la page OUI de téléphonie.

ÉTAPE 3 Configurez l'appartenance VLAN OUI de téléphonie pour les ports sur la page Interface des OUI de téléphonie.

Configuration de VLAN voix

Cette section explique comment configurer le VLAN voix. Elle couvre les rubriques suivantes :

- **Configuration des propriétés du VLAN voix**
- **Paramètres de VLAN voix automatique**
- **OUI de téléphonie**

Configuration des propriétés du VLAN voix

Utilisez la page Propriétés du VLAN voix pour effectuer les opérations suivantes :

- Affichez les paramètres de configuration actuels du VLAN voix.
- Configurez l'ID de VLAN du VLAN voix.
- Configurez les paramètres QoS du VLAN voix.
- Configurez le mode VLAN voix (OUI de téléphonie ou VLAN voix automatique).
- Configurez la façon dont le VLAN voix automatique se déclenche.

Pour afficher et configurer les propriétés du VLAN voix :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **Propriétés**.

- Les paramètres VLAN voix configurés sur le périphérique s'affichent dans le bloc **Paramètres du VLAN voix (État administratif)**.
- Les paramètres VLAN voix actuellement appliqués au déploiement VLAN voix s'affichent dans le bloc **Paramètres du VLAN voix (État opérationnel)**.

ÉTAPE 2 Saisissez les valeurs appropriées dans les champs suivants :

- **ID VLAN voix** : entrez le VLAN qui sera le VLAN voix.

  REMARQUE Les modifications apportées à l'ID du VLAN voix, CoS/802.1p et/ou DSCP obligent le périphérique à annoncer le VLAN voix administratif en tant que VLAN voix statique. Si l'option *Activation du VLAN voix automatique* déclenchée par le VLAN voix externe est sélectionnée, les valeurs par défaut doivent être conservées.

- **CoS/802.1p** : sélectionnez une valeur CoS/802.1p utilisée par LLDP-MED en tant que stratégie de réseau voix. Pour plus d'informations, reportez-vous à *Administration > Détection > LLDP > Stratégie réseau LLD PMED*.
- **DSCP** : sélection de valeurs DSCP utilisées par LLDP-MED en tant que stratégie de réseau voix. Pour plus d'informations, reportez-vous à *Administration > Détection > LLDP > Stratégie réseau LLD PMED*.
- **VLAN voix dynamique** : sélectionnez ce champ pour désactiver ou activer la fonction VLAN voix de l'une des manières suivantes :
  - *Activer le VLAN voix automatique* : active le VLAN voix dynamique en mode VLAN voix automatique.
  - *Activer OUI de téléphonie* : active le VLAN voix dynamique en mode OUI de téléphonie.
  - *Désactiver* : désactive le VLAN voix automatique ou le OUI de téléphonie.

- **Activation du VLAN voix automatique** : sélectionnez l'une des options suivantes pour activer le VLAN voix automatique :
  - *Immédiat* : le VLAN voix automatique du périphérique est activé et immédiatement opérationnel.
  - *Par déclenchement du VLAN voix externe* : le VLAN voix automatique du périphérique est activé et opérationnel uniquement si le périphérique détecte un périphérique qui annonce le VLAN voix.

REMARQUE La reconfiguration manuelle de l'ID de VLAN voix, CoS/802.1p et/ou DSCP à partir de leurs valeurs par défaut génère un VLAN voix statique ayant une priorité plus élevée que le VLAN voix automatique qui a été appris des sources externes.

ÉTAPE 3 Cliquez sur **Appliquer**. Les propriétés du VLAN sont écrites dans le fichier de Configuration d'exécution.

Paramètres de VLAN voix automatique

Si le mode VLAN voix automatique est activé, utilisez la page VLAN voix automatique pour afficher les paramètres globaux et d'interface appropriés.

Vous pouvez aussi utiliser cette page pour redémarrer manuellement le VLAN voix automatique, en cliquant sur **Redémarrer VLAN voix automatique**. Au bout de quelques instants, le système rétablit le VLAN voix par défaut, et relance la détection VLAN voix automatique et le processus de synchronisation sur tous les commutateurs du LAN pour lesquels le mode VLAN voix automatique est activé.

REMARQUE Cette opération rétablit uniquement le VLAN voix par défaut si le type de source est dans l'état *Inactif*.

Pour afficher les paramètres de VLAN voix automatique :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **VLAN voix automatique**.

Le bloc État opérationnel figurant sur cette page affiche les informations sur le VLAN voix actuel et sa source :

- **État de VLAN voix automatique** : indique si le VLAN voix automatique est activé.
- **ID du VLAN voix** : identificateur du VLAN voix actuel.
- **Type de source** : affiche le type de source où le VLAN voix a été détecté par le périphérique racine.
- **CoS/802.1p** : affiche les valeurs CoS/802.1p utilisées par LLDP-MED en tant que stratégie de réseau voix.
- **DSCP** : affiche les valeurs DSCP utilisées par LLDP-MED en tant que stratégie de réseau voix.

- **Adresse MAC commutateur racine** : adresse MAC du périphérique racine VLAN voix automatique qui détecte ou est configuré avec le VLAN voix à partir duquel le VLAN voix est appris.
- **Adresse MAC du commutateur** : adresse MAC de base du périphérique. Si l'adresse MAC du commutateur du périphérique est l'adresse MAC du commutateur racine, le périphérique est le périphérique racine VLAN voix automatique.
- **Heure de changement de l'ID VLAN voix** : heure de la dernière mise à jour du VLAN voix.

ÉTAPE 2 Cliquez sur **Redémarrer VLAN voix automatique** pour rétablir le VLAN voix par défaut et relancer la détection VLAN voix automatique sur tous les commutateurs du LAN pour lesquels la fonction VLAN voix automatique est activée.

La Table locale VLAN voix affiche le VLAN voix configuré sur le périphérique ainsi que toute configuration VLAN voix annoncée par des périphériques voisins à connexion directe. Elle contient les champs suivants :

- **Interface** : affiche l'interface sur laquelle la configuration VLAN voix a été reçue ou configurée. Si S/O est affiché, cela signifie que la configuration a été effectuée sur le périphérique lui-même. Si une interface est affichée, cela signifie qu'une configuration de voix a été reçue d'un voisin.
- **Adresse MAC source** : adresse MAC de l'UC de provenance de la configuration de voix.
- **Type de source** : type d'UC de provenance de la configuration de voix. Les options suivantes sont disponibles :
  - *Par défaut* : configuration VLAN voix par défaut sur le périphérique.
  - *Statique* : configuration VLAN voix définie par l'utilisateur programmée sur le périphérique.
  - *CDP* : indique que l'UC qui a annoncé la configuration VLAN voix exécute CDP.
  - *LLDP* : indique que l'UC qui a annoncé la configuration VLAN voix exécute LLDP.
  - *ID du VLAN voix* : identificateur du VLAN voix annoncé ou configuré.
- **ID du VLAN voix** : identificateur du VLAN voix actuel.
- **CoS/802.1p** : valeurs CoS/802.1p annoncées ou configurées qui sont utilisées par LLDP-MED en tant que stratégie de réseau voix.
- **DSCP** : valeurs DSCP annoncées ou configurées qui sont utilisées par LLDP-MED en tant que stratégie réseau de voix.
- **Meilleure source locale** : indique si ce VLAN voix a été utilisé par le périphérique. Les options suivantes sont disponibles :
  - *Oui* : le périphérique utilise ce VLAN voix pour se synchroniser avec les autres commutateurs pour lesquels la fonction VLAN voix automatique est activée. Ce VLAN voix est celui utilisé pour le réseau, sauf si un VLAN voix provenant d'une source de priorité plus élevée est détecté. Une seule source locale peut être la meilleure source locale.

- *Non* : il ne s'agit pas de la meilleure source locale.

ÉTAPE 3 Cliquez sur **Actualiser** pour actualiser les informations figurant sur la page.

OUI de téléphonie

Les OUI (Organizationally Unique Identifiers) sont attribués par l'autorité d'enregistrement intégrée IEEE (Institute of Electrical and Electronics Engineers). Étant donné que le numéro des fabricants de téléphones IP est limité et connu, les valeurs d'OUI connues entraînent l'affectation automatique au VLAN voix des trames concernées et du port sur lequel elles sont détectées.

La table globale des OUI peut contenir jusqu'à 128 entrées.

Cette section aborde les points suivants :

- **Table des OUI de téléphonie**
- **Interface des OUI de téléphonie**

Table des OUI de téléphonie

Utilisez la page OUI de téléphonie pour configurer les propriétés QoS des OUI de téléphonie. Vous pouvez également configurer le Délai d'expiration d'appartenance automatique. Si la période expire sans aucune activité téléphonique, le port est supprimé du VLAN voix.

Utilisez la page OUI de téléphonie pour afficher les OUI existants et en ajouter de nouveaux.

Pour configurer les OUI de téléphonie et/ou ajouter un nouveau OUI de VLAN voix :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **OUI de téléphonie**.

La page OUI de téléphonie contient les champs suivants :

- **État opérationnel OUI de téléphonie** : indique si les OUI sont utilisés pour identifier le trafic vocal.
- **CoS/802.1p** : sélectionnez la file d'attente CoS à attribuer au trafic vocal.
- **Remarquer CoS/802.1p** : sélectionnez cette option pour remarquer le trafic sortant.
- **Délai d'expiration d'appartenance automatique** : entrez le délai à l'issue duquel supprimer un port du VLAN voix une fois que toutes les adresses MAC des téléphones détectés sur les ports ont expiré.

ÉTAPE 2 Cliquez sur **Appliquer** pour intégrer ces valeurs à la Configuration d'exécution du périphérique.

La Table des OUI de téléphonie s'affiche :

- **OUI de téléphonie** : six premiers chiffres de l'adresse MAC réservés aux OUI.
- **Description** : description du OUI affecté par l'utilisateur.

ÉTAPE 3 Cliquez sur **Restaurer les OUI par défaut** pour supprimer tous les OUI créés par l'utilisateur et conserver uniquement les OUI par défaut dans la table. Les informations OUI risquent d'être inexactes tant que la restauration n'est pas terminée. Cette opération peut prendre plusieurs secondes. Au bout de quelques secondes, actualisez la page en la quittant et y accédant à nouveau.

Pour supprimer tous les OUI, cochez la case du haut. Tous les OUI sont sélectionnés et peuvent être supprimés en cliquant sur **Supprimer**. Si vous cliquez ensuite sur **Restaurer les OUI par défaut**, le système récupère les OUI connus.

ÉTAPE 4 Pour ajouter un nouveau OUI, cliquez sur **Ajouter**.

ÉTAPE 5 Entrez les valeurs des champs suivants :

- **OUI de téléphonie** : saisissez un nouveau OUI.
- **Description** : saisissez un nom d'OUI.

ÉTAPE 6 Cliquez sur **Appliquer**. Le OUI est ajouté à la Table des OUI de téléphonie.

Interface des OUI de téléphonie

Les attributs QoS peuvent être affectés aux paquets voix pour chaque port dans l'un des deux modes suivants :

- **Tout** : les valeurs de qualité de service (QoS) configurées sur le VLAN voix sont appliquées à toutes les trames entrantes reçues sur l'interface et catégorisées comme VLAN voix.
- **Adresse MAC source de téléphonie** : les valeurs de QoS configurées pour le VLAN voix sont appliquées à toute trame entrante catégorisée comme VLAN voix et contenant un OUI dans l'adresse MAC source qui correspond à un OUI de téléphonie configuré.

Utilisez la page Interface des OUI de téléphonie pour ajouter une interface au VLAN voix sur la base de l'identificateur OUI et pour configurer le mode QoS OUI du VLAN voix.

Pour configurer le mode OUI de téléphonie sur une interface :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **Interface des OUI de téléphonie**.

La page Interface des OUI de téléphonie contient les paramètres OUI du VLAN voix pour toutes les interfaces.

ÉTAPE 2 Pour configurer une interface en tant que port candidat du VLAN voix basé sur les OUI de téléphonie, cliquez sur **Modifier**.

ÉTAPE 3 Entrez les valeurs des champs suivants :

- **Interface** : sélectionnez une interface.
- **Adhésion VLAN OUI de téléphonie** : si cette option est activée, l'interface est un port candidat du VLAN voix basé sur les OUI de téléphonie. Lorsque des paquets correspondant à l'un des OUI de téléphonie configurés sont reçus, le port est ajouté au VLAN voix.
- **Mode de QoS VLAN voix** : sélectionnez l'une des options suivantes :
  - *Tous* : les attributs QoS sont appliqués à tous les paquets catégorisés comme VLAN voix.
  - *Adresse MAC source de téléphonie* : les attributs QoS sont uniquement appliqués aux paquets provenant de téléphones IP.

ÉTAPE 4 Cliquez sur **Appliquer**. L'OUI est ajouté.

15

Spanning Tree

Cette section décrit le protocole STP (Spanning Tree Protocol) (IEEE802.1D et IEEE802.1Q) et couvre les rubriques suivantes :

- **Types de STP**
- **État STP et paramètres globaux**
- **Paramètres d'interface Spanning Tree**
- **Paramètres Rapid Spanning Tree**

Types de STP

Le protocole STP protège un domaine de diffusion de couche 2 (Layer 2) contre les tempêtes de diffusion en paramétrant sélectivement des liens sur le mode de réserve pour empêcher les boucles. En mode de réserve, ces liens cessent temporairement de transférer des données d'utilisateur. Les liens sont automatiquement réactivés lorsque la topologie permet à nouveau le transfert de données.

Des boucles se produisent lorsque des chemins alternatifs existent entre les hôtes. Les boucles d'un réseau étendu peuvent utiliser des commutateurs pour acheminer indéfiniment le trafic, ce qui augmente la charge de ce dernier et diminue l'efficacité du réseau.

Le protocole STP fournit une topologie en arborescence pour l'agencement de commutateurs et de liens d'interconnexion afin de créer un chemin d'accès unique entre des stations d'arrivée sur un réseau et d'éliminer les boucles.

Le périphérique prend en charge les versions de protocole STP suivantes :

- Le STP classique fournit un chemin d'accès unique entre deux stations d'arrivée afin d'empêcher et d'éliminer les boucles.
- Le STP rapide (RSTP) détecte les topologies de réseau afin de fournir une convergence du Spanning Tree plus rapide. Ce protocole est plus efficace lorsque la topologie du réseau est naturellement structurée en arborescence et permet une convergence plus rapide. RSTP est activé par défaut.

  REMARQUE Les commutateurs de la série 200 ne prennent pas en charge le STP multiple (MSTP).

État STP et paramètres globaux

La page État STP et paramètres globaux contient les paramètres permettant d'activer le protocole STP ou RSTP.

Utilisez respectivement la page Paramètres d'interface STP et la page Paramètres d'interface RSTP pour configurer les ports par rapport à ces modes.

Pour définir l'état et les paramètres globaux STP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **État STP et paramètres globaux**.

ÉTAPE 2 Saisissez les paramètres.

Paramètres globaux :

- **État Spanning Tree** : sélectionnez cette option pour l'activer sur le périphérique.
- **Protection de bouclage STP** : sélectionnez cette option pour activer la protection de bouclage sur le périphérique.
- **Mode de fonctionnement STP** : sélectionnez un mode STP.
- **Gestion BPDU** : définissez la façon dont les paquets BPDU sont gérés lorsque le protocole STP est désactivé sur le port ou le périphérique. Les BPDU servent à transmettre des informations du protocole STP.
  - *Filtrage* : filtre les paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
  - *Inondation* : inonde de paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
- **Valeurs par défaut du coût de chemin** : sélectionne la méthode utilisée pour assigner des coûts de chemin par défaut aux ports STP. Le coût de chemin par défaut assigné à une interface varie selon la méthode sélectionnée.
  - *Court* : spécifie la plage de 1 à 65 535 pour les coûts de chemin des ports.
  - *Long* : spécifie la plage de 1 à 200 000 000 pour les coûts de chemin des ports.

Paramètres des ponts :

- **Priorité** : définit la valeur de priorité du pont. Après l'échange de BPDU, le périphérique de priorité moindre devient le pont racine. Si tous les ponts utilisent la même priorité, leurs adresses MAC sont alors utilisées pour déterminer le pont racine. La valeur de priorité du pont est fournie par incréments de 4096. Par exemple, 4096, 8192, 12288, etc.
- **Délai Hello** : définissez le temps d'attente en secondes d'un pont racine entre deux messages de configuration.
- **Âge maximum** : définissez la durée d'attente maximale (en secondes) du périphérique avant qu'il ne tente de redéfinir sa propre configuration lorsqu'il ne reçoit pas de message de configuration.

- **Délai de transfert** : définissez la durée en secondes pendant laquelle le pont reste en mode d'apprentissage avant de transférer des paquets. Pour plus d'informations, reportez-vous à la section **Paramètres d'interface Spanning Tree**.

Racine désignée :

- **ID du pont** : priorité du pont concaténée avec l'adresse MAC du périphérique.
- **ID du pont racine** : priorité du pont racine concaténée avec l'adresse MAC du pont racine.
- **Port racine** : port offrant le chemin de moindre coût entre ce pont et le pont racine. (Cette information est importante lorsque le pont n'est pas le pont racine.)
- **Coût du chemin racine** : coût du chemin entre ce pont et la racine.
- **Nombre de changements de topologie** : nombre total des changements de topologie STP effectués.
- **Dernier changement de topologie** : temps écoulé depuis le dernier changement de topologie. Cette durée s'affiche au format jours/heures/minutes/secondes.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres globaux STP sont écrits dans le fichier de Configuration d'exécution.

Paramètres d'interface Spanning Tree

La page Paramètres d'interface STP vous permet de configurer le protocole STP port par port et d'afficher les informations apprises par le protocole, comme le pont désigné.

La configuration définie est valide pour toutes les variantes du protocole STP.

Pour configurer STP sur une interface :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **Paramètres d'interface STP**.

ÉTAPE 2 Sélectionnez une interface et cliquez sur **Modifier**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez le port ou le LAG sur lequel Spanning Tree est configuré.
- **STP** : active ou désactive STP sur le port.
- **Port de bordure** : active ou désactive Fast Link sur le port. Si le mode Fast Link est activé pour un port, le port est automatiquement placé en mode Transfert lorsque le lien du port est actif. Fast Link optimise la convergence du protocole STP. Les options sont les suivantes :
  - *Activer* : active immédiatement Fast Link.

- *Auto* : active Fast Link quelques secondes après l'activation de l'interface. Ceci permet à STP de résoudre les problèmes de boucles avant d'activer Fast Link.
- *Désactiver* : désactive Fast Link.

  REMARQUE Il est recommandé de définir la valeur sur Auto afin que le périphérique place le port en mode Fast Link lorsqu'un hôte y est connecté, ou qu'il le définisse comme étant un port STP normal lorsqu'il est connecté à un autre périphérique. Cela permet d'éviter les boucles.

- **Gestion BPDU** : définissez la façon dont les paquets BPDU sont gérés lorsque le protocole STP est désactivé sur le port ou le périphérique. Les BPDU servent à transmettre des informations du protocole STP.
  - *Utiliser les paramètres globaux* : sélectionnez cette option pour utiliser les paramètres définis sur la page État STP et paramètres globaux.
  - *Filtrage* : filtre les paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
  - *Inondation* : inonde de paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
- **Coût de chemin** : définissez la contribution du port au coût du chemin racine ou utilisez le coût par défaut généré par le système.
- **Priorité** : définissez la valeur de priorité du port. La valeur de priorité influence le choix du port lorsqu'un pont dispose de deux ports connectés au sein d'une boucle. La priorité est une valeur comprise entre 0 et 240, définie par incréments de 16.
- **État du port** : affiche l'état STP actuel d'un port.
  - *Désactivé* : le protocole STP est actuellement désactivé sur le port. Le port transfère le trafic tout en apprenant les adresses MAC.
  - *Blocage* : le port est actuellement bloqué et ne peut ni transférer le trafic (à l'exception des données BPDU) ni apprendre les adresses MAC.
  - *Écoute* : le port est en mode Écoute. Il ne peut ni transférer le trafic ni connaître les adresses MAC.
  - *Apprentissage* : le port est en mode Apprentissage. Il ne peut pas transférer le trafic mais il peut prendre connaissance de nouvelles adresses MAC.
  - *Transfert* : le port est en mode Transfert. Il peut réacheminer du trafic et apprendre de nouvelles adresses MAC.
- **ID du pont désigné** : affiche la priorité du pont et l'adresse MAC du pont désigné.
- **ID du port désigné** : affiche la priorité et l'interface du port sélectionné.
- **Coût désigné** : affiche le coût du port participant à la topologie STP. Les ports de coûts inférieurs sont peu susceptibles d'être bloqués si STP détecte des boucles.

- **Transitions de transfert** : affiche le nombre de fois où le port est passé de l'état **Blocage** à l'état **Transfert**.
- **Vitesse** : affiche la vitesse du port.
- **LAG** : affiche le LAG auquel appartient le port. Si un port est membre d'un LAG, les paramètres du LAG remplacent ceux du port.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres d'interface sont écrits dans le fichier de Configuration d'exécution.

Paramètres Rapid Spanning Tree

Le protocole RSTP (Rapid Spanning Tree Protocol) permet une convergence STP plus rapide sans création de boucles de réacheminement.

La page Paramètres d'interface RSTP vous permet de configurer le protocole RSTP par port. Toute configuration effectuée sur cette page est active lorsque le mode STP global est défini sur RSTP.

Pour entrer les paramètres RSTP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **État STP et paramètres globaux**. Activez **RSTP**.

ÉTAPE 2 Cliquez sur **Spanning Tree** > **Paramètres d'interface RSTP**. La page Paramètres d'interface RSTP s'ouvre :

ÉTAPE 3 Sélectionnez un port.

REMARQUE Activer la migration des protocoles est uniquement disponible après avoir sélectionné le port connecté au pont associé en cours de test.

ÉTAPE 4 Si un partenaire de lien est détecté via STP, cliquez sur **Activer la migration des protocoles** pour effectuer un test de migration des protocoles. Cette opération détecte si le partenaire de liaison utilisant le protocole STP existe toujours et, si c'est le cas, s'il a migré vers RSTP. S'il existe toujours en tant que lien STP, le périphérique continue de communiquer avec lui via STP. En revanche, s'il a migré vers RSTP, le périphérique communique avec lui via RSTP.

ÉTAPE 5 Sélectionnez une interface et cliquez sur **Modifier**.

ÉTAPE 6 Configurez les paramètres suivants :

- **Interface** : définissez l'interface et précisez le port ou LAG où RSTP doit être configuré.

- **État administratif point à point** : définissez l'état de la liaison point à point. Les ports définis en tant que Full Duplex sont considérés comme liens de port point à point.
  - *Activer* : ce port devient un port de bordure RSTP lorsque cette option est activée et il est placé rapidement en mode Transfert (généralement en 2 secondes).
  - *Désactiver* : le port n'est pas considéré comme port point à point pour le protocole RSTP ; par conséquent, STP fonctionne sur ce port à vitesse normale et non à haute vitesse.
  - *Automatique* : détermine automatiquement l'état du périphérique en utilisant les unités BPDU RSTP.
- **État opérationnel point à point** : affiche l'état opérationnel point à point si l'**État administratif point à point** est défini sur Auto.
- **Rôle** : affiche le rôle du port qui a été assigné par STP pour fournir des chemins STP. Les rôles possibles sont :
  - *Racine* : chemin de moindre coût pour transférer des paquets vers le pont racine.
  - *Désigné* : interface via laquelle le pont est connecté au LAN et qui fournit le chemin de moindre coût du LAN au pont racine.
  - *Autre* : fournit un chemin alternatif de l'interface racine au pont racine.
  - *Sauvegarde* : fournit un chemin de secours pour le chemin du port désigné vers les nœuds terminaux STP. Cela fournit une configuration dans laquelle deux ports sont reliés dans une boucle par un lien point à point. Des ports de secours sont également utilisés lorsqu'un LAN possède deux ou plusieurs connexions établies à un segment partagé.
  - *Désactivé* : le port ne participe pas au Spanning Tree.
- **Mode** : affiche le mode Spanning Tree actuel : RSTP ou STP classique.
- **État opérationnel Fast Link** : indique si Fast Link (port de bordure) est activé, désactivé ou automatique pour l'interface. Les valeurs disponibles sont les suivantes :
  - *Activé* : Fast Link est activé.
  - *Désactivé* : Fast Link est désactivé.
  - *Auto* : le mode Fast Link s'active quelques secondes après l'activation de l'interface.
- **État du port** : affiche l'état RSTP sur le port spécifique.
  - *Désactivé* : le protocole STP est actuellement désactivé sur le port.
  - *Blocage* : le port est actuellement bloqué et ne peut ni transférer le trafic ni apprendre les adresses MAC.
  - *Écoute* : le port est en mode Écoute. Il ne peut ni transférer le trafic ni connaître les adresses MAC.

- *Apprentissage* : le port est en mode Apprentissage. Il ne peut pas transférer le trafic mais il peut prendre connaissance des nouvelles adresses MAC.
- *Transfert* : le port est en mode Transfert. Il peut réacheminer du trafic et apprendre de nouvelles adresses MAC.

ÉTAPE 7 Cliquez sur **Appliquer**. Le fichier de configuration de fonctionnement est mis à jour.

16

Gestion des tables d'adresses MAC

Cette section explique comment ajouter des adresses MAC au système. Elle couvre les rubriques suivantes :

- **Adresses MAC statiques**
- **Adresses MAC dynamiques**

Il existe deux types d'adresses MAC : statiques et dynamiques. Selon leur type, les adresses MAC sont stockées dans la *table des adresses statiques* ou dans la *table des adresses dynamiques* avec les informations relatives aux VLAN et aux ports.

Les adresses statiques sont configurées par l'utilisateur, par conséquent elles n'expirent jamais.

Une nouvelle adresse MAC source qui apparaît dans une trame reçue par le périphérique est ajoutée à la table des adresses dynamiques. Cette adresse MAC est conservée pendant une période que vous pouvez configurer. Si aucune autre trame disposant de la même adresse MAC source n'apparaît sur le périphérique avant l'expiration de ce délai, l'entrée MAC est supprimée (expirée) de la table.

Lorsqu'une trame arrive au niveau du périphérique, celui-ci recherche une adresse MAC de destination correspondant à une entrée de la table des adresses statiques ou dynamiques. En cas de correspondance, la trame est marquée en sortie sur un port spécifique de la table. Les trames adressées à une adresse MAC n'ayant pas été trouvée dans les tables sont diffusées/transmises à tous les ports du VLAN approprié. Ces trames sont appelées trames de destination unique inconnue.

Le périphérique prend en charge un maximum de 8 000 adresses MAC statiques et dynamiques.

Adresses MAC statiques

Les adresses MAC statiques sont affectées à une interface physique et à un VLAN spécifiques sur le périphérique. Si une adresse MAC est détectée sur une autre interface, elle est ignorée et n'est pas consignée dans la table des adresses.

Pour définir une adresse statique :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC > Adresses statiques**.

La page Adresses statiques affiche les adresses statiques actuellement définies.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **ID VLAN** : sélectionnez l'ID VLAN du port.
- **Adresse MAC** : saisissez l'adresse MAC de l'interface.
- **Interface** : sélectionnez une interface (port ou LAG) pour l'entrée.
- **État** : sélectionnez le mode de traitement de l'entrée. Les options sont les suivantes :
  - *Permanent* : le système ne supprime jamais cette adresse MAC. Si l'adresse MAC statique est enregistrée dans la Configuration de démarrage, elle est conservée après redémarrage.
  - *Suppr. à la réinitialisation* : l'adresse MAC statique est supprimée lorsque le périphérique est réinitialisé.
  - *Supprimer à l'expiration* : l'adresse MAC est supprimée à expiration du délai.
  - *Sécurisé* : l'adresse MAC est sécurisée lorsque l'interface est en mode verrouillé classique (voir **Configuration de la sécurité des ports**).

ÉTAPE 4 Cliquez sur **Appliquer**. Une nouvelle entrée apparaît dans la table.

Adresses MAC dynamiques

La table des adresses dynamiques (table de pontage) contient les adresses MAC obtenues en surveillant les adresses source des trames entrant dans le périphérique.

Pour éviter le débordement de cette table et garder de l'espace pour de nouvelles adresses MAC, une adresse est supprimée si elle ne reçoit aucun trafic pendant une période appelée délai d'expiration.

Configuration du délai d'expiration d'adresses MAC dynamiques

Pour configurer le délai d'expiration des adresses dynamiques :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC > Paramètres des adresses dynamiques**.

ÉTAPE 2 Saisissez le **Délai d'expiration**. Le délai d'expiration est une valeur comprise entre la valeur configurée par l'utilisateur et deux fois cette valeur moins 1. Par exemple, si vous avez saisi 300 secondes, le délai d'expiration sera compris entre 300 et 599 secondes.

ÉTAPE 3 Cliquez sur **Appliquer**. Le délai d'expiration est mis à jour.

Interrogation d'adresses dynamiques

Pour interroger la table des adresses dynamiques :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC > Adresses dynamiques**.

ÉTAPE 2 Dans le bloc *Filtre*, vous pouvez saisir les critères d'interrogation suivants :

- **ID VLAN** : saisissez l'ID du VLAN pour lequel la table est interrogée.
- **Adresse MAC** : saisissez l'adresse MAC pour laquelle la table est interrogée.
- **Interface** : sélectionnez l'interface au sujet de laquelle la table est interrogée. L'interrogation peut également rechercher des unités/logements, ports ou LAG spécifiques.

ÉTAPE 3 Cliquez sur **OK**. La Table des adresses MAC dynamiques est interrogée et les résultats s'affichent.

Cliquez sur **Effacer la table** pour supprimer toutes les adresses MAC dynamiques.

-

ÉTAPE 4

17

Multidiffusion

Cette section décrit la fonction de transfert de multidiffusion et couvre les rubriques suivantes :

- **Réacheminement multidestination**
- **Propriétés de multidiffusion**
- **Adresse de groupe MAC**
- **Adresses IP de groupe de multidiffusion**
- **Configuration de la multidiffusion IPv4**
- **Configuration de la multidiffusion IPv6**
- **Groupe de multidiffusion IP de surveillance IGMP/MLD**
- **Ports de routeur de multidiffusion**
- **Tout transférer**
- **Multidiffusion non enregistrée**

Réacheminement multidestination

Le réacheminement multidestination permet la transmission d'informations en mode 1-à-n. Les applications multidestination sont particulièrement utiles pour transmettre des informations à plusieurs clients lorsque ces clients n'ont pas besoin de l'intégralité du contenu. Ceci est par exemple le cas dans le cadre d'une application de TV par câble où les clients peuvent contacter une chaîne au milieu d'une transmission et interrompre la connexion avant la fin.

Les données sont uniquement envoyées aux ports pertinents. Le fait de ne réacheminer les données que vers les ports pertinents permet d'économiser de la bande passante et des ressources d'hôte sur les liaisons.

Par défaut, toutes les trames multidestination sont envoyées à tous les ports du VLAN. Il est possible de transférer les données de façon sélective uniquement vers les ports concernés et de filtrer (éliminer) le flux de multidiffusion sur les autres ports en activant l'État du filtrage multidiffusion par ponts sur la page Multidiffusion > Propriétés.

Si le filtrage est activé, les trames de multidiffusion sont transférées vers un sous-ensemble des ports sur le VLAN concerné, comme défini dans la base de données de transfert de multidiffusion (MFDB, Multicast Forwarding Data Base). Le filtrage multidiffusion s'exerce sur l'ensemble du trafic.

L'une des méthodes couramment utilisées de représentation des membres de multidiffusion est la notation (S,G), où S représente la source (unique) qui envoie un flux de données de multidiffusion et G représente l'adresse IPv4 ou IPv6 de groupe. Si un client Multicast peut recevoir du trafic de multidiffusion à partir de n'importe quelle source d'un groupe de multidiffusion donné, celui-ci est enregistré sous (*,G).

Vous pouvez configurer l'un des modes suivants de transfert des trames de multidiffusion :

- **Adresse MAC de groupe** : basée sur l'adresse MAC de destination dans la trame Ethernet.

  REMARQUE Il est possible de mapper une ou plusieurs adresses IP de groupe de multidiffusion à une seule adresse MAC de groupe. Le transfert basé sur une adresse MAC de groupe peut provoquer le transfert d'un flux de multidiffusion IP vers des ports qui ne possèdent aucun récepteur pour ce flux.

- **Adresse IP de groupe** : basée sur l'adresse IP de destination du paquet IP (*,G).
- **Adresse du groupe IP spécifique source** : basée à la fois sur l'adresse IP de destination et l'adresse IP source du paquet IP (S,G).

(S,G) est pris en charge par IGMPv3 et MLDv2 alors qu'IGMPv1/2 et MLDv1 ne prennent en charge que (*.G), qui inclut uniquement l'ID de groupe.

Le périphérique peut prendre en charge jusqu'à 256 adresses de groupe de multidiffusion statiques et dynamiques.

Vous ne pouvez configurer qu'une seule option de filtrage par VLAN.

Configuration de multidiffusion typique

Alors que les routeurs de multidiffusion routent les paquets de multidiffusion d'un sous-réseau IP à un autre, les commutateurs de couche 2 compatibles avec la multidiffusion transfèrent les paquets de multidiffusion vers les nœuds enregistrés au sein d'un LAN ou d'un VLAN.

La configuration type inclut un routeur qui transfère les flux de multidiffusion entre des réseaux IP privés et/ou publics, un périphérique doté de fonctions de surveillance IGMP/MLD et un client de multidiffusion qui souhaite recevoir un flux de multidiffusion. Dans cette configuration, le routeur envoie périodiquement des requêtes IGMP/MLD.

Fonctionnement de la multidiffusion

Dans un service de multidiffusion Couche 2, un commutateur Couche 2 reçoit une seule trame, adressée à une adresse de multidiffusion spécifique. Il crée des copies de la trame pour les transmettre à chacun des ports concernés.

Lorsque la surveillance IGMP/MLD est activée sur le périphérique et que celui-ci reçoit une trame du flux de multidiffusion, il la transfère à tous les ports enregistrés pour recevoir le flux de multidiffusion à l'aide de messages d'adhésion IGMP/MLD.

Le système gère des listes de groupes de multidiffusion pour chaque VLAN. Ceci permet de gérer les informations de multidiffusion que chaque port doit recevoir. Les groupes de multidiffusion et les ports destinataires associés peuvent être configurés de manière statique ou appris de manière dynamique via la surveillance des protocoles IGMP ou MLD.

Enregistrement de multidiffusion (surveillance IGMP/MLD)

L'enregistrement multidestination est le processus qui consiste à écouter les protocoles d'enregistrement multidestination et à y répondre. Les protocoles disponibles sont IGMP pour IPv4 et MLD pour IPv6.

Lorsque le traçage IGMP/MLD Snooping est activé sur un périphérique d'un VLAN, il analyse les paquets IGMP/MLD que le périphérique reçoit du VLAN et de tous les routeurs multidestination du réseau.

Lorsqu'un périphérique apprend qu'un hôte demande à recevoir un flux de multidiffusion à l'aide de messages IGMP/MLD, éventuellement à partir d'une source spécifique, ce périphérique ajoute cet hôte à sa base MFDB.

Les versions suivantes sont prises en charge :

- IGMP v1/v2/ v3
- MLD v1/v2

REMARQUE Le périphérique ne prend en charge la surveillance IGMP/MLD que sur les VLAN statiques. Il ne prend pas en charge la surveillance IGMP/MLD sur les VLAN dynamiques.

Lorsque vous activez la surveillance IGMP/MLD, globalement ou sur un VLAN, tous les paquets IGMP/MLD sont transmis au processeur. Le processeur analyse les paquets entrants et détermine ce qui suit :

- les ports qui demandent à rejoindre tel ou tel groupe de multidiffusion sur un VLAN spécifique ;
- les ports connectés aux routeurs de multidiffusion (Mrouters) qui génèrent des requêtes IGMP/MLD ;
- les ports qui reçoivent les protocoles de requête PIM, DVMRP ou IGMP/MLD.

Ces VLAN sont affichés sur la page Surveillance IGMP/MLD.

Les ports demandant à rejoindre un groupe de multidiffusion spécifique envoient un rapport IGMP/MLD qui spécifie le ou les groupes que l'hôte concerné souhaite rejoindre. Cela provoque la création d'une entrée de transfert dans la base de données de transfert de multidiffusion.

Propriétés d'adresse de multidiffusion

Les adresses de multidiffusion possèdent les propriétés suivantes :

- Chaque adresse multidestination IPv4 se trouve dans la plage d'adresses 224.0.0.0 à 239.255.255.255.
- L'adresse multidestination IPv6 est FF00:/8.
- Pour mapper une adresse IP de groupe de multidiffusion à une adresse de multidiffusion de couche 2 :
  - Pour IPv4, le mappage s'effectue en prenant les 23 bits de poids faible de l'adresse IPv4 et en les ajoutant au préfixe 01:00:5e. Normalement, les 9 bits de poids fort de l'adresse IP sont ignorés et toutes les adresses IP qui diffèrent uniquement par ces bits de poids fort sont mappées à la même adresse de couche 2 puisque les 23 bits de poids faible sont identiques. Par exemple, 234.129.2.3 est mappée à une adresse MAC de groupe de multidiffusion 01:00:5e:01:02:03. Jusqu'à 32 adresses IP de groupe de multidiffusion peuvent être mappées à la même adresse de couche 2 .
  - Pour IPv6, le mappage s'effectue en prenant les 32 bits de poids faible de l'adresse de multidiffusion et en ajoutant le préfixe 33:33. Par exemple, l'adresse de multidiffusion IPv6 FF00:1122:3344 est mappée à l'adresse de multidiffusion de couche 2 : 33:33:11:22:33:44.

Proxy IGMP/MLD

Le Proxy IGMP/MLD est un protocole simple de multidiffusion IP.

