



GUIDE D'ADMINISTRATION

Cisco Small Business Commutateur intelligent série SG200 à 8 ports

Chapitre 1 : Prise en main	8
Démarrage de l'utilitaire Web de configuration du commutateur	8
Lancement de l'utilitaire	9
Connexion	9
Déconnexion	10
Configuration de l'appareil - Démarrage rapide	11
Navigation dans les fenêtres	12
En-tête d'application	12
Autres ressources	13
Fenêtre de navigation	14
Boutons de gestion	15
Chapitre 2 : État et statistiques	19
Récapitulatif du système	19
Affichage du récapitulatif du système	19
Configuration des paramètres système	22
Statistiques relatives aux interfaces	23
Statistiques relatives à Etherlike	24
Statistiques EAP 802.1X	25
Statistiques DHCP IPv6	26
Statistiques RADIUS	27
RMON	28
Journaux	30
Journal de la mémoire RAM	30
Journal de la mémoire flash	31
Chapitre 3 : Administration	34
Configuration des paramètres système	35
Interface de gestion	36
Configuration d'une interface de gestion IPv4	36
Configuration d'une interface de gestion IPv6	38

Ajout d'adresses IPv6	38
Table des routeurs par défaut IPv6	39
Affichage et ajout de voisins IPv6	40
Gestion des comptes d'utilisateurs	41
Ajout d'un utilisateur	41
Modification d'un mot de passe utilisateur	42
Suppression d'un utilisateur	43
Activation des services de gestion	43
Configuration du délai d'expiration de session inactive	44
Sessions de connexion	44
Historique de connexion	45
Paramètres de l'heure	45
Définition de l'heure système	45
Configuration des paramètres SNTP	48
Configuration de l'authentification SNTP	52
Journaux système	53
Configuration des paramètres de journal	53
Configuration des serveurs de journalisation distants	55
Gestion de fichiers	56
Mise à niveau et sauvegarde des fichiers de micrologiciel et de langue	58
Téléchargement et sauvegarde des fichiers de configuration et journaux	60
Téléchargement d'un fichier de configuration pour restaurer des paramètres	60
Sauvegarde du fichier de configuration et des journaux	62
Supprimer la configuration	63
Copie et enregistrement des fichiers de configuration	64
Configuration automatique DHCP	65
Présentation	65
Détails des messages du serveur DHCP	66
Serveur TFTP secondaire et nom de fichier	67
Détails de téléchargement du fichier de configuration	67
Définition de la configuration automatique DHCP	70

Récupération du micrologiciel via HTTP	71
Redémarrage du commutateur	73
Envoi de requêtes ping à des hôtes	74
Configuration du transfert de paquets de contrôle	75
Diagnostics	76
Test des ports cuivre	76
Configuration de la mise en miroir des ports	77
Utilisation de la mémoire/des CPU	79
Activation de Bonjour	80
LLDP-MED	81
Configuration des propriétés LLDP-MED globales	82
Configuration de LLDP-MED sur un port	83
Détails sur l'état des ports LLDP-MED	84
Informations sur le voisinage LLDP-MED	86
Configuration des options de fournisseur de client DHCP	88

Chapitre 4 : Gestion des ports **89**

Configuration des paramètres des ports	89
Agrégation de liaisons	91
Configuration des LAG	91
Configuration des paramètres des LAG	92
Configuration des paramètres LACP	93
Configuration de PoE	95
Configuration des propriétés PoE	95
Configuration des paramètres des ports PoE	96
Green Ethernet	99
Configuration des propriétés Green Ethernet	100
Configuration des paramètres Green Ethernet des ports	101

Chapitre 5 : Gestion des VLAN	104
Création d'un VLAN	105
Configuration des paramètres d'interface VLAN	106
Modification du mode VLAN de l'interface	108
Configuration d'une appartenance VLAN	109
Configuration de ports vers un VLAN	110
Configuration d'une appartenance VLAN des ports	111
Définition du VLAN par défaut	113
Trafic vocal et multimédia	114
Affichage et ajout des OUI de téléphonie	114
Configuration de la fonctionnalité Trafic vocal et multimédia basé sur OUI	115
Configuration de la fonctionnalité Trafic vocal et multimédia basé sur les protocoles SIP/H323	116
VLAN multimédia	117
Sessions VoIP automatique	120
Chapitre 6 : Arbre recouvrant	121
Description du protocole d'arbre recouvrant	121
Configuration de l'état et des paramètres globaux du protocole d'arbre recouvrant	122
Configuration des paramètres globaux et des ponts	123
Configuration des paramètres d'interface STP	125
Paramètres d'interface RSTP	127
Chapitre 7 : Tables d'adresses MAC	129
Configuration d'adresses MAC statiques	129
Configuration du délai d'expiration des adresses dynamiques	131
Adresses MAC dynamiques	131