L'utilisation du Proxy IGMP/MLD pour répliquer le trafic de multidiffusion sur des périphériques, tels que « edge box », peut grandement simplifier la conception et la mise en œuvre de ces périphériques. Le fait de ne pas prendre en charge des protocoles de routage de multidiffusion plus compliqués, tels que la multidiffusion indépendante du protocole (PIM) ou le protocole de routage multidiffusion distance-vecteur (DVMRP), réduit non seulement le coût des périphériques, mais aussi les frais de fonctionnement. Un autre avantage est que cela rend les périphériques proxy indépendants du protocole de routage de multidiffusion utilisé par les routeurs de base du réseau. Par conséquent, les périphériques proxy sont facilement déployables dans un réseau de multidiffusion.

Arborescence Proxy IGMP/MLD

Le Proxy IGMP/MLD fonctionne dans une topologie arborescente simple dans laquelle il n'est pas nécessaire d'exécuter un protocole de routage de multidiffusion robuste (par exemple, PIM). Il suffit d'utiliser un protocole simple de routage IPM basé sur l'apprentissage des informations concernant l'appartenance à un groupe ou l'appartenance à un groupe proxy et de transférer les paquets de multidiffusion en fonction de ces informations.

L'arborescence doit être configurée manuellement en désignant les interfaces amont et aval sur chaque périphérique proxy. En outre, le système d'adressage IP appliqué à la topologie arborescente proxy doit être configuré de manière à assurer qu'un périphérique proxy peut gagner l'élection du demandeur IGMP/MLD pour être en mesure de transférer le trafic de multidiffusion. Il ne doit pas y avoir d'autres routeurs de multidiffusion dans l'arborescence hormis les périphériques proxy, et la racine de l'arborescence doit être connectée à une infrastructure de multidiffusion plus large.

Un périphérique proxy effectuant le transfert basé sur IGMP/MLD a une seule interface amont et une ou plusieurs interfaces aval. Ces désignations sont configurées de façon explicite ; il n'y a pas de protocole pour déterminer le type de chaque interface. Un périphérique proxy effectue la partie routeur d'IGMP/MLD sur ses interfaces aval, et la partie hôte d'IGMP/MLD sur son interface amont.

Une seule arborescence est prise en charge.

Règles de transfert et demandeur

Les règles suivantes sont appliquées :

- Un paquet de multidiffusion reçu sur l'interface amont est transmis sur toutes les interfaces aval demandant le paquet uniquement si le périphérique proxy est le demandeur sur les interfaces.
- Un périphérique proxy supprime les paquets de multidiffusion reçus sur une interface aval s'il n'est pas le demandeur sur l'interface.
- Un paquet de multidiffusion reçu sur une interface aval pour laquelle le périphérique proxy est le demandeur est transmis sur l'interface amont et sur toutes les interfaces aval demandant le paquet uniquement si le périphérique proxy est le demandeur sur les interfaces.

Protection d'interface aval

Par défaut, le trafic de multidiffusion IP arrivant sur une interface de l'arborescence IGMP/MLD est transmis. Vous pouvez désactiver le transfert du trafic de multidiffusion IP arrivant sur les interfaces aval. Cela peut être fait globalement ou sur une interface aval donnée.

Propriétés de multidiffusion

Pour activer le filtrage multidiffusion et sélectionner la méthode de transfert :

ÉTAPE 1 Cliquez sur **Multidiffusion > Propriétés**.

ÉTAPE 2 Saisissez les paramètres.

- **État du filtrage multidiffusion par ponts** : sélectionnez cette option pour activer le filtrage.
- **ID VLAN** : sélectionnez l'ID du VLAN dont définir la méthode de transfert.
- **Méthode de transfert pour IPv6** : choisissez l'une des méthodes de transfert suivantes pour les adresses IPv6 : Adresse MAC de groupe, Adresse IP de groupe ou Adresse IP source de groupe.
- **Méthode de transfert pour IPv4** : choisissez l'une des méthodes de transfert suivantes pour les adresses IPv4 : Adresse MAC de groupe, Adresse IP de groupe ou Adresse IP source de groupe.

ÉTAPE 3 Cliquez sur **Appliquer**. Le fichier de configuration de fonctionnement est mis à jour.

Adresse de groupe MAC

La page Adresse de groupe MAC offre les fonctions suivantes :

- Interrogation et affichage d'informations tirées de la base de données de transfert de multidiffusion (MFDB, Multicast Forwarding Data Base) concernant un ID de VLAN spécifique ou un groupe spécifique d'adresses MAC. Ces données sont acquises de manière dynamique par traçage IGMP/MLD Snooping ou de manière statique par saisie manuelle.
- Ajout ou suppression d'entrées statiques dans la base MFDB, qui fournissent les informations de transfert statiques basées sur les adresses MAC de destination.
- Affichage de la liste de tous les ports/LAG membres de chaque ID de VLAN ou adresse MAC de groupe, et indication précisant si le trafic doit ou non être transféré vers cette destination.

Pour définir et afficher des groupes de multidiffusion MAC :

ÉTAPE 1 Cliquez sur **Multidiffusion > Adresse MAC de groupe**.

ÉTAPE 2 Saisissez les paramètres de filtre.

- **ID VLAN est égal à** : saisissez l'ID de VLAN du groupe à afficher.

- **Adresse MAC de groupe égale à** : définissez l'adresse MAC du groupe de multidiffusion à afficher. Si aucune adresse MAC de groupe n'est indiquée, la page contient toutes les adresses MAC de groupe du VLAN sélectionné.

ÉTAPE 3 Cliquez sur **OK**. Les adresses MAC de groupe de multidiffusion sont affichées dans le bloc inférieur.

Le système affiche les entrées qui ont été créées sur cette page et sur la page Adresse IP de groupe de multidiffusion. Pour celles qui ont été créées sur la page Adresse IP de groupe de multidiffusion, les adresses IP sont converties en adresses MAC.

ÉTAPE 4 Cliquez sur **Ajouter** pour ajouter une adresse MAC de groupe statique.

ÉTAPE 5 Saisissez les paramètres.

- **ID VLAN** : définit l'ID de VLAN du nouveau groupe de multidiffusion.
- **Adresse MAC de groupe** : définit l'adresse MAC du nouveau groupe de multidiffusion.

ÉTAPE 6 Cliquez sur **Appliquer** et l'adresse MAC du groupe de multidiffusion est enregistrée dans le fichier de configuration d'exécution.

Pour configurer et afficher l'enregistrement des interfaces au sein du groupe, sélectionnez une adresse et cliquez sur **Détails**.

La page affiche les éléments suivants :

- **ID VLAN** : ID de VLAN du groupe de multidiffusion.
- **Adresse MAC de groupe** : adresse MAC du groupe.

ÉTAPE 7 Sélectionnez dans le menu **Filtre : Type d'interface** le port ou le LAG à afficher.

ÉTAPE 8 Cliquez sur **OK** pour afficher les membres (ports ou LAG) du VLAN.

ÉTAPE 9 Sélectionnez la façon dont chaque interface est associée au groupe de multidiffusion :

- **Statique** : rattache l'interface au groupe de multidiffusion en tant que membre statique.
- **Dynamique** : indique que l'interface a été ajoutée au groupe de multidiffusion via la surveillance IGMP/MLD.
- **Interdit** : spécifie que ce port n'est pas autorisé à rejoindre ce groupe de multidiffusion sur ce VLAN.
- **Aucun** : spécifie que le port n'est actuellement pas membre de ce groupe de multidiffusion sur ce VLAN.

ÉTAPE 10 Cliquez sur **Appliquer** ; le fichier de configuration d'exécution est mis à jour.

REMARQUE Les entrées qui ont été créées sur la page Adresse IP de groupe de multidiffusion ne peuvent pas être supprimées sur cette page (même si elles sont sélectionnées).

Adresses IP de groupe de multidiffusion

La page *Adresse IP de groupe de multidiffusion* est similaire à la page *Adresse de groupe MAC*, à la seule différence que les groupes de multidiffusion y sont identifiés par leurs adresses IP.

La page Adresse IP de groupe de multidiffusion vous permet d'interroger et d'ajouter des groupes de multidiffusion IP.

Pour définir et afficher des groupes de multidiffusion IP :

ÉTAPE 1 Cliquez sur **Multidiffusion > Adresse IP de groupe de multidiffusion**.

La page contient toutes les adresses IP de multidiffusion de groupe apprises via le traçage (Snooping).

ÉTAPE 2 Saisissez les paramètres nécessaires pour le filtrage.

- **ID VLAN est égal à** : définissez l'ID de VLAN du groupe à afficher.
- **Version IP est égale à** : sélectionnez IPv6 ou IPv4.
- **Adresse IP de groupe de multidiffusion égale à** : définissez l'adresse IP du groupe de multidiffusion à afficher. Cela s'applique uniquement lorsque le mode de transfert est (S,G).
- **Adresse IP source est égale à** : définissez l'adresse IP source du périphérique émetteur. Si le mode est (S,G), saisissez la valeur S (indiquant l'expéditeur). Combinée à l'adresse IP de groupe, cette valeur définit l'ID de multidiffusion du groupe (S,G) à afficher. Si le mode est (*.G), saisissez un astérisque (*) pour indiquer que le groupe de multidiffusion n'est défini que par sa destination.

ÉTAPE 3 Cliquez sur **OK**. Les résultats s'affichent dans le bloc inférieur.

ÉTAPE 4 Cliquez sur **Ajouter** pour ajouter une adresse IP de multidiffusion statique de groupe.

ÉTAPE 5 Saisissez les paramètres.

- **ID VLAN** : définit l'ID de VLAN du groupe à ajouter.
- **Version IP** : sélectionnez le type d'adresse IP.
- **Adresse IP de groupe de multidiffusion** : définit l'adresse IP du nouveau groupe de multidiffusion.

- **Propre à la source** : indique que l'entrée contient une source spécifique et ajoute l'adresse correspondante dans le champ Adresse IP source. Dans le cas contraire, l'entrée est ajoutée sous la forme (*,G), c'est-à-dire une adresse IP de groupe associée à toutes les sources IP.
- **Adresse IP source** : définit l'adresse source à inclure.

ÉTAPE 6 Cliquez sur **Appliquer**. L'IP de multidiffusion du groupe est ajouté et le périphérique est mis à jour.

ÉTAPE 7 Pour configurer et afficher l'enregistrement d'une adresse IP de groupe, sélectionnez une adresse puis cliquez sur **Détails**.

Les ID de VLAN, Version IP, Adresse IP de groupe de multidiffusion et Adresse IP source sélectionnés s'affichent en lecture seule en haut de la fenêtre. Vous pouvez sélectionner le type de filtre :

- **Type d'interface est égal à** : choisissez d'afficher les ports ou les LAG.

ÉTAPE 8 Sélectionnez le type d'association de chaque interface. Les options disponibles sont les suivantes :

- **Statique** : rattache l'interface au groupe de multidiffusion en tant que membre statique.
- **Dynamique** : rattache l'interface au groupe de multidiffusion en tant que membre dynamique.
- **Interdit** : spécifie que ce port n'est pas autorisé à rejoindre ce groupe sur ce VLAN.
- **Aucun** : indique que le port n'est actuellement pas membre de ce groupe de multidiffusion sur ce VLAN. Cette option est définie par défaut tant que l'option Statique ou Interdit n'est pas sélectionnée.

ÉTAPE 9 Cliquez sur **Appliquer**. Le fichier de configuration de fonctionnement est mis à jour.

Configuration de la multidiffusion IPv4

Les pages suivantes décrivent la configuration de la multidiffusion IPv4 :

- **Configuration de la surveillance IGMP**
- **Paramètres de VLAN IGMP**

Configuration de la surveillance IGMP

Pour prendre en charge le transfert sélectif de multidiffusion IPv4, vous devez activer le filtrage multidiffusion par ponts (sur la page Multidiffusion > Propriétés). Vous devez aussi activer la surveillance IGMP globalement ainsi que pour chacun des VLAN concernés, sur les pages Surveillance IGMP.

Pour activer le traçage IGMP Snooping et identifier le périphérique en tant qu'émetteur de requêtes de traçage IGMP Snooping sur un VLAN :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Configuration de la multidiffusion IPv4 > Surveillance IGMP**.

Lorsque la surveillance IGMP est activée globalement, le périphérique qui surveille le trafic réseau peut détecter les hôtes qui ont demandé à recevoir le trafic de multidiffusion. Le périphérique n'exécute la surveillance IGMP que si vous avez activé à la fois la surveillance IGMP et le filtrage multidiffusion par ponts.

ÉTAPE 2 Activez ou désactivez les fonctionnalités suivantes :

- **État de surveillance IGMP** : sélectionnez cette option pour activer la surveillance IGMP globalement sur toutes les interfaces.

ÉTAPE 3 Pour configurer proxy IGMP sur une interface, sélectionnez un VLAN statique et cliquez sur **Modifier**. Renseignez les champs suivants :

- **État de surveillance IGMP** : sélectionnez cette option pour activer la surveillance IGMP sur le VLAN. Le périphérique surveille le trafic réseau pour déterminer les hôtes qui ont demandé à recevoir du trafic de multidiffusion. Le périphérique n'exécute la surveillance IGMP que si la surveillance IGMP et le filtrage multidiffusion par ponts sont tous deux activés.
- **Apprentissage automatique des ports MRouter** : sélectionnez cette option pour activer l'apprentissage automatique du routeur de multidiffusion.
- **Sortie immédiate** : sélectionnez cette option pour autoriser le commutateur à supprimer une interface qui envoie un message de sortie de la table de transfert sans envoyer au préalable à l'interface des requêtes générales basées sur MAC. Lorsqu'un message de sortie de groupe IGMP est reçu de la part d'un hôte, le système supprime le port hôte de l'entrée de la table. Après avoir transmis les requêtes IGMP en provenance du routeur de multidiffusion, il supprime les entrées périodiquement s'il ne reçoit aucun rapport d'appartenance IGMP de la part des clients de multidiffusion. Lorsqu'elle est activée, cette fonction réduit le temps nécessaire au blocage du trafic IGMP inutile envoyé à un port du périphérique.
- **Nombre de requêtes du dernier membre** : nombre de requêtes propres au groupe IGMP envoyées avant que le périphérique considère qu'il n'existe pas d'autre membre dans le groupe, dans la mesure où ce périphérique est le demandeur choisi.

ÉTAPE 4 Sélectionnez un VLAN et cliquez sur **Modifier**.

ÉTAPE 5 Saisissez les paramètres comme décrit ci-dessus.

ÉTAPE 6 Cliquez sur **Appliquer**. Le fichier de configuration de fonctionnement est mis à jour.

REMARQUE Changements dans la configuration des temporisations de surveillance IGMP, tels que : Robustesse des requêtes, Intervalle de requête, etc. ne prennent pas effet sur les temporisations déjà créées.

Paramètres de VLAN IGMP

Pour configurer le protocole IGMP sur un VLAN spécifique :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Configuration de la multidiffusion IPv4 > Paramètres de VLAN IGMP**.

Les champs suivants sont affichés pour chaque VLAN sur lequel IGMP est activé :

- **Nom de l'interface** : VLAN sur lequel la surveillance IGMP est définie.
- **Version IGMP du routeur** : version de la surveillance IGMP.
- **Robustesse des requêtes** : entrez le nombre de pertes de paquets prévues sur une liaison.
- **Intervalle de requête (s)** : intervalle à appliquer entre deux requêtes générales si ce périphérique est le demandeur choisi.
- **Intervalle de réponse max aux requêtes (s)** : délai utilisé pour calculer le code de réponse maximum inséré dans les requêtes générales périodiques.
- **Intervalle de requête du dernier membre (ms)** : saisissez le délai maximal de réponse à utiliser si le périphérique ne peut pas lire cette valeur dans les requêtes propres au groupe envoyées par le demandeur choisi.

ÉTAPE 2 Sélectionnez une interface et cliquez sur **Modifier**. Renseignez les valeurs des champs décrits ci-dessus.

ÉTAPE 3 Cliquez sur **Appliquer**. Le fichier de configuration de fonctionnement est mis à jour.

Configuration de la multidiffusion IPv6

Les pages suivantes décrivent la configuration de la multidiffusion IPv6 :

- **Surveillance MLD**
- **Paramètres de VLAN MLD**

Surveillance MLD

Pour prendre en charge le transfert sélectif de la multidiffusion IPv6, vous devez activer le filtrage multidiffusion par ponts (sur la page Multidiffusion > Propriétés). Vous devez aussi activer la surveillance MLD globalement ainsi que pour chacun des VLAN concernés, sur les pages Surveillance MLD.

Pour activer la surveillance MLD et la configurer sur un VLAN :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Configuration de la multidiffusion IPv6 > Surveillance MLD**.

Lorsque le traçage MLD Snooping est activé au niveau global, le périphérique qui surveille le trafic réseau peut détecter les hôtes qui ont demandé à recevoir le trafic de multidiffusion. Le périphérique exécute uniquement le traçage MLD Snooping si vous avez activé à la fois MLD Snooping et le filtrage multidiffusion par ponts.

ÉTAPE 2 Activez ou désactivez les fonctionnalités suivantes :

- **État de surveillance MLD** : sélectionnez cette option pour activer la surveillance MLD globalement sur toutes les interfaces.

ÉTAPE 3 Pour configurer proxy MLD sur une interface, sélectionnez un VLAN statique et cliquez sur **Modifier**. Renseignez les champs suivants :

- **État de surveillance MLD** : sélectionnez cette option pour activer la surveillance MLD sur le VLAN. Le périphérique surveille le trafic réseau pour déterminer les hôtes qui ont demandé à recevoir du trafic de multidiffusion. Le périphérique n'exécute la surveillance MLD que si la surveillance MLD et le filtrage multidiffusion par ponts sont tous deux activés.
- **Apprentissage automatique des ports MRouter** : sélectionnez cette option pour activer l'apprentissage automatique du routeur de multidiffusion.
- **Sortie immédiate** : sélectionnez cette option pour autoriser le commutateur à supprimer une interface qui envoie un message de sortie de la table de transfert sans envoyer au préalable à l'interface des requêtes générales basées sur MAC. Lorsqu'un message de sortie de groupe MLD est reçu de la part d'un hôte, le système supprime le port hôte de l'entrée de la table. Après avoir transmis les requêtes MLD en provenance du routeur de multidiffusion, il supprime les entrées périodiquement s'il ne reçoit aucun rapport d'appartenance MLD de la part des clients de multidiffusion. Lorsqu'elle est activée, cette fonction réduit le temps nécessaire au blocage du trafic MLD inutile envoyé à un port du périphérique.
- **Nombre de requêtes du dernier membre** : nombre de requêtes propres au groupe MLD envoyées avant que le périphérique considère qu'il n'existe pas d'autre membre dans le groupe, dans la mesure où ce périphérique est le demandeur choisi.
  - *Utiliser robustesse des requêtes* : cette valeur est définie sur la page **Paramètres de VLAN MLD**.
  - *Défini par l'utilisateur* : saisissez une valeur définie par l'utilisateur.

ÉTAPE 4 Sélectionnez un VLAN et cliquez sur **Modifier**.

ÉTAPE 5 Saisissez les paramètres comme décrit ci-dessus.

ÉTAPE 6 Cliquez sur **Appliquer**. Le fichier de configuration de fonctionnement est mis à jour.

REMARQUE Changements dans la configuration des temporisations de surveillance MLD, tels que : Robustesse des requêtes, Intervalle de requête, etc. ne prennent pas effet sur les temporisations déjà créées.

Paramètres de VLAN MLD

Pour configurer le protocole MLD sur un VLAN spécifique :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Configuration de la multidiffusion IPv6 > Paramètres de VLAN MLD**.

Les champs suivants sont affichés pour chaque VLAN sur lequel MLD est activé :

- **Nom de l'interface** : VLAN pour lequel afficher les informations MLD.
- **Version du routeur MLD** : version du routeur MLD.
- **Robustesse des requêtes** : entrez le nombre de pertes de paquets prévues sur une liaison.
- **Intervalle de requête (s)** : intervalle à appliquer entre deux requêtes générales si ce périphérique est le demandeur choisi.
- **Intervalle de réponse max aux requêtes (s)** : délai utilisé pour calculer le code de réponse maximum inséré dans les requêtes générales périodiques.
- **Intervalle de requête du dernier membre (ms)** : saisissez le délai maximal de réponse à utiliser si le périphérique ne le reconnaît pas à partir des requêtes propres au groupe envoyées par l'émetteur de requêtes choisi.

ÉTAPE 2 Pour configurer un VLAN, sélectionnez-le et cliquez sur **Modifier**. Renseignez les champs décrits ci-dessus.

ÉTAPE 3 Cliquez sur **Appliquer**. Le fichier de configuration de fonctionnement est mis à jour.

Groupe de multidiffusion IP de surveillance IGMP/MLD

La page Groupe de multidiffusion IP de surveillance IGMP/MLD affiche les adresses de groupes IPv4 et IPv6 apprises à partir des messages IGMP/MLD.

Il peut y avoir une différence entre les informations affichées sur cette page et celles affichées sur la page Adresse de groupe MAC. Le cas suivant est un exemple : supposons que le système filtre en fonction des groupes basés sur MAC et qu'un port a demandé de se joindre aux groupes de multidiffusion 224.1.1.1 et 225.1.1.1, les deux étant mappés à la même adresse MAC de multidiffusion 01:00:5e:01:01. Dans ce cas, il n'y a qu'une seule entrée sur la page Multidiffusion MAC, mais deux entrées sur cette page.

Pour émettre une requête de recherche d'un groupe de multidiffusion IP :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **IGMP/MLD Snooping IP Multicast Group (Groupe de multidiffusion IP de surveillance IGMP/MLD)**.

ÉTAPE 2 Définissez le type de groupe de traçage (Snooping) à rechercher : IGMP ou MLD.

ÉTAPE 3 Saisissez tout ou partie des critères de filtrage des requêtes suivants :

- **Adresse de groupe est égale à** : définit l'adresse MAC ou IP du groupe de multidiffusion à interroger.
- **Adresse source est égale à** : définit l'adresse de l'expéditeur à interroger.
- **ID VLAN est égal à** : définit l'ID de VLAN à interroger.

ÉTAPE 4 Cliquez sur **OK**. Les champs suivants s'affichent pour chaque groupe de multidiffusion :

- **VLAN** : ID du VLAN.
- **Adresse de groupe** : adresse MAC ou IP du groupe de multidiffusion.
- **Adresse source** : adresse de l'expéditeur pour tous les ports du groupe spécifié.
- **Ports inclus** : liste des ports de destination pour le flux de multidiffusion.
- **Ports exclus** : liste des ports non membres du groupe.
- **Mode de compatibilité** : version d'enregistrement IGMP/MLD la plus ancienne que le périphérique reçoit des hôtes à l'adresse IP du groupe.

Ports de routeur de multidiffusion

Un port de routeur multidestination (Mrouter) est un port qui se connecte à un routeur multidestination. Le périphérique inclut le ou les numéros de ports de routeur de multidiffusion lorsqu'il transfère les flux de multidiffusion et les messages d'enregistrement IGMP/MLD. Cela est indispensable pour que les routeurs de multidiffusion puissent, à leur tour, transférer les flux de multidiffusion et propager les messages d'enregistrement vers d'autres sous-réseaux.

Pour configurer de manière statique les ports qui sont connectés au routeur de multidiffusion, ou afficher ceux dynamiquement détectés :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Port de routeur de multidiffusion**.

ÉTAPE 2 Saisissez tout ou partie des critères de filtrage des requêtes suivants :

- **ID VLAN est égal à** : sélectionnez l'ID de VLAN des ports du routeur décrits.
- **Version IP est égale à** : sélectionnez la version IP prise en charge par le routeur de multidiffusion.
- **Type d'interface est égal à** : choisissez d'afficher les ports ou les LAG.

ÉTAPE 3 Cliquez sur **OK**. Les interfaces répondant aux critères de requête s'affichent.

ÉTAPE 4 Sélectionnez le type d'association de chaque port ou LAG. Les options disponibles sont les suivantes :

- **Statique** : le port est configuré de manière statique en tant que port de routeur de multidiffusion.
- **Dynamique** : (affichage uniquement) le port est configuré de manière dynamique en tant que port de routeur de multidiffusion par une requête MLD/IGMP. Pour activer l'apprentissage dynamique des ports de routeurs de multidiffusion, accédez à la page **Multidiffusion** > **IGMP Snooping** et à la page **Multidiffusion** > **MLD Snooping**.
- **Interdit** : ce port ne doit pas être configuré en tant que port de routeur de multidiffusion, même s'il reçoit des requêtes IGMP ou MLD. Si l'option Interdit est activée sur un port, l'apprentissage des ports MRouter n'a pas lieu sur ce port (ce qui signifie que l'option Apprentissage automatique des ports MRouter n'est pas activée sur ce port).
- **Aucun** : le port n'est actuellement pas un port de routeur de multidiffusion.

ÉTAPE 5 Cliquez sur **Appliquer** pour mettre à jour le périphérique.

Tout transférer

La page Tout transférer active la configuration des ports et/ou LAG qui doivent recevoir des flux de multidiffusion en provenance d'un VLAN spécifique. Cette fonction exige que vous activiez le filtrage multidiffusion par ponts sur la page Propriétés. Si cette fonction est désactivée, tout le trafic de multidiffusion est envoyé aux ports du périphérique.

Vous pouvez configurer (manuellement) un port en mode Tout transférer de manière statique si les périphériques qui se connectent à ce port ne prennent pas en charge IGMP et/ou MLD.

Les messages IGMP ou MLD ne sont pas transférés aux ports définis en mode *Tout transférer*.

REMARQUE Cette configuration concerne uniquement les ports membres du VLAN sélectionné.

Pour définir la multidiffusion Tout transférer :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Tout transférer**.

ÉTAPE 2 Définissez les éléments suivants :

- **ID VLAN est égal à** : ID du VLAN dont afficher les ports/LAG.
- **Type d'interface est égal à** : choisissez d'afficher les ports ou les LAG.

ÉTAPE 3 Cliquez sur **OK**. L'état de tous les ports/LAG est affiché.

ÉTAPE 4 Sélectionnez le port/LAG à définir en mode Tout transférer à l'aide des méthodes suivantes :

- **Statique** : le port reçoit tous les flux de multidiffusion.
- **Interdit** : le port ne peut pas recevoir de flux de multidiffusion, même si la surveillance IGMP/MLD l'a désigné pour rejoindre un groupe de multidiffusion.
- **Aucun** : le port n'est actuellement pas un port en mode Tout transférer.

ÉTAPE 5 Cliquez sur **Appliquer**. Le fichier de configuration de fonctionnement est mis à jour.

Multidiffusion non enregistrée

Cette fonction permet de garantir que le client reçoit uniquement les groupes de multidiffusion demandés (enregistrés) et non d'autres groupes éventuellement transmis sur le réseau (non enregistrés).

En général, les trames de multidiffusion non enregistrées sont transférées vers tous les ports du VLAN.

Vous pouvez sélectionner un port pour qu'il reçoive ou refuse (filtre) les flux de multidiffusion non enregistrés. Cette configuration est valide pour tout VLAN dont le port est (ou sera) membre.

Pour définir des paramètres de multidiffusion non enregistrée :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Multidiffusion non enregistrée**.

ÉTAPE 2 Sélectionnez **Type d'interface est égal à** : pour afficher les ports ou les LAG.

ÉTAPE 3 Cliquez sur **OK**.

ÉTAPE 4 Définissez les éléments suivants :

- **Port/LAG** : affiche l'ID du port ou du LAG.
- Affiche l'état de transfert de l'interface sélectionnée. Les valeurs possibles sont :
  - *Transfert* : active le transfert des trames de multidiffusion non enregistrée vers l'interface sélectionnée.
  - *Filtrage* : active le filtrage (rejet) des trames de multidiffusion non enregistrée sur l'interface sélectionnée.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres sont enregistrés et le fichier de Configuration d'exécution est mis à jour.

18

Configuration IP

Les adresses d'interface IP peuvent être configurées manuellement par l'utilisateur ou automatiquement via un serveur DHCP. Cette section fournit des informations sur la définition des adresses IP du périphérique, soit manuellement soit en faisant du périphérique un client DHCP.

Cette section aborde les points suivants :

- **Présentation**
- **IPv4 Management and Interfaces (Interfaces et gestion IPv4)**
- **Nom de domaine**

Présentation

Adressage IP Layer 2

Le périphérique ne dispose que d'une adresse IPv4 et de deux interfaces IPv6 (soit interface « native », soit Tunnel) dans la gestion VLAN. Cette adresse IP et la passerelle par défaut peuvent être configurées manuellement ou par DHCP. Vous pouvez configurer l'adresse IP statique et la passerelle par défaut sur la page Interface IPv4. Le périphérique utilise la passerelle par défaut (si elle existe) pour communiquer avec les périphériques qui ne se trouvent pas sur le même sous-réseau IP. Par défaut, VLAN 1 est le VLAN de gestion mais vous pouvez modifier ce paramètre. Le périphérique n'est accessible à l'adresse IP configurée que via son VLAN de gestion.

Le paramètre d'usine par défaut de la configuration de l'adresse IPv4 est *DHCPv4*. Cela signifie que le périphérique joue le rôle de client DHCPv4 et envoie une demande DHCPv4 lors de l'amorçage.

Si le périphérique reçoit une réponse DHCPv4 du serveur DHCPv4 (contenant une adresse IPv4), il envoie des paquets ARP (Address Resolution Protocol, protocole de résolution d'adresse) pour vérifier que cette adresse IP est unique. Si la réponse ARP indique que l'adresse IPv4 est déjà utilisée, le périphérique envoie le message DHCPDECLINE (Refus DHCP) au serveur DHCP répondu. Il envoie ensuite un nouveau paquet DHCPDISCOVER (Détection DHCP) pour relancer le processus.

Si le périphérique n'a reçu aucune réponse DHCPv4 au bout de 60 secondes, il continue à lancer des requêtes DHCPDISCOVER et utilise l'adresse IPv4 : 192.168.1.254/24.

Des collisions d'adresse IP se produisent lorsqu'une même adresse IP est utilisée par plusieurs périphériques sur un même sous-réseau IP. Les collisions d'adresse nécessitent une action de la part de l'administrateur sur le serveur DHCP et/ou sur les périphériques en conflit avec le périphérique.

Lorsqu'un VLAN est configuré pour utiliser des adresses IP dynamiques, le périphérique envoie des demandes DHCPv4 jusqu'à ce qu'un serveur DHCPv4 lui attribue une adresse IPv4. Vous pouvez configurer le VLAN de gestion avec une adresse IP statique ou dynamique.

Les règles d'affectation d'adresse IP au périphérique sont les suivantes :

- Si le périphérique n'est pas configuré avec une adresse IPv4 statique, il émet des requêtes DHCPv4 jusqu'à ce qu'il reçoive une réponse d'un serveur DHCPv4.
- Si l'adresse IP du périphérique change, ce dernier envoie des paquets ARP gratuits au VLAN correspondant pour rechercher les éventuelles collisions d'adresse IP. Cette règle s'applique également lorsque le périphérique revient à l'adresse IP par défaut.
- La LED d'état du système s'allume en vert lorsque le serveur DHCP envoie une nouvelle adresse IP unique. Si une adresse IP statique a été définie, la LED d'état du système s'allume également en vert. Cette LED clignote pendant que le périphérique acquiert son adresse IP et qu'il utilise l'adresse IP par défaut définie en usine 192.168.1.254.
- Les mêmes règles s'appliquent lorsqu'un client doit renouveler son bail avant la date d'expiration, via un message DHCPREQUEST (Demande DHCP).
- Avec les paramètres d'usine, si aucune adresse IP n'est disponible (qu'elle soit définie de manière statique ou acquise via DHCP), le système utilise l'adresse IP par défaut. Lorsque d'autres adresses IP deviennent disponibles, elles sont automatiquement utilisées. L'adresse IP par défaut se trouve toujours sur le VLAN de gestion.

Interface de bouclage

Présentation

L'interface de bouclage est une interface virtuelle dont l'état opérationnel est toujours actif. Si l'adresse IP qui est configurée sur cette interface virtuelle est utilisée comme adresse locale lors de la communication avec les applications IP distantes, la communication ne sera pas interrompue même si la route vers l'application distante a été modifiée.

L'état opérationnel de l'interface de bouclage est toujours actif. Définissez une adresse IP sur celle-ci et utilisez-cette adresse-IP comme adresse IP locale pour la communication IP avec les applications IP distantes. La communication est maintenue tant que les applications distantes restent joignables à partir de n'importe quelle interface IP (sans bouclage) active du commutateur. En revanche, si l'adresse IP d'une interface IP est utilisée pour la communication avec des applications distantes, la communication est interrompue lorsque l'interface IP est arrêtée.

Une interface de bouclage ne prend pas en charge le pontage ; elle ne peut pas être membre d'un VLAN et aucun protocole Couche 2 ne peut être activé sur celui-ci.

L'identifiant de l'interface de liaison locale IPv6 est 1.

Lorsque le commutateur est en mode système Couche 2, les règles suivantes sont prises en charge :

- Une seule interface de bouclage est prise en charge.
- Deux interfaces IPv4 peuvent être configurées : une sur un port VLAN ou Ethernet et une sur l'interface de bouclage.
- Si l'adresse IPv4 a été configurée sur le VLAN par défaut et que ce dernier a été changé, le commutateur déplace l'adresse IPv4 vers le nouveau VLAN par défaut.

Configuration d'une interface de bouclage

Pour configurer une interface de bouclage IPv4, procédez comme suit :

- En mode Couche 2, activez l'interface de bouclage et configurez son adresse sur la page Administration > Interface de gestion > Interface IPv4.
- En mode Couche 3, ajoutez une interface de bouclage en Configuration IP > IPv4 Management and Interfaces (Interfaces et gestion IPv4) > Interface IPv4.

IPv4 Management and Interfaces (Interfaces et gestion IPv4)

Définition d'une interface IPv4

Pour que vous puissiez gérer le périphérique à l'aide de l'utilitaire de configuration Web, vous devez définir et connaître l'adresse de gestion IPv4 du périphérique. L'adresse IP du périphérique peut être configurée manuellement ou reçue automatiquement depuis un serveur DHCP.

Pour configurer une adresse IPv4 pour le périphérique :

ÉTAPE 1 Cliquez sur **Administration > Interface de gestion > Interface IPv4**.

ÉTAPE 2 Saisissez les valeurs appropriées dans les champs suivants :

- **VLAN de gestion** : sélectionnez le VLAN de gestion utilisé pour accéder au périphérique via telnet ou l'interface utilisateur graphique (GUI) Web. VLAN1 est le VLAN de gestion par défaut.
- **Type d'adresse IP** : sélectionnez l'une des options suivantes :
  - *Dynamique* : détectez l'adresse IP via DHCP sur le VLAN de gestion.
  - *Statique* : définissez manuellement une adresse IP statique.

REMARQUE L'option 12 DHCP (option Nom d'hôte) est prise en charge lorsque le périphérique est un client DHCP. Si l'option 12 DHCP est reçue d'un serveur DHCP, elle est enregistrée en tant que nom d'hôte du serveur. L'option 12 DHCP ne sera pas demandée par le périphérique. Le serveur DHCP doit être configuré pour envoyer l'option 12 indépendamment de ce qui est demandé afin de pouvoir utiliser cette fonctionnalité.

Pour définir une adresse IP statique, configurez les champs suivants.

- **Adresse IP** : saisissez l'adresse IP et configurez l'un des champs **Masque** suivants :
  - **Network Mask** : sélectionnez et saisissez le masque d'adresse IP.
  - **Prefix Length** : sélectionnez et saisissez la longueur du préfixe d'adresse IPv4.
- **Interface de bouclage** : sélectionnez cette option pour activer la configuration d'une interface de bouclage (voir **Interface de bouclage**).
- **Adresse IP de bouclage** : saisissez l'adresse IPv4 de l'interface de bouclage.

Renseignez l'un des champs suivants pour le **Masque de bouclage** :

- **Masque de réseau** : saisissez le masque de l'adresse IPv4 de l'interface de bouclage.
- **Longueur du préfixe** : saisissez la longueur du préfixe de l'adresse IPv4 de l'interface de bouclage.

- **Passerelle par défaut administrative** : sélectionnez **Défini par l'utilisateur** et saisissez l'adresse IP de la passerelle par défaut. Vous pouvez aussi sélectionner **Aucun** pour supprimer de l'interface l'adresse IP de passerelle par défaut sélectionnée.
- **Passerelle opérationnelle par défaut** : indique l'état de la passerelle par défaut actuelle.

  REMARQUE Si aucune passerelle par défaut n'est configurée pour le périphérique, ce dernier ne peut pas communiquer avec les périphériques qui ne font pas partie du même sous-réseau IP.

Si le système récupère une adresse IP dynamique auprès du serveur DHCP, parmi les champs suivants, sélectionnez ceux que vous souhaitez activer :

- **Renouveler l'adresse IP maintenant** : l'adresse IP dynamique du périphérique peut être renouvelée à tout moment après son affectation par un serveur DHCP. Remarque : selon la configuration de votre serveur DHCP, le périphérique peut recevoir une nouvelle adresse IP après le renouvellement, ce qui nécessite le paramétrage de l'utilitaire de configuration Web à la nouvelle adresse IP.
- **Configuration automatique via DHCP** : affiche l'état de la fonction Configuration automatique. Vous pouvez configurer cette fonction à l'aide de l'option *Administration* > *Gestion de fichiers* > *Configuration automatique DHCP*.

ÉTAPE 3 Cliquez sur **Apply**. Les paramètres d'interface IPv4 sont modifiés et écrits dans le fichier de Configuration d'exécution.

- *Local* : indique que la route est un chemin local. Ce type ne peut pas être sélectionné, mais il est créé par le système.

ARP

Le périphérique gère une table ARP (Address Resolution Protocol, protocole de résolution d'adresse) pour tous les périphériques connus résidant sur ses sous-réseaux IP à connexion directe. Un sous-réseau IP à connexion directe désigne un sous-réseau auquel une interface IPv4 du périphérique est connectée. Lorsque le périphérique doit envoyer/acheminer un paquet vers un périphérique local, il effectue une recherche dans la table ARP pour obtenir l'adresse MAC du périphérique en question. La table ARP contient à la fois des adresses statiques et des adresses dynamiques. Les adresses statiques sont configurées manuellement et n'ont pas de limite de validité. Le périphérique crée des adresses dynamiques à partir des paquets ARP qu'il reçoit. Les adresses dynamiques ont une durée de vie limitée, que vous configurez.

REMARQUE La mise en correspondance d'adresse IP/MAC de la table ARP sert à transférer le trafic en provenance du périphérique.

Pour définir les tables ARP :

ÉTAPE 1 Cliquez sur **Configuration IP > IPv4 Management and Interfaces (Interfaces et gestion IPv4) > ARP**.

ÉTAPE 2 Saisissez les paramètres.

- **Délai d'expiration des entrées ARP** : saisissez la durée en secondes pendant laquelle les adresses dynamiques peuvent rester dans la table ARP. Les adresses dynamiques ne sont valides dans la table que pour la durée définie par Délai d'expiration des entrées ARP. Lorsqu'une adresse dynamique arrive à expiration, elle est supprimée de la table et doit être réapprise pour figurer à nouveau dans cette table.
- **Effacer les entrées de la table ARP** : sélectionnez le type des entrées ARP à effacer du système.
  - *Tout* : supprime immédiatement toutes les adresses statiques et dynamiques.
  - *Dynamique* : supprime immédiatement toutes les adresses dynamiques.
  - *Statique* : supprime immédiatement toutes les adresses statiques.
  - *Délai d'expiration normal* : supprime les adresses dynamiques en fonction de la durée de vie configurée pour les entrées ARP.

ÉTAPE 3 Cliquez sur **Appliquer.** Les paramètres globaux ARP sont écrits dans le fichier de Configuration d'exécution.

La table ARP contient les champs suivants :

- **Interface** : interface IPv4 du sous-réseau IP à connexion directe où réside le périphérique IP.

- **Adresse IP** : adresse IP du périphérique IP.
- **Adresse MAC** : adresse MAC du périphérique IP.
- **État** : indique si l'entrée a été saisie manuellement ou apprise de manière dynamique.

ÉTAPE 4 Cliquez sur **Ajouter**.

ÉTAPE 5 Configurez les paramètres suivants :

- **Version IP** : format d'adresse IP pris en charge par l'hôte. Seul IPv4 est pris en charge.
- **Interface** : affiche l'ID du VLAN de gestion.

  Pour les périphériques en mode Couche 2, il existe un seul sous-réseau IP à connexion directe, toujours situé sur le VLAN de gestion. Toutes les adresses statiques et dynamiques de la table ARP résident sur le VLAN de gestion.
- **Adresse IP** : saisissez l'adresse IP du périphérique local.
- **Adresse MAC** : saisissez l'adresse MAC du périphérique local.

ÉTAPE 6 Cliquez sur **Apply**. L'entrée ARP est enregistrée dans le fichier de Configuration d'exécution.

Configuration globale IPv6

Pour définir des paramètres IPv6 globaux et les paramètres de client DHCPv6 :

ÉTAPE 1 Cliquez sur **Administration > Interface de gestion > Configuration globale IPv6**.

ÉTAPE 2 Saisissez les valeurs appropriées dans les champs suivants :

- **Intervalle de limites de débit ICMPv6** : saisissez la fréquence à laquelle les messages d'erreur ICMP sont générés.
- **Taille des cases de limite de débit ICMPv6** : saisissez le nombre maximal de messages d'erreur ICMP que le périphérique peut envoyer dans chaque intervalle.

Paramètres de client DHCPv6

- **Unique Identifier (DUID) Format (Format de l'identificateur unique (DUID))** : il s'agit de l'identificateur du client DHCP utilisé par le serveur DHCP pour localiser le client. Les formats suivants sont disponibles :
  - *Link-Couche (Couche de liaison)* : (par défaut). Si vous sélectionnez cette option, l'adresse MAC du périphérique est utilisée.
  - *Enterprise Number (Numéro d'entreprise)* : lorsque vous sélectionnez cette option, renseignez les champs suivants.

- **Enterprise Number (Numéro d'entreprise)** : numéro d'entreprise privé enregistré par les fournisseurs comme géré par IANA.
- **Identifier (Identificateur)** : chaîne hexadécimale définie par le fournisseur (jusqu'à 64 caractères hexadécimaux). Si le nombre de caractères est impair, un zéro est ajouté à droite. Vous pouvez ajouter un point ou une virgule tous les deux caractères hexadécimaux pour les séparer.
- **DHCPv6 Unique Identifier (DUID) (Identificateur unique DHCPv6 (DUID))** : affiche l'identificateur sélectionné.

ÉTAPE 3 Cliquez sur **Apply**. Les paramètres globaux IPv6 et les paramètres de client DHCPv6 sont mis à jour.

Interface IPv6

Vous pouvez configurer l'interface IPv6 sur un port, un LAG, un VLAN, une interface de bouclage ou un tunnel.

Contrairement aux autres types d'interfaces, une interface de tunnel est d'abord créée sur la page Tunnel IPv6, puis l'interface IPv6 est configurée sur le tunnel sur cette page.

Pour définir une interface IPv6 :

ÉTAPE 1 Cliquez sur **Administration** > **Interface de gestion** > **Interfaces IPv6**.

ÉTAPE 2 Cliquez sur **Appliquer** pour configurer la zone par défaut.

ÉTAPE 3 Cliquez sur **Ajouter** pour ajouter une nouvelle interface sur laquelle IPv6 est activé.

ÉTAPE 4 Renseignez les champ :

- **Interface IPv6** : sélectionnez un port, un LAG, un VLAN, une interface de bouclage ou un tunnel ISATAP spécifique pour l'adresse IPv6.

ÉTAPE 5 Pour configurer l'interface comme client DHCPv6, ce qui signifie activer l'interface pour recevoir des informations depuis le serveur DHCPv6, comme la configuration SNTP et des informations DNS, renseignez les champs **Client DHCPv6** :

- **Sans état** : sélectionnez cette option pour activer l'interface comme client DHCPv6 sans état. Cela permet la réception des informations de configuration à partir d'un serveur DHCP.
- **Minimum Information Refresh Time (Intervalle minimal d'actualisation des informations)** : cette valeur est utilisée pour mettre une limite sur la valeur de l'intervalle d'actualisation. Lorsque le serveur envoie une option d'intervalle d'actualisation inférieure à cette valeur, cette valeur est utilisée en substitution. Sélectionnez **Infini** (aucune actualisation sauf si le serveur envoie cette option) ou **Défini par l'utilisateur** pour définir une valeur.

- **Information Refresh Time (Intervalle d'actualisation des informations)** : cette valeur indique la fréquence d'actualisation par le périphérique des informations reçues du serveur DHCPv6. Si cette option n'est pas reçue du serveur, la valeur entrée ici est utilisée. Sélectionnez **Infini** (aucune actualisation sauf si le serveur envoie cette option) ou **Défini par l'utilisateur** pour définir une valeur.

ÉTAPE 6 Pour configurer des paramètres IPv6 supplémentaires, renseignez les champs suivants :

- **Configuration automatique d'adresses IPv6** : sélectionne la configuration automatique des adresses à partir des annonces de routeur envoyées par des voisins.

REMARQUE Le périphérique ne prend pas en charge la configuration automatique des adresses avec conservation d'état à partir d'un serveur DHCPv6.

- **Nombre de tentatives DAD** : saisissez le nombre de messages de sollicitation des voisins consécutifs à envoyer lors du processus DAD (Duplicate Address Detection, détection des adresses en double) sur les adresses IPv6 Unicast de l'interface. DAD vérifie l'unicité d'une nouvelle adresse IPv6 Unicast avant de l'attribuer. Les nouvelles adresses restent à l'état provisoire pendant la vérification DAD. Saisissez **0** dans ce champ pour désactiver le traitement de détection des adresses en double sur l'interface indiquée. Saisissez **1** dans ce champ pour indiquer une transmission unique, sans transmission de suivi.
- **Envoyer des messages ICMPv6** : active la génération de messages concernant les destinations injoignables.

ÉTAPE 7 Cliquez sur **Appliquer** pour activer le traitement IPv6 sur l'interface sélectionnée. Pour les interfaces IPv6 standard, les adresses suivantes sont configurées automatiquement :

- Adresse de liaison locale, à l'aide de l'ID d'interface au format EUI-64, sur la base de l'adresse MAC d'un périphérique
- Toutes les adresses de multidiffusion de liaison locale des nœuds (FF02::1)
- Adresse de multidiffusion de nœud sollicité (au format FF02::1:FFXX:XXXX)

ÉTAPE 8 Cliquez sur **Table des adresses IPv6** pour affecter manuellement des adresses IPv6 à l'interface, si nécessaire. Cette page est décrite à la section **Définition d'adresses IPv6**.

ÉTAPE 9 Pour modifier un tunnel, sélectionnez une interface (définie en tant que tunnel sur la page Interfaces IPv6) dans la table des tunnels IPv6 et cliquez sur **Table de tunnels IPv6**. Reportez-vous à la section **Tunnel IPv6**

ÉTAPE 10 Appuyez sur le bouton **Restart (Redémarrer)** pour lancer l'actualisation des informations sans état reçues du serveur DHCPv6.

Détails de client DHCPv6

Le bouton **Détails** affiche les informations reçues sur l'interface à partir d'un serveur DHCPv6.

Cette option est activée lorsque l'interface sélectionnée est définie comme client DHCPv6 sans état.

Lorsque vous appuyez sur ce bouton, les champs suivants s'affichent (pour les informations reçues du serveur DHCP) :

- **DHCPv6 Operational Mode (Mode de fonctionnement DHCPv6)** : permet d'afficher Enabled (Activé) lorsque les conditions suivantes sont remplies :
  - L'interface est active.
  - IPv6 y est activé.
  - Le client DHCPv6 sans état y est activé.
- **Stateless Service (Service sans état)** : configure si le client est défini comme sans état (il reçoit les informations d'un serveur DHCP) ou non.
- **Délai d'actualisation minimum des informations** : voir ci-dessus.
- **Information Refresh Time (Intervalle d'actualisation des informations)** : voir ci-dessus.
- **Received Information Refresh Time (Intervalle reçu pour l'actualisation des informations)** : intervalle d'actualisation reçu du serveur DHCPv6.
- **Remaining Information Refresh Time (Intervalle restant avant l'actualisation des informations)** : temps restant jusqu'à la prochaine actualisation.
- **DNS Servers (Serveurs DNS)** : liste des serveurs DNS reçue du serveur DHCPv6.
- **DNS Domain Search List (Liste de recherche de domaines DNS)** : liste des domaines reçue du serveur DHCPv6.
- **SNTP Servers (Serveurs SNTP)** : liste des serveurs SNTP reçue du serveur DHCPv6.
- **POSIX Timezone String (Chaîne de fuseau horaire POSIX)** : fuseau horaire reçu du serveur DHCPv6.
- **Configuration Server (Serveur de configuration)** : serveur contenant un fichier de configuration reçu du serveur DHCPv6.
- **Configuration Path Name (Nom du chemin de configuration)** : chemin vers le fichier de configuration sur le serveur de configuration reçu du serveur DHCPv6.

Tunnel IPv6

Les tunnels permettent la transmission des paquets IPv6 sur des réseaux IPv4. Chaque tunnel a une adresse IPv4 source et s'il s'agit d'un tunnel manuel, il dispose également d'une adresse IPv4 de destination. Le paquet IPv6 est encapsulé entre ces adresses.

Tunnels ISATAP

Le type de tunnel pouvant être configuré sur le périphérique est nommé tunnel ISATAP (Intra-Site Automatic Tunnel Addressing Protocol, ou protocole d'adressage automatique de tunnel intrasite) qui peut être un tunnel point à multipoint. L'adresse source est l'adresse IPv4 du périphérique.

Lors de la configuration d'un tunnel ISATAP, l'adresse IPv4 de destination est fournie par le routeur. Notez les éléments suivants :

- Une adresse IPv6 de liaison locale est affectée à l'interface ISATAP. L'adresse IP initiale est affectée à l'interface, qui est alors activée.
- Si une interface ISATAP est active, l'adresse IPv4 du routeur ISATAP est résolue via DNS à l'aide d'un mappage ISATAP-à-IPv4. Si l'enregistrement DNS ISATAP n'est pas résolu, le mappage nom d'hôte-à-adresse ISATAP est recherché dans la table de mappage des hôtes.
- S'il est impossible de résoudre l'adresse IPv4 du routeur ISATAP à l'aide du processus DNS, l'interface IP ISATAP reste active. Le système ne comportera un routeur par défaut pour le trafic ISATAP qu'après résolution du processus DNS.

Configuration des tunnels

REMARQUE Après avoir configuré un tunnel, configurez l'interface IPv6 sur la page Interfaces IPv6.

Pour configurer un tunnel IPv6 :

ÉTAPE 1 Cliquez sur **Administration > Interface de gestion > Tunnel IPv6**.

ÉTAPE 2 Saisissez les valeurs appropriées dans les champs suivants :

- **Numéro du tunnel** : affiche le numéro de domaine du routeur de tunnel automatique.
- **Type du tunnel** : toujours ISATAP.
- **Adresse IPv4 source** : l'adresse IPv4 de l'interface sélectionnée sur le périphérique actuel utilisée pour constituer une partie de l'adresse IPv6.
  - *Auto* : sélectionne automatiquement l'adresse IPv4 la plus basse parmi toutes les interfaces IPv4 configurées sur le périphérique. Cette option est équivalente à l'option d'interface en mode Couche 3 car en mode Couche 2, il n'y a qu'une interface.

REMARQUE Lorsque l'adresse IPv4 est modifiée, l'adresse locale de l'interface de tunnel est également modifiée.

- *Manuel* : saisissez l'adresse IPv4 source à utiliser. L'adresse IPv4 configurée doit être l'une des adresses IPv4 des interfaces IPv4 du périphérique.
- *Interface* : (Couche 3) sélectionnez l'interface IPv4 à utiliser.

- **ISATAP Router Name (Nom de routeur ISATAP)** : chaîne globale qui représente un nom de domaine de routeur de tunnel automatique spécifique. Il peut s'agir du nom par défaut (ISATAP) ou d'un nom défini par l'utilisateur.
- **Intervalle de sollicitation ISATAP** : nombre de secondes entre deux messages de sollicitation de routeur ISATAP, si aucun routeur ISATAP n'est actif. Il peut s'agir de l'intervalle par défaut ou d'une valeur d'intervalle définie par l'utilisateur.
- **Robustesse ISATAP** : permet de calculer l'intervalle des requêtes DNS ou de sollicitation de routeur. Plus la valeur est élevée, plus les requêtes sont fréquentes.

REMARQUE Le tunnel ISATAP ne sera pas opérationnel si l'interface IPv4 sous-jacente n'est pas active.

ÉTAPE 3 Cliquez sur **Apply**. Le tunnel est enregistré dans le fichier de Configuration d'exécution.

REMARQUE Pour créer un tunnel ISATAP, cliquez sur le bouton **Create ISATAP Tunnel (Créer un tunnel ISATAP)**. Un tunnel ISATAP est créé avec l'adresse IPv4 source automatique. Lorsqu'un tunnel ISATAP est créé, ce bouton devient **Delete ISATAP Tunnel (Supprimer le tunnel ISATAP)**. Cliquez sur ce bouton pour supprimer le tunnel ISATAP.

REMARQUE Pour fermer un tunnel, cliquez sur **Modifier** et désélectionnez État du tunnel.

Définition d'adresses IPv6

Pour affecter une adresse IPv6 à une interface IPv6 :

ÉTAPE 1 Cliquez sur **Administration** > **Interface de gestion** > **Adresses IPv6**

ÉTAPE 2 Pour filtrer la table, sélectionnez un nom d'interface et cliquez sur **OK**. L'interface s'affiche dans la table des adresses IPv6.

ÉTAPE 3 Cliquez sur **Add**.

ÉTAPE 4 Saisissez les valeurs des champs.

- **Interface IPv6** : affiche l'interface sur laquelle l'adresse IPv6 doit être définie. Si un astérisque (*) s'affiche, cela signifie que l'interface IPv6 n'est pas activée mais a été configurée.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 à ajouter.
  - *Liaison locale* : une adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : une adresse IPv6 qui est de type global IPV6 monodiffusion, visible et joignable à partir d'autres réseaux.
  - *Pluridiffusion* : l'adresse IPv6 est une adresse de pluridiffusion. Il s'agit d'une adresse attribuée à un ensemble d'interfaces appartenant généralement à des nœuds différents. Un paquet envoyé à une adresse pluridiffusion est délivré à l'interface la plus proche (comme défini par les protocoles de routage utilisés) identifiée par l'adresse pluridiffusion.
- **Adresse IPv6** : en mode Couche 2, le périphérique prend en charge une seule interface IPv6. Outre les adresses de liaison locale et de multidiffusion par défaut, le périphérique ajoute aussi automatiquement des adresses globales à l'interface sur la base des annonces de routeur qu'il reçoit. Le périphérique prend en charge un maximum de 128 adresses sur l'interface. Chaque adresse doit correspondre à une adresse IPv6 valide, spécifiée au format hexadécimal au moyen de valeurs de 16 bits séparées par le signe deux-points.

  Vous pouvez ajouter les types d'adresses suivants aux différents types de tunnels :
  - Tunnels manuels : adresse globale ou de pluridiffusion
  - Tunnels ISATAP : adresse globale avec EUI-6
  - Tunnels 6to4 : aucune
- **Longueur du préfixe** : la longueur du préfixe IPv6 global est une valeur comprise entre 0 et 128 qui indique le nombre de bits contigus les plus significatifs de l'adresse dont se compose le préfixe (la partie réseau de l'adresse).
- **EUI-64** : sélectionnez cette option pour employer le paramètre EUI-64 afin d'identifier la portion de l'adresse IPv6 globale correspondant à l'ID d'interface en utilisant le format EUI-64 sur la base de l'adresse MAC d'un périphérique.

ÉTAPE 5 Cliquez sur **Apply**. Le fichier de configuration de fonctionnement est mis à jour.

Liste des routeurs par défaut IPv6

La page Liste des routeurs par défaut IPv6 vous permet de configurer et d'afficher les adresses de routeur IPv6 par défaut. Cette liste contient les routeurs susceptibles de devenir le routeur par défaut du périphérique pour le trafic non local (elle peut être vide). Le périphérique sélectionne un routeur au hasard dans la liste. Le périphérique prend en charge un seul routeur IPv6 statique par défaut. Les routeurs dynamiques par défaut sont des routeurs qui ont envoyé des annonces de routeur à l'interface IPv6 du périphérique.

Lorsque vous ajoutez ou supprimez des adresses IP, les événements suivants se produisent :

- Lorsque vous supprimez une interface IP, toutes les adresses IP de routeur par défaut sont supprimées. Il est impossible de supprimer des adresses IP dynamiques.
- Un message d'alerte apparaît lorsque vous tentez d'insérer plusieurs adresses définies par l'utilisateur.
- Un message d'alerte apparaît lorsque vous tentez d'insérer une adresse d'un type autre qu'une liaison locale « fe80: ».

Pour définir un routeur par défaut :

ÉTAPE 1 Cliquez sur **Administration** > **Interface de gestion** > **Liste des routeurs par défaut IPv6**.

Cette page affiche les champs suivants pour chaque routeur par défaut :

- **Interface** : interface IPv6 sortante où réside le routeur par défaut.
- **Adresse IPv6 du routeur par défaut** : adresse IP de liaison locale du routeur par défaut.
- **Type** : configuration du routeur par défaut qui inclut les options suivantes :
  - *Statique* : le routeur par défaut a été ajouté manuellement à cette table à l'aide du bouton **Ajouter**.
  - *Dynamique* : le routeur par défaut a été configuré de manière dynamique.
- **État** : indique l'état du routeur. Les valeurs disponibles sont les suivantes :
  - *Joignable* : le routeur est identifié comme joignable.
  - *Injoignable* : le routeur est identifié comme injoignable.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un routeur par défaut statique.

ÉTAPE 3 Renseignez les champs suivants :

- **Interface de liaison locale (Couche 2)** : affiche l'interface Liaison locale sortante.
- **Adresse IPv6 du routeur par défaut** : adresse IP du routeur par défaut.

ÉTAPE 4 Cliquez sur **Appliquer**. Le routeur par défaut est enregistré dans le fichier de Configuration d'exécution.

Définition des informations sur les voisins IPv6

La page Voisins IPv6 vous permet de configurer et d'afficher la liste des voisins IPv6 sur l'interface IPv6. La table Voisins IPv6, également appelée Cache de détection du voisinage IPv6, affiche les adresses MAC des voisins IPv6 qui font partie du même sous-réseau IPv6 que le périphérique. C'est l'équivalent IPv6 de la table ARP IPv4. Lorsque le périphérique a besoin de communiquer avec ses voisins, il utilise la table de voisinage IPv6 pour déterminer les adresses MAC à partir de leurs adresses IPv6.

Cette page affiche les voisins détectés automatiquement ou configurés manuellement. Chaque entrée indique l'interface à laquelle le voisin est connecté, les adresses IPv6 et MAC de ce voisin, son type de configuration (statique ou dynamique) et l'état du voisin.

Pour définir des voisins IPv6 :

ÉTAPE 1 Cliquez sur **Administration> Interface de gestion >Voisins IPv6**.

Vous pouvez sélectionner une option **Effacer la table** afin d'effacer certaines adresses IPv6 (ou toutes) de la table des voisins IPv6.

- **Statique uniquement** : supprime les entrées d'adresse IPv6 statiques.
- **Dynamique uniquement** : supprime les entrées d'adresse IPv6 dynamiques.
- **Dynamique et statique** : supprime les entrées d'adresse IPv6 statiques et dynamiques.

Les champs suivants sont affichés pour les interfaces de voisinage :

- **Interface** : type d'interface de voisinage IPv6.
- **Adresse IPv6** : adresse IPv6 d'un voisin.
- **Adresse MAC** : adresse MAC mappée sur l'adresse IPv6 spécifiée.
- **Type** : type de saisie des informations de cache de découverte des voisins (statique ou dynamique).
- **État** : indique l'état du voisin IPv6. Les valeurs disponibles sont les suivantes :
  - *Incomplet* : résolution d'adresse en cours. Le voisin n'a pas encore répondu.
  - *Atteignable* : le voisin est reconnu comme étant accessible.
  - *Périmé* : un voisin précédemment connu est inaccessible. Aucune action n'est entreprise pour vérifier son accessibilité tant qu'il n'est pas nécessaire de lui envoyer du trafic.
  - *Retard* : un voisin précédemment connu est inaccessible. L'interface reste à l'état Retard pour la durée prédéfinie indiquée par Délai de retard. Si aucune confirmation d'accessibilité n'est reçue, l'état passe à Sonde.
  - *Sonde* : le voisin n'est plus reconnu comme inaccessible et des sondes UNS (Unicast Neighbor Solicitation, sollicitation de voisinage Unicast) sont envoyées pour vérifier son accessibilité.

- **Routeur** : spécifie si le voisin est un routeur (**Oui** ou **Non**).

ÉTAPE 2 Pour ajouter un voisin à la table, cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les valeurs appropriées dans les champs suivants :

- **Interface** : interface de voisinage IPv6 à ajouter.
- **Adresse IPv6** : saisissez l'adresse réseau IPv6 affectée à l'interface. Cette adresse doit être une adresse IPv6 valide.
- **Adresse MAC** : saisissez l'adresse MAC mappée sur l'adresse IPv6 spécifiée.

ÉTAPE 4 Cliquez sur **Apply**. Le fichier de configuration de fonctionnement est mis à jour.

ÉTAPE 5 Pour remplacer le type d'une adresse IP **Dynamique** par **Statique**, sélectionnez l'adresse, cliquez sur **Modifier** et utilisez la page Modifier les voisins IPv6.

Les listes de préfixes sont configurées avec les mots clés **autoriser** ou **refuser** afin d'autoriser ou de refuser un préfixe sur la base d'une condition correspondante. Un refus implicite s'applique au trafic qui ne correspond à aucune entrée de liste de préfixes.

Une entrée de liste de préfixes se compose d'une adresse IP et d'un masque de bits. L'adresse IP peut être destinée à la route d'un réseau classful, d'un sous-réseau ou d'un seul hôte. Le masque de bits est un nombre compris entre 1 et 32.

Les listes de préfixes sont configurées pour filtrer le trafic à partir d'une correspondance de longueur de préfixe exacte ou d'une correspondance au sein d'une plage lorsque les mots clés ge et le sont utilisés.

Les paramètres **Supérieur à** et **Inférieur à** permettent de spécifier une plage de longueurs de préfixe et d'offrir une configuration plus souple que si vous utilisiez seulement l'argument réseau/longueur. Une liste de préfixes est traitée par le biais d'une correspondance exacte lorsque ni le paramètre **Supérieur à** ni le paramètre **Inférieur à** n'est spécifié. Si seul le paramètre **Supérieur à** est spécifié, la plage va de la valeur saisie pour **Supérieur à** à une longueur 32 bits complète. Si seul le paramètre **Inférieur à** est spécifié, la plage va de la valeur saisie pour l'argument réseau/longueur à la valeur **Inférieur à**. Si les arguments **Inférieur à** et **Supérieur à** sont tous les deux entrés, la plage est comprise entre les valeurs utilisées pour **Inférieur à** et **Supérieur à**.

Affichage des tables de routage IPv6

L'IPv6 Forwarding Table (Table de redirection IPv6) contient les différents acheminements qui ont été configurés. L'un de ces acheminements est un acheminement par défaut (adresse IPv6:0), qui utilise le routeur par défaut sélectionné dans la liste des routeurs par défaut IPv6 afin d'envoyer des paquets aux périphériques de destination qui ne font pas partie du même sous-réseau IPv6 que le périphérique. Outre

l'acheminement par défaut, la table contient aussi des acheminements dynamiques, qui sont des acheminements de redirection ICMP reçues des routeurs IPv6 via des messages de redirection ICMP. Cela peut se produire lorsque le routeur par défaut que le périphérique utilise n'est pas celui défini pour le trafic des sous-réseaux IPv6 avec lesquels le périphérique veut communiquer.

Pour visualiser les acheminements IPv6 :

ÉTAPE 1 Cliquez sur **Administration > Interface de gestion > Routes IPv6**.

Cette rubrique affiche les champs suivants :

- **Adresse IPv6** : adresse du sous-réseau IPv6.
- **Longueur du préfixe** : longueur du préfixe d'acheminement IP pour l'adresse de sous-réseau IPv6 de destination. Il est précédé d'une barre oblique.
- **Interface** : interface utilisée pour transférer le paquet.
- **Saut suivant** : adresse vers laquelle le paquet est transféré. En général, il s'agit de l'adresse d'un routeur du voisinage. Les types suivants sont disponibles :
  - *Liaison locale* : une interface IPv6 et une adresse IPv6 qui identifient uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : une adresse IPv6 qui est de type global IPV6 monodiffusion, visible et joignable à partir d'autres réseaux.
  - *Point-to-Point (Point à point)* : un tunnel point à point.
- **Métrique** : valeur utilisée pour comparer cet acheminement à d'autres acheminements vers la même destination dans la table des routeurs IPv6. Tous les acheminements par défaut ont la même valeur.
- **Durée de vie** : laps de temps durant lequel le paquet peut être envoyé et renvoyé, avant sa suppression.
- **Type d'acheminement** : mode de rattachement de la destination et méthode utilisée pour obtenir l'entrée. Les valeurs sont les suivantes :
  - *Local* : un réseau connecté directement dont le préfixe est dérivé de l'adresse IPv6 d'un périphérique configuré manuellement.
  - *Dynamique* : la destination est une adresse de sous-réseau IPv6 attachée de façon indirecte (à distance). L'entrée a été obtenue de manière dynamique via le protocole ND ou ICMP.
  - *Statique* : l'entrée a été configurée manuellement par un utilisateur.

Nom de domaine

Le DNS (Domain Name System, système de noms de domaine) convertit les noms de domaine en adresses IP en vue de localiser et de gérer des hôtes.

En tant que client DNS, le périphérique convertit les noms de domaine en adresses IP via un ou plusieurs serveurs DNS configurés.

Paramètres DNS

Utilisez la page Paramètres DNS pour activer la fonction DNS, configurer les serveurs DNS et définir le domaine par défaut utilisé par le périphérique.

ÉTAPE 1 Cliquez sur **IP Configuration** > **Domain Name System** > **DNS Settings**.

ÉTAPE 2 Saisissez les paramètres.

- **DNS** : sélectionnez cette option pour désigner le périphérique comme client DNS et lui permettre de convertir les noms DNS en adresses IP via un ou plusieurs serveurs DNS configurés.
- **Polling Retries (Tentatives d'interrogation)** : saisissez le nombre de fois où le périphérique peut envoyer une requête DNS à un serveur DNS avant de conclure que ce serveur DNS n'existe pas.
- **Polling Timeout (Délai de l'interrogation)** : saisissez la durée en secondes pendant laquelle le périphérique attend une réponse à une requête DNS.
- **Intervalle d'interrogation** : saisissez la fréquence (en secondes) à laquelle le périphérique envoie des paquets de requête DNS lorsque le nombre maximal de tentatives a été atteint.
  - *Valeurs par défaut* : cette option permet d'utiliser la valeur par défaut.

    Cette valeur = 2*(Polling Retries (Tentatives d'interrogation) + 1)* Polling Timeout (Délai de l'interrogation)
  - *Défini par l'utilisateur* : cette option permet de saisir une valeur définie par l'utilisateur.
- **Paramètres par défaut** : saisissez les paramètres par défaut suivants :
  - **Nom de domaine par défaut** : saisissez le nom de domaine DNS utilisé pour compléter des noms d'hôte incomplets. Le périphérique ajoute ces informations à tous les noms de domaine incomplets (NFQDN), afin de les convertir en noms de domaine complets (FQDN).

    REMARQUE N'incluez pas le point initial qui sépare un nom incomplet du nom de domaine (comme cisco.com).

- **DHCP Domain Search List (Liste de recherche de domaine DHCP)** : cliquez sur **Détails** pour afficher la liste des serveurs DNS configurés sur le périphérique.

ÉTAPE 3 Cliquez sur **Apply**. Le fichier de configuration de fonctionnement est mis à jour.

Table des serveurs DNS : Les champs suivants sont affichés pour chaque serveur DNS configuré :

- **Serveur DNS** : adresse IP du serveur DNS.
- **Préférence** : chaque serveur dispose d'une valeur de préférence ; une valeur plus petite signifie une plus grande probabilité d'être utilisée.
- **Source** : source de l'adresse IP du serveur (statique ou DHCPv4 ou DHCPv6)
- **Interface** : interface de l'adresse IP du serveur.

ÉTAPE 4 Vous pouvez définir jusqu'à huit serveurs DNS. Pour ajouter un serveur DNS, cliquez sur **Ajouter**.

Saisissez les paramètres.

- **Version IP** : sélectionnez Version 6 pour IPv6 ou Version 4 pour IPv4.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, sélectionnez l'interface de réception.
- **Adresse IP du serveur DNS** : saisissez l'adresse IP du serveur DNS.
- **Préférence** : sélectionnez une valeur déterminant l'ordre dans lequel les domaines sont utilisés (du bas vers le haut). Cette option détermine efficacement l'ordre dans lequel les noms incomplets sont complétés au cours des requêtes DNS.

ÉTAPE 5 Cliquez sur **Apply**. Le serveur DNS est enregistré dans le fichier de Configuration d'exécution.

Liste de recherche

La liste de recherche peut contenir une entrée statique définie par l'utilisateur sur la page Paramètres DNS et des entrées dynamiques reçues des serveurs DHCPv4 et DHCPv6.

Pour afficher les noms de domaine qui ont été configurés sur le périphérique :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Système de noms de domaine** > **Liste de recherche**.

Les champs suivants sont affichés pour chaque serveur DNS configuré sur le périphérique :

- **Nom de domaine** : nom de domaine qui peut être utilisé sur le périphérique.
- **Source** : source de l'adresse IP du serveur (statique ou DHCPv4 ou DHCPv6) pour ce domaine.
- **Interface** : interface de l'adresse IP du serveur pour ce domaine.
- **Préférence** : ordre dans lequel les domaines sont utilisés (du bas vers le haut). Cette option détermine efficacement l'ordre dans lequel les noms incomplets sont complétés au cours des requêtes DNS.

Mappage d'hôtes

Les mappages Nom d'hôte/Adresse IP sont enregistrés dans la zone Table de mappage d'hôtes (cache DNS).

Ce cache peut contenir les types d'entrée suivants :

- **Entrées statiques** : paires de mappage qui ont été manuellement ajoutées au cache. Un maximum de 64 entrées statiques est possible.
- **Entrées dynamiques** : paires de mappage qui ont été ajoutées par le système suite à une utilisation par l'utilisateur ou et une entrée pour chaque adresse IP configurée sur le périphérique par DHCP. Un maximum de 256 entrées dynamiques est possible.

La résolution des noms commence toujours par la vérification des entrées statiques, se poursuit par la vérification des entrées dynamiques et se termine par l'envoi de demandes au serveur DNS externe.

Vous pouvez associer huit adresses IP à chaque serveur DNS pour chaque nom d'hôte.

Pour ajouter un nom d'hôte et son adresse IP :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Système de noms de domaine** > **Mappage d'hôtes**.

ÉTAPE 2 Si nécessaire, sélectionnez l'option **Effacer la table** afin d'effacer certaines entrées ou toutes les entrées de la Table de mappage d'hôtes.

- **Statique uniquement** : supprime les hôtes statiques.

- **Dynamique uniquement** : supprime les hôtes dynamiques.
- **Dynamique et statique** : supprime les hôtes statiques et dynamiques.

La Table de mappage d'hôtes contient les champs suivants :

- **Nom d'hôte** : nom d'hôte défini par l'utilisateur ou nom complet.
- **IP Address** : adresse IP d'hôte.
- **IP Version** : version IP de l'adresse IP de l'hôte.
- **Type** : une entrée **dynamique** ou **statique** dans le cache.
- **État** : affiche les résultats des tentatives d'accéder à l'hôte.
  - *OK* : tentative réussie.
  - *Negative Cache (Cache négatif)* : tentative échouée, ne réessayez pas.
  - *Pas de réponse* : pas de réponse mais le système peut effectuer ultérieurement une nouvelle tentative.
- **TTL (s)** : s'il s'agit d'une entrée dynamique, cette option indique sa durée de conservation dans le cache.
- **TTL restant (s)** : s'il s'agit d'une entrée dynamique, cette option indique combien de temps encore elle va rester dans le cache.

ÉTAPE 3 Pour ajouter un mappage d'hôtes, cliquez sur **Add**.

ÉTAPE 4 Saisissez les paramètres.

- **Version IP** : sélectionnez **Version 6** pour IPv6 ou **Version 4** pour IPv4.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, sélectionnez l'interface de réception.

- **Host Name** : saisissez un nom d'hôte défini par l'utilisateur ou un nom complet. Les noms d'hôte sont limités aux lettres ASCII de A à Z (avec distinction majuscules/minuscules), les chiffres de 0 à 9, le caractère souligné et le tiret. Le point (.) est utilisé pour séparer les étiquettes.
- **Adresse IP** : saisissez une seule adresse ou jusqu'à huit adresses IP associées (IPv4 ou IPv6).

ÉTAPE 5 Cliquez sur **Apply**. Les paramètres sont enregistrés dans le fichier Configuration d'exécution.

19

Sécurité

Cette section décrit le contrôle d'accès et la sécurité du périphérique. Le système gère différents types de sécurité.

La liste de rubriques suivante décrit les différents types de fonctions de sécurité présentées dans cette section. Certaines fonctionnalités sont utilisées pour plusieurs types de sécurité ou de contrôle et s'affichent donc à plusieurs reprises dans la liste des rubriques présentée ci-dessous.

L'autorisation d'administrer le périphérique est décrite dans les sections suivantes :

- **Définition d'utilisateurs**
- **Configuration de RADIUS**
- **Méthode d'accès de gestion**
- **Authentification de l'accès de gestion**
- **Gestion sécurisée des données confidentielles**
- **Serveur SSL**

La protection contre les attaques visant le CPU du périphérique est décrite dans les sections suivantes :

- **Configuration des services TCP/UDP**
- **Définition du contrôle des tempêtes**

Le contrôle d'accès au réseau des utilisateurs finaux par l'intermédiaire du périphérique est décrit dans les sections suivantes :

- **Méthode d'accès de gestion**
- **Méthode d'accès de gestion**
- **Configuration de RADIUS**
- **Configuration de la sécurité des ports**
- **802.1X**

La protection contre les autres utilisateurs du réseau est décrite dans les sections suivantes. Il s'agit d'attaques qui transitent par le périphérique, mais qui ne sont pas dirigées vers ce dernier.

- **Prévention du déni de service**
- **Serveur SSL**
- **Définition du contrôle des tempêtes**
- **Configuration de la sécurité des ports**

Définition d'utilisateurs

Le nom d'utilisateur/mot de passe par défaut est **cisco/cisco**. Lors de votre première ouverture de session avec le nom d'utilisateur et le mot de passe par défaut, vous devez saisir un nouveau mot de passe. La complexité des mots de passe est activée par défaut. Si le mot de passe que vous choisissez n'est pas suffisamment complexe (les **Paramètres de complexité du mot de passe** peuvent être activés sur la page Sécurité du mot de passe), le système vous invite à créer un autre mot de passe.

Définition de comptes d'utilisateurs

La page Comptes d'utilisateur vous permet de saisir des utilisateurs supplémentaires autorisés à accéder au périphérique (en lecture seule ou en lecture/écriture) ou de modifier les mots de passe d'utilisateurs existants.

Après l'ajout d'un utilisateur (comme décrit ci-dessous), l'utilisateur par défaut est supprimé du système.

REMARQUE Il est impossible de supprimer tous les utilisateurs. Si tous les utilisateurs sont sélectionnés, le bouton **Supprimer** est désactivé.

Pour ajouter un nouvel utilisateur :

ÉTAPE 1 Cliquez sur **Administration** > **User Accounts**.

Cette page affiche les utilisateurs définis dans le système ainsi que leur niveau de privilèges.

ÉTAPE 2 Sélectionnez **Service de récupération du mot de passe** pour activer cette fonction. Lorsque cette fonction est activée, un utilisateur final disposant d'un accès physique au port de console du périphérique peut accéder au menu de démarrage et déclencher le processus de récupération du mot de passe. Lorsque le processus de démarrage du système est terminé, vous êtes autorisé à vous connecter au périphérique sans authentification de mot de passe. L'accès au périphérique est autorisé uniquement par le biais de la console et exclusivement lorsque la console est connectée au périphérique avec accès physique.