Chapitre 8 : Multidiffusion	133
Propriétés de multidiffusion	134
Configuration d'un mode de transfert multidiffusion sur tous les VLAN	134
Configuration de propriétés de multidiffusion sur un VLAN	135
Configuration d'adresses MAC de groupe	136
Affichage de la Table des adresses MAC de groupes	136
Ajout d'une entrée statique à la Table des adresses MAC de groupes	137
Configuration de l'appartenance des ports à des groupes d'adresses MAC	137
Configuration de la surveillance de trafic IGMP	138
Configuration de la surveillance de trafic MLD	140
Configuration d'interfaces de routeur de multidiffusion IGMP	142
Configuration d'interfaces de routeur de multidiffusion MLD	143
Chapitre 9 : Configuration IP	145
Table ARP	145
Système de noms de domaine	146
Configuration de serveurs DNS	146
Configuration des paramètres DNS globaux	146
Ajout de serveurs DNS	147
Mappage des noms d'hôte	147
Configuration des mappages DNS statiques	148
Affichage et suppression d'entrées DNS dynamiques	148
Chapitre 10 : Sécurité	150
RADIUS	150
Configuration des paramètres RADIUS globaux	151
Ajout d'un serveur RADIUS	152
Fiabilité du mot de passe	153
Règles du profil d'accès de gestion	154
Configuration du profil et des règles d'accès	155

Modification et suppression des profils et des règles d'accès	156
Méthodes d'authentification	158
Contrôle des tempêtes	159
Sécurité des ports	160
Activation de la sécurité des ports	161
Affichage et configuration des adresses MAC sécurisées	162
802.1X	163
Définition des propriétés 802.1X	164
Modification des fonctionnalités des extensions d'adresse physique des ports	165
Configuration de l'authentification des ports	166
Configuration de l'authentification des ports du demandeur	168
Affichage des hôtes authentifiés	169

Chapitre 11 : Qualité de service 170

Propriétés de QoS	171
Définition de files d'attente	173
Recommandations en matière de configuration des files d'attente	173
Configuration des files d'attente	174
Mappage de priorités CoS/802.1p aux files d'attente	175
Mappage de la priorité IP aux files d'attente	176
Mappage de valeurs DSCP aux files d'attente	178
Définition de profils de limitation de débit	179
Application de profils de limitation de débit à des interfaces	180
Mise en forme du trafic	181

Prise en main

Ce chapitre propose une introduction à l'utilitaire Web de configuration du commutateur et contient les rubriques suivantes :

- **Démarrage de l'utilitaire Web de configuration du commutateur**
- **Configuration de l'appareil - Démarrage rapide**
- **Navigation dans les fenêtres**

Démarrage de l'utilitaire Web de configuration du commutateur

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

Les restrictions suivantes s'appliquent aux navigateurs :

- Si vous utilisez Internet Explorer 8, ouvrez une fenêtre du navigateur et configurez les paramètres suivants :

Cliquez sur **Outils > Options Internet**, puis sélectionnez l'onglet **Sécurité**. Sélectionnez **Intranet local** et cliquez sur **Sites**. Cliquez sur **Avancé**, puis sur **Ajouter**. Ajoutez l'adresse Intranet du commutateur (<http://<adresse-ip>>) dans la zone Intranet locale. L'adresse IP peut également être spécifiée en tant qu'adresse IP du sous-réseau, afin que toutes les adresses du sous-réseau soient ajoutées à la zone Intranet locale.
- Si vous utilisez Internet Explorer 6, vous ne pouvez pas utiliser directement une adresse IPv6 pour accéder au commutateur. Vous pouvez néanmoins utiliser le serveur DNS (Domain Name System, système de noms de domaine) pour créer un nom de domaine contenant l'adresse IPv6, puis utiliser ce nom de domaine dans la barre d'adresse à la place de l'adresse IPv6.