Lorsque le mécanisme de récupération du mot de passe est désactivé, l'accès au menu de démarrage est toujours autorisé et vous pouvez déclencher le processus de récupération du mot de passe. La différence est que dans ce cas, tous les fichiers de configuration et les fichiers des utilisateurs sont supprimés durant le processus de démarrage du système et un message de journal approprié est généré sur le terminal.

ÉTAPE 3 Cliquez sur **Add** pour ajouter un nouvel utilisateur ou sur **Edit** pour en modifier un.

ÉTAPE 4 Saisissez les paramètres.

- **Nom d'utilisateur** : saisissez un nouveau nom d'utilisateur comportant 20 caractères maximum. Les caractères UTF-8 sont interdits.
- **Mot de passe** : saisissez un mot de passe (les caractères UTF-8 sont interdits). Si la fiabilité et la complexité du mot de passe sont définies, le mot de passe utilisateur doit être conforme à la stratégie configurée dans **Définition de règles de complexité des mots de passe**.
- **Confirm Password** : saisissez à nouveau le mot de passe.
- **Password Strength Meter** : affiche le niveau de sécurité du mot de passe. Vous pouvez définir la stratégie de sécurité et de complexité du mot de passe sur la page Sécurité du mot de passe.

ÉTAPE 5 Cliquez sur **Appliquer**. L'utilisateur est ajouté au fichier de Configuration d'exécution du périphérique.

Définition de règles de complexité des mots de passe

Les mots de passe permettent d'authentifier les utilisateurs qui accèdent au périphérique. Les mots de passe simples constituent des risques de sécurité potentiels. Par conséquent, les exigences de complexité du mot de passe sont appliquées par défaut et peuvent être configurées si nécessaire. Vous pouvez configurer les exigences de complexité du mot de passe sur la page **Sécurité du mot de passe** accessible via le menu déroulant Sécurité. En outre, le délai d'expiration du mot de passe peut être configuré sur cette page.

Pour définir les règles de complexité des mots de passe :

ÉTAPE 1 Cliquez sur **Security** > **Password Strength**.

ÉTAPE 2 Saisissez les paramètres d'expiration suivants pour les mots de passe :

- **Expiration du mot de passe** : si cette option est sélectionnée, l'utilisateur sera invité à modifier le mot de passe une fois le **Délai d'expiration du mot de passe** atteint.
- **Délai d'expiration du mot de passe** : saisissez la durée en jours à l'issue de laquelle le système invite l'utilisateur à changer de mot de passe.

REMARQUE L'expiration du mot de passe s'applique aussi aux mots de passe de longueur nulle (pas de mot de passe).

ÉTAPE 3 Sélectionnez **Paramètres de complexité du mot de passe** afin d'activer les règles de complexité pour les mots de passe.

Si la complexité du mot de passe est activée, les nouveaux mots de passe doivent être conformes aux paramètres par défaut suivants :

- Avoir une longueur minimale de huit caractères.
- Contenir des caractères appartenant à au moins trois classes de caractères (caractères majuscules, minuscules, numériques et spéciaux disponibles sur un clavier standard).
- Être différents du mot de passe actuel.
- Ne pas contenir de caractère répété plus de trois fois consécutivement.
- Ne pas répéter ou inverser le nom d'utilisateur ou toute variante obtenue en changeant la casse des caractères.
- Ne pas répéter ou inverser le nom du fabricant ou toute variante obtenue en changeant la casse des caractères.

ÉTAPE 4 Si les **Paramètres de complexité du mot de passe** sont activés, les paramètres suivants peuvent être configurés :

- **Minimal Password Length** : saisissez le nombre minimum de caractères requis pour les mots de passe.

  REMARQUE Un mot de passe de longueur nulle (pas de mot de passe) est autorisé, et un délai d'expiration du mot de passe peut lui être attribué.

- **Allowed Character Repetition** : saisissez le nombre de fois qu'un caractère peut être répété.
- **Minimal Number of Character Classes** : saisissez le nombre de classes de caractères qui doivent être présentes dans un mot de passe. Les classes de caractères sont minuscules (1), majuscules (2), chiffres (3) et symboles ou caractères spéciaux (4).
- **The New Password Must Be Different than the Current One** : si cette option est sélectionnée, lors de la modification du mot de passe, le nouveau mot de passe ne peut pas être identique au mot de passe actuel.

ÉTAPE 5 Cliquez sur **Apply**. Les paramètres de mot de passe sont écrits dans le fichier de Configuration d'exécution.

Configuration de RADIUS

Les serveurs RADIUS (Remote Authorization Dial-In User Service) offrent un contrôle d'accès réseau basé sur MAC ou 802.1X centralisé. Le périphérique est un client RADIUS pouvant utiliser un serveur RADIUS pour fournir une sécurité centralisée.

Une société peut établir un serveur RADIUS (Remote Authorization Dial-In User Service, service d'authentification à distance des utilisateurs) pour fournir un contrôle d'accès réseau basé MAC ou 802.1X centralisé à tous ses périphériques. Ainsi, les stratégies d'authentification et d'autorisation peuvent être traitées sur un seul serveur pour tous les périphériques de l'entreprise.

Le périphérique peut servir de client RADIUS utilisant le serveur RADIUS pour les services suivants :

- **Authentification** : assure l'authentification des utilisateurs normaux et 802.1X se connectant au périphérique en utilisant des noms d'utilisateur et des mots de passe définis par l'utilisateur.
- **Autorisation** : effectuée au moment de la connexion. Une fois la session d'authentification terminée, une session d'autorisation commence en utilisant le nom d'utilisateur authentifié. Le serveur RADIUS vérifie ensuite les privilèges de l'utilisateur.
- **Comptabilité** : activez la gestion de comptes des sessions de connexion à l'aide du serveur RADIUS. Cela permet à l'administrateur système de générer des rapports de gestion de comptes depuis le serveur RADIUS.

Gestion de comptes utilisant un serveur RADIUS

L'utilisateur peut activer la gestion de comptes des sessions de connexion à l'aide d'un serveur RADIUS.

Le port TCP configurable par l'utilisateur utilisé pour la gestion de comptes du serveur RADIUS est le même port TCP utilisé pour l'authentification et l'autorisation du serveur RADIUS.

Valeurs par défaut

Les valeurs par défaut suivantes concernent cette fonction :

- Aucun serveur RADIUS n'est défini par défaut.
- Si vous configurez un serveur RADIUS, la fonction de gestion de comptes est désactivée par défaut.

Interactions avec les autres fonctions

Aucune.

Flux de travail du serveur RADIUS

Pour utiliser un serveur RADIUS, procédez comme suit :

ÉTAPE 1 Ouvrez un compte pour le périphérique sur le serveur RADIUS.

ÉTAPE 2 Configurez ce serveur et les autres paramètres sur les pages RADIUS et Ajouter un serveur RADIUS.

REMARQUE Si plusieurs serveurs RADIUS ont été configurés, le périphérique utilise les priorités configurées des serveurs RADIUS disponibles pour sélectionner le serveur RADIUS à utiliser par le périphérique.

Pour définir les paramètres du serveur RADIUS :

ÉTAPE 1 Cliquez sur **Security** > **RADIUS**.

ÉTAPE 2 Saisissez les paramètres RADIUS par défaut, si nécessaire. Les valeurs entrées dans les Paramètres par défaut sont appliquées à tous les serveurs. Si une valeur n'est pas entrée pour un serveur spécifique (sur la page Ajouter un serveur RADIUS), le périphérique utilise les valeurs contenues dans ces champs.

- **Retries** : saisissez le nombre de demandes transmises qui sont envoyées au serveur RADIUS avant que le système considère qu'une défaillance s'est produite.
- **Délai de réponse** : saisissez le nombre de secondes pendant lesquelles le périphérique attend une réponse du serveur RADIUS avant de relancer la demande ou de passer au serveur suivant.
- **Délai d'inactivité** : saisissez le nombre de minutes qui s'écoulent avant qu'un serveur RADIUS non réactif soit contourné pour les demandes de services. Si la valeur est égale à 0, le serveur n'est pas contourné.
- **Chaîne de clé** : saisissez la chaîne de clé par défaut utilisée pour l'authentification et le cryptage entre le périphérique et le serveur RADIUS. Cette clé doit correspondre à la clé configurée sur le serveur RADIUS. Une chaîne de clé est utilisée pour crypter les communications à l'aide de MD5. Vous pouvez saisir la clé en mode **Chiffré** ou **Texte en clair**. Si vous ne disposez pas de chaîne de clé cryptée (à partir d'un autre périphérique), saisissez la chaîne de clé en texte en clair et cliquez sur **Apply**. La chaîne de clé cryptée est générée et affichée.

Cette clé remplace la chaîne de clé par défaut, si une telle clé a été définie.

- **Interface IPv4 source** : sélectionnez l'interface source IPv4 du périphérique à utiliser dans les messages pour les communications avec le serveur RADIUS.
- **Interface IPv6 source** : sélectionnez l'interface source IPv6 du périphérique à utiliser dans les messages pour les communications avec le serveur RADIUS.

REMARQUE Si l'option Auto est sélectionnée, le système récupère l'adresse IP source de l'adresse IP définie dans l'interface sortante.

ÉTAPE 3 Cliquez sur **Apply**. Les paramètres RADIUS par défaut du périphérique sont mis à jour dans le fichier de Configuration d'exécution.

Pour ajouter un serveur RADIUS, cliquez sur **Ajouter**.

ÉTAPE 4 Entrez les valeurs dans les champs pour chaque serveur RADIUS. Pour utiliser les valeurs par défaut entrées sur la page RADIUS, sélectionnez **Valeurs par défaut**.

- **Définition de serveur** : indiquez si vous souhaitez spécifier le serveur RADIUS par son adresse IP ou son nom.
- **Version IP** : sélectionnez la version de l'adresse IP du serveur RADIUS.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée).
- **Nom/Adresse IP du serveur** : spécifiez le serveur RADIUS par son adresse IP ou son nom.
- **Priority** : saisissez la priorité du serveur. La priorité détermine l'ordre dans lequel le périphérique essaie de contacter les serveurs pour authentifier un utilisateur. Le périphérique commence par le serveur RADIUS ayant la priorité la plus élevée (priorité zéro).

  Chaîne de clé : saisissez la chaîne de clé utilisée pour l'authentification et le cryptage des communications entre le périphérique et le serveur RADIUS. Cette clé doit correspondre à la clé configurée sur le serveur RADIUS. Vous pouvez la saisir en mode **Chiffré** ou **Texte en clair**. Si l'option **Valeurs par défaut** est sélectionnée, le périphérique essaie de s'authentifier sur le serveur RADIUS en utilisant la chaîne de clé par défaut.
- **Délai de réponse** : sélectionnez **Défini par l'utilisateur** et saisissez le nombre de secondes pendant lesquelles le périphérique attend une réponse du serveur RADIUS avant de relancer la demande ou de passer au serveur suivant si le nombre maximal de tentatives a été atteint. Si l'option **Valeurs par défaut** est sélectionnée, le périphérique utilise la valeur de délai par défaut.

- **Port d'authentification** : saisissez le numéro de port UDP du port du serveur RADIUS pour les demandes d'authentification.
- **Port de gestion de comptes** : saisissez le numéro de port UDP du port du serveur RADIUS pour les demandes de gestion de comptes.
- **Tentatives** : sélectionnez **Défini par l'utilisateur** et entrez le nombre de demandes envoyées au serveur RADIUS avant qu'un échec soit réputé être survenu. Si l'option **Valeurs par défaut** est sélectionnée, le périphérique utilise la valeur par défaut du nombre de tentatives.
- **Délai d'inactivité** : sélectionnez **Défini par l'utilisateur** et saisissez le nombre de minutes qui doivent s'écouler avant qu'un serveur RADIUS non réactif soit contourné pour les demandes de services. Si l'option **Valeurs par défaut** est sélectionnée, le périphérique utilise la valeur par défaut du délai d'inactivité. Si vous saisissez 0 minute, aucun délai d'inactivité ne sera appliqué.
- **Type d'utilisation** : saisissez le type d'authentification du serveur RADIUS. Les options sont les suivantes :
  - *Connexion* : le serveur RADIUS est utilisé pour l'authentification des utilisateurs qui demandent à administrer le périphérique.
  - *802.1X* : le serveur RADIUS est utilisé pour l'authentification 802.1x.
  - *Tous* : le serveur RADIUS est utilisé pour l'authentification des utilisateurs qui demandent à administrer le périphérique et pour l'authentification 802.1X.

ÉTAPE 5 Cliquez sur **Apply**. La définition du serveur RADIUS est ajoutée au fichier de Configuration d'exécution du périphérique.

ÉTAPE 6 Pour afficher les données sensibles sous forme de texte en clair sur la page, cliquez sur **Afficher les données sensibles sous forme de texte clair**.

Méthode d'accès de gestion

Les profils d'accès déterminent la façon d'authentifier les utilisateurs et de les autoriser à accéder au périphérique via différentes méthodes d'accès. Les profils d'accès peuvent limiter l'accès de gestion à partir de sources spécifiques.

Seuls les utilisateurs qui passent le profil d'accès actif et les méthodes d'authentification de l'accès de gestion peuvent accéder au périphérique.

Un seul profil d'accès à la fois peut être actif sur le périphérique.

Les profils d'accès contiennent une ou plusieurs règles. Les règles sont exécutées dans l'ordre c'est-à-dire en fonction de leur priorité dans le profil d'accès (de haut en bas).

Les règles sont composées de filtres qui incluent les éléments suivants :

- **Méthodes d'accès** : méthodes permettant l'accès au périphérique et sa gestion :
  - Hypertext Transfer Protocol (HTTP)
  - Secure HTTP (HTTPS)
  - Simple Network Management Protocol (SNMP)
  - Tous les éléments ci-dessus
- **Action** : permet d'autoriser ou de refuser l'accès à une interface ou à une adresse source.
- **Interface** : ports, LAG ou VLAN, autorisés à accéder à l'utilitaire de configuration Web ou interdits d'accès à celui-ci.
- **Adresse IP source** : adresses ou sous-réseaux IP auxquels l'accès est autorisé.

Profil d'accès actif

La page Access Profiles affiche les profils d'accès définis et permet de sélectionner un profil d'accès en tant que profil actif.

Lorsqu'un utilisateur tente d'accéder au périphérique par le biais d'une méthode d'accès, le périphérique vérifie si le profil d'accès actif autorise explicitement l'accès de gestion au périphérique via cette méthode. Si aucune correspondance n'est trouvée, l'accès est refusé.

Lorsqu'une tentative d'accès au périphérique s'effectue en violation du profil d'accès actif, le périphérique génère un message SYSLOG pour en avertir l'administrateur système.

Pour plus d'informations, reportez-vous à la section **Définition de règles de profils**.

Utilisez la page Access Profiles pour créer un profil d'accès et ajouter sa première règle. Si le profil d'accès ne contient qu'une seule règle, vous avez terminé. Pour ajouter des règles supplémentaires au profil, utilisez la page Profile Rules.

ÉTAPE 1 Cliquez sur **Sécurité** > **Méthode d'accès de gestion** > **Profils d'accès**.

Cette page affiche tous les profils d'accès, qu'ils soient actifs ou non.

ÉTAPE 2 Pour modifier le profil d'accès actif, sélectionnez un profil dans le menu déroulant **Profil d'accès actif** et cliquez sur **Appliquer**. Le profil choisi devient alors le profil d'accès actif.

Si vous sélectionnez un autre profil d'accès, un message s'affiche pour vous avertir que, selon le profil d'accès sélectionné, vous pourriez être déconnecté de l'utilitaire de configuration Web.

ÉTAPE 3 Cliquez sur **OK** pour sélectionner le profil d'accès actif ou sur **Annuler** pour abandonner cette action.

ÉTAPE 4 Cliquez sur **Ajouter** pour ouvrir la page Ajouter un profil d'accès. Cette page vous permet de configurer un nouveau profil ainsi qu'une règle.

ÉTAPE 5 Saisissez le **Nom du profil d'accès**. Ce nom peut comporter jusqu'à 32 caractères.

ÉTAPE 6 Saisissez les paramètres.

- **Rule Priority** : saisissez la priorité des règles. Lorsque le paquet est mis en correspondance avec une règle, les groupes d'utilisateurs se voient accorder ou refuser l'accès au périphérique. La priorité des règles est indispensable pour faire correspondre les paquets aux règles, la correspondance des paquets étant établie sur une base de première correspondance. Le 1 correspond à la priorité la plus élevée.
- **Management Method** : sélectionnez la méthode de gestion pour laquelle la règle est définie. Les options sont les suivantes :
  - *All* : affecte toutes les méthodes de gestion à la règle.
  - *HTTP* : les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès HTTP se voient autoriser ou refuser l'accès.
  - *HTTP sécurisé (HTTPS)* : les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès HTTPS se voient autoriser ou refuser l'accès.
  - *SNMP* : les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès SNMP se voient autoriser ou refuser l'accès.
- **Action** : sélectionnez l'action rattachée à la règle. Les options sont les suivantes :
  - *Autoriser* : autorise l'accès au périphérique dans la mesure où l'utilisateur correspond aux paramètres du profil.
  - *Refuser* : refuse l'accès au périphérique dans la mesure où l'utilisateur correspond aux paramètres du profil.
- **Applies to Interface** : sélectionnez l'interface rattachée à la règle. Les options sont les suivantes :
  - *All* : s'applique à tous les ports, VLAN et LAG.
  - *Défini par l'utilisateur* : s'applique à l'interface sélectionnée.
- **Interface** : entrez le numéro d'interface si l'option Défini par l'utilisateur a été sélectionnée.

- **Applies to Source IP Address** : sélectionnez le type d'adresse IP source auquel le profil d'accès s'applique. Le champ *Adresse IP source* est valide pour un sous-réseau. Sélectionnez l'une des valeurs suivantes :
  - *Tout* : s'applique à tous les types d'adresses IP.
  - *User Defined* : s'applique uniquement aux types d'adresses IP définis dans les champs.
- **Version IP** : entrez la version de l'adresse IP source : Version 6 ou Version 4.
- **IP Address** : saisissez l'adresse IP source.
- **Mask** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs suivants :
  - *Network Mask* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Prefix Length* : sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l'adresse IP source.

ÉTAPE 7 Cliquez sur **Apply**. Le profil d'accès est écrit dans le fichier de Configuration d'exécution. Vous pouvez à présent sélectionner ce profil d'accès en tant que profil d'accès actif.

Définition de règles de profils

Les profils d'accès peuvent comporter jusqu'à 128 règles afin de déterminer qui est autorisé à gérer le périphérique ainsi qu'à y accéder et les méthodes d'accès pouvant être utilisées.

Chaque règle d'un profil d'accès comporte une action et des critères (un ou plusieurs paramètres) à faire correspondre. Une priorité est affectée à chaque règle. Les règles ayant la priorité la plus basse sont vérifiées en premier. Si le paquet entrant correspond à une règle, l'action associée à cette dernière est appliquée. Si aucune règle correspondante n'est trouvée dans le profil d'accès actif, le paquet est abandonné.

Par exemple, vous pouvez limiter l'accès au périphérique depuis toutes les adresses IP à l'exception de celles qui sont attribuées au centre de gestion informatique. Le périphérique peut ainsi continuer à être géré tout en bénéficiant d'un autre niveau de sécurité.

Pour ajouter des règles de profil à un profil d'accès :

ÉTAPE 1 Cliquez sur **Sécurité** > **Méthode d'accès de gestion** > **Règles de profils**.

ÉTAPE 2 Sélectionnez le champ Filtre et un profil d'accès. Cliquez sur **Go**.

Le profil d'accès sélectionné apparaît dans la Table des règles de profil.

ÉTAPE 3 Cliquez sur **Ajouter** pour ajouter une règle.

ÉTAPE 4 Saisissez les paramètres.

- **Nom du profil d'accès** : sélectionnez un profil d'accès.
- **Rule Priority** : saisissez la priorité des règles. Lorsque le paquet est mis en correspondance avec une règle, les groupes d'utilisateurs se voient accorder ou refuser l'accès au périphérique. La priorité des règles est indispensable pour faire correspondre les paquets aux règles, la correspondance des paquets étant établie sur une base de première correspondance.
- **Management Method** : sélectionnez la méthode de gestion pour laquelle la règle est définie. Les options sont les suivantes :
  - *All* : affecte toutes les méthodes de gestion à la règle.
  - *HTTP* : affecte un accès HTTP à la règle. Les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès HTTP se voient autoriser ou refuser l'accès.
  - *HTTP sécurisé (HTTPS)* : les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès HTTPS se voient autoriser ou refuser l'accès.
  - *SNMP* : les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès SNMP se voient autoriser ou refuser l'accès.
- **Action** : sélectionnez **Autoriser** pour autoriser les utilisateurs qui essaient d'accéder au périphérique en utilisant la méthode d'accès configurée depuis l'interface et la source IP définies dans cette règle. Ou sélectionnez **Refuser** pour refuser l'accès.
- **Applies to Interface** : sélectionnez l'interface rattachée à la règle. Les options sont les suivantes :
  - *All* : s'applique à tous les ports, VLAN et LAG.
  - *Défini par l'utilisateur* : s'applique uniquement au port, VLAN ou LAG sélectionné.
- **Interface** : entrez le numéro d'interface.
- **Applies to Source IP Address** : sélectionnez le type d'adresse IP source auquel le profil d'accès s'applique. Le champ *Adresse IP source* est valide pour un sous-réseau. Sélectionnez l'une des valeurs suivantes :
  - *Tout* : s'applique à tous les types d'adresses IP.
  - *User Defined* : s'applique uniquement aux types d'adresses IP définis dans les champs.
- **Version IP** : sélectionnez la version IP prise en charge pour l'adresse source : IPv6 ou IPv4.
- **IP Address** : saisissez l'adresse IP source.

- **Masque** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs :
  - *Masque de réseau* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Longueur du préfixe* : sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l'adresse IP source.

ÉTAPE 5 Cliquez sur **Appliquer**. La règle est ajoutée au profil d'accès.

Authentification de l'accès de gestion

Vous pouvez attribuer des méthodes d'authentification aux différentes méthodes d'accès de gestion, telles que SSH, console, HTTP et HTTPS. L'authentification peut être effectuée localement ou sur un serveur RADIUS.

Si l'autorisation est activée, l'identité et les privilèges de lecture/écriture de l'utilisateur font l'objet d'une vérification. Si l'autorisation n'est pas activée, seule l'identité de l'utilisateur est vérifiée.

La méthode d'autorisation/authentification utilisée est déterminée par l'ordre de sélection des méthodes d'authentification. Si la première méthode d'authentification n'est pas disponible, la méthode suivante sera utilisée. Par exemple, si les méthodes d'authentification sélectionnées sont RADIUS et Local, et que tous les serveurs RADIUS configurés sont interrogés en vertu de leur ordre de priorité et qu'ils ne répondent pas, l'utilisateur est autorisé/authentifié au niveau local.

Si l'autorisation est activée et si une méthode d'authentification échoue ou si le niveau de privilège de l'utilisateur est insuffisant, ce dernier se voit refuser l'accès au périphérique. En d'autres termes, si l'authentification échoue pour une méthode d'authentification, le périphérique n'essaie pas d'utiliser la méthode d'authentification suivante et s'arrête.

De la même façon, si l'autorisation n'est pas activée et que l'authentification échoue pour une méthode, le périphérique arrête la tentative d'authentification.

Pour définir les méthodes d'authentification d'une méthode d'accès :

ÉTAPE 1 Cliquez sur **Security** > **Management Access Authentication**.

ÉTAPE 2 Renseignez le champ **Application** (type) de la méthode d'accès de gestion.

ÉTAPE 3 Sélectionnez **Autorisation** pour activer l'authentification et l'autorisation de l'utilisateur selon la liste des méthodes décrites ci-dessous. Si vous ne sélectionnez pas le champ, seule l'authentification est exécutée. Si l'autorisation est activée, les privilèges de lecture/écriture des utilisateurs font l'objet d'une vérification. Le niveau de privilège est défini sur la page Comptes d'utilisateur.

ÉTAPE 4 Utilisez les flèches pour déplacer la méthode d'autorisation/authentification entre la colonne **Méthodes facultatives** et la colonne **Méthodes sélectionnées**. Les méthodes sont essayées dans l'ordre de leur apparition.

ÉTAPE 5 Utilisez les flèches pour déplacer la méthode d'authentification entre la colonne **Méthodes facultatives** et la colonne **Méthodes sélectionnées**. La première méthode sélectionnée correspond à celle qui sera utilisée en premier.

- *RADIUS* : l'utilisateur est autorisé/authentifié sur un serveur RADIUS. Vous devez avoir configuré un ou plusieurs serveurs RADIUS. Pour que le serveur RADIUS accorde l'accès à l'utilitaire de configuration Web, ce serveur doit renvoyer cisco-avpair = shell:priv-lvl=15.
- *Aucun* : l'utilisateur est autorisé à accéder au périphérique sans autorisation/authentification.
- *Locale* : le nom d'utilisateur et le mot de passe sont comparés aux données stockées sur le périphérique local. Ces paires de nom d'utilisateur et mot de passe sont définies sur la page Comptes d'utilisateur.

REMARQUE La méthode d'authentification **Local** ou **None** doit toujours être sélectionnée en dernier. Toutes les méthodes d'authentification sélectionnées après **Local** ou **None** sont ignorées.

ÉTAPE 6 Cliquez sur **Apply**. Les méthodes d'authentification sélectionnées sont associées à la méthode d'accès.

Gestion sécurisée des données confidentielles

Reportez-vous à la section **Sécurité : Gestion sécurisée des données confidentielles**.

Serveur SSL

Cette section décrit la fonctionnalité SSL (Secure Socket Layer).

Présentation de SSL

La fonctionnalité SSL (Secure Socket Layer) permet d'ouvrir une session HTTPS sur l'appareil.

Une session HTTPS peut être ouverte avec le certificat par défaut qui est présent sur l'appareil.

Certains navigateurs génèrent des avertissements lors de l'utilisation d'un certificat par défaut, car ce certificat n'est pas signé par une autorité de certification (CA, Certification Authority). Il est recommandé d'utiliser un certificat signé par une CA de confiance.

Pour ouvrir une session HTTPS avec un certificat créé par l'utilisateur, procédez comme suit :

1. Générez un certificat.
2. Demandez que le certificat soit certifié par une CA.
3. Importez le certificat signé dans l'appareil.

Configuration et paramètres par défaut

Par défaut, le périphérique contient un certificat qui peut être modifié.

HTTPS est activé par défaut.

Paramètres d'authentification de serveur SSL

Il peut être nécessaire de générer un nouveau certificat pour remplacer le certificat par défaut présent sur l'appareil.

Pour créer un certificat :

ÉTAPE 1 Cliquez sur **Sécurité > Serveur SSL > Paramètres d'authentification de serveur SSL.**

Les informations concernant les certificats 1 et 2 apparaissent dans la Table de clés de serveur SSL. Ces champs sont définis sur la page **Modifier**, excepté pour les champs suivants :

- **Valide du** : spécifie la date à partir de laquelle le certificat est valide.
- **Valide jusqu'au** : spécifie la date jusqu'à laquelle le certificat est valide.
- **Source du certificat** : spécifie si le certificat a été généré par le système (Autogénéré) ou l'utilisateur (Défini par l'utilisateur).

ÉTAPE 2 Sélectionnez un certificat actif.

ÉTAPE 3 Cliquez sur **Générer une demande de certificat**.

ÉTAPE 4 Renseignez les champs suivants :

- **ID de certificat** : sélectionnez le certificat actif.
- **Nom courant** : spécifie l'adresse IP ou l'URL complète de l'appareil. Si elle n'est pas indiquée, le système utilisera l'adresse IP la plus basse de l'appareil (lors de la génération du certificat).
- **Unité organisationnelle** : spécifie l'unité organisationnelle ou le nom du service.
- **Nom de l'organisation** : spécifie le nom de l'organisation.

- **Lieu** : spécifie l'emplacement ou le nom de la ville.
- **État** : spécifie le nom de l'état ou de la province.
- **Pays** : spécifie le nom du pays.
- **Demande de certificat** : affiche la clé créée lorsque vous cliquez sur le bouton **Demande de génération d'un certificat**.

ÉTAPE 5 Cliquez sur **Générer une demande de certificat**. Le système crée alors une clé qui doit être entrée dans l'autorité de certification (Certification Authority, CA). Copiez-la du champ **Demande de certificat**.

Pour importer un certificat :

ÉTAPE 1 Cliquez sur **Sécurité > Serveur SSL > Paramètres d'authentification de serveur SSL.**

ÉTAPE 2 Cliquez sur **Importer le certificat**.

ÉTAPE 3 Renseignez les champs suivants :

- **ID de certificat** : sélectionnez le certificat actif.
- **Source du certificat** : indique que le certificat est défini par l'utilisateur.
- **Certificat** : copiez dans le certificat reçu.
- **Importer une paire de clés RSA** : sélectionnez cette option pour autoriser la copie dans la nouvelle paire de clés RSA.
- **Clé publique** : copiez dans la clé publique RSA.
- **Clé privée (chiffrée)** : sélectionnez et copiez dans la clé privée RSA sous forme chiffrée.
- **Clé privée (texte en clair)** : sélectionnez et copiez dans la clé privée RSA sous forme de texte en clair.

ÉTAPE 4 Cliquez sur **Appliquer** pour appliquer les modifications dans la Configuration d'exécution.

ÉTAPE 5 Cliquez sur **Afficher les données sensibles sous forme chiffrée** pour afficher cette clé sous forme chiffrée. Une fois que vous avez cliqué sur ce bouton, les clés privées sont écrites dans le fichier de configuration sous forme chiffrée (dès que vous cliquez sur Appliquer). Lorsque le texte s'affiche sous forme chiffrée, le bouton devient **Afficher les données sensibles sous forme de texte clair,** ce qui vous permet de réafficher le texte en clair.

Le bouton **Détails** affiche le certificat et la paire de clés RSA. Cela vous permet de copier le certificat et la paire de clés RSA vers un autre appareil (via la fonction copier/coller). Lorsque vous cliquez sur **Afficher les données sensibles sous forme chiffrée**, les clés privées apparaissent sous forme chiffrée.

Client SSH

Reportez-vous à la section **Sécurité : Client SSH**.

Configuration des services TCP/UDP

La page Services TCP/UDP active les services TCP ou UDP sur le périphérique, généralement pour des raisons de sécurité.

Le périphérique fournit les services TCP/UDP suivants :

- **HTTP** : activé par défaut
- **HTTPS** : activé par défaut en usine
- **SNMP** : désactivé par défaut en usine

Les connexions TCP actives sont également affichées dans cette fenêtre.

Pour configurer les services TCP/UDP :

ÉTAPE 1 Cliquez sur **Security** > **TCP/UDP Services**.

ÉTAPE 2 Activez ou désactivez les services TCP/UDP suivants sur les services affichés.

- **Service HTTP** : indique si le service HTTP est activé ou désactivé.
- **Service HTTPS** : indique si le service HTTPS est activé ou désactivé.
- **Service SNMP** : indique si le service SNMP est activé ou désactivé.

ÉTAPE 3 Cliquez sur **Appliquer**. Les services sont écrits dans le fichier de Configuration d'exécution.

La table des services TCP contient les champs suivants pour chaque service :

- **Nom de service** : méthode d'accès utilisée par le périphérique pour fournir le service TCP.
- **Type** : protocole IP utilisé par le service.
- **Adresse IP locale** : adresse IP locale via laquelle le périphérique propose le service.
- **Port local** : port TCP local via lequel le périphérique propose le service.
- **Remote IP Address** : adresse IP de l'appareil distant qui demande le service.
- **Remote Port** : port TCP de l'appareil distant qui demande le service.
- **État** : état du service.

La table des services UDP affiche les informations suivantes :

- **Nom de service** : méthode d'accès utilisée par le périphérique pour fournir le service UDP.
- **Type** : protocole IP utilisé par le service.
- **Adresse IP locale** : adresse IP locale via laquelle le périphérique propose le service.
- **Port local** : port UDP local via lequel le périphérique propose le service.
- **Instance d'application** : instance de service du service UDP (Par exemple, lorsque deux expéditeurs envoient des données vers la même destination.)

Définition du contrôle des tempêtes

Lorsque des trames de Diffusion (Broadcast), Multidiffusion (Multicast) ou Monodiffusion inconnue (Unknown Unicast) sont reçues, elles sont dupliquées et une copie est envoyée à tous les ports de sortie possibles. Cela signifie dans la pratique qu'elles sont envoyées à tous les ports appartenant au VLAN approprié. De cette manière, une seule trame d'entrée est convertie en plusieurs trames, ce qui peut potentiellement occasionner une tempête de trafic.

La protection contre les tempêtes vous permet de limiter le nombre de trames entrant dans le périphérique et de définir les types de trames pris en compte dans le calcul de cette limite.

Lorsque la fréquence d'images de Diffusion, Multidiffusion ou Monodiffusion inconnue est supérieure au seuil défini par l'utilisateur, les images reçues au-delà du seuil sont rejetées.

Pour définir le contrôle des tempêtes :

ÉTAPE 1 Cliquez sur **Security** > **Storm Control**.

Tous les champs de cette page sont décrits sur la page Modifier le contrôle des tempêtes, excepté pour le **Seuil de débit de contrôle des tempêtes (%)**. Il affiche le pourcentage de la bande passante totale disponible pour les paquets de Monodiffusion inconnue (Unknown Unicast), Multidiffusion (Multicast) et Diffusion (Broadcast) avant que le contrôle des tempêtes ne soit appliqué sur le port. La valeur par défaut est 10 % du débit maximal du port. Vous pouvez la définir sur la page Modifier le contrôle des tempêtes.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez le port pour lequel activer le contrôle des tempêtes.
- **Contrôle des tempêtes** : sélectionnez cette option pour activer le contrôle des tempêtes.

- **Seuil de débit de contrôle des tempêtes** : saisissez le débit maximum auquel les paquets inconnus peuvent être transmis. La valeur par défaut de ce seuil est 10 000 pour les appareils FE et 100 000 pour les appareils GE.
- **Mode de contrôle des tempêtes** : sélectionnez l'un des modes suivants.
  - *Monodiffusion inconnue, multidiffusion et diffusion* : intègre le trafic de Monodiffusion inconnue (Unknown Unicast), Diffusion (Broadcast) et Multidiffusion (Multicast) au sein du seuil de la bande passante.
  - *Multidiffusion et diffusion* : intègre le trafic de Diffusion (Broadcast) et Multidiffusion (Multicast) au sein du seuil de la bande passante.
  - *Diffusion uniquement* : intègre uniquement le trafic de diffusion au sein du seuil de la bande passante.

ÉTAPE 4 Cliquez sur **Apply.** Le contrôle des tempêtes est modifié et le fichier de Configuration d'exécution est mis à jour.

Configuration de la sécurité des ports

Vous pouvez accroître la sécurité réseau en limitant l'accès à un port pour des utilisateurs disposant d'adresses MAC spécifiques. Les adresses MAC peuvent être apprises de façon dynamique ou configurées de manière statique.

La sécurité des ports surveille les paquets reçus et appris. L'accès aux ports verrouillés est limité aux utilisateurs disposant d'adresses MAC spécifiques.

La sécurité des ports dispose de quatre modes :

- **Verrouillage classique** : toutes les adresses MAC apprises sur le port sont verrouillées et le port n'apprend aucune nouvelle adresse MAC. Les adresses apprises ne sont pas soumises à un délai d'expiration ni à un réapprentissage.
- **Verrouillage dynamique limité** : le périphérique apprend des adresses MAC jusqu'à la limite configurée des adresses autorisées. Une fois la limite atteinte, le périphérique n'apprend pas d'adresses supplémentaires. Dans ce mode, les adresses sont soumises à un délai d'expiration ainsi qu'à un réapprentissage.
- **Sécurisé en permanence** : conserve les adresses MAC dynamiques actuellement associées au port et apprend au maximum le nombre d'adresses autorisées sur le port (défini par l'option Nombre max. d'adresses autorisées). Les opérations de réapprentissage et de délai d'expiration sont désactivées.

- **Suppression sécur. à la réinitialisation** : supprime les adresses MAC dynamiques actuellement associées au port après la réinitialisation. Les nouvelles adresses MAC peuvent être apprises en tant qu'adresses supprimées à la réinitialisation (Delete-On-Reset) jusqu'au nombre d'adresses autorisées sur le port. Les opérations de réapprentissage et de délai d'expiration sont désactivées.

Lorsqu'une trame d'une nouvelle adresse MAC est détectée sur un port sur lequel elle n'est pas autorisée (le port est verrouillé de façon classique et une nouvelle adresse MAC est détectée ou bien le port est verrouillé de façon dynamique et le nombre maximal des adresses autorisées a été dépassé), il est fait appel au mécanisme de protection et l'une des actions suivantes peut s'appliquer :

- La trame est rejetée.
- La trame est transmise.
- Le port est fermé.

Lorsque l'adresse MAC sécurisée est détectée sur un autre port, la trame est transmise mais l'adresse MAC n'est pas apprise sur ce port.

Outre l'une de ces actions, vous pouvez également générer des interceptions ainsi qu'en limiter la fréquence ou le nombre afin d'éviter de surcharger les appareils.

REMARQUE Pour utiliser 802.1X sur un port, il doit être en mode Hôtes multiples ou Sessions multiples. La sécurité des ports ne peut pas être définie sur un port si ce dernier est un mode unique (reportez-vous à la page 802.1x, Authentification hôtes et sessions).

Pour configurer la sécurité des ports :

ÉTAPE 1 Cliquez sur **Security** > **Port Security**.

ÉTAPE 2 Sélectionnez une interface à modifier et cliquez sur **Modifier**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez le nom de l'interface.
- **État de l'interface** : sélectionnez l'état de verrouillage du port.
- **Learning Mode** : sélectionnez le type de verrouillage du port. L'État de l'interface doit être déverrouillé pour que ce champ puisse être configuré. Le champ Mode d'apprentissage est uniquement activé si le champ *État de l'interface* est verrouillé. Pour modifier le Mode d'apprentissage, État de l'interface doit être désactivé. Une fois ce mode modifié, vous pouvez rétablir l'état de l'interface. Les options sont les suivantes :
  - *Verrouillage classique* : verrouille immédiatement le port, quel que soit le nombre d'adresses ayant déjà été apprises.
  - *Verrouillage dynamique limité* : verrouille le port en supprimant les adresses MAC dynamiques actuellement associées au port. Le port apprend au maximum le nombre d'adresses autorisées sur le port. Le réapprentissage et le délai d'expiration des adresses MAC sont activés.

- *Sécurisé en permanence* : conserve les adresses MAC dynamiques actuellement associées au port et apprend au maximum le nombre d'adresses autorisées sur le port (défini par l'option **Nombre max. d'adresses autorisées**). Les opérations de réapprentissage et de délai d'expiration sont activées.
- *Suppression sécur. à la réinitialisation* : supprime les adresses MAC dynamiques actuellement associées au port après la réinitialisation. Les nouvelles adresses MAC peuvent être apprises en tant qu'adresses supprimées à la réinitialisation (Delete-On-Reset) jusqu'au nombre d'adresses autorisées sur le port. Les opérations de réapprentissage et de délai d'expiration sont désactivées.

- **Nombre max. d'adresses autorisées** : saisissez le nombre maximum d'adresses MAC pouvant être apprises sur le port dans la mesure où le mode d'apprentissage *Verrouillage dynamique limité* est sélectionné. Le chiffre 0 indique que seules les adresses statiques sont prises en charge dans l'interface.
- **Action en cas de violation** : sélectionnez l'action à appliquer aux paquets qui arrivent sur un port verrouillé. Les options sont les suivantes :
  - *Abandonner* : supprime les paquets en provenance d'une source non apprise.
  - *Transférer* : transfère les paquets en provenance d'une source inconnue sans apprendre l'adresse MAC.
  - *Arrêter* : abandonne les paquets en provenance d'une source non apprise et ferme le port. Le port reste fermé jusqu'à ce qu'il soit réactivé ou jusqu'à ce que le périphérique soit réinitialisé.
- **« Trap »** : sélectionnez cette option pour activer les messages « trap » lorsqu'un paquet est reçu sur un port verrouillé. Ceci est approprié pour les violations de verrouillage. Pour le Verrouillage classique, ceci correspondra à toute nouvelle adresse reçue. Pour le Verrouillage dynamique limité, cela correspondra à toute nouvelle adresse qui dépassera le nombre des adresses autorisées.
- **Fréquence du/des message(s) « trap »** : saisissez la durée minimale qui s'écoulera entre deux messages « trap ».

ÉTAPE 4 Cliquez sur **Apply**. La sécurité des ports est modifiée et le fichier de Configuration d'exécution est mis à jour.

802.1X

Reportez-vous au chapitre **Sécurité : Authentification 802.1X** pour obtenir de plus amples informations sur l'authentification 802.1x.

Prévention du déni de service

Le déni de service (DoS) est une tentative de piratage visant à rendre le périphérique indisponible pour les utilisateurs.

Les attaques DoS saturent le périphérique avec des demandes de communication externes, de telle manière que le périphérique ne peut pas répondre au trafic légitime. Ces attaques provoquent souvent la surcharge du processeur du périphérique.

Secure Core Technology (SCT)

Une méthode pour contrer les dénis de service (DoS) employée par le périphérique est la fonction SCT. La fonction SCT est activée par défaut sur l'appareil et ne peut pas être désactivée.

Le périphérique Cisco est un périphérique avancé qui gère le trafic de gestion, de protocole et de surveillance, outre le trafic de l'utilisateur final (TCP).

La fonction SCT garantit que le périphérique reçoive et traite le trafic de gestion et de protocole, quel qu'il soit le trafic reçu. Ceci est possible en limitant le débit du trafic TCP sur le processeur.

Il n'y a pas d'interactions avec les autres fonctions.

La fonction SCT peut être contrôlée sur la page Déni de service > Prévention du déni de service > Paramètres de la suite de sécurité (bouton **Détails**).

Types de dénis de service (DoS)

Un déni de service peut être provoqué de l'une des manières suivantes (parmi d'autres) :

- Paquets TCP SYN : une saturation de paquets TCP SYN, souvent avec une adresse d'expéditeur fausse, peut signifier une attaque. Chacun de ces paquets provoque une connexion semi-ouverte du périphérique en renvoyant un paquet TCP/SYN-ACK (confirmation) et en attendant un paquet de réponse en provenance de l'adresse de l'expéditeur (réponse au paquet ACK). Cependant, étant donné que l'adresse de l'expéditeur est fausse, la réponse n'arrive jamais. Ces connexions semi-ouvertes saturent le nombre de connexions disponibles que le périphérique peut effectuer, l'empêchant ainsi de répondre aux requêtes légitimes. En outre, le nombre de paquets pouvant être envoyés vers le CPU est limité et le trafic de l'attaque risque d'utiliser la totalité de ces paquets.

  Ces paquets peuvent être bloqués sur la page Protection SYN.

- Paquets TCP SYN-FIN : les paquets SYN sont envoyés pour créer une nouvelle connexion TCP. Les paquets TCP FIN sont envoyés pour fermer une connexion. Un paquet où les indicateurs SYN et FIN sont définis ne devrait jamais exister. En conséquence, ces paquets peuvent constituer une attaque au périphérique et doivent être bloqués.

Une définition de ce que constitue une attaque SYN peut être créée sur la page Protection SYN. Lorsque le périphérique identifie une telle attaque sur une interface, elle est rapportée sur cette page.

Défense contre les dénis de service (DoS)

*La fonctionnalité Prévention du déni de service (Do*S) permet à l'administrateur système de résister aux dénis de service en suivant l'une des méthodes ci-dessous :

- Activer la protection TCP SYN. Si cette fonctionnalité est activée, des rapports sont émis lorsqu'une attaque de paquet SYN est identifiée. Une attaque SYN est identifiée lorsque le nombre de paquets SYN par seconde dépasse le seuil défini par l'utilisateur.
- Les paquets SYN-FIN peuvent être bloqués.

Dépendances entre les fonctions

Il n'y a aucune dépendance entre cette fonctionnalité et d'autres fonctionnalités.

Configuration par défaut

La fonctionnalité Prévention du déni de service (DoS) est configurée par défaut comme suit :

- La fonctionnalité Prévention du déni de service (DoS) est désactivée par défaut.
- La protection SYN-FIN est activée par défaut (même si la fonctionnalité Prévention du déni de service (DoS) est désactivée).
- Si la protection SYN est activée, le réglage par défaut est Rapport. Le seuil par défaut est de 30 paquets SYN par seconde.
- Toutes les autres fonctionnalités de prévention du déni de service (DoS) sont désactivées par défaut.

Configuration de la prévention du déni de service (DoS)

Les pages suivantes sont utilisées pour configurer cette fonctionnalité.

Paramètres de la suite de sécurité

Pour configurer les paramètres globaux de prévention du déni de service et contrôler la fonction SCT :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Paramètres de suite de sécurité**. La page *Paramètres de la suite de sécurité* s'affiche.

Mécanisme de protection CPU : Activé indique que la fonction SCT est activée.

ÉTAPE 2 Cliquez sur **Détails** en regard de **Utilisation du CPU** pour accéder à la page Utilisation du CPU et afficher les informations d'utilisation des ressources du CPU.

ÉTAPE 3 Cliquez sur **Modifier** en regard de **Protection TCP SYN** pour accéder à la page Protection SYN et activer cette fonctionnalité.

Protection SYN

Les ports du réseau risquent d'être utilisés par les pirates pour attaquer le périphérique lors d'une attaque SYN, ce qui utilise des ressources TCP (tampons) et de l'énergie du CPU.

Étant donné que le CPU est protégé à l'aide de la fonction SCT, le trafic TCP vers le CPU est limité. Cependant, si un ou plusieurs ports sont attaqués par un grand nombre de paquets SYN, le CPU reçoit uniquement les paquets du pirate, ce qui crée un déni de service.

Lors de l'utilisation de la fonctionnalité de protection SYN, le processeur compte les paquets SYN entrants par seconde par chaque port de réseau vers le processeur.

Si le nombre est supérieur au seuil, un message SYSLOG est généré, mais les paquets ne sont pas bloqués.

Pour configurer la protection SYN :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Protection SYN**.

ÉTAPE 2 Saisissez les paramètres.

- **Bloquer les paquets SYN-FIN** : sélectionnez cette option pour activer la fonctionnalité. Si les paquets TCP avec les indicateurs SYN et FIN sont détectés, un message SYSLOG est généré.
- **Mode de protection SYN** : sélectionnez l'un des trois modes ci-dessous :
  - *Désactiver* : la fonctionnalité est désactivée sur une interface spécifique.
  - *Rapport* : génère un message SYSLOG. L'état du port bascule vers **Attaqué** lorsque le seuil est dépassé.
- **Seuil de protection SYN** : nombre de paquets SYN par seconde avant de bloquer les paquets SYN (un SYN de déni avec une règle MAC-to-me sera appliqué sur le port).

ÉTAPE 3 Cliquez sur **Appliquer**. La protection SYN est défini et le fichier de Configuration d'exécution est mis à jour.

La Table des interfaces de protection SYN affiche les champs suivants pour chaque port ou LAG (en fonction des besoins de l'utilisateur)

- **État actuel** : état de l'interface. Ce champ peut prendre les valeurs suivantes :
  - *Normal* : aucune attaque n'a été identifiée sur cette interface.
  - *Attaqué* : une attaque a été identifiée sur cette interface.
- **Dernière attaque** : date de la dernière attaque SYN-FIN identifiée par le système et action du système (**Rapporté**).

20

Sécurité : Authentification 802.1X

Cette section décrit l'authentification 802.1X.

Elle couvre les rubriques suivantes :

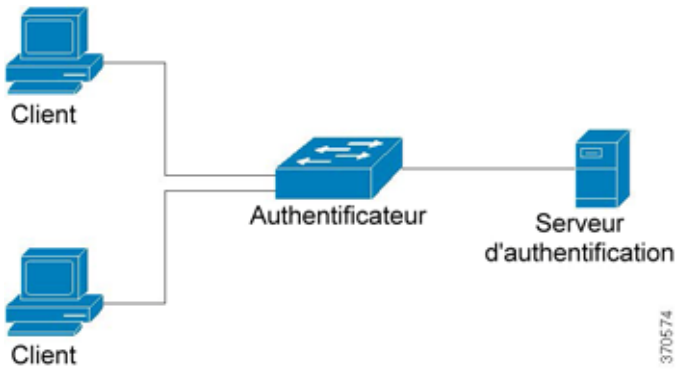
- **Présentation de 802.1X**
- **Présentation de l'authentificateur**
- **Tâches courantes**
- **Configuration de 802.1X via l'interface utilisateur graphique (GUI)**

Présentation de 802.1X

L'authentification 802.1x empêche les clients non autorisés de se connecter à un réseau LAN par le biais de ports accessibles à la publicité. L'authentification 802.1x est un modèle client-serveur. Dans ce modèle, les périphériques réseau ont les rôles spécifiques suivants.

- Client ou demandeur
- Authentificateur
- Serveur d'authentification

Il est décrit dans la figure ci-dessous :



Sur chaque port, un périphérique réseau peut être un client/demandeur, un authentificateur ou les deux.

Client ou demandeur

Un client ou un demandeur est un périphérique réseau qui demande accès au LAN. Le client est connecté à un authentificateur.

Si le client utilise le protocole 802.1x pour l'authentification, il exécute la partie demandeur du protocole 802.1x et la partie client du protocole EAP.

Authentificateur

Un authentificateur est un périphérique réseau qui fournit des services réseau et auquel les ports du demandeur sont connectés.

Les modes d'authentification suivants sur les ports sont pris en charge (vous pouvez définir ces modes dans Sécurité > Authentification 802.1X > Hôte et Authentification) :

- **Hôte unique** : prend en charge l'authentification basée sur les ports avec un seul client par port.
- **Hôtes multiples** : prend en charge l'authentification basée sur les ports avec plusieurs clients par port.
- **Sessions multiples** : prend en charge l'authentification basée sur les clients avec plusieurs clients par port.

Pour plus d'informations, reportez-vous à la section **Modes hôte de port**.

Dans l'authentification 802.1x, l'authentificateur extrait les messages EAP des messages 802.1x (trames EAPOL) et les transmet au serveur d'authentification, via le protocole RADIUS.

Serveur d'authentification

Le serveur d'authentification effectue l'authentification du client. Le serveur d'authentification pour le périphérique est un serveur d'authentification RADIUS avec extensions EAP.

Open Access (Accès ouvert)

La fonction Open (Monitoring) Access (Accès (en surveillance) ouvert) facilite la distinction entre les échecs d'authentification véritables et les échecs causés par une configuration incorrecte et/ou un manque de ressources dans un environnement 802.1x.

La fonction Open Access (Accès ouvert) permet aux administrateurs système de mieux comprendre les problèmes de configuration des hôtes qui se connectent au réseau, de surveiller les situations critiques et de résoudre ces problèmes.

Lorsque la fonction Open Access (Accès ouvert) est activée sur une interface, le commutateur considère tous les échecs reçus d'un serveur RADIUS comme des réussites et autorise les stations connectées à l'interface à accéder au réseau quels que soient les résultats de l'authentification.

La fonction Open Access (Accès ouvert) modifie le paramétrage standard qui consiste à bloquer le trafic sur un port à authentification jusqu'à la réussite des procédures d'authentification et d'autorisation. Le comportement d'authentification par défaut est toujours de bloquer l'ensemble du trafic à l'exception du protocole EAPoL (Extensible Authentication Protocol over LAN). Toutefois, la fonction Open Access (Accès ouvert) offre à l'administrateur la possibilité de donner un libre accès à l'ensemble du trafic, même si l'authentification (802.1X, MAC et/ou Web) est activée.

Lorsque la gestion de comptes RADIUS est activée, vous pouvez consigner les tentatives d'authentification et obtenir une meilleure visibilité sur les utilisateurs et les appareils qui se connectent au réseau grâce à une piste d'audit.

Tout se déroule sans impact sur les utilisateurs finaux ni sur les hôtes connectés au réseau. Vous pouvez activer la fonction Open Access (Accès ouvert) sur la page **Authentification des ports 802.1X**.

Présentation de l'authentificateur

États d'authentification administrative du port

L'état administratif du port détermine si le client a accès au réseau.

L'état administratif du port peut être configuré sur la page Sécurité > Authentification 802.1X > Authentification des ports.

La valeurs suivantes sont disponibles :

- **Autorisation forcée**

  L'authentification du port est désactivée et le port transmet tout le trafic conformément à sa configuration statique sans demander d'authentification. Le commutateur envoie le paquet EAP 802.1x qui intègre le message de réussite EAP lorsqu'il reçoit le message de démarrage EAPOL 802.1x.

  Il s'agit de l'état par défaut.

- **Non-autorisation forcée**

  L'authentification du port est désactivée et le port transmet tout le trafic via le VLAN invité et les VLAN non authentifiés. Pour plus d'informations, reportez-vous à la section **Définition de l'authentification des hôtes et sessions**. Le commutateur envoie les paquets EAP 802.1x qui intègrent les messages d'erreur EAP lorsqu'il reçoit les messages de démarrage EAPOL 802.1x.

- **auto**

  Active les authentifications 802.1 x conformément au mode hôte de port configuré et aux méthodes d'authentification configurées sur le port.

Modes hôte de port

Les ports peuvent être définis dans les modes hôte de port suivants (configurés sur la page Sécurité > Authentification 802.1X > Hôte et Authentification) :

- **Mode Hôte unique**

  Un port est autorisé s'il y a un client autorisé. Un seul hôte peut être autorisé sur un port.

  Lorsqu'un port n'est pas autorisé et que le VLAN invité est activé, le trafic non balisé est remappé sur le VLAN invité. Le trafic balisé est abandonné sauf s'il appartient au VLAN invité ou à un VLAN non authentifié. Si un VLAN invité n'est pas activé sur le port, seul le trafic balisé appartenant aux VLAN non authentifiés est ponté.

  Lorsqu'un port est autorisé, le trafic balisé et non balisé provenant de l'hôte autorisé est ponté en fonction de la configuration du port d'appartenance au VLAN statique. Le trafic provenant des autres hôtes est abandonné.

  Un utilisateur peut spécifier que le trafic non balisé provenant de l'hôte autorisé doit être remappé sur un VLAN qui est attribué par un serveur RADIUS au cours du processus d'authentification. Le trafic balisé est abandonné sauf s'il appartient au VLAN affecté par RADIUS ou aux VLAN non authentifiés. Vous pouvez définir l'affectation VLAN RADIUS sur un port via la page Sécurité > Authentification 802.1X > Authentification des ports.

- **Mode Hôtes multiples**

  Un port est autorisé s'il y a au moins un client autorisé.

  Lorsqu'un port n'est pas autorisé et qu'un VLAN invité est activé, le trafic non balisé est remappé sur le VLAN invité. Le trafic balisé est abandonné sauf s'il appartient au VLAN invité ou à un VLAN non authentifié. Si le VLAN invité n'est pas activé sur un port, seul le trafic balisé appartenant aux VLAN non authentifiés est ponté.

  Lorsqu'un port est autorisé, le trafic balisé et non balisé provenant de tous les hôtes connectés au port est ponté en fonction de la configuration du port d'appartenance au VLAN statique.

  Vous pouvez spécifier que le trafic non balisé provenant du port autorisé doit être remappé sur un VLAN qui est attribué par un serveur RADIUS au cours du processus d'authentification. Le trafic balisé est abandonné sauf s'il appartient au VLAN affecté par RADIUS ou aux VLAN non authentifiés. Vous pouvez définir l'affectation VLAN RADIUS sur un port via la page Authentification des ports.

- **Mode Sessions multiples**

  À la différence des modes Hôte unique et Hôtes multiples, un port en mode Sessions multiples n'a pas d'état d'authentification. Cet état est attribué à chaque client connecté au port. Ce mode requiert une recherche TCAM. Puisque les commutateurs du mode Couche 3 n'ont pas de recherche TCAM allouée pour le mode Sessions multiples, ils prennent en charge une forme limitée du mode Sessions multiples, qui n'autorise pas les attributs VLAN invité et VLAN RADIUS. Le nombre maximal d'hôtes autorisés sur le port doit être configuré sur la page Authentification des ports.

  Le trafic balisé appartenant à un VLAN non authentifié est toujours ponté, que l'hôte soit autorisé ou pas.

  Le trafic balisé et non balisé qui provient d'hôtes non autorisés n'appartenant pas à un VLAN non authentifié est remappé sur le VLAN invité s'il est défini et activé sur le VLAN, ou est abandonné si le VLAN invité n'est pas activé sur le port.

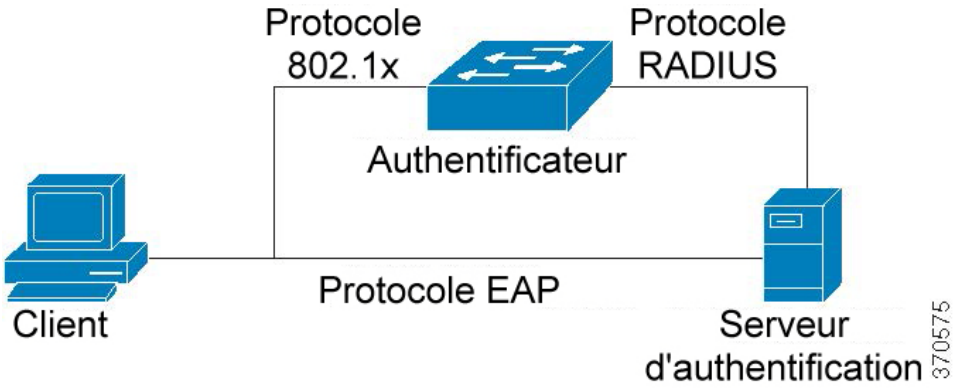
  Si un hôte autorisé se voit attribuer un VLAN par un serveur RADIUS, tout son trafic balisé et non balisé n'appartenant pas aux VLAN non authentifiés est ponté via le VLAN ; si le VLAN n'est pas attribué, tout son trafic est ponté en fonction de la configuration du port d'appartenance au VLAN statique.

Authentification 802.1x

L'authentificateur 802.1x relaie les messages EAP transparents entre les demandeurs 802.1x et les serveurs d'authentification. Les messages EAP entre les demandeurs et l'authentificateur sont encapsulés dans les messages 802.1x, et les messages EAP entre l'authentificateur et les serveurs d'authentification sont encapsulés dans les messages RADIUS.

Ce processus est décrit dans la figure ci-dessous :

Figure 1 Authentification 802.1x



Le périphérique prend en charge le mécanisme d'authentification 802.1X, tel que décrit dans la norme pour authentifier et autoriser les demandeurs 802.1X.

Mode Violation

En mode Hôte unique, vous pouvez configurer l'action à effectuer lorsqu'un hôte non autorisé sur un port autorisé tente d'accéder à l'interface. Cette opération s'effectue sur la page Authentification hôtes et sessions.

Les options suivantes sont disponibles :

- **restreindre** : génère une interception lorsqu'une station, dont l'adresse MAC n'est pas l'adresse MAC du demandeur, tente d'accéder à l'interface. La durée minimale entre les interceptions est de 1 seconde. Ces trames sont transmises, mais leurs adresses source ne sont pas apprises.
- **protéger** : ignore les trames dont l'adresse source n'est pas celle du demandeur.
- **arrêter** : ignore les trames dont l'adresse source n'est pas celle du demandeur et ferme le port.

Vous pouvez aussi configurer le périphérique pour qu'il envoie des interceptions SNMP, avec une durée minimale configurable entre deux interceptions consécutives. Si secondes = 0, les interceptions sont désactivées. Si aucune durée minimale n'est spécifiée, la valeur par défaut utilisée est 1 seconde pour le mode restreindre et 0 pour les autres modes.

Période silencieuse

La période silencieuse est une période au cours de laquelle le port (mode Hôte unique ou Hôtes multiples) ou le client (mode Sessions multiples) ne peut pas effectuer de tentative d'authentification suite à l'échec d'un échange d'authentification. En mode Hôte unique ou Hôtes multiples, la période est définie par port ; en mode Sessions multiples, la période est définie par client. Au cours de la période silencieuse, le commutateur ne peut pas accepter, ni initialiser les requêtes d'authentification.

Vous pouvez aussi spécifier le nombre maximal de tentatives de connexion avant le début de la période silencieuse. La valeur 0 indique un nombre illimité de tentatives de connexion.

La durée de la période silencieuse et le nombre maximal de tentatives de connexion peuvent être définis sur la page Authentification des ports.

Tâches courantes

Flux de travail 1 : activer l'authentification 802.1x sur un port

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X > Propriétés**.

ÉTAPE 2 Activez l'authentification basée sur les ports.

ÉTAPE 3 Sélectionnez la **Méthode d'authentification**.

ÉTAPE 4 Cliquez sur **Appliquer** ; le fichier de Configuration d'exécution est mis à jour.

ÉTAPE 5 Cliquez sur **Sécurité > Authentification 802.1X > Authentification hôtes et sessions**.

ÉTAPE 6 Sélectionnez le port souhaité et cliquez sur **Modifier**.

ÉTAPE 7 Définissez le mode Authentification des hôtes.

ÉTAPE 8 Cliquez sur **Appliquer** ; le fichier de Configuration d'exécution est mis à jour.

ÉTAPE 9 Cliquez sur **Sécurité > Authentification 802.1X > Authentification des ports**.

ÉTAPE 10 Sélectionnez un port et cliquez sur **Edit**.

ÉTAPE 11 Définissez le champ Contrôle de port administratif sur **Auto**.

ÉTAPE 12 Définissez les méthodes d'authentification.

ÉTAPE 13 Cliquez sur **Appliquer** ; le fichier de Configuration d'exécution est mis à jour.

Flux de travail 2 : configurer les interceptions

ÉTAPE 1 Cliquez sur **Sécurité** > **Authentification 802.1X** > **Propriétés**.

ÉTAPE 2 Sélectionnez les interceptions requises.

ÉTAPE 3 Cliquez sur **Appliquer** ; le fichier de Configuration d'exécution est mis à jour.

Flux de travail 3 : configurer l'authentification 802.1x ou

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X > Authentification des ports**.

ÉTAPE 2 Sélectionnez le port souhaité et cliquez sur **Modifier**.

ÉTAPE 3 Renseignez les champs requis pour le port.

Les champs de cette page sont décrits à la section **Authentification des ports 802.1X**.

ÉTAPE 4 Cliquez sur **Appliquer** ; le fichier de Configuration d'exécution est mis à jour.

Utilisez le bouton **Copier les paramètres** pour copier les paramètres d'un port vers un autre.

Flux de travail 4 : configurer la période silencieuse

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X > Authentification des ports**.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Edit**.

ÉTAPE 3 Saisissez la période silencieuse dans le champ Période silencieuse.

ÉTAPE 4 Cliquez sur **Appliquer** ; le fichier de Configuration d'exécution est mis à jour.

Configuration de 802.1X via l'interface utilisateur graphique (GUI)

Définition des propriétés 802.1X

La page Propriétés 802.1X permet d'activer 802.1X globalement et de définir la façon dont les ports sont authentifiés. Pour que 802.1X puisse fonctionner, il doit être activé à la fois globalement et individuellement sur chaque port.

Pour définir l'authentification basée sur les ports :

ÉTAPE 1 Cliquez sur **Sécurité** > **Authentification 802.1X** > **Propriétés**.

ÉTAPE 2 Saisissez les paramètres.

- **Authentification basée sur les ports** : activez ou désactivez l'authentification basée sur les ports.

  Si cette fonction est désactivée, 802.1X est désactivée.

- **Méthode d'authentification** : sélectionnez les méthodes d'authentification des utilisateurs. Les options sont les suivantes :
  - *RADIUS, aucune* : effectue tout d'abord l'authentification des ports en utilisant le serveur RADIUS. Si aucune réponse n'est reçue de ce serveur (par exemple s'il n'est pas actif), aucune authentification n'est réalisée et la session est autorisée.
  - *RADIUS* : authentifie l'utilisateur sur le serveur RADIUS. Si aucune authentification n'est effectuée, la session n'est pas autorisée.
  - *Aucune* : n'authentifie pas l'utilisateur. Autorise la session.
- **Paramètres de filtre** : pour activer les interceptions, sélectionnez une ou plusieurs des options suivantes :
  - *Interceptions d'échec d'authentification 802.1x* : sélectionnez cette option pour générer une interception si l'authentification 802.1x échoue.
  - *Interceptions de réussite d'authentification 802.1x* : sélectionnez cette option pour générer une interception si l'authentification 802.1x réussit.

ÉTAPE 3 Cliquez sur **Appliquer**. Les propriétés 802.1X sont écrites dans le fichier de Configuration d'exécution.

Authentification des ports 802.1X

La page Authentification des ports permet de définir les paramètres 802.1X pour chaque port. Puisque certaines modifications de la configuration ne sont possibles que si le port a l'état Autorisation forcée (par exemple, l'authentification des hôtes), il est recommandé de changer le contrôle du port en Autorisation forcée avant d'effectuer des modifications. Une fois la configuration terminée, rétablissez l'état précédent du contrôle de port.

REMARQUE Un port sur lequel 802.1X est défini ne peut pas devenir membre d'un LAG.

Pour définir l'authentification 802.1X :

ÉTAPE 1 Cliquez sur **Sécurité** > **Authentification 802.1X** > **Authentification des ports**.

Cette page affiche les paramètres d'authentification de tous les ports.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez un port.
- **Contrôle de port actuel** : affiche l'état actuel de l'autorisation du port. Si l'état est *Autorisé*, le port est authentifié ou le *Contrôle de port administratif* est en *Autorisation forcée*. À l'inverse, si l'état est *Non autorisé*, le port est non authentifié ou le *Contrôle de port administratif* est en *Non-autorisation forcée*.
- **Contrôle de port administratif** : affiche l'état d'autorisation du port administratif. Les options sont les suivantes :
  - *Non-autorisation forcée* : refuse l'accès à l'interface en passant cette dernière en mode non autorisé. Le périphérique ne fournit pas de services d'authentification au client via l'interface.
  - *Automatique* : active l'authentification et l'autorisation basées sur les ports sur le périphérique. L'interface bascule entre un état autorisé ou non autorisé en fonction de l'échange d'authentification entre le périphérique et le client.
  - *Autorisation forcée* : autorise l'interface sans authentification.
- **Open Access (Accès ouvert)** : sélectionnez cette option pour authentifier le port avec succès même en cas d'échec de l'authentification. Reportez-vous à la section **Open Access (Accès ouvert)**.
- **Authentification 802.1X** : l'authentification 802.1X est la seule méthode d'authentification appliquée sur le port.
- **Authentification MAC** : le port est authentifié en fonction de l'adresse MAC du demandeur. Seules huit authentifications basées sur MAC peuvent être utilisées sur le port.

  REMARQUE Pour que l'authentification MAC réussisse, le nom d'utilisateur et le mot de passe de demandeur du serveur RADIUS doivent être l'adresse MAC du demandeur. L'adresse MAC doit être en minuscules et saisie sans les séparateurs « . » ou « - », par exemple : 0020aa00bbcc.
- **Authentification Web** : Sélectionnez cette option pour activer l'authentification Web sur le commutateur.
- **Réauthentification périodique** : sélectionnez cette option pour autoriser les tentatives de réauthentification du port une fois la Période de réauthentification spécifiée expirée.

- **Reauthentication Period** : saisissez le délai (en secondes) au bout duquel le port sélectionné est réauthentifié.
- **Réauthentifier maintenant** : sélectionnez cette option pour permettre la réauthentification immédiate du port.
- **Authenticator State** : affiche l'état défini de l'autorisation du port. Les options sont les suivantes :
  - *Initialiser* : processus de démarrage.
  - *Force-Authorized* : l'état du port contrôlé est défini sur Force-Authorized (le trafic est réacheminé).

    REMARQUE Si le port n'est pas en Non-autorisation forcée, il est en mode automatique et l'authentificateur affiche l'état de l'authentification en cours. Une fois le port authentifié, l'état indique Authenticated.
- **Période** : affecte une limite au temps d'autorisation d'utilisation du port spécifique si 802.1X a été activé (Authentification basée sur les ports est coché).
- **Nom de période** : sélectionnez le profil qui spécifie la période.
- **Nombre d'hôtes max.** : entrez le nombre maximal d'hôtes autorisés dans l'interface. Sélectionnez **Infini** pour ne spécifier aucune limite ou **Défini par l'utilisateur** pour spécifier une limite.

  REMARQUE Définissez cette valeur à 1 pour simuler le mode Hôte unique pour l'authentification Web en mode Sessions multiples.
- **Période silencieuse** : saisissez le délai (en secondes) pendant lequel le périphérique reste en état silencieux après l'échec d'un échange d'authentification.
- **Renvoi d'EAP** : saisissez le nombre de secondes pendant lesquelles le périphérique attend une réponse à une demande/trame d'identité EAP (Extensible Authentication Protocol) du demandeur (client) avant de renvoyer la demande.
- **Max EAP Requests** : saisissez le nombre maximum de demandes EAP pouvant être envoyées. Si aucune réponse n'est reçue après la période définie (délai pour demandeur), le processus d'authentification est relancé.
- **Supplicant Timeout** : saisissez le nombre de secondes qui s'écoulent avant que les demandes EAP soient renvoyées au demandeur.
- **Délai pour serveur** : saisissez le nombre de secondes qui s'écoulent avant que le périphérique renvoie une demande au serveur d'authentification.

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres des ports sont écrits dans le fichier de Configuration d'exécution.

Définition de l'authentification des hôtes et sessions

La page Authentification hôtes et sessions permet de définir le mode de fonctionnement de 802.1X sur le port, ainsi que l'action à réaliser si une violation a été détectée.

Pour obtenir une explication de ces modes, reportez-vous à la section **Modes hôte de port**.

Pour définir les paramètres 802.1X avancés pour les ports :

ÉTAPE 1 Cliquez sur **Sécurité** > **Authentification 802.1X** > **Authentification hôtes et sessions**.

Les paramètres d'authentification 802.1X sont décrits pour tous les ports. Tous les champs à l'exception des suivants sont décrits sur la page **Modifier**.

- **Nombre de violations** : affiche le nombre de paquets qui arrivent sur l'interface en mode hôte unique en provenance d'un hôte dont l'adresse MAC ne correspond pas à celle du demandeur.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : entrez un numéro de port pour lequel l'authentification des hôtes est activée.
- **Authentification des hôtes** : sélectionnez l'un des modes. Ces modes sont décrits ci-dessus dans la rubrique **Modes hôte de port**.

Paramètres de violation d'hôte unique (option seulement affichée si l'authentification des hôtes est définie sur Hôte unique) :

- **Action en cas de violation** : sélectionnez l'action à appliquer aux paquets arrivant en mode session unique/hôte unique en provenance d'un hôte dont l'adresse MAC ne correspond pas à celle du demandeur. Les options sont les suivantes :
  - *Protéger (Abandonner)* : abandonne les paquets.
  - *Restreindre (Transférer)* : transfère les paquets.
  - *Arrêter* : abandonne les paquets et ferme le port. Les ports restent fermés jusqu'à ce qu'ils soient réactivés ou jusqu'à ce que le périphérique soit réinitialisé.
- **Message « trap »** : sélectionnez cette option pour activer les « traps ».
- **Fréquence des interceptions** : définit la fréquence d'envoi des interceptions à l'hôte. Ce champ ne peut être défini que si plusieurs hôtes sont désactivés.

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres sont consignés dans le fichier de Configuration d'exécution.

Affichage des hôtes authentifiés

Pour afficher des informations détaillées sur les utilisateurs authentifiés :

ÉTAPE 1 Cliquez sur **Sécurité** > **Authentification 802.1X** > **Hôtes authentifiés**.

Cette page affiche les champs suivants :

- **User Name** : nom des demandeurs authentifiés sur chaque port.
- **Port** : numéro du port.
- **Session Time (DD:HH:MM:SS)** : durée pendant laquelle le demandeur a été connecté au port.
- **Serveur d'authentification** : serveur RADIUS.
- **MAC Address** : affiche l'adresse MAC du demandeur.

REMARQUE Jusqu'à 5 utilisateurs HTTP et 1 utilisateur HTTPS peuvent demander simultanément l'authentification Web. Lorsque ces utilisateurs sont authentifiés, d'autres utilisateurs peuvent demander l'authentification.

21

Sécurité : Client SSH

Cette section décrit l'appareil lorsqu'il fonctionne en tant que client SSH.

Elle couvre les rubriques suivantes :

- **Secure Copy (SCP) et SSH**
- **Méthodes de protection**
- **Authentification du serveur SSH**
- **Authentification du client SSH**
- **Avant de commencer**
- **Tâches courantes**
- **Configuration du client SSH via l'interface utilisateur graphique (GUI)**

Secure Copy (SCP) et SSH

Secure Shell ou SSH est un protocole réseau qui permet aux données d'être échangées sur un canal sécurisé entre un client SSH (dans ce cas précis, l'appareil) et un serveur SSH.

Le client SSH aide l'utilisateur à gérer un réseau composé d'un ou plusieurs commutateurs dans lesquels différents systèmes de fichiers sont stockés sur un serveur SSH central. Lorsque les fichiers de configuration sont transférés via le réseau, Secure Copy (SCP), qui est une application utilisant le protocole SSH, s'assure que les données sensibles telles que le nom d'utilisateur/mot de passe ne sont pas interceptées.

Secure Copy (SCP) permet de transférer de manière sécurisée le micrologiciel, l'image d'amorçage, les fichiers de configuration, les fichiers de langue et les fichiers journaux d'un serveur SCP central vers un appareil.

En ce qui concerne SSH, la SCP exécutée sur l'appareil est une application client SSH et le serveur SCP est une application serveur SSH.

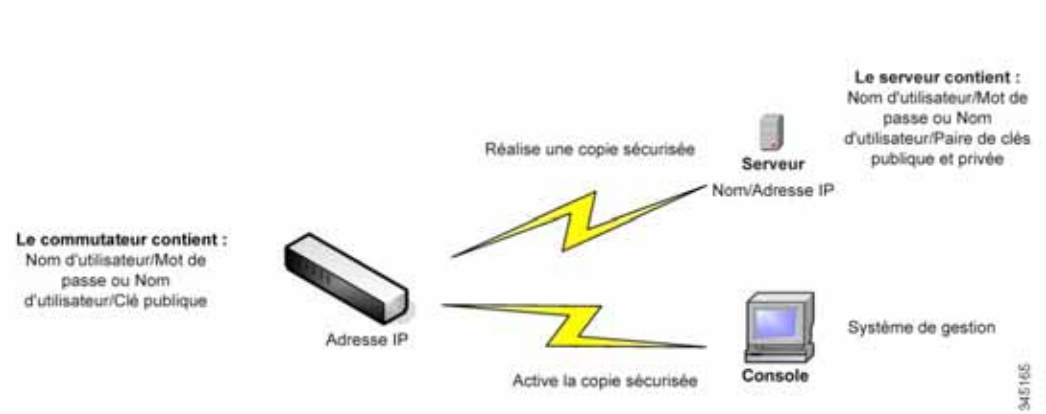
Lorsque des fichiers sont téléchargés via TFTP ou HTTP, les transfert des données n'est pas sécurisé.

Lorsque des fichiers sont téléchargés via SCP, les informations sont téléchargées du serveur SCP vers l'appareil via un canal sécurisé. La création de ce canal sécurisé est précédée d'une authentification, ce qui garantit que l'utilisateur est autorisé à effectuer l'opération.

Les informations d'authentification doivent être entrées par l'utilisateur sur l'appareil et le serveur SSH, même si ce guide ne décrit pas les opérations réalisées sur le serveur.

Vous trouverez ci-après la présentation d'une configuration réseau standard dans laquelle la fonctionnalité SCP peut être utilisée.

Configuration réseau standard



Méthodes de protection

Lorsque des données sont transférées d'un serveur SSH vers un appareil (client), le serveur SSH utilise différentes méthodes pour l'authentification client. Elles sont décrites ci-dessous.