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

Lancement de l'utilitaire

Pour ouvrir l'utilitaire Web de configuration du commutateur :

-
- ÉTAPE 1** Ouvrez un navigateur Web.
- ÉTAPE 2** Saisissez l'adresse IP du commutateur à configurer dans la barre d'adresse du navigateur, puis appuyez sur **Entrée**. L'écran *Connexion* s'ouvre.
-

Connexion

Pour vous connecter à l'utilitaire Web de configuration du commutateur :

-
- ÉTAPE 1** Saisissez le *nom d'utilisateur* et le *mot de passe*. Le nom d'utilisateur définit en usine est **cisco**, et le mot de passe par défaut **cisco**.

Remarque : lorsque le commutateur démarre avec la configuration d'usine par défaut, l'utilitaire Web de configuration du commutateur s'affiche dans la langue par défaut. Une fois que vous vous êtes connecté, vous pouvez télécharger des langues supplémentaires depuis la page *Mettre à niveau/sauvegarder micrologiciel/langue*.

- ÉTAPE 2** S'il s'agit de votre première ouverture de session avec le nom d'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 d'administrateur* s'ouvre. Saisissez le nouveau mot de passe, confirmez-le, cliquez sur **Appliquer**, puis cliquez sur **Fermer**. Le nouveau mot de passe est enregistré.

- ÉTAPE 3** Cliquez sur **Se connecter**.

Une fois la connexion établie, la page *Prise en main* 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 à l'écran.

Sélectionnez **Ne pas afficher cette rubrique au démarrage** pour que la page *Prise en main* ne s'affiche pas à chaque fois que vous vous connectez au système. Si vous sélectionnez cette option, la page *Récapitulatif du système* s'ouvre à la place de la rubrique *Prise en main*.

Déconnexion

Par défaut, l'application vous déconnecte automatiquement au bout de dix minutes d'inactivité. Consultez la section **Configuration du délai d'expiration de session inactive** pour obtenir des instructions sur la modification du délai d'expiration par défaut.

Pour vous déconnecter à tout moment, cliquez sur **Se déconnecter** en haut à droite de n'importe quelle page.



ATTENTION

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

Une icône **X** rouge qui s'affiche à gauche du bouton Enregistrer indique que des changements apportés à la Configuration d'exécution n'ont pas encore été enregistrés dans le type de fichier Configuration de démarrage.

Lorsque vous cliquez sur **Enregistrer**, la page s'affiche (voir la section **Téléchargement et sauvegarde des fichiers de configuration et journaux**). Pour enregistrer la configuration d'exécution, copiez-la vers le type de fichier Configuration de démarrage. Une fois cet enregistrement effectué, l'icône **X** rouge et le bouton Enregistrer ne s'affichent plus.

Configuration de l'appareil - Démarrage rapide

Pour simplifier la configuration de l'appareil, vous pouvez accéder rapidement aux pages les plus fréquemment utilisées, à l'aide des liens fournis à la page *Prise en main*.

Liens de la page Prise en main

Catégorie	Nom du lien (sur la page)	Page correspondante
Configuration initiale	Modifier l'adresse IP de l'appareil	<i>Interface IPv4</i>
	Créer un VLAN	<i>Création d'un VLAN</i>
	Configurer les paramètres de port	<i>Paramètres des ports</i>
État de l'appareil	Récapitulatif du système	<i>Récapitulatif du système</i>
	Statistiques des ports	<i>Interface</i>
	Statistiques RMON	<i>RMON Statistiques</i>
	Afficher le journal	<i>Mémoire RAM</i>
Accès rapide	Modifier le mot de passe de l'appareil	<i>Comptes d'utilisateurs</i>
	Mettre à niveau le logiciel de l'appareil	<i>Mettre à niveau/sauvegarder micrologiciel/langue</i>
	Sauvegarder la configuration de l'appareil	<i>Télécharger/sauvegarder configuration/journal</i>
	Configurer la QoS	<i>Propriétés de QoS</i>
	Configurer la mise en miroir des ports	<i>Mise en miroir de ports</i>



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. Il comporte les boutons suivants :

Boutons

Nom du bouton	Description
	Le bouton d'état d'alerte Syslog (cercle rouge comportant un X) s'affiche en cas de journalisation d'un nouveau message Syslog dont le niveau