Mots de passe

Pour utiliser la méthode du mot de passe, assurez-vous d'abord qu'un nom d'utilisateur/mot de passe a été défini sur le serveur SSH. Cette opération ne s'effectue pas via le système de gestion de l'appareil même si, lorsqu'un nom d'utilisateur a été défini sur le serveur, le mot de passe du serveur peut être modifié par l'intermédiaire de ce système de gestion.

Le nom d'utilisateur/mot de passe doit alors être créé directement sur l'appareil. Lorsque des données sont transférées du serveur vers l'appareil, le nom d'utilisateur/mot de passe fourni par l'appareil doit correspondre au nom d'utilisateur/mot de passe sur le serveur.

Les données peuvent être chiffrées à l'aide d'une clé symétrique unique négociée pendant la session.

Chaque appareil géré doit avoir son propre nom d'utilisateur/mot de passe, bien que le même nom d'utilisateur/mot de passe puisse être utilisé pour plusieurs commutateurs.

La méthode du mot de passe est la méthode par défaut sur l'appareil.

Clés publiques/privées

Pour utiliser la méthode de la clé publique/privée, créez un nom d'utilisateur et une clé publique sur le serveur SSH. Comme décrit ci-dessous, la clé publique est générée sur l'appareil, puis copiée vers le serveur. Les actions de création d'un nom d'utilisateur sur le serveur et de copie de la clé publique vers le serveur ne sont pas décrites dans ce guide.

Les paires de clés par défaut RSA et DSA sont générées pour l'appareil au démarrage de celui-ci. L'une de ces clés est utilisée pour crypter les données téléchargées à partir du serveur SSH. La clé RSA est utilisée par défaut.

Si l'utilisateur supprime l'une de ces clés, ou les deux, elles sont regénérées.

Les clés publique/privée sont chiffrées et stockées dans la mémoire de l'appareil. Les clés sont incluses dans le fichier de configuration de l'appareil et la clé privée peut être visualisée par l'utilisateur, sous forme chiffrée ou de texte en clair.

Puisque la clé privée ne peut pas être copiée directement vers la clé privée d'un autre appareil, une méthode d'importation vous permet de copier des clés privées d'un appareil à un autre (reportez-vous à la section **Importer des clés**).

Importer des clés

Dans le cadre de la méthode par clé, des clés publiques/privées individuelles doivent être créées pour chaque appareil. Ces clés privées ne peuvent pas, pour des raisons de sécurité, être copiées directement d'un appareil à un autre.

Si plusieurs commutateurs sont présents sur le réseau, le processus de création des clés publique/privée pour tous les commutateurs peut prendre beaucoup de temps, car chaque clé publique/privée doit être créée puis chargée sur le serveur SSH.

Pour faciliter ce processus, une autre fonction permet le transfert sécurisé de la clé privée chiffrée vers tous les commutateurs du système.

Lorsqu'une clé privée est créée sur un appareil, un *mot de passe* peut être défini et associé à cette clé. Ce mot de passe permet de crypter la clé privée et de l'importer dans les commutateurs restants. De cette manière, tous les commutateurs peuvent utiliser la même clé publique/privée.

Authentification du serveur SSH

En tant que clients SSH, les appareils communiquent seulement avec les serveur SSH de confiance. Lorsque l'authentification du serveur SSH est désactivée (paramètre par défaut), tout serveur SSH est considéré comme étant de confiance. Lorsque l'authentification du serveur SSH est activée, l'utilisateur doit ajouter une entrée pour les serveurs de confiance dans la Table des serveurs SSH de confiance. Cette table stocke les informations suivantes pour chaque serveur SSH de confiance, pour un maximum de 16 serveurs :

- Adresse IP/nom d'hôte du serveur
- Empreinte de clé publique du serveur

Lorsque l'authentification du serveur SSH est activée, le client SSH exécuté sur l'appareil authentifie le serveur SSH à l'aide du processus d'authentification suivant :

- L'appareil calcule l'empreinte de la clé publique du serveur SSH reçue.
- Le périphérique recherche l'adresse IP/le nom d'hôte du serveur SSH dans la Table des serveurs SSH de confiance. Trois cas peuvent se présenter :
  - Si une correspondance est trouvée pour l'adresse IP/le nom d'hôte du serveur et son empreinte, le serveur est authentifié.
  - Si une adresse IP/un nom d'hôte correspondant(e) est trouvé(e), mais qu'il n'y a aucune empreinte associée, la recherche continue. Si aucune empreinte correspondante n'est trouvée, la recherche prend fin et l'authentification échoue.
  - Si aucune adresse IP/aucun nom d'hôte correspondant(e) n'est trouvé(e), la recherche prend fin et l'authentification échoue.
- Si l'entrée du serveur SSH n'est pas trouvée dans la liste des serveurs de confiance, le processus échoue.

Authentification du client SSH

L'authentification du client SSH par mot de passe est activée par défaut, le nom d'utilisateur/mot de passe étant « anonyme ».

L'utilisateur doit configurer les informations suivantes pour l'authentification :

- La méthode d'authentification à utiliser.
- Le nom d'utilisateur/mot de passe ou la paire de clés publique/privée.

Afin de prendre en charge la configuration automatique d'un appareil directement opérationnel (appareil avec configuration d'usine), l'authentification du serveur SSH est désactivée par défaut.

Algorithmes pris en charge

Lorsque la connexion entre un appareil (en tant que client SSH) et un serveur SSH est établie, le client et le serveur SSH échangent des données afin de déterminer les algorithmes à utiliser dans la couche transport SSH.

Les algorithmes suivants sont pris en charge côté client :

- Algorithme d'échange de clés Diffie-Hellman
- Algorithmes de cryptage
  - aes128-cbc
  - 3des-cbc
  - arcfour
  - aes192-cbc
  - aes256-cbc
- Algorithmes de code d'authentification de message
  - hmac-sha1
  - hmac-md5

REMARQUE Les algorithmes de compression ne sont pas pris en charge.

Avant de commencer

Vous devez effectuer les actions suivantes avant d'utiliser la fonction SCP :

- Lorsque vous utilisez la méthode d'authentification par mot de passe, un nom d'utilisateur/mot de passe doit être configuré sur le serveur SSH.
- Lorsque vous utilisez la méthode d'authentification par clés publique/privée, la clé publique doit être stockée sur le serveur SSH.

Tâches courantes

Cette section décrit quelques tâches courantes réalisées à l'aide du client SSH. Toutes les pages référencées sont disponibles sous la branche Client SSH de l'arborescence du menu.

Flux de travail 1 : pour configurer le client SSH et transférer des données de/vers un serveur SSH, procédez comme suit :

ÉTAPE 1 Choisissez la méthode à utiliser : mot de passe ou clé publique/privée. Utilisez la page Authentification des utilisateurs SSH.

ÉTAPE 2 Si la méthode du mot de passe a été sélectionnée, procédez comme suit :

a. Créez un mot de passe global sur la page Authentification des utilisateurs SSH ou créez un mot de passe temporaire sur la page Mettre à niveau/sauvegarder micrologiciel/langue ou la page Télécharger/sauvegarder configuration/journal, au moment où vous activez le transfert de données sécurisé.

b. Mettez à niveau le micrologiciel, l'image d'amorçage ou le fichier de langue via SCP en sélectionnant l'option **via SCP (sur SSH)** de la page Mettre à niveau/sauvegarder micrologiciel/langue. Vous pouvez saisir le mot de passe directement dans cette page ou utiliser le mot de passe saisi à l'aide de la page Authentification des utilisateurs SSH.

c. Téléchargez/sauvegardez le fichier de configuration, via SCP, en sélectionnant l'option **via SCP (sur SSH)** sur la page Télécharger/sauvegarder configuration/journal. Vous pouvez saisir le mot de passe directement dans cette page ou utiliser le mot de passe saisi à l'aide de la page Authentification des utilisateurs SSH.

ÉTAPE 3 Configurez les nom d'utilisateur et mot de passe sur le serveur SSH ou modifiez le mot de passe existant, sur ce même serveur. Cette activité dépend du serveur et n'est pas décrite ici.

ÉTAPE 4 Si la méthode de la clé publique/privée est utilisée, procédez comme suit :

a. Indiquez si vous souhaitez utiliser une clé RSA ou DSA, créez un nom d'utilisateur, puis générez les clés publique/privée.

b. Affichez la clé générée en cliquant sur le bouton **Détails**, puis transférez le nom d'utilisateur et la clé publique vers le serveur SSH. Cette action dépend du serveur et n'est pas décrite dans ce guide.

c. Mettez à niveau/sauvegardez le micrologiciel ou le fichier de langue via SCP en sélectionnant l'option **via SCP (sur SSH)** de la page Mettre à niveau/sauvegarder micrologiciel/langue.

d. Téléchargez/sauvegardez le fichier de configuration, via SCP, en sélectionnant l'option **via SCP (sur SSH)** sur la page Télécharger/sauvegarder configuration/journal.

Flux de travail 2 : pour importer des clés publiques/privées d'un appareil vers un autre :

ÉTAPE 1 Générez une clé publique/privée sur la page Authentification des utilisateurs SSH.

ÉTAPE 2 Définissez les propriétés SSD, puis créez un nouveau mot de passe local sur la page Gestion sécurisée des données confidentielles > Propriétés.

ÉTAPE 3 Cliquez sur **Détails** pour afficher les clés chiffrées générées, puis copiez-les (y compris les pieds de page Début et Fin) de la page Détails vers un appareil externe. Copiez séparément les clés publique et privée.

ÉTAPE 4 Connectez-vous à un autre appareil, puis ouvrez la page Authentification des utilisateurs SSH. Sélectionnez le type de clé requis, puis cliquez sur **Modifier**. Collez-le dans les clés publiques/privées.

ÉTAPE 5 Cliquez sur **Appliquer** pour copier les clés publiques/privées vers le deuxième appareil.

Flux de travail 3 : pour modifier votre mot de passe sur un serveur SSH :

ÉTAPE 1 Identifiez le serveur sur la page Modifier le mot de passe utilisateur du serveur SSH.

ÉTAPE 2 Saisissez le nouveau mot de passe.

ÉTAPE 3 Cliquez sur **Apply**.

Configuration du client SSH via l'interface utilisateur graphique (GUI)

Cette section décrit les pages utilisées pour configurer la fonction Client SSH.

Authentification des utilisateurs SSH

Utilisez cette page pour sélectionner une méthode d'authentification des utilisateurs SSH, définir un nom d'utilisateur et un mot de passe sur l'appareil, si la méthode du mot de passe est sélectionnée ou générer une clé RSA ou DSA, si la méthode de la clé publique/privée est sélectionnée.

Pour sélectionner une méthode d'authentification et définir le nom d'utilisateur/le mot de passe/les clés :

ÉTAPE 1 Cliquez sur **Sécurité** > **Client SSH** > **Authentification des utilisateurs SSH**.

ÉTAPE 2 Sélectionnez une **Méthode d'authentification des utilisateurs SSH**. Il s'agit de la méthode globale définie pour la copie sécurisée (SCP). Sélectionnez l'une des options disponibles :

- **Par mot de passe** : il s'agit du paramètre par défaut. Si vous sélectionnez cette option, conservez le mot de passe par défaut ou saisissez-en un nouveau.
- **Par clé publique RSA** : si vous sélectionnez cette option, créez une clé privée et publique RSA dans le bloc **Table des clés des utilisateurs SSH**.

- **Par clé publique DSA** : si vous sélectionnez cette option, créez une clé privée et publique DSA dans le bloc **Table des clés des utilisateurs SSH**.

ÉTAPE 3 Saisissez le **Nom d'utilisateur** (peu importe la méthode sélectionnée) ou conservez le nom d'utilisateur par défaut. Il doit correspondre au nom d'utilisateur défini sur le serveur SSH.

ÉTAPE 4 Si la méthode *Par mot de passe* a été sélectionnée, entrez un mot de passe (**Chiffré** ou **Texte en clair**) ou conservez le mot de passe chiffré par défaut.

ÉTAPE 5 Effectuez l'une des actions suivantes :

- **Appliquer** : les méthodes d'authentification sélectionnées sont associées à la méthode d'accès.
- **Restaurer les infos d'identification par défaut** : le nom d'utilisateur et le mot de passe (anonymes) par défaut sont restaurés.
- **Afficher les données sensibles en texte clair** : les données sensibles de la page actuelle sont affichées sous forme de texte en clair.

La **Table des clés des utilisateurs SSH** affiche les champs suivants pour chaque clé :

- **Type de clé** : RSA ou DSA.
- **Source de la clé** : Autogénérée ou Définie par l'utilisateur.
- **Empreinte** : empreinte générée à partir de la clé.

ÉTAPE 6 Pour gérer une clé RSA ou DSA, sélectionnez RSA ou DSA et effectuez l'une des actions suivantes :

- **Générer** : générez une nouvelle clé.
- **Modifier** : affichez les clés pour effectuer un copier/coller vers un autre appareil.
- **Supprimer** : supprimez la clé.
- **Détails** : affichez les clés.

Authentification du serveur SSH

Pour activer l'authentification du serveur SSH et définir les serveurs de confiance :

ÉTAPE 1 Cliquez sur **Sécurité** > **Client SSH** > **Authentification du serveur SSH**.

ÉTAPE 2 Sélectionnez **Activer** pour activer l'authentification du serveur SSH.

- **Interface source IPv4** : sélectionnez l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source pour les messages utilisés dans les communications avec les serveurs SSH IPv4.
- **Interface source IPv6** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source pour les messages utilisés dans les communications avec les serveurs SSH IPv6.

REMARQUE Si l'option Auto est sélectionnée, le système récupère l'adresse IP source de l'adresse IP définie dans l'interface sortante.

ÉTAPE 3 Cliquez sur **Ajouter** et renseignez les champs suivants pour le serveur de confiance SSH :

- **Définition du serveur** : sélectionnez l'une des méthodes d'identification du serveur SSH ci-après :
  - *Par adresse IP* : si vous avez sélectionné cette option, entrez l'adresse IP du serveur dans les champs situés au-dessous.
  - *Par nom* : si vous avez sélectionné cette option, entrez le nom du serveur dans le champ **Nom/ Adresse IP du serveur**.
- **Version IP** : si vous avez choisi de définir le serveur SSH par son adresse IP, indiquez s'il s'agit d'une adresse IPv6 IPv4.
- **Type d'adresse IP** : si l'adresse IP du serveur SSH est une adresse IPv6, sélectionnez le type d'adresse correspondant, à savoir IPv6. Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe FE80, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez, dans la liste des interfaces, l'interface de liaison locale.
- **Adresse IP/Nom serveur** : saisissez l'adresse IP ou le nom du serveur SSH, selon l'information sélectionnée dans le champ **Définition de serveur**.
- **Empreinte** : entrez l'empreinte du serveur SSH (copiée à partir de ce serveur).

ÉTAPE 4 Cliquez sur **Apply**. La définition du serveur de confiance est stockée dans le fichier de Configuration d'exécution.

Modification du mot de passe utilisateur du serveur SSH

Pour modifier un mot de passe sur un serveur SSH :

ÉTAPE 1 Cliquez sur **Sécurité** > **Client SSH** > **Modifier le mot de passe utilisateur du serveur SSH**.

ÉTAPE 2 Renseignez les champs suivants :

- **Définition de serveur** : définissez le serveur SSH en sélectionnant **Par adresse IP** ou **Par nom**. Saisissez le nom ou l'adresse IP du serveur dans le champ **Adresse IP/Nom serveur**.
- **Version IP** : si vous avez choisi de définir le serveur SSH par son adresse IP, indiquez s'il s'agit d'une adresse IPv6 IPv4.
- **Type d'adresse IP** : si l'adresse IP du serveur SSH est une adresse IPv6, sélectionnez le type d'adresse correspondant, à savoir IPv6. Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe FE80, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez, dans la liste des interfaces, l'interface de liaison locale.
- **Adresse IP/Nom serveur** : saisissez l'adresse IP ou le nom du serveur SSH, selon l'information sélectionnée dans le champ **Définition de serveur**.
- **Nom d'utilisateur** : doit correspondre au nom d'utilisateur défini sur le serveur.
- **Ancien mot de passe** : doit correspondre au mot de passe défini sur le serveur.
- **Nouveau mot de passe** : saisissez le nouveau mot de passe, puis confirmez-le dans le champ **Confirmer le mot de passe**.

ÉTAPE 3 Cliquez sur **Apply**. Le mot de passe du serveur SSH a été modifié.

22

Sécurité : Gestion sécurisée des données confidentielles

Secure Sensitive Data (SSD) est une architecture qui simplifie la protection des données confidentielles, comme les mots de passe et les clés, sur un appareil. Cette fonctionnalité utilise les mots de passe, le cryptage, le contrôle d'accès et l'authentification des utilisateurs afin de fournir une solution sécurisée pour la gestion des données confidentielles.

Elle a été étendue afin de protéger l'intégrité des fichiers de configuration, sécuriser le processus de configuration et prendre en charge la configuration automatique sans intervention SSD.

- **Introduction**
- **Règles SSD**
- **Propriétés SSD**
- **Fichiers de configuration**
- **Canaux de gestion SSD**
- **Interface de ligne de commande (CLI) et récupération du mot de passe**
- **Configuration de SSD**

Introduction

SSD protège les données confidentielles présentes sur un appareil, telles que les mots de passe et les clés, autorise et refuse l'accès aux données confidentielles sous forme chiffrée et de texte en clair en fonction des informations d'identification de l'utilisateur et des règles SSD, mais protège également contre toute altération des fichiers de configuration contenant des données confidentielles.

En outre, SSD permet la sauvegarde et le partage sécurisés des fichiers de configuration qui contiennent des données confidentielles.

SSD offre aux utilisateurs la flexibilité de configurer le niveau de protection souhaité pour leurs données confidentielles ; à savoir aucune protection des données confidentielles sous forme de texte en clair, une protection minimale avec un cryptage basé sur le mot de passe par défaut ou une protection améliorée avec un cryptage basé sur le mot de passe défini par l'utilisateur.

SSD accorde une autorisation en lecture sur les données confidentielles uniquement aux utilisateurs authentifiés et autorisés, et conformément aux règles SSD. Un appareil authentifie et autorise l'accès de gestion pour les utilisateurs par l'intermédiaire du processus d'authentification des utilisateurs.

Que vous utilisiez ou non SSD, il est recommandé que l'administrateur sécurise le processus d'authentification par l'intermédiaire de la base de données d'authentification locale, et/ou sécurise la communication vers les serveurs d'authentification externes utilisés dans le processus d'authentification des utilisateurs.

En résumé, SSD protège les données sensibles sur un appareil à l'aide des règles SSD, des propriétés SSD et de l'authentification des utilisateurs. Et les règles SSD, les propriétés SSD et les configurations d'authentification des utilisateurs sur l'appareil sont elles-mêmes des données protégées par SSD.

Gestion de SSD

La gestion SSD inclut un ensemble de paramètres de configuration qui définissent le traitement et la sécurité des données confidentielles. Les paramètres de configuration SSD eux-mêmes sont des données confidentielles et sont protégés par SSD.

Toute la configuration de SSD s'effectue via les pages SSD qui sont uniquement disponibles pour les utilisateurs disposant des autorisations appropriées (reportez-vous à la section **Règles SSD**).

Règles SSD

Les règles SSD définissent les autorisations en lecture et le mode de lecture par défaut attribués à une session utilisateur sur un canal de gestion.

Une règle SSD est identifiée de manière unique par son utilisateur et le canal de gestion SSD. Il peut y avoir différentes règles SSD pour le même utilisateur mais pour différents canaux. Inversement, il peut y avoir différentes règles pour le même canal, mais pour différents utilisateurs.

Les autorisations en lecture déterminent la façon dont les données confidentielles peuvent être affichées : sous forme chiffrée uniquement, sous forme de texte en clair uniquement, sous forme chiffrée ou de texte en clair, ou aucune autorisation d'afficher les données confidentielles. Les règles SSD elles-mêmes sont protégées en tant que données confidentielles.

Un appareil peut prendre en charge un total de 32 règles SSD.

Un appareil accorde à un utilisateur l'autorisation en lecture SSD de la règle SSD qui correspond le mieux à l'identité/aux informations d'identification de l'utilisateur et au type de canal de gestion à partir duquel l'utilisateur accède ou accédera aux données confidentielles.

À l'origine, un appareil comporte un ensemble de règles SSD par défaut. Un administrateur peut ajouter, supprimer et modifier des règles SSD comme il le souhaite.

REMARQUE Il se peut qu'un appareil ne puisse pas prendre en charge tous les canaux définis par SSD.

Éléments d'une règle SSD

Une règle SSD inclut les éléments suivants :

- **Type d'utilisateur** : les types d'utilisateur pris en charge dans l'ordre de préférence (de la plus haute à la plus basse) sont les suivants : (Si un utilisateur correspond à plusieurs règles SSD, la règle avec le Type d'utilisateur ayant la préférence la plus haute sera appliquée).
  - **Spécifique** : la règle s'applique à un utilisateur spécifique.
  - **Utilisateur par défaut (cisco)** : la règle s'applique à l'utilisateur par défaut (cisco).
  - **Niveau 15** : la règle s'applique aux utilisateurs ayant le niveau de privilège 15.
  - **Tous** : la règle s'applique à tous les utilisateurs.
- **Nom d'utilisateur** : si le type d'utilisateur est Spécifique, un nom d'utilisateur est requis.
- **Canal** type de canal de gestion SSD auquel la règle s'applique. Les types de canaux pris en charge sont :
  - **Sécurisé** : spécifie que la règle s'applique uniquement aux canaux sécurisés. Selon le périphérique, elle peut prendre en charge tous les canaux sécurisés suivants ou seulement certains d'entre eux :
    Interface de port de console, SCP, SSH et HTTPS.
  - **Non sécurisé** : spécifie que cette règle s'applique uniquement aux canaux non sécurisés. Selon le périphérique, elle peut prendre en charge tous les canaux non sécurisés suivants ou seulement certains d'entre eux :
    Telnet, TFTP et HTTP.
  - **SNMP XML sécurisé** : spécifie que cette règle s'applique uniquement au XML sur HTTPS ou SNMPv3 avec confidentialité. Un appareil est susceptible de ne pas prendre en charge tous les canaux XML et SNMP sécurisés.
  - **SNMP XML non sécurisé** : spécifie que cette règle s'applique uniquement au XML sur HTTP ou SNMPv1/v2 et SNMPv3 sans confidentialité. Un appareil est susceptible de ne pas prendre en charge tous les canaux XML et SNMP sécurisés.

- **Autorisation en lecture** : autorisations en lecture associées aux règles. Elles peuvent être les suivantes :
  - (Basse) **Exclure** : les utilisateurs ne sont pas autorisés à accéder aux données confidentielles sous quelque forme que ce soit.
  - (Moyenne) **Chiffré uniquement** : les utilisateurs sont autorisés à accéder aux données confidentielles sous forme chiffrée uniquement.
  - (Haute) **Texte en clair uniquement** : les utilisateurs sont autorisés à accéder aux données confidentielles sous forme de texte en clair uniquement. Les utilisateurs sont également autorisés à accéder aux paramètres SSD en lecture et en écriture.
  - (Très haute) **Les deux** : les utilisateurs ont les autorisations Chiffré et Texte en clair, et sont autorisés à accéder aux données confidentielles sous forme chiffrée et de texte en clair. Les utilisateurs sont également autorisés à accéder aux paramètres SSD en lecture et en écriture.

  Chaque canal de gestion permet des autorisations en lecture spécifiques. Elles sont récapitulées dans le tableau suivant.

Canal de gestion	Options d'autorisation en lecture permises
Sécurisé	Les deux, Chiffré uniquement
Non sécurisé	Les deux, Chiffré uniquement
SNMP XML sécurisé	Exclure, Texte en clair uniquement
SNMP XML non sécurisé	Exclure, Texte en clair uniquement

- **Mode de lecture par défaut** : tous les modes de lecture par défaut sont sujets à l'autorisation en lecture de la règle. Les options suivantes sont disponibles, mais certaines sont susceptibles d'être refusées en fonction de l'autorisation en lecture. Si l'autorisation en lecture définie par l'utilisateur pour un utilisateur est Exclure (par exemple), et que le mode de lecture par défaut est Chiffré, l'autorisation en lecture définie par l'utilisateur s'applique.
  - **Exclure** : n'autorise pas la lecture des données confidentielles.
  - **Chiffré** : les données confidentielles sont présentées sous forme chiffrée.
  - **Texte en clair** : les données confidentielles sont présentées sous forme de texte en clair.

Chaque canal de gestion permet des autorisations en lecture spécifiques. Elles sont récapitulées dans le tableau suivant.

Autorisation en lecture	Mode de lecture par défaut autorisé
Exclure	Exclure
Chiffré uniquement	*Chiffré
Texte en clair uniquement	*Texte en clair
Les deux	*Texte en clair, Chiffré

* Le mode de lecture d'une session peut être temporairement changé sur la page Propriétés SSD si le nouveau mode de lecture n'enfreint pas l'autorisation en lecture.

REMARQUE Notez les éléments suivants :

- Le mode de lecture par défaut pour les canaux de gestion SNMP XML sécurisé et SNMP XML non sécurisé doit être identique à leur autorisation en lecture.
- L'autorisation en lecture Exclure est uniquement permise pour les canaux de gestion SNMP XML sécurisé et SNMP XML non sécurisé ; l'autorisation Exclure n'est pas permise pour les canaux sécurisés et non sécurisés standard.
- L'exclusion des données confidentielles dans les canaux de gestion SNMP XML sécurisé et SNMP XML non sécurisé indique que les données confidentielles sont présentées en tant que 0 (ce qui signifie une chaîne nulle ou numérique 0). Si l'utilisateur souhaite afficher les données confidentielles, la règle doit être changée en texte en clair.
- Par défaut, un utilisateur SNMPv3 ayant des autorisations de canaux confidentiels et XML-over-secure est considéré comme un utilisateur de niveau 15.
- Les utilisateurs SNMP sur un canal SNMP et XML non sécurisé (SNMPv1, v2 et v3 sans confidentialité) sont considérés comme Tous les utilisateurs.
- Les noms de communauté SNMP ne sont pas utilisés comme noms d'utilisateur pour correspondre aux règles SSD.
- L'accès d'un utilisateur SNMPv3 spécifique peut être contrôlé en configurant une règle SSD avec un nom d'utilisateur qui correspond au nom d'utilisateur SNMPv3.
- Il doit toujours y avoir au moins une règle avec une autorisation en lecture : Texte en clair uniquement ou Les deux, car seuls les utilisateurs qui disposent de ces autorisations peuvent accéder aux pages SSD.

- Les changements apportés au mode de lecture par défaut et aux autorisations en lecture d'une règle deviennent effectifs et sont appliqués aux utilisateurs concernés et au canal de toutes les sessions de gestion actives immédiatement, à l'exclusion de la session qui effectue les changements même si la règle est applicable. Lorsqu'une règle est changée (ajout, suppression, modification), un système met à jour toutes les sessions CLI/GUI concernées.

  REMARQUE Lorsque la règle SSD appliquée lors de la connexion à une session est modifiée à partir de cette session, l'utilisateur doit se déconnecter puis se reconnecter pour voir la modification.

  REMARQUE Lors d'un transfert de fichier initié par une commande XML ou SNMP, le protocole sous-jacent utilisé est TFTP. Par conséquent, la règle SSD du canal non sécurisé s'appliquera.

Règles SSD et authentification des utilisateurs

SSD accorde une autorisation SSD uniquement aux utilisateurs authentifiés et autorisés, et conformément aux règles SSD. Un appareil dépend de son processus d'authentification des utilisateurs pour authentifier et autoriser l'accès de gestion. Pour protéger un appareil et ses données contre tout accès non autorisé, y compris les données confidentielles et les configurations SSD, il est recommandé de sécuriser le processus d'authentification des utilisateurs. Pour sécuriser le processus d'authentification des utilisateurs, vous pouvez utiliser la base de données d'authentification locale, mais aussi sécuriser la communication via les serveurs d'authentification externes, tels qu'un serveur RADIUS. La configuration de la communication sécurisée vers les serveurs d'authentification externes constitue des données confidentielles et est protégée par SSD.

REMARQUE Les informations d'identification des utilisateurs contenues dans la base de données d'authentification locale sont déjà protégées par un mécanisme non lié à SSD.

Si un utilisateur présent sur un canal exécute une action qui utilise un autre canal, l'appareil applique l'autorisation en lecture et le mode de lecture par défaut à partir de la règle SSD qui correspond aux informations d'identification des utilisateurs et à l'autre canal. Par exemple, si un utilisateur se connecte via un canal sécurisé et démarre une session de chargement TFTP, l'autorisation en lecture SSD de l'utilisateur sur le canal non sécurisé (TFTP) est appliquée.

Règles SSD par défaut

Les règles par défaut suivantes sont définies pour l'appareil :

Tableau 1

Clé de règle		Action de règle	
Utilisa-teur	Canal	Autorisation en lecture	Mode de lecture par défaut
Niveau 15	SNMP XML sécurisé	Texte en clair uniquement	Texte en clair
Niveau 15	Sécurisé	Les deux	Chiffré

Tableau 1

Clé de règle		Action de règle	
Utilisa-teur	Canal	Autorisation en lecture	Mode de lecture par défaut
Niveau 15	Non sécurisé	Les deux	Chiffré
Toutes	SNMP XML non sécurisé	Exclure	Exclure
Toutes	Sécurisé	Chiffré uniquement	Chiffré
Toutes	Non sécurisé	Chiffré uniquement	Chiffré

Il est possible de modifier les règles par défaut, mais pas de les supprimer. Si les règles par défaut SSD ont été modifiées, elles peuvent être restaurées.

Remplacement du mode de lecture par défaut SSD de la session

Le système affiche les données confidentielles dans une session, sous forme chiffrée ou de texte en clair, en fonction de l'autorisation en lecture et du mode de lecture par défaut de l'utilisateur.

Le mode de lecture par défaut peut être temporairement remplacé tant que cela n'occasionne pas de conflit avec l'autorisation en lecture SSD de la session. Cette modification est effective immédiatement dans la session actuelle, jusqu'à ce que l'un des événements suivants se produise :

- L'utilisateur le change à nouveau.
- La session est terminée.
- L'autorisation en lecture de la règle SSD qui est appliquée à l'utilisateur de la session est modifiée et n'est plus compatible avec le mode de lecture actuel de la session. Dans ce cas, le mode de lecture de la session redevient le mode de lecture par défaut de la règle SSD.

Propriétés SSD

Les propriétés SSD sont un ensemble de paramètres qui, conjointement avec les règles SSD, définissent et contrôlent l'environnement SSD d'un appareil. L'environnement SSD comporte les propriétés suivantes :

- Contrôle de la façon dont les données confidentielles sont chiffrées.
- Contrôle du niveau de sécurité sur les fichiers de configuration.
- Contrôle de la façon dont les données confidentielles sont affichées dans la session en actuelle.

Mot de passe

Le mot de passe constitue la base du mécanisme de sécurité dans la fonction SSD. Il permet de générer la clé de cryptage et de décryptage des données confidentielles. Les commutateurs Sx200, Sx300, Sx500 et SG500X/SG500XG/ESW2-550X qui ont le même mot de passe peuvent décrypter mutuellement leurs données confidentielles qui ont été cryptées avec la clé générée à partir du mot de passe en question.

Un mot de passe doit respecter les règles suivantes :

- **Longueur** : entre 8 et 16 caractères.
- **Classes de caractères** : le mot de passe doit comporter au moins un caractère en majuscule, un caractère en minuscule, un chiffre et un caractère spécial (# ou $, par exemple).

Mot de passe par défaut et mot de passe défini par l'utilisateur

Tous les appareils disposent d'un mot de passe par défaut qui est transparent pour les utilisateurs. Le mot de passe par défaut ne s'affiche jamais dans le fichier de configuration ou la CLI/GUI.

Pour bénéficier d'une meilleure sécurité et d'une meilleure protection, un administrateur doit configurer SSD sur un appareil, afin qu'il utilise un mot de passe défini par l'utilisateur au lieu du mot de passe par défaut. Un mot de passe défini par l'utilisateur doit être gardé secret pour que la sécurité des données confidentielles sur l'appareil ne soit pas compromise.

Un mot de passe défini par l'utilisateur peut être configuré manuellement sous forme de texte en clair. Il peut aussi être issu d'un fichier de configuration (Reportez-vous à la section **Configuration automatique sans intervention des données confidentielles**.) Un appareil affiche toujours sous forme chiffrée les mots de passe définis par l'utilisateur.

Mot de passe local

Un appareil conserve un mot de passe local qui est celui de sa configuration d'exécution. SSD effectue normalement le cryptage et le décryptage des données confidentielles avec la clé générée à partir du mot de passe local.

Le mot de passe local peut être configuré pour être le mot de passe par défaut ou un mot de passe défini par l'utilisateur. Par défaut, le mot de passe local et le mot de passe par défaut sont identiques. Il peut être changé via des actions d'administration à partir de l'interface de ligne de commande (si disponible) ou de l'interface Web. Il est automatiquement remplacé par le mot de passe figurant dans le fichier de Configuration de démarrage lorsque la configuration de démarrage devient la configuration active de l'appareil. Lorsqu'un appareil est réinitialisé à ses valeurs par défaut, le mot de passe local est réinitialisé au mot de passe par défaut.

Contrôle du mot de passe du fichier de configuration

Le contrôle du mot de passe du fichier constitue une protection supplémentaire pour un mot de passe défini par l'utilisateur, et les données confidentielles qui sont chiffrées avec la clé générée à partir du mot de passe défini par l'utilisateur, dans les fichiers de configuration textuels.

Les modes de contrôle du mot de passe existants sont indiqués ci-après :

- **Sans restriction** (par défaut) : l'appareil inclut son mot de passe lors de la création d'un fichier de configuration. Cela permet à tout appareil qui accepte le fichier de configuration d'apprendre le mot de passe à partir du fichier.
- **Restreint** : l'appareil empêche l'exportation de son mot de passe vers un fichier de configuration. Le mode Restreint protège les données confidentielles chiffrées présentes dans un fichier de configuration contre les appareils qui ne disposent pas de mot de passe. Ce mode doit être utilisé lorsqu'un utilisateur ne souhaite pas exposer le mot de passe dans un fichier de configuration.

Une fois qu'un appareil a été réinitialisé à ses valeurs par défaut, son mot de passe local est réinitialisé au mot de passe par défaut. Ainsi, l'appareil ne pourra plus décrypter les données confidentielles chiffrées à partir d'un mot de passe défini par l'utilisateur qui a été entré depuis une session de gestion (GUI/CLI), ou dans tout fichier de configuration avec le mode Restreint, y compris les fichiers créés par l'appareil lui-même avant qu'il ne soit réinitialisé à ses valeurs par défaut. Cette situation reste inchangée tant que l'appareil n'est pas manuellement reconfiguré avec le mot de passe défini par l'utilisateur ou qu'il n'apprend pas le mot de passe défini par l'utilisateur à partir d'un fichier de configuration.

Contrôle de l'intégrité du fichier de configuration

Un utilisateur peut protéger un fichier de configuration contre toute altération ou modification en créant le fichier de configuration avec le Contrôle de l'intégrité du fichier de configuration. Il est recommandé d'activer le Contrôle de l'intégrité du fichier de configuration lorsqu'un appareil utilise un mot de passe défini par l'utilisateur et que le Contrôle du mot de passe du fichier de configuration est défini sur Sans restriction.

ATTENTION Toute modification apportée à un fichier configuration dont l'intégrité est protégée est considérée comme une altération.

Un appareil détermine si l'intégrité d'un fichier de configuration est protégée en examinant la commande Contrôle de l'intégrité du fichier dans le bloc de contrôle SSD du fichier. Si la protection de l'intégrité est définie pour un fichier, mais qu'un appareil détecte que l'intégrité du fichier n'est pas intacte, l'appareil refuse le fichier. Sinon, le fichier est accepté pour traitement ultérieur.

Un appareil vérifie l'intégrité d'un fichier de configuration textuel lorsque le fichier est téléchargé ou copié vers le fichier de Configuration de démarrage.

Mode Lecture

Chaque session comporte un mode de lecture. Il détermine la façon dont les données confidentielles s'affichent. Le mode de lecture peut être Texte en clair, auquel cas les données confidentielles apparaissent en texte normal ou Chiffré, auquel cas les données confidentielles apparaissent sous forme chiffrée.

Fichiers de configuration

Un fichier de configuration contient la configuration d'un appareil. Un appareil comporte un fichier de Configuration d'exécution, un fichier de Configuration de démarrage, un fichier de Configuration miroir (facultatif) et un fichier de Configuration de secours. Un utilisateur peut charger et télécharger un fichier de configuration de et vers un serveur de fichiers distant. Un appareil peut télécharger automatiquement sa configuration de démarrage à partir d'un serveur de fichiers distant pendant l'étape de configuration automatique via DHCP. Les fichiers de configuration stockés sur des serveurs de fichiers distants sont appelés des fichiers de configuration à distance.

Un fichier de Configuration d'exécution contient la configuration actuellement utilisée par un appareil. La configuration dans un fichier de Configuration de démarrage devient la configuration d'exécution une fois le redémarrage effectué. Les fichiers de Configuration d'exécution et de Configuration de démarrage ont un format interne. Les fichiers de Configuration miroir, de secours et à distance sont des fichiers textuels qui sont généralement stockés à des fins d'archivage, d'enregistrement ou de récupération. Lors de la copie, du chargement et du téléchargement d'un fichier de configuration source, un appareil convertit automatiquement le contenu source dans le format du fichier de destination si les deux fichiers ont un format différent.

Indicateur SSD de fichier

Lors de la copie du fichier de Configuration d'exécution ou de démarrage dans un fichier de configuration textuel, l'appareil génère et place l'indicateur SSD de fichier dans le fichier de configuration textuel pour indiquer si le fichier contient des données confidentielles sous forme chiffrée, des données confidentielles sous forme de texte en clair, ou s'il exclut les données confidentielles.

- L'indicateur SSD, s'il existe, doit se trouver dans le fichier d'en-tête de configuration.
- Une configuration textuelle qui n'inclut pas d'indicateur SSD ne contient normalement pas de données confidentielles.
- L'indicateur SSD permet d'appliquer les autorisations en lecture SSD à des fichiers de configuration textuels, mais il est ignoré lors de la copie des fichiers de configuration vers le fichier de Configuration d'exécution ou de démarrage.

L'indicateur SSD dans un fichier est défini conformément à l'instruction de l'utilisateur, au cours de la copie, pour inclure les données confidentielles sous forme chiffrée ou de texte en clair, ou exclure les données confidentielles d'un fichier.

Bloc de contrôle SSD

Lorsqu'un appareil crée un fichier de configuration textuel à partir de son fichier de Configuration de démarrage ou d'exécution, il insère un bloc de contrôle SSD dans le fichier si un utilisateur demande que le fichier doit inclure les données confidentielles. Le bloc de contrôle SSD, qui est protégé contre toute altération, contient les règles SSD et les propriétés SSD de l'appareil qui crée le fichier. Un bloc de contrôle SSD commence et finit respectivement avec « ssd-control-start » et « ssd-control-end ».

Fichier de Configuration de démarrage

L'appareil prend actuellement en charge la copie depuis les fichiers de Configuration d'exécution, de secours, miroir et à distance vers un fichier de Configuration de démarrage. Les configurations définies dans la configuration de démarrage sont effectives et deviennent la configuration d'exécution une fois le redémarrage effectué. Un utilisateur peut récupérer les données confidentielles sous forme chiffrée ou de texte en clair à partir d'un fichier de Configuration de démarrage, sujet à l'autorisation en lecture SSD et au mode de lecture SSD actuel de la session de gestion.

L'accès en lecture aux données confidentielles dans la configuration de démarrage sous toutes ses formes est exclu si le mot de passe défini dans le fichier de Configuration de démarrage diffère du mot de passe local.

SSD ajoute les règles suivantes lors de la copie des fichiers de Configuration de secours, miroir et à distance vers le fichier de Configuration de démarrage :

- Une fois qu'un appareil a été réinitialisé à ses valeurs par défaut, toutes ses configurations y compris les règles et les propriétés SSD sont réinitialisées à leurs valeurs par défaut.
- Si un fichier de configuration source contient des données confidentielles chiffrées, mais pas de bloc de contrôle SSD, l'appareil refuse le fichier source et la copie échoue.
- S'il n'y a pas de bloc de contrôle SSD dans le fichier de configuration source, la configuration SSD définie dans le fichier de Configuration de démarrage est réinitialisée à ses valeurs par défaut.
- Si un mot de passe est présent dans le bloc de contrôle SSD du fichier de configuration source, l'appareil refuse le fichier source, et la copie échoue s'il y a des données confidentielles chiffrées dans le fichier qui ne sont pas chiffrées par la clé générée à partir du mot de passe dans le bloc de contrôle SSD.
- S'il y a un bloc de contrôle SSD dans le fichier de configuration source et que le fichier échoue lors du contrôle d'intégrité SSD et/ou lors du contrôle d'intégrité du fichier, l'appareil refuse le fichier source et la copie échoue.
- S'il n'y a aucun mot de passe dans le bloc de contrôle SSD du fichier de configuration source, toutes les données confidentielles chiffrées dans le fichier doivent être chiffrées soit par la clé générée à partir du mot de passe local, soit par la clé générée à partir du mot de passe par défaut, mais pas par les deux. Sinon, le fichier source est refusé et la copie échoue.

- L'appareil configure le mot de passe, le contrôle du mot de passe et l'intégrité du fichier le cas échéant à partir du bloc de contrôle SSD dans le fichier de configuration source vers le fichier de Configuration de démarrage. Il configure le fichier de Configuration de démarrage avec le mot de passe qui est utilisé pour générer la clé permettant de décrypter les données confidentielles dans le fichier de configuration source. Toutes les configurations SSD introuvables sont réinitialisées à leurs valeurs par défaut.
- S'il y a un bloc de contrôle SSD dans le fichier de configuration source et que le fichier contient des données confidentielles sous forme de texte en clair, à l'exclusion des configurations SSD dans le bloc de contrôle SSD, le fichier est accepté.

Fichier de Configuration d'exécution

Un fichier de Configuration d'exécution contient la configuration actuellement utilisée par l'appareil. Un utilisateur peut récupérer les données confidentielles sous forme chiffrée ou de texte en clair à partir d'un fichier de Configuration d'exécution, sujet à l'autorisation en lecture SSD et au mode de lecture SSD actuel de la session de gestion. L'utilisateur peut changer la configuration d'exécution en copiant les fichiers de Configuration de secours ou miroir, à travers d'autres actions de gestion via CLI, XML, SNMP, etc.

Un appareil applique les règles suivantes lorsqu'un utilisateur change directement la configuration SSD dans la configuration d'exécution :

- Si l'utilisateur qui a ouvert la session de gestion ne dispose pas des autorisations SSD (à savoir les autorisations en lecture Les deux ou Texte en clair uniquement), l'appareil refuse toutes les commandes SSD.
- En cas de copie à partir d'un fichier source, l'indicateur SSD de fichier, l'intégrité du bloc de contrôle SSD et l'intégrité du fichier SSD ne sont ni vérifiés ni appliqués.
- En cas de copie à partir d'un fichier source, la copie échoue si le mot de passe contenu dans le fichier source est sous forme de texte en clair. Si le mot de passe est chiffré, il est ignoré.
- Lors de la configuration directe du mot de passe (pas de copie de fichier), dans la configuration d'exécution, le mot de passe contenu dans la commande doit être saisi sous forme de texte en clair. Sinon, la commande est refusée.
- Les commandes de configuration contenant des données confidentielles chiffrées, qui sont chiffrées avec la clé générée à partir du mot de passe local, sont configurées dans la configuration d'exécution. Sinon, la commande de configuration échoue et n'est pas intégrée au fichier de Configuration d'exécution.

Fichier de configuration de secours et miroir

Un appareil génère fréquemment son fichier de Configuration miroir à partir du fichier de Configuration de démarrage si le service de configuration miroir automatique est activé. Un appareil génère toujours un fichier de Configuration miroir avec des données confidentielles chiffrées. Par conséquent, l'indicateur SSD de fichier dans un fichier de Configuration miroir indique toujours que le fichier contient des données confidentielles chiffrées.

Par défaut, le service de configuration miroir automatique est activé. Pour activer ou désactiver la configuration miroir automatique, cliquez sur **Administration > Gestion de fichiers > Propriétés des fichiers de configuration**.

Un utilisateur peut afficher, copier et charger les fichiers complets de Configuration miroir et de secours, sujets à l'autorisation en lecture SSD, au mode de lecture actuel dans la session et à l'indicateur SSD de fichier dans le fichier source comme suit :

- S'il n'y a pas d'indicateur SSD de fichier dans un fichier de configuration miroir ou de sauvegarde, tous les utilisateurs sont autorisés à accéder au fichier.
- Un utilisateur disposant de l'autorisation en lecture Les deux peut accéder à tous les fichiers de Configuration miroir et de secours. Toutefois, si le mode de lecture actuel de la session est différent de l'indicateur SSD de fichier, l'utilisateur reçoit un message indiquant que cette action n'est pas autorisée.
- Un utilisateur disposant de l'autorisation Texte en clair uniquement peut accéder aux fichiers de Configuration miroir et de secours si leur indicateur SSD de fichier affiche les données confidentielles Exclure ou Texte en clair uniquement.
- Un utilisateur disposant de l'autorisation Chiffré uniquement peut accéder aux fichiers de Configuration miroir et de secours si leur indicateur SSD de fichier affiche les données confidentielles Exclure ou Chiffré.
- Un utilisateur disposant de l'autorisation Exclure ne peut pas accéder aux fichiers de Configuration miroir et de secours si leur indicateur SSD de fichier affiche les données confidentielles Chiffré ou Texte en clair.

L'utilisateur ne doit pas changer manuellement l'indicateur SSD de fichier en cas de conflit (le cas échéant) avec les données confidentielles dans le fichier. Sinon, les données confidentielles sous forme de texte en clair peuvent être exposées de manière inattendue.

Configuration automatique sans intervention des données confidentielles

La configuration automatique sans intervention SSD est la configuration automatique des appareils cible contenant des données confidentielles. Elle ne nécessite pas de préconfigurer manuellement les appareils cible avec le mot de passe dont la clé permet de crypter les données confidentielles.

L'appareil prend actuellement en charge la Configuration automatique, qui est activée par défaut. Lorsque la Configuration automatique est activée sur un appareil et que l'appareil reçoit les options DHCP qui spécifient un serveur de fichiers et un fichier de démarrage, l'appareil télécharge le fichier de démarrage (fichier de configuration à distance) dans le fichier de Configuration de démarrage à partir d'un serveur de fichiers, puis redémarre.

REMARQUE Le serveur de fichiers peut être spécifié par les champs bootp siaddr et sname, ainsi que l'option DHCP 150 et statiquement configuré sur l'appareil.

L'utilisateur peut en toute sécurité configurer automatiquement les appareils cible contenant des données confidentielles, en créant d'abord le fichier de configuration qui doit être utilisé dans la configuration automatique à partir d'un appareil qui contient les configurations. L'appareil doit être configuré et défini pour :

- Crypter les données confidentielles dans le fichier
- Assurer l'intégrité du contenu du fichier
- Inclure les règles SSD et les commandes de configuration d'authentification sécurisées qui contrôlent et sécurisent correctement l'accès aux appareils et aux données confidentielles

Si le fichier de configuration a été généré avec un mot de passe utilisateur et que le contrôle du mot de passe du fichier SSD est Restreint, le fichier de configuration qui en résulte peut être configuré automatiquement pour les appareils cible souhaités. Néanmoins, pour que la configuration automatique réussisse avec un mot de passe défini par l'utilisateur, les appareils cible doivent être préconfigurés manuellement avec le même mot de passe que celui de l'appareil qui génère les fichiers, ce qui ne correspond donc pas à une configuration sans intervention.

Si l'appareil qui crée le fichier de configuration est défini sur le mode de contrôle du mot de passe Sans restriction, l'appareil inclut le mot de passe dans le fichier. Par conséquent, l'utilisateur peut configurer automatiquement les appareils cible, y compris les appareils neufs ou définis à leurs paramètres par défaut, avec le fichier de configuration sans devoir manuellement préconfigurer les appareils cible avec le mot de passe. Il s'agit là d'une configuration sans intervention, car les appareils cible apprennent le mot de passe directement à partir du fichier de configuration.

REMARQUE Les appareils neufs ou définis à leurs paramètres par défaut recourent à l'utilisateur anonyme par défaut pour accéder au serveur SCP.

Canaux de gestion SSD

Les appareils peuvent être gérés via des canaux de gestion comme telnet, SSH et web. SSD classe les canaux en différentes types en fonction de leur sécurité et/ou leurs protocoles : sécurisé, non sécurisé, SNMP XML sécurisé et SNMP XML non sécurisé.

Le tableau suivant indique si chaque canal de gestion est considéré par SSD comme sécurisé ou non sécurisé. S'il est non sécurisé, le tableau indique le canal sécurisé parallèle.

Canal de gestion	Type de canal de gestion SSD	Canal de gestion sécurisé parallèle
GUI/HTTP	Non sécurisé	GUI/HTTPS
GUI/HTTPS	Sécurisé	
XML/HTTP	SNMP XML non sécurisé	XML/HTTPS
XML/HTTPS	SNMP XML sécurisé	
SNMPv1/v2/v3 sans confidentialité	SNMP XML non sécurisé	SNMP XML sécurisé
SNMPv3 avec confidentialité	SNMP XML sécurisé (utilisateurs de niveau 15)	
TFTP	Non sécurisé	SCP
SCP (Secure Copy Protocol)	Sécurisé	
Transfert de fichier basé sur HTTP	Non sécurisé	Transfert de fichier basé sur HTTPS
Transfert de fichier basé sur HTTPS	Sécurisé	

Interface de ligne de commande (CLI) et récupération du mot de passe

L'interface de ligne de commande (CLI) est uniquement accessible aux utilisateurs dont les autorisations en lecture sont Les deux ou Texte en clair uniquement. Les autres utilisateurs n'y ont pas accès. Les données confidentielles contenues dans l'interface de ligne de commande (CLI) s'affichent toujours sous forme de texte en clair.

La récupération du mot de passe est actuellement activée à partir du menu de démarrage et permet à l'utilisateur de se connecter au terminal sans authentification. Si SSD est pris en charge, cette option est uniquement autorisée lorsque le mot de passe local est identique au mot de passe par défaut. Si un appareil est configuré avec un mot de passe défini par l'utilisateur, l'utilisateur ne peut pas activer la récupération du mot de passe.

Configuration de SSD

La configuration de la fonction SSD est décrite aux pages suivantes :

- Vous pouvez définir les propriétés SSD sur la page Propriétés.
- Vous pouvez définir les règles SSD sur la page Règles SSD.

Propriétés SSD

Seuls les utilisateurs qui disposent de l'autorisation en lecture SSD Texte en clair uniquement ou Les deux sont autorisés à définir les propriétés SSD.

Pour définir les propriétés SSD globales :

ÉTAPE 1 Cliquez sur **Sécurité** > **Gestion sécurisée des données confidentielles** > **Propriétés**. Le champ suivant s'affiche :

- **Type de mot de passe local actuel** : indique si le mot de passe par défaut ou un mot de passe défini par l'utilisateur est actuellement utilisé.

ÉTAPE 2 Renseignez les champs **Paramètres persistants** suivants :

- **Contrôle du mot de passe du fichier de configuration** : sélectionnez une option, comme indiqué à la section **Contrôle du mot de passe du fichier de configuration**.
- **Contrôle de l'intégrité du fichier de configuration** : sélectionnez cette fonction pour l'activer. Reportez-vous à la section **Contrôle de l'intégrité du fichier de configuration**.

ÉTAPE 3 Sélectionnez un mode de lecture pour la session actuelle (reportez-vous à **Éléments d'une règle SSD**).

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres sont enregistrés dans le fichier Configuration d'exécution.

Pour changer le mot de passe local :

ÉTAPE 1 Cliquez sur **Modifier le mot de passe local**, puis entrez un nouveau **Mot de passe local** :

- **Par défaut** : permet d'utiliser le mot de passe par défaut des appareils.
- **Défini par l'utilisateur (texte en clair)** : saisissez un nouveau mot de passe.
- **Confirmer le mot de passe** : confirmez le nouveau mot de passe.

ÉTAPE 2 Cliquez sur **Apply**. Les paramètres sont enregistrés dans le fichier Configuration d'exécution.

Configuration des règles SSD

Seuls les utilisateurs qui disposent de l'autorisation en lecture SSD Texte en clair uniquement ou Les deux sont autorisés à définir les règles SSD.

Pour configurer les règles SSD :

ÉTAPE 1 Cliquez sur **Sécurité** > **Gestion sécurisée des données confidentielles** > **Règles SSD**.

Les règles actuellement définies sont affichées.

ÉTAPE 2 Pour ajouter une nouvelle règle, cliquez sur **Ajouter**. Renseignez les champs suivants :

- **Utilisateur** : définit le ou les utilisateurs auxquels la règle s'applique : Sélectionnez une des options suivantes :
  - *Utilisateur spécifique* : sélectionnez et entrez le nom d'utilisateur spécifique auquel cette règle s'applique (cet utilisateur ne doit pas nécessairement être défini).
  - *Utilisateur par défaut (cisco)* : indique que cette règle s'applique à l'utilisateur par défaut.
  - *Niveau 15* : indique que cette règle s'applique à tous les utilisateurs ayant le niveau de privilège 15.
  - *Tous* : indique que cette règle s'applique à tous les utilisateurs.
- **Canal** : définit le niveau de sécurité du canal d'entrée auquel la règle s'applique : Sélectionnez une des options suivantes :
  - *Sécurisé* : indique que cette règle s'applique uniquement aux canaux sécurisés (console, SCP, SSH et HTTPS), mais pas les canaux SNMP et XML.

- *Non sécurisé* : indique que cette règle s'applique uniquement aux canaux non sécurisés (Telnet, TFTP et HTTP), mais pas aux canaux SNMP et XML.
- *SNMP XML sécurisé* : indique que cette règle s'applique uniquement au XML sur HTTPS et SNMPv3 avec confidentialité.
- *SNMP XML non sécurisé* : indique que cette règle s'applique uniquement au XML sur HTTP ou/et au SNMPv1/v2 et SNMPv3 sans confidentialité.

- **Autorisation en lecture** : autorisations en lecture associées aux règles. Elles peuvent être les suivantes :
  - *Exclure* : autorisation en lecture la plus basse. Les utilisateurs ne sont pas autorisés à accéder aux données confidentielles sous quelque forme que ce soit.
  - *Texte en clair uniquement* : autorisation en lecture de niveau plus élevé que la précédente. Les utilisateurs sont autorisés à accéder aux données confidentielles sous forme de texte en clair uniquement.
  - *Chiffré uniquement* : autorisation en lecture de niveau moyen. Les utilisateurs sont autorisés à accéder aux données confidentielles sous forme chiffrée uniquement.
  - *Les deux (Texte en clair et Chiffré)* : autorisation en lecture la plus haute. Les utilisateurs ont les autorisations Chiffré et Texte en clair, et sont autorisés à accéder aux données confidentielles sous forme chiffrée et de texte en clair.
- **Mode de lecture par défaut** : tous les modes de lecture par défaut sont sujets à l'autorisation en lecture de la règle. Les options suivantes sont disponibles, mais certaines sont susceptibles d'être refusées en fonction de l'autorisation en lecture de la règle.
  - *Exclure* : n'autorise pas la lecture des données confidentielles.
  - *Chiffré* : les données confidentielles sont présentées sous forme chiffrée.
  - *Texte en clair* : les données confidentielles sont présentées sous forme de texte en clair.

ÉTAPE 3 Cliquez sur **Apply**. Les paramètres sont enregistrés dans le fichier Configuration d'exécution.

ÉTAPE 4 Les actions suivantes peuvent être effectuées sur les règles sélectionnées :

- Règles **Ajouter**, **Modifier** ou **Supprimer**
- **Restaurer les valeurs par défaut** : rétablit les valeurs d'origine d'une règle par défaut qui a été modifiée par l'utilisateur.

23

Qualité de service

La fonction QoS (Quality of Service, qualité de service) est appliquée à l'ensemble du réseau pour garantir que le trafic réseau est géré en fonction des critères fixés et que les données voulues reçoivent un traitement préférentiel.

Cette section aborde les points suivants :

- **Fonctions et composants QoS**
- **Configuration de la QoS - Général**
- **Gestion des statistiques de QoS**

Fonctions et composants QoS

La fonction QoS permet d'optimiser les performances du réseau.

La QoS fournit les éléments suivants :

- Classification du trafic entrant en différentes classes sur la base d'attributs, notamment :
  - Configuration du périphérique
  - Interface d'entrée
  - Contenu des paquets
  - Combinaison de ces attributs

La QoS inclut :

- **Traffic Classification** : permet de marquer chaque paquet entrant comme appartenant à un flux de trafic spécifique, sur la base du contenu de ce paquet et/ou du port. **Assignment to Hardware Queues** : affecte les paquets entrants à des files d'attente de réacheminement. Les paquets sont envoyés à une file d'attente particulière pour gestion en tant que fonction de la classe de trafic à laquelle ils appartiennent. Reportez-vous à la section **Configuration de files d'attente de QoS**.
- **Autre attribut de gestion de classe de trafic** : applique des mécanismes QoS à diverses classes, y compris la gestion de bande passante.

Fonctionnement de QoS

Lors de l'utilisation de la fonction QoS, tout le trafic d'une même classe reçoit un traitement identique, à savoir l'action unique de QoS consistant à déterminer la file d'attente de sortie sur le port de sortie, ceci sur la base de la valeur QoS indiquée dans la trame entrante. En mode Couche 2, il s'agit de la valeur VPT (VLAN Priority Tag, balise de priorité de VLAN) 802.1p. En mode Couche 3, le système utilise la valeur DSCP (Differentiated Service Code Point, point de code de service différencié) pour IPv4 et la valeur TC (Traffic Class, classe de trafic) pour IPv6. Lorsqu'il fonctionne en mode De base, le périphérique fait confiance à cette valeur de QoS affectée en externe. La valeur de QoS affectée en externe à un paquet détermine sa classe de trafic et la QoS.

Flux de travail de QoS

Pour configurer les paramètres de QoS généraux, procédez comme suit :

ÉTAPE 1 Activez QoS dans la page Propriétés QoS pour sélectionner le mode de confiance. Activez ensuite QoS sur les ports dans la page Paramètres d'interface.

ÉTAPE 2 Attribuez à chaque interface une priorité CoS ou DSCP par défaut, via la page Propriétés de QoS.

ÉTAPE 3 Attribuez une méthode de planification (Priorité stricte ou WRR) et une valeur d'allocation de bande passante WRR aux files d'attente de sortie, via la page File d'attente.

ÉTAPE 4 Désignez une file d'attente de sortie pour chaque valeur IP DSCP/TC sur la page DSCP vers la file d'attente. Si le périphérique fonctionne en mode de confiance DSCP, les paquets entrants sont placés dans les files d'attente de sortie en fonction de leur valeur DSCP/TC.

ÉTAPE 5 Associez une file d'attente de sortie à chaque priorité CoS/802.1p. Si le périphérique fonctionne en mode de confiance CoS/802.1, tous les paquets entrants sont placés dans les files d'attente de sortie prévues en fonction de la priorité CoS/802.1 des paquets. Pour ce faire, utilisez la page CoS/802.1p vers file d'attente.

ÉTAPE 6 Saisissez les limites de bande passante et de débit dans les pages suivantes :

a. Définissez le lissage en sortie pour chaque file d'attente sur la page Modelage de sortie par file d'attente.

b. Définissez la limite de vitesse d'entrée et le taux de lissage en sortie pour chaque port sur la page Bande passante.

Configuration de la QoS - Général

La rubrique Propriétés de QoS contient des champs permettant d'activer QoS et de sélectionner le mode de confiance à utiliser. En outre, vous pouvez définir la priorité CoS ou la valeur DSCP par défaut de chaque interface.

Configuration des propriétés QoS

Pour activer QoS :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Propriétés de QoS**.

ÉTAPE 2 Pour activer QoS sur le périphérique.

ÉTAPE 3 Sélectionnez un mode de confiance (CoS/802.1p ou DSCP)

ÉTAPE 4 Cochez la case Remplacer DSCP d'entrée pour l'activer, puis cliquez sur **Appliquer**.

ÉTAPE 5 Si vous avez sélectionné DSCP, passez à l'**ÉTAPE 6** ; si vous avez sélectionné CoS, procédez à l'étape suivante :

ÉTAPE 6 Sélectionnez **Port/LAG** et cliquez sur **Ok** pour afficher/modifier tous les ports/LAG sur le périphérique ainsi que leurs informations de CoS.

Les champs suivants sont affichés pour tous les ports/LAG :

- **Interface** : type de l'interface.
- **CoS par défaut** : valeur VPT par défaut pour les paquets entrants qui ne possèdent pas de balise VLAN. La valeur CoS par défaut est 0. Elle s'applique uniquement aux trames non balisées si CoS de confiance est sélectionné.

Sélectionnez **Restaurer les valeurs par défaut** pour rétablir le paramètre de CoS par défaut défini en usine pour cette interface.

ÉTAPE 7 Cliquez sur **Table de substitution DSCP** pour saisir les valeurs DSCP.

ÉTAPE 8 DSCP en entrée affiche la valeur DSCP du paquet entrant qui doit à nouveau être marqué d'une autre valeur. Sélectionnez la nouvelle valeur DSCP qui remplacera la valeur entrante.

Sélectionnez Restaurer les valeurs par défaut pour restaurer les valeurs DSCP d'origine.

ÉTAPE 9 Cliquez sur **Apply**. Le fichier de configuration de fonctionnement est mis à jour.

Pour définir une QoS sur une interface, sélectionnez-la et cliquez sur **Modifier**.

ÉTAPE 1 Saisissez les paramètres.

- **Interface** : sélectionnez le port ou LAG.

- **CoS par défaut** : sélectionnez la valeur de CoS (Class-of-Service, classe de service) à affecter aux paquets entrants qui ne possèdent pas de balise VLAN.

ÉTAPE 2 Cliquez sur **Apply**. La valeur CoS par défaut de l'interface est enregistrée dans le fichier de Configuration d'exécution.

Paramètres QoS de l'interface

La page Paramètres d'interface vous permet de configurer la QoS sur chaque port du périphérique, comme suit :

QoS désactivée sur l'interface : tout le trafic entrant sur le port est mappé sur la file d'attente Meilleur effort (Best effort) et aucune classification/attribution de priorité n'est effectuée.

QoS activée sur le port : le trafic d'entrée sur le port reçoit un ordre de priorité qui dépend du mode de confiance configuré à l'échelle du système, à savoir CoS/802.1p ou DSCP.

Pour entrer les paramètres de QoS de chaque interface :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Paramètres d'interface**.

ÉTAPE 2 Sélectionnez **Port** ou **LAG** pour afficher la liste des ports ou LAG.

La liste des ports/LAG s'affiche. **État de QoS** indique si la QoS est activée sur l'interface.

ÉTAPE 3 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 4 Sélectionnez le **port** ou l'interface **LAG**.

ÉTAPE 5 Cliquez pour activer ou désactiver l'**état de QoS** pour cette interface.

ÉTAPE 6 Cliquez sur **Apply**. Le fichier de configuration de fonctionnement est mis à jour.

Configuration de files d'attente de QoS

Il existe deux façons de déterminer le mode de gestion du trafic dans les files d'attente : Priorité stricte et WRR (Weighted Round Robin, technique du tourniquet pondéré).

- **Priorité stricte** : le trafic sortant émanant de la file d'attente de priorité la plus élevée est transmis en premier. Le trafic des files d'attente de priorité(s) plus faible(s) n'est traité qu'après transmission des files d'attente de priorité(s) supérieure(s), ce qui donne le niveau de priorité le plus élevé au trafic de la file d'attente portant le numéro le plus élevé.

- **Weighted Round Robin (WRR)** : En mode WRR, le nombre de paquets envoyés depuis la file d'attente est proportionnel à la pondération de cette file d'attente (plus la pondération est élevée, plus le nombre de trames transmises est important). Par exemple, s'il y a un maximum de quatre files d'attente possible et qu'elles sont toutes de type WRR et que les pondérations par défaut sont appliquées, la file d'attente 1 reçoit 1/15 de la bande passante (en supposant que toutes les files d'attente sont saturées et qu'il y a encombrement), la file d'attente 2 en reçoit 2/15, la file d'attente 3 en reçoit 4/15 et la file d'attente 4 reçoit 8/15 de la bande passante. Le type d'algorithme WRR utilisé sur le périphérique n'est pas l'algorithme standard DWRR (Deficit WRR, WRR avec déficit) mais l'algorithme SDWRR (Shaped Deficit WRR, WRR avec déficit lissé).

Vous sélectionnez les modes de mise en file d'attente dans la page File d'attente. Lorsque le mode de mise en file d'attente se fait par priorité stricte, l'ordre de priorité définit l'ordre de traitement des files d'attente, en commençant par la file d'attente 4 ou 8 (celle dont la priorité est la plus élevée), puis en passant à la file d'attente de niveau immédiatement inférieur à la fin du traitement de chaque file.

Lorsque la mise en file d'attente est de type WRR (Weighted Round Robin), chaque file d'attente est traitée jusqu'à ce que son quota soit atteint. Le système passe ensuite à une autre file d'attente.

Il est également possible d'affecter une WRR à certaines des files d'attente de priorité plus faible tout en maintenant le traitement Priorité stricte pour des files d'attente de niveau(x) plus élevé(s). Dans ce cas, le trafic des files d'attente à priorité stricte est toujours envoyé avant celui des files d'attente WRR. Le trafic des files d'attente WRR n'est transféré que lorsque les files d'attente à priorité stricte sont vides. (La portion relative en provenance de chaque file d'attente WRR dépend de sa pondération.)

Pour sélectionner la méthode de priorité et entrer les données WRR :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **Queue**.

ÉTAPE 2 Saisissez les paramètres.

- **Queue** : affiche le numéro de la file d'attente.
- **Méthode de planification :** Sélectionnez une des options suivantes :
  - *Strict Priority* : la planification du trafic de la file d'attente sélectionnée et de toutes les files d'attente supérieures est strictement basée sur la priorité de chaque file d'attente.
  - *WRR* : la planification du trafic de la file d'attente sélectionnée se base sur une WRR. Chaque période est divisée entre les files d'attente WRR qui ne sont pas vides (celles qui ont des descripteurs de sortie). Ceci ne s'applique que lorsque les files d'attente à priorité stricte sont vides.
  - *Pondération WRR* : si vous choisissez WRR, saisissez la pondération WRR attribuée à la file d'attente.
  - *% de bande passante WRR* : affiche la quantité de bande passante affectée à la file d'attente. Ces valeurs représentent un pourcentage de la pondération WRR.

ÉTAPE 3 Cliquez sur **Apply**. Les files d'attente sont configurées et le fichier de Configuration d'exécution est mis à jour.

Mappage CoS/802.1p vers une file d'attente

La page CoS/802.1p vers file d'attente mappe des priorités 802.1p sur des files d'attente de sortie. La table CoS/802.1p vers file d'attente détermine les files d'attente de sortie des paquets entrants sur la base de la priorité 802.1p figurant dans leurs balises VLAN. Pour les paquets entrants non balisés, la priorité 802.1p utilisée est la priorité CoS/802.1p par défaut affectée aux ports d'entrée.

Le tableau suivant décrit le mappage par défaut lorsque 4 files d'attente sont utilisées :

Valeurs 802.1p (0-7, 7 étant la valeur la plus élevée)	File d'attente (4 files d'attente numérotées de 1 à 4, 4 étant la priorité la plus élevée)	Notes
0	1	Arrière-plan
1	1	Meilleur effort (Best effort)
2	2	Excellent effort
3	3	Application critique - SIP pour téléphone LVS
4	3	Vidéo
5	4	Voix - Valeur par défaut de téléphone IP Cisco
6	4	Contrôle de l'interfonctionnement - RTP pour téléphone LVS
7	4	Contrôle du réseau

En modifiant le mappage CoS/802.1p vers file d'attente (CoS/802.1p vers file d'attente), et la méthode de planification des files d'attente ainsi que l'allocation de la bande passante (page File d'attente), il est possible d'obtenir la qualité de service voulue sur un réseau.

Le mappage CoS/802.1p vers file d'attente est applicable seulement si le mode de confiance est CoS/802.1p et que les paquets appartiennent à des flux CoS de confiance.

La file d'attente 1 a la plus basse priorité et la file d'attente 4 ou 8 a la plus haute priorité.

Pour mapper des valeurs de CoS sur des files d'attente de sortie :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **CoS/802.1p to Queue**.

ÉTAPE 2 Saisissez les paramètres.

- **802.1p** : affiche les valeurs de balise de priorité 802.1p à affecter à une file d'attente de sortie, où 0 est la priorité la plus faible et 7 la plus élevée.
- **Output Queue** : sélectionnez la file d'attente de sortie sur laquelle la priorité 802.1p est mappée. Le système prend en charge quatre ou huit files d'attente de sortie, parmi lesquelles la File d'attente 4 ou 8 dispose de la priorité la plus élevée et la File d'attente 1 de la priorité la plus faible.

ÉTAPE 3 Pour chaque priorité 802.1p, sélectionnez la file d'attente de sortie sur laquelle elle est mappée.

ÉTAPE 4 Cliquez sur **Appliquer, Annuler** ou **Restaurer déf.** Les valeurs de priorité 801.1p vers les files d'attente sont mappées et le fichier Configuration d'exécution est mis à jour. Les modifications saisies sont annulées ou les valeurs préalablement définies sont restaurées.

Mappage DSCP vers file d'attente

La page DSCP (IP Differentiated Services Code Point, point de code de service différencié IP) vers file d'attente mappe des valeurs DSCP vers des files d'attente de sortie. La table DSCP vers file d'attente détermine la file d'attente de sortie des paquets IP entrants sur la base de leur valeur DSCP. La valeur VPT (VLAN Priority Tag, marquage de priorité VLAN) du paquet reste inchangée.

En modifiant simplement le mappage DSCP vers file d'attente, la méthode de planification des files d'attente ainsi que l'allocation de bande passante, il est possible d'obtenir la qualité de service voulue sur un réseau.

Le mappage DSCP vers file d'attente s'applique aux paquets IP si le mode de confiance est DSCP.

Les paquets non IP sont toujours classés comme appartenant à la file d'attente Meilleur effort (Best effort).

Les tableaux suivants décrivent le mappage DSCP vers file d'attente par défaut pour un système à 4 files d'attente :

DSCP	63	55	47	39	31	23	15	7
File d'attente	3	3	4	3	3	2	1	1
DSCP	62	54	46	38	30	22	14	6
File d'attente	3	3	4	3	3	2	1	1

DSCP	61	53	45	37	29	21	13	5
File d'attente	3	3	4	3	3	2	1	1
DSCP	60	52	44	36	28	20	12	4
File d'attente	3	3	4	3	3	2	1	1
DSCP	59	51	43	35	27	19	11	3
File d'attente	3	3	4	3	3	2	1	1
DSCP	58	50	42	34	26	18	10	2
File d'attente	3	3	4	3	3	2	1	1
DSCP	57	49	41	33	25	17	9	1
File d'attente	3	3	4	3	3	2	1	1
DSCP	56	48	40	32	24	16	8	0
File d'attente	3	3	4	3	3	2	1	1

Pour mapper DSCP à des files d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **DSCP vers file d'attente**.

La page DSCP vers file d'attente contient **DSCP d'entrée**. Il affiche la valeur DSCP du paquet entrant et la classe associée.

ÉTAPE 2 Sélectionnez la **file d'attente de sortie** (file d'attente de transfert du trafic) sur laquelle la valeur DSCP est mappée.

ÉTAPE 3 Sélectionnez **Restaurer les valeurs par défaut** pour rétablir le paramètre de CoS par défaut défini en usine pour cette interface.

ÉTAPE 4 Cliquez sur **Apply**. Le fichier de configuration de fonctionnement est mis à jour.

Configuration de la bande passante

La page Bande passante permet aux utilisateurs de définir deux valeurs (Limite de vitesse d'entrée et Taux de modelage en sortie), qui déterminent la quantité de trafic que le système peut recevoir et envoyer.

La limite de débit d'entrée indique le nombre de bits par seconde que l'interface d'entrée peut recevoir. La bande passante dépassant cette limite est éliminée.

Les valeurs suivantes sont entrées pour le lissage en sortie (egress shaping) :

- **L'option Débit minimal garanti (CIR)** définit la quantité moyenne maximale de données que le système est autorisé à envoyer à l'interface de sortie, en bits par seconde.
- **L'option Taille de rafale garantie (CBS)** indique la rafale de données que le système est autorisé à envoyer même au-delà de la valeur CIR. Cette valeur est exprimée en nombre d'octets de données.

Pour indiquer la limite de bande passante :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **Bandwidth**.

La page Bande passante affiche les informations de bande passante de chaque interface.

La colonne % indique la limite de débit entrant pour le port divisée par la quantité totale de bande passante du port.

ÉTAPE 2 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 3 Sélectionnez le **port ou l'interface LAG**.

ÉTAPE 4 Remplissez les champs pour l'interface sélectionnée :

- **Limite de débit d'entrée** : sélectionnez cette option pour activer la limite de débit d'entrée, que vous définissez ensuite dans le champ situé au-dessous.
- **Limite de débit d'entrée** : saisissez la quantité maximale de bande passante autorisée sur l'interface.

  REMARQUE Les deux champs **Limite de vitesse d'entrée** ne s'affichent pas lorsque le type d'interface est LAG.
- **Taille de rafale garantie (CBS)** : saisissez la taille maximale de rafale de données de l'interface d'entrée, en octets de données. Cette quantité de données peut être envoyée même si cela provoque un dépassement temporaire de la limite de la bande passante autorisée. Ce champ est disponible uniquement si l'interface est un port.
- **Taux de lissage en sortie (egress shaping)** : sélectionnez cette option pour activer le lissage en sortie (egress shaping) sur le port.
- **Débit minimal garanti (CIR)** : saisissez la quantité maximale de bande passante de l'interface de sortie.
- **Taille de rafale garantie en sortie (CBS)** : saisissez la taille maximale de rafale de données de l'interface de sortie, en octets de données. Cette quantité de données peut être envoyée même si cela provoque un dépassement temporaire de la limite de la bande passante autorisée.

ÉTAPE 5 Cliquez sur **Apply**. Les paramètres de bande passante sont écrits dans le fichier de Configuration d'exécution.

Configuration du lissage en sortie par file d'attente

Outre la limitation du débit de transmission de chaque port, que vous configurez dans la page Bande passante, le périphérique peut limiter le débit de transmission des trames en sortie sélectionnées pour chaque file d'attente et pour chaque port. La limitation du débit en sortie est réalisée par mise en forme de la charge de sortie.

Le périphérique limite toutes les trames, à l'exception des trames de gestion. Toutes les trames non limitées sont ignorées dans le calcul du débit, ce qui signifie que leur taille n'est pas incluse dans la limite totale.

Vous pouvez désactiver le lissage (shaping) du débit en sortie pour chaque file d'attente.

Pour définir la mise en forme en sortie pour chaque file d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Modelage de sortie par file d'attente**.

La page Modelage de sortie par file d'attente affiche la limite de débit et la taille de rafale applicables à chaque file d'attente.

ÉTAPE 2 Sélectionnez un type d'interface (Port ou LAG) et cliquez sur **Go**.

ÉTAPE 3 Sélectionnez un port/LAG et cliquez sur **Modifier**.

Cette page vous permet de lisser la sortie pour un maximum de huit files d'attente sur chaque interface.

ÉTAPE 4 Sélectionnez l'**interface** voulue.

ÉTAPE 5 Pour chacune des files d'attente nécessaires, remplissez les champs suivants :

- **Activer le lissage** : sélectionnez cette option pour activer le modelage en sortie sur cette file d'attente.
- **Débit minimal garanti (CIR)** : saisissez le débit maximal (CIR) en kilobits par seconde (kbits/s). Le CIR est la quantité maximale moyenne de données pouvant être envoyée.
- **Taille de rafale garantie (CBS)** : saisissez la taille maximale de rafale (CBS), en octets. Le CBS indique la taille maximale de rafale de données dont l'envoi est autorisé même si cela dépasse le CIR.

ÉTAPE 6 Cliquez sur **Apply**. Les paramètres de bande passante sont écrits dans le fichier de Configuration d'exécution.

- **CoS par défaut** : Valeur VPT par défaut pour les paquets entrants qui ne possèdent pas de balise VLAN. La valeur CoS par défaut est 0. Elle s'applique uniquement aux trames non balisées si CoS de confiance est sélectionné.

ÉTAPE 7 Sélectionnez **Restaurer les valeurs par défaut** pour rétablir le paramètre de CoS par défaut défini en usine pour cette interface.

Gestion des statistiques de QoS

Sur cette page, vous pouvez gérer les statistiques des files d'attente.

Affichage des statistiques de file d'attente

La page Statistiques des files d'attente affiche les statistiques concernant les files d'attente, dont le nombre de paquets transférés et éliminés, ceci sur la base de l'interface, de la file d'attente et de la priorité d'élimination.

Pour afficher les statistiques de file d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Statistiques de QoS** > **Statistiques de file d'attente**.

Cette page affiche les champs suivants :

- **Taux d'actualisation** : sélectionnez la durée qui s'écoule avant l'actualisation des statistiques Ethernet de l'interface. Les options disponibles sont les suivantes :
  - *No Refresh* : les statistiques ne sont pas actualisées.
  - *15 s* : les statistiques sont actualisées toutes les 15 secondes.
  - *30 s* : les statistiques sont actualisées toutes les 30 secondes.
  - *60 s* : les statistiques sont actualisées toutes les 60 secondes.
- **Jeu de compteurs** : les options disponibles sont les suivantes :
  - *Jeu 1* : affiche les statistiques du jeu 1, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) élevée.
  - *Jeu 2* : affiche les statistiques du jeu 2, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) faible.
- **Interface** : interface à laquelle correspondent les statistiques de file d'attente affichées.
- **File d'attente** : file d'attente d'où proviennent les paquets transférés ou éliminés, la file étant pleine (tail drop).
- **Priorité d'élimination** : les paquets portant la priorité d'élimination la plus faible ont davantage de chances d'être conservés.
- **Nombre total de paquets** : nombre de paquets transférés ou éliminés, la file étant pleine (tail drop).
- **Paquets éliminés** : pourcentage de paquets éliminés, la file étant pleine (tail drop).

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Jeu de compteurs** : sélectionnez le jeu voulu :
  - *Jeu 1* : affiche les statistiques du jeu 1, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) élevée.
  - *Jeu 2* : affiche les statistiques du jeu 2, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) faible.
- **Interface** : sélectionnez les ports auxquels correspondent les statistiques affichées. Les options sont les suivantes :
  - *Port* : sélectionnez le port pour lequel vous voulez afficher les statistiques, pour le numéro d'unité sélectionné.
  - *Tous les ports* : l'écran affiche les statistiques pour tous les ports.
- **File d'attente** : sélectionnez la file d'attente pour laquelle vous voulez afficher les statistiques.
- **Priorité d'élimination** : saisissez la priorité d'élimination, c'est-à-dire la probabilité de suppression des paquets.

ÉTAPE 4 Cliquez sur **Apply**. Le compteur de statistiques de files d'attente est ajouté et le fichier de Configuration d'exécution est mis à jour.

24

SNMP

Cette section décrit la fonctionnalité SNMP (Simple Network Management Protocol), qui fournit une méthode de gestion des unités de réseau.

Elle couvre les rubriques suivantes :

- **Versions et flux de travail SNMP**
- **ID d'objet du modèle**
- **ID de moteur SNMP**
- **Configuration de vues SNMP**
- **Création de groupes SNMP**
- **Création d'utilisateurs SNMP**
- **Définition de communautés SNMP**
- **Définition de paramètres d'interceptions**
- **Destinataires de notifications**
- **Filtres de notification SNMP**

Versions et flux de travail SNMP

Le périphérique fonctionne comme un agent SNMP et prend en charge SNMPv1, v2 et v3. Il crée également des rapports sur les événements système pour les destinataires des interceptions, à l'aide des interceptions définies dans la base MIB prise en charge.

SNMPv1 et v2

Pour contrôler l'accès au système, une liste d'entrées de communauté est définie. Chaque entrée de communauté est constituée d'une *chaîne de communauté* et de son privilège d'accès. Le système répond uniquement aux messages SNMP spécifiant la communauté qui dispose des autorisations correctes et de l'opération correcte.

Les agents SNMP conservent une liste de variables utilisées pour gérer le périphérique. Ces variables sont définies dans une *base d'informations de gestion* (MIB, Management Information Base).

REMARQUE En raison des vulnérabilités en matière de sécurité détectées dans les autres versions, il est recommandé d'utiliser SNMPv3.

SNMPv3

En plus de la fonctionnalité fournie par SNMPv1 et v2, SNMPv3 applique un contrôle d'accès et de nouveaux mécanismes de filtre aux PDU SNMPv1 et SNMPv2. SNMPv3 définit également un modèle de sécurité utilisateur (USM, User Security Model) qui inclut :

- **Authentification** : fournit une intégrité des données et une authentification de leur origine.
- **Confidentialité** : fournit une protection contre la divulgation du contenu des messages. *Cipher Block-Chaining* (CBC-DES) est utilisé pour le cryptage. Sur un message SNMP, vous pouvez activer soit l'authentification seule, soit l'authentification et la confidentialité. Cependant, la confidentialité ne peut pas être activée sans authentification.
- **Actualité** : fournit une protection contre les retards de messages ou les attaques de lecture. L'agent SNMP compare l'horodatage du message entrant par rapport à l'heure d'arrivée du message.

Flux de travail SNMP

REMARQUE Pour des raisons de sécurité, SNMP est désactivé par défaut. Avant de pouvoir gérer le périphérique via SNMP, vous devez activer SNMP sur la page Sécurité > Services TCP/UDP.

Ci-dessous figure une série d'actions recommandées pour la configuration de SNMP :

Si vous décidez d'utiliser SNMPv1 ou v2 :

ÉTAPE 1 Accédez à la page SNMP -> Communautés, puis cliquez sur **Ajouter**. La communauté peut être associée à des droits d'accès et à un affichage en mode De base ou à un groupe en mode Avancé. Il existe deux méthodes pour définir les droits d'accès d'une communauté :

- **Mode De base** : les droits d'accès d'une communauté peuvent être définis en Lecture seule, Lecture/écriture ou Admin SNMP. Vous pouvez en outre restreindre l'accès à la communauté à certains objets MIB uniquement, en sélectionnant une vue (définie sur la page Vues).

- **Mode Avancé** : les droits d'accès à une communauté sont définis par un groupe (défini sur la page **Groupes**). Vous pouvez configurer le groupe avec un modèle de sécurité spécifique. Les groupes disposent des droits d'accès de lecture, d'écriture et de notification.

ÉTAPE 2 Indiquez si vous souhaitez restreindre la station de gestion SNMP à une seule adresse ou autoriser la gestion SNMP à partir de toutes les adresses. Si vous choisissez de restreindre la gestion SNMP à une seule adresse, saisissez l'adresse de votre ordinateur de gestion SNMP dans le champ Adresse IP.

ÉTAPE 3 Saisissez la chaîne de communauté unique dans le champ Chaîne de communauté.

ÉTAPE 4 (Facultatif) Activez les interceptions via la page Paramètres de filtre.

ÉTAPE 5 (Facultatif) Définissez un ou plusieurs filtres de notification via la page Filtre de notification.

ÉTAPE 6 Configurez les destinataires de notifications sur la page Destinataires de notifications SNMPv1,2.

Si vous décidez d'utiliser SNMPv3 :

ÉTAPE 1 Définissez le moteur SNMP sur la page ID du moteur. Vous pouvez soit créer un ID de moteur unique, soit utiliser l'ID de moteur par défaut. L'application d'une configuration ID du moteur efface le contenu de la base de données SNMP.

ÉTAPE 2 Vous pouvez également définir une ou plusieurs vues SNMP à l'aide de la page Vues (facultatif). Vous limitez ainsi la plage des ID d'objet (OID) disponibles pour une communauté ou un groupe.

ÉTAPE 3 Définissez des groupes sur la page Groupes.

ÉTAPE 4 Définissez des utilisateurs sur la page Utilisateurs SNMP. Vous pouvez ainsi les associer à un groupe. Si l'ID de moteur SNMP n'est pas défini, il se peut que vous ne puissiez pas créer d'utilisateurs.

ÉTAPE 5 Activez ou désactivez les interceptions (filtre) via la page Paramètres de filtre (facultatif).

ÉTAPE 6 (Facultatif) Définissez un ou plusieurs filtres de notification via la page Filtre de notification.

ÉTAPE 7 Définissez un ou plusieurs destinataires de notifications sur la page Destinataires de notifications SNMPv3.

Bases MIB prises en charge

Pour obtenir la liste des bases MIB prises en charge, visitez l'URL suivante et accédez à la zone de téléchargement nommée **Cisco MIBS** :

www.cisco.com/cisco/software/navigator.html

ID d'objet du modèle

Ci-dessous figurent les *ID d'objet* (OID) du modèle de périphérique :

	Description	ID d'objet
SG200-18	16 ports GE + 2 ports GE combinés spécifiques	9.6.1.88.18.1
SG200-26	24 ports GE + 2 ports GE combinés spécifiques	9.6.1.88.26.1
SG200-26P	24 ports GE + 2 ports GE combinés spécifiques	9.6.1.88.26.2
SG200-50	48 ports GE + 2 ports GE combinés spécifiques	9.6.1.88.50.1
SG200-50P	48 ports GE + 2 ports GE combinés spécifiques	9.6.1.88.50.2
SF200-24	24 ports FE + 2 ports GE combinés spécifiques	9.6.1.87.24.1
SF200-24P	24 ports FE + 2 ports GE combinés spécifiques	9.6.1.87.24.2
SF200-48	48 ports FE + 2 ports GE combinés spécifiques	9.6.1.87.48.1
SF200-48P	FE1-FE48, GE1-GE4. 48 ports FE + 2 ports GE combinés spécifiques	9.6.1.87.48.2
SG200-10FP	Commutateur intelligent PoE Gigabit à 10 ports	9.6.1.88.10.3
SF200-24FP	Commutateur intelligent PoE 24 ports 10/100	9.6.1.88.24.3

	Description	ID d'objet
SG200-26FP	Commutateur intelligent PoE Gigabit à 26 ports	9.6.1.88.26.3
SG200-50FP	Commutateur intelligent PoE Gigabit à 50 ports	9.6.1.88.50.3

Les ID d'objet privés se trouvent dans : enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1).switch001(101).

ID de moteur SNMP

L'ID de moteur est utilisé par des entités SNMPv3 afin de les identifier de façon unique. Un agent SNMP est considéré comme un moteur SNMP faisant autorité. Cela signifie que l'agent répond aux messages entrants (Get, GetNext, GetBulk, Set) et qu'il envoie des interceptions à un gestionnaire. Les informations locales de l'agent sont encapsulées dans des champs au sein du message.

Chaque agent SNMP conserve des informations locales utilisées dans des échanges de messages SNMPv3. L'ID de moteur SNMP par défaut est constitué du numéro d'entreprise et de l'adresse MAC par défaut. Cet ID de moteur doit être unique pour le domaine d'administration afin que deux unités dans un réseau ne possèdent pas le même ID de moteur.

Les informations locales sont stockées dans quatre variables MIB en lecture seule (snmpEngineId, snmpEngineBoots, snmpEngineTime et snmpEngineMaxMessageSize).

ATTENTION Lorsque l'ID de moteur est modifié, tous les utilisateurs et groupes configurés sont effacés.

Pour définir l'ID de moteur SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Engine ID**.

ÉTAPE 2 Choisissez l'option souhaitée pour **ID du moteur local**.

- **Valeurs par défaut :** sélectionnez cette option pour utiliser l'ID du moteur généré par le périphérique. L'ID du moteur par défaut est basé sur l'adresse MAC du périphérique. Il est défini de manière standard par :
  - *4 premiers octets* : premier bit = 1, le reste correspond au numéro d'entreprise IANA.
  - *Cinquième octet* : défini à l'aide de la valeur 3 pour indiquer l'adresse MAC qui suit.
  - *6 derniers octets* : adresse MAC du périphérique.
- **Aucun** : aucun ID de moteur n'est utilisé.

- **Défini par l'utilisateur** : saisissez l'ID de moteur de l'unité locale. La valeur du champ est une chaîne hexadécimale **(plage : 10 - 64)**. Chaque octet dans les chaînes de caractères hexadécimales est représenté par deux chiffres hexadécimaux.

Tous les ID de moteur distant et leurs adresses IP sont affichés dans la table ID de moteur distant.

ÉTAPE 3 Cliquez sur **Apply**. Le fichier de configuration de fonctionnement est mis à jour.

La table ID de moteur distant affiche le mappage entre les adresses IP du moteur et l'ID de moteur. Pour ajouter l'adresse IP d'un ID de moteur :

ÉTAPE 4 Cliquez sur **Add**. Renseignez les champs suivants :

- **Server Definition** : indiquez si vous souhaitez spécifier le serveur d'ID de moteur par son adresse IP ou son nom.
- **Version IP** : sélectionnez le format IP pris en charge.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée).
- **Adresse IP du serveur/Nom** : saisissez l'adresse IP ou le nom de domaine du serveur de journalisation.
- **ID de moteur** : saisissez l'ID de moteur.

ÉTAPE 5 Cliquez sur **Apply**. Le fichier de configuration de fonctionnement est mis à jour.

Configuration de vues SNMP

Une vue est une étiquette définie par l'utilisateur pour une collecte de sous-arborescences MIB. Chaque ID de sous-arborescence est défini par l'*ID d'objet* (OID) de la racine des sous-arborescences concernées. Des noms célèbres peuvent être utilisés pour spécifier la racine de la sous-arborescence souhaitée ou un ID d'objet peut être saisi (voir **ID d'objet du modèle**).

Chaque sous-arborescence est soit incluse, soit exclue dans la vue en cours de définition.

La page Vues permet de créer et de modifier des vues SNMP. Les vues par défaut (Default, DefaultSuper) ne peuvent pas être modifiées.

Vous pouvez joindre des vues à des groupes via la page Groupes ou à une communauté qui utilise le mode d'accès de base via la page Communautés.

Pour définir des vues SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Views**.

ÉTAPE 2 Cliquez sur **Ajouter** pour définir de nouvelles vues.

ÉTAPE 3 Saisissez les paramètres.

- **Nom de la vue** : saisissez un nom de vue qui ne comporte pas plus de 30 caractères.
- **Sous-arborescence d'ID d'objet** : sélectionnez le nœud dans l'arborescence MIB, qui est inclus ou exclu dans la vue SNMP. Les options de sélection de l'objet sont les suivantes :
  - *Sélectionner dans la liste* : vous permet de parcourir l'arborescence MIB. Appuyez sur la touche *Haut* pour accéder au niveau du parent et des frères du nœud sélectionné ; appuyez sur la touche *Bas* pour descendre au niveau des enfants du nœud sélectionné. Cliquez sur les nœuds dans la vue pour passer d'un nœud à son frère. Utilisez la barre de défilement pour faire apparaître les frères dans la vue.
  - *Défini par l'utilisateur* : saisissez un ID d'objet qui n'est pas proposé dans l'option *Sélectionner dans la liste*.

ÉTAPE 4 Sélectionnez ou désélectionnez **Inclure dans la vue.** Si cette option est sélectionnée, les bases MIB sélectionnées sont incluses dans la vue ; sinon, elles sont exclues.

ÉTAPE 5 Cliquez sur **Apply**.

ÉTAPE 6 Afin de vérifier votre configuration des vues, sélectionnez les vues définies par l'utilisateur dans la liste **Filtre : Nom de la vue**. Les vues suivantes existent par défaut :

- **Par défaut** : vue SNMP par défaut pour les vues en lecture et en lecture/écriture.
- **DefaultSuper** : vue SNMP par défaut pour les vues d'administrateur.

D'autres vues peuvent être ajoutées.

- **Sous-arborescence d'ID d'objet** : affiche la sous-arborescence à inclure dans la vue SNMP ou à exclure de cette dernière.
- **Vue de sous-arborescence d'ID d'objet** : indique si la sous-arborescence définie est incluse ou exclue dans la vue SNMP sélectionnée.

Création de groupes SNMP

Dans SNMPv1 et SNMPv2, une chaîne de communauté est envoyée accompagnée des trames SNMP. La chaîne de communauté agit en tant que mot de passe pour accéder à un agent SNMP. Cependant, ni les trames, ni la chaîne de communauté ne sont cryptées. Par conséquent, SNMPv1 et SNMPv2 ne sont pas sécurisés.

Dans SNMPv3, les mécanismes de sécurité suivants peuvent être configurés.

- **Authentification** : le périphérique vérifie que l'utilisateur SNMP est un administrateur système autorisé. Cette opération est effectuée pour chaque trame.
- **Confidentialité** : les trames SNMP peuvent accueillir des données cryptées.

Ainsi, dans SNMPv3, il existe trois niveaux de sécurité :

- Pas de sécurité (Aucune authentification et aucune confidentialité)
- Authentification (Authentification et aucune confidentialité)
- Authentification et confidentialité

SNMPv3 permet de contrôler le contenu que chaque utilisateur peut lire ou écrire, ainsi que les notifications qu'il reçoit. Un groupe définit des privilèges de lecture/écriture et un niveau de sécurité. Il devient opérationnel lorsqu'il est associé à un utilisateur ou une communauté SNMP.

REMARQUE Pour associer à un groupe une vue qui n'est pas une vue par défaut, créez d'abord la vue sur la page Vues.

Pour créer un groupe SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Groups**.

Cette page contient les groupes SNMP existants ainsi que leurs niveaux de sécurité.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez les paramètres.

- **Nom de groupe** : saisissez le nom du nouveau groupe.
- **Modèle de sécurité** : sélectionnez la version SNMP qui est jointe au groupe, à savoir SNMPv1, v2 ou v3.

Il est possible de définir trois types de vues avec différents niveaux de sécurité. Pour chaque niveau de sécurité, sélectionnez les vues correspondant aux privilèges Lecture, Écriture et Notifier en saisissant les champs suivants :

- **Activer** : sélectionnez ce champ pour activer le niveau de sécurité.
- **Niveau de sécurité** : définissez le niveau de sécurité joint au groupe. SNMPv1 et SNMPv2 ne prennent pas en charge l'authentification, ni la confidentialité. Si SNMPv3 est sélectionné, choisissez l'une des options suivantes :
  - *Aucune authentification et aucune confidentialité* : les niveaux de sécurité Authentification ou Confidentialité ne sont pas affectés au groupe.
  - *Authentification et aucune confidentialité* : authentifie les messages SNMP et s'assure que l'origine du message SNMP est authentifiée, mais ne les crypte pas.
  - *Authentification et confidentialité* : authentifie les messages SNMP et les crypte.
- **Afficher** : sélectionnez cette option pour associer une vue avec les privilèges d'accès Lire, Écrire et/ou Notifier du groupe afin de limiter l'étendue de l'arborescence MIB à laquelle le groupe a un accès Lire, Écrire et Notifier.
  - *Read* : l'accès est en lecture seule pour la vue sélectionnée. Sinon, un utilisateur ou une communauté associés à ce groupe peuvent lire toutes les bases MIB, à l'exception de celles qui contrôlent le SNMP lui-même.
  - *Write* : l'accès à la gestion est en écriture pour la vue sélectionnée. Sinon, un utilisateur ou une communauté associés à ce groupe peuvent écrire dans toutes les bases MIB, à l'exception de celles qui contrôlent le SNMP lui-même.
  - *Notifier* : limite le contenu disponible des interceptions à ceux inclus dans la vue sélectionnée. Sinon, il n'existe aucune restriction sur le contenu des filtres. Cette option peut être sélectionnée pour SNMPv3.

ÉTAPE 4 Cliquez sur **Apply.** Le groupe SNMP est enregistré dans le fichier Configuration d'exécution.

Création d'utilisateurs SNMP

Un utilisateur SNMP est défini par les informations de connexion (nom d'utilisateur, mots de passe et méthode d'authentification), ainsi que par le contexte et l'étendue de son fonctionnement en association avec un groupe et un ID de moteur.

L'utilisateur configuré a les attributs de son groupe et dispose des privilèges d'accès définis dans la vue associée.

Les groupes permettent aux gestionnaires de réseaux d'affecter des droits d'accès à un groupe d'utilisateurs plutôt qu'à un utilisateur unique.

Un utilisateur peut être membre d'un seul groupe.

Pour créer un utilisateur SNMPv3, les éléments ci-dessous doivent exister au préalable :

- Un ID de moteur doit d'abord être configuré sur le périphérique. Cette opération s'effectue sur la page ID du moteur.
- Un groupe SNMPv3 doit être disponible. Vous pouvez définir un groupe SNMPv3 sur la page Groupes.

Pour afficher des utilisateurs SNMP et en définir de nouveaux :

ÉTAPE 1 Cliquez sur **SNMP** > **Users**.

Cette page contient les utilisateurs existants.

ÉTAPE 2 Cliquez sur **Ajouter**.

Cette page fournit des informations quant à l'affectation de privilèges de contrôle d'accès SNMP à des utilisateurs SNMP.

ÉTAPE 3 Saisissez les paramètres.

- **User Name** : saisissez un nom d'utilisateur.
- **ID du moteur** : sélectionnez l'entité SNMP locale ou distante à laquelle l'utilisateur est connecté. La modification ou la suppression de l'ID de moteur SNMP local supprime la base de données d'utilisateurs SNMPv3. Pour recevoir des messages d'information et demander des informations, vous devez définir un utilisateur local et un utilisateur distant.
  - *Local* : l'utilisateur est connecté au périphérique local.
  - *Adresse IP distante* : l'utilisateur est connecté à une autre entité SNMP, en plus du périphérique local. Si un ID de moteur distant est défini, les unités distantes reçoivent des messages d'information, mais ne peuvent effectuer de demandes d'information.

    Saisissez l'ID de moteur distant.

- **Group Name** : sélectionnez le groupe SNMP auquel appartient l'utilisateur SNMP. Vous pouvez définir les groupes SNMP sur la page Ajouter un groupe.

  REMARQUE Les utilisateurs appartenant à des groupes qui ont été supprimés sont conservés, mais sont inactifs.

- **Méthode d'authentification** : sélectionnez la méthode d'authentification qui varie en fonction du Nom de groupe qui a été attribué. Si le groupe ne requiert pas d'authentification, alors l'utilisateur ne peut configurer aucune authentification. Les options sont les suivantes :

  - *None* : aucune authentification d'utilisateur n'est utilisée.
  - *MD5* : mot de passe utilisé pour la génération d'une clé par la méthode d'authentification MD5.
  - *SHA* : mot de passe utilisé pour la génération d'une clé par la méthode d'authentification SHA (Secure Hash Algorithm).

- **Mot de passe d'authentification** : si l'authentification est effectuée via un mot de passe MD5 ou SHA, saisissez le mot de passe de l'utilisateur local en mode **Chiffré** ou **Texte en clair**. Les mots de passe d'utilisateur local sont comparés à la base de données locale et peuvent contenir jusqu'à 32 caractères ASCII.

- **Méthode de confidentialité** : sélectionnez l'une des options suivantes :

  - *Aucune* : le mot de passe de confidentialité n'est pas crypté.
  - *DES* : le mot de passe de confidentialité est crypté conformément à la norme de cryptage de données (DES, Data Encryption Standard).

- **Mot de passe de confidentialité** : 16 octets sont requis (clé de cryptage DES) si la méthode de confidentialité DES a été sélectionnée. Ce champ doit contenir exactement 32 caractères hexadécimaux. Vous pouvez sélectionner le mode **Chiffré** ou **Texte en clair**.

ÉTAPE 4 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Définition de communautés SNMP

Vous pouvez gérer les droits d'accès dans SNMPv1 et SNMPv2 en définissant des communautés sur la page Communautés. Le nom de la communauté correspond à un type de mot de passe partagé entre la station de gestion SNMP et l'unité. Il sert à authentifier la station de gestion SNMP.

Les communautés sont uniquement définies dans SNMPv1 et v2, car SNMPv3 fonctionne avec des utilisateurs et non avec des communautés. Les utilisateurs appartiennent à des groupes qui disposent de droits d'accès qui leur sont affectés.

La page Communauté associe des communautés à des droits d'accès, soit directement (mode de base), soit via des groupes (mode avancé) :

- **Mode De base** : les droits d'accès d'une communauté peuvent être définis en Lecture seule, Lecture/écriture ou Admin SNMP. Vous pouvez en outre restreindre l'accès à la communauté à certains objets MIB uniquement, en sélectionnant une vue (définie sur la page Vues SNMP).
- **Mode Avancé** : les droits d'accès à une communauté sont définis par un groupe (défini sur la page **Groupes**). Vous pouvez configurer le groupe avec un modèle de sécurité spécifique. Les groupes disposent des droits d'accès de lecture, d'écriture et de notification.

Pour définir des communautés SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Communities**.

Cette page contient une table des communautés SNMP configurées et de leurs propriétés.

ÉTAPE 2 Cliquez sur **Ajouter**.

Cette page permet aux gestionnaires de réseaux de définir et de configurer de nouvelles communautés SNMP.

ÉTAPE 3 **Station de gestion SNMP** : cliquez sur **Défini par l'utilisateur** pour saisir l'adresse IP de la station de gestion pouvant accéder à la communauté SNMP. Cliquez sur **Toutes** pour indiquer que n'importe quel périphérique IP peut accéder à la communauté SNMP.

- **Version IP** : sélectionnez IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 pris en charge, en cas d'utilisation d'IPv6. Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, spécifiez si la réception s'effectue via VLAN ou ISATAP.
- **Adresse IP** : saisissez l'adresse IP de la station de gestion SNMP.
- **Chaîne de communauté** : saisissez le nom de la communauté permettant d'authentifier la station de gestion sur le périphérique.

- **De base** : sélectionnez ce mode pour une communauté spécifique. Avec ce mode, aucune connexion n'est établie avec quelque groupe que ce soit. Vous pouvez uniquement choisir le niveau d'accès de la communauté (Lecture seule, Lecture/écriture ou Admin SNMP) et, facultativement, le faire davantage correspondre à une vue. Par défaut, cela s'applique à la totalité d'une base MIB. Si cette option est sélectionnée, saisissez les champs suivants :
  - *Mode d'accès* : sélectionnez les droits d'accès de la communauté. Les options sont les suivantes :

    Lecture seule : l'accès à la gestion se fait en lecture seule uniquement. Aucune modification ne peut être apportée à la communauté.

    Lecture/écriture : l'accès à la gestion se fait en lecture et écriture. Des modifications ne peuvent être apportées qu'à la configuration d'unité, pas à la communauté.

    Admin SNMP : l'utilisateur dispose d'un accès à toutes les options de configuration d'unité ainsi qu'aux autorisations de modification de la communauté. Admin SNMP équivaut à Lecture/écriture pour toutes les bases MIB, à l'exception des bases MIB SNMP. Admin SNMP est requis pour l'accès aux bases MIB SNMP.
  - *Nom de la vue* : sélectionnez une vue SNMP (collection de sous-arborescences de bases MIB auxquelles un accès est accordé).
- **Avancé** : sélectionnez ce mode pour une communauté spécifique.
  - *Nom du groupe* : sélectionnez un groupe SNMP qui détermine les droits d'accès.

ÉTAPE 4 Cliquez sur **Apply**. La communauté SNMP est définie et le fichier de Configuration d'exécution est mis à jour.

Définition de paramètres d'interceptions

La page Paramètres de filtre permet de spécifier si les notifications SNMP doivent être envoyées à partir du périphérique, et à quelles conditions. Vous pouvez configurer les destinataires des notifications SNMP sur la page Destinataires de notifications SNMPv1,2 ou sur la page Destinataires de notifications SNMPv3.

Pour définir des paramètres d'interception :

ÉTAPE 1 Cliquez sur **SNMP** > **Paramètres d'interception**.

ÉTAPE 2 Sélectionnez **Activer** pour **Notifications SNMP** et indiquez que le périphérique peut envoyer des notifications SNMP.

ÉTAPE 3 Sélectionnez **Activer** pour **Notifications d'authentification** pour activer la notification d'échec d'authentification SNMP.

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres de filtre SNMP sont écrits dans le fichier de Configuration d'exécution.

Destinataires de notifications

Des filtres sont générés pour signaler des événements système, tels que défini dans la RFC 1215. Le système peut générer des filtres définis dans la base MIB qu'il prend en charge.

Les récepteurs d'interruption (connus sous le nom de destinataires de notifications) sont des nœuds réseau où des interceptions sont envoyées par le périphérique. Plusieurs destinataires de notification sont répertoriés comme cibles des filtres.

Une entrée de destination de l'interception contient l'adresse IP du nœud et les informations SNMP qui correspondent à la version qui doit être incluse dans l'interception. Lorsqu'un événement nécessite l'envoi d'un message d'interception, ce dernier est envoyé vers chaque nœud répertorié dans la Table des destinataires de notifications.

La page Destinataires de notifications SNMPv1,2 et la page Destinataires de notifications SNMPv3 permettent de configurer la destination d'envoi des notifications SNMP, ainsi que les types de notifications SNMP envoyées vers chaque destination (interceptions ou informations). Les messages contextuels Ajouter/Modifier permettent la configuration des attributs des notifications.

Une notification SNMP est un message envoyé depuis le périphérique vers la station de gestion SNMP, qui indique qu'un événement spécifique s'est produit, tel que l'activation ou la désactivation d'une liaison.

Vous pouvez également filtrer certaines notifications. Pour ce faire, vous devez créer un filtre sur la page Filtre de notification et le joindre à un destinataire de notification SNMP. Le filtre de notification permet le filtrage du type des notifications SNMP envoyées à la station de gestion, en fonction de l'ID d'objet de la notification sur le point d'être envoyée.

Définition de destinataires de notifications SNMPv1,2

Pour définir un destinataire dans SNMPv1,2 :

ÉTAPE 1 Cliquez sur **SNMP** > **Notification Recipients SNMPv1,2**.

Cette page affiche les destinataires pour SNMPv1,2.

ÉTAPE 2 Renseignez les champs suivants :

- **Informe l'interface IPv4 source** : sélectionnez l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source dans les messages d'information utilisés dans les communications avec les serveurs SNMP IPv4.
- **Déroute l'interface IPv4 source** : sélectionnez l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source dans les interceptions utilisés dans les communications avec les serveurs SNMP IPv4.
- **Informe l'interface IPv6 source** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source dans les messages d'information utilisés dans les communications avec les serveurs SNMP IPv6.
- **Déroute l'interface IPv6 source** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source dans les interceptions utilisés dans les communications avec les serveurs SNMP IPv6.

  REMARQUE Si l'option Auto est sélectionnée, le système récupère l'adresse IP source de l'adresse IP définie dans l'interface sortante.

  ÉTAPE 3 Cliquez sur **Ajouter**.

  ÉTAPE 4 Saisissez les paramètres.
- **Définition de serveur** : indiquez si vous souhaitez spécifier le serveur de journalisation distant par son adresse IP ou son nom.
- **Version IP** : sélectionnez IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez soit *Liaison locale*, soit *Global*.
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, spécifiez si la réception s'effectue via VLAN ou ISATAP.
- **Adresse IP/Nom du destinataire** : saisissez l'adresse IP ou le nom du serveur où les interceptions sont envoyées.
- **UDP Port** : saisissez le port UDP utilisé pour les notifications sur l'unité du destinataire.
- **Type de notification** : indiquez le type de données à envoyer (interceptions ou informations). Si les deux sont nécessaires, deux destinataires doivent être créés.
- **Délai** : saisissez la durée en secondes pendant laquelle le périphérique doit attendre avant de renvoyer des informations.

- **Tentatives** : saisissez le nombre de fois que le périphérique peut renvoyer une demande d'information.
- **Chaîne de communauté** : dans le menu déroulant, saisissez la chaîne de communauté du gestionnaire d'interceptions. Les noms de chaîne de communauté sont générés à partir de ceux répertoriés sur la page Communauté.
- **Version de notification** : sélectionnez la version SNMP du filtre.
  Vous pouvez utiliser SNMPv1 ou SNMPv2 comme version des interceptions, mais une seule version peut être activée à la fois.
- **Filtre de notification** : sélectionnez cette option pour activer le filtrage du type des notifications SNMP transmises à la station de gestion. Les filtres sont créés sur la page Filtre de notification.
- **Nom du filtre** : sélectionnez le filtre SNMP qui spécifie les informations contenues dans les interceptions (définies sur la page Filtre de notification).

ÉTAPE 5 Cliquez sur **Apply**. Les paramètres de destinataire de notification SNMP sont écrits dans le fichier de Configuration d'exécution.

Définition de destinataires de notification SNMPv3

Pour définir un destinataire dans SNMPv3 :

ÉTAPE 1 Cliquez sur **SNMP** > **Notification Recipients SNMPv3**.

Cette page affiche les destinataires pour SNMPv3.

- **Informe l'interface IPv4 source** : sélectionnez l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source dans les messages d'information utilisés dans les communications avec les serveurs SNMP IPv4.
- **Déroute l'interface IPv4 source** : sélectionnez l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source dans les interceptions utilisés dans les communications avec les serveurs SNMP IPv4.
- **Informe l'interface IPv6 source** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source dans les messages d'information utilisés dans les communications avec les serveurs SNMP IPv6.
- **Déroute l'interface IPv6 source** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source dans les interceptions utilisés dans les communications avec les serveurs SNMP IPv6.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Définition de serveur** : indiquez si vous souhaitez spécifier le serveur de journalisation distant par son adresse IP ou son nom.
- **Version IP** : sélectionnez IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez l'interface de liaison locale dans la liste déroulante (si la liaison locale du type d'adresse IPv6 est sélectionnée).
- **Adresse IP/Nom du destinataire** : saisissez l'adresse IP ou le nom du serveur où les interceptions sont envoyées.
- **Port UDP** : saisissez le port UDP utilisé pour les notifications sur l'unité du destinataire.
- **Type de notification** : indiquez le type de données à envoyer (interceptions ou informations). Si les deux sont nécessaires, deux destinataires doivent être créés.
- **Délai** : saisissez la durée (en secondes) pendant laquelle le périphérique attend avant de renvoyer des informations/interceptions. Expiration : Plage de 1 à 300, 15 par défaut
- **Tentatives** : saisissez le nombre de fois que le périphérique peut renvoyer une demande d'information. Tentatives : plage de 1 à 255, 3 par défaut
- **Nom d'utilisateur** : dans la liste déroulante, sélectionnez l'utilisateur auquel les notifications SNMP sont envoyées. Pour recevoir les notifications, cet utilisateur doit être défini sur la page Utilisateur SNMP, et son ID de moteur doit être distant.
- **Niveau de sécurité** : sélectionnez le niveau d'authentification appliqué au paquet.

  REMARQUE Le niveau de sécurité dépend du nom d'utilisateur qui a été sélectionné. Si le paramètre Aucune authentification a été défini pour ce nom d'utilisateur, le niveau de sécurité est uniquement Aucune authentification. Cependant, si le paramètre Authentification et confidentialité a été défini pour ce nom d'utilisateur sur la page Utilisateur, le niveau de sécurité sur cet écran peut être Aucune authentification, Authentification ou Authentification et confidentialité.

  Les options sont les suivantes :
  - *Aucune authentification* : indique que le paquet n'est pas authentifié ni crypté.
  - *Authentification* : indique que le paquet est authentifié, mais pas crypté.
  - *Confidentialité* : indique que le paquet est à la fois authentifié et crypté.

- **Filtre de notification** : sélectionnez cette option pour activer le filtrage du type des notifications SNMP transmises à la station de gestion. Les filtres sont créés sur la page Filtre de notification.
- **Nom du filtre** : sélectionnez le filtre SNMP qui spécifie les informations contenues dans les interceptions (définies sur la page Filtre de notification).

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres de destinataire de notification SNMP sont écrits dans le fichier de Configuration d'exécution.

Filtres de notification SNMP

La page Filtre de notification permet de configurer des filtres de notification SNMP et des ID d'objet (OID) soumis à vérification. Après avoir créé un filtre de notification, vous pouvez le joindre à un destinataire de notification via la page Destinataires de notifications SNMPv1,2 et la page Destinataires de notifications SNMPv3.

Le filtre de notification permet le filtrage du type des notifications SNMP envoyées à la station de gestion, en fonction de l'ID d'objet de la notification à envoyer.

Pour définir un filtre de notification :

ÉTAPE 1 Cliquez sur **SNMP** > **Filtre de notification**.

La page Filtre de notification contient les informations de notification relatives à chaque filtre. Ce tableau peut filtrer des entrées de notification par nom de filtre.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez les paramètres.

- **Nom du filtre** : saisissez un nom qui ne comporte pas plus de 30 caractères.
- **Sous-arborescence d'ID d'objet** : sélectionnez le nœud dans l'arborescence MIB, qui est inclus dans le filtre SNMP sélectionné ou exclu de celui-ci. Les options de sélection de l'objet sont les suivantes :
  - *Sélectionner dans la liste* : vous permet de parcourir l'arborescence MIB. Appuyez sur la touche *Haut* pour accéder au niveau du parent et des frères du nœud sélectionné ; appuyez sur la touche *Bas* pour descendre au niveau des enfants du nœud sélectionné. Cliquez sur les nœuds dans la vue pour passer d'un nœud à son frère. Utilisez la barre de défilement pour faire apparaître les frères dans la vue.

- Si vous utilisez l'*ID d'objet*, l'**identificateur d'objet saisi** est inclus dans la vue si l'option **Inclure dans le filtre** est sélectionnée.

ÉTAPE 4 Sélectionnez ou désélectionnez **Inclure dans le filtre.** Si cette option est sélectionnée, les bases MIB sélectionnées sont incluses dans le filtre ; sinon, elles sont exclues.

ÉTAPE 5 Cliquez sur **Apply.** Les vues SNMP sont définies et le fichier de Configuration d'exécution est mis à jour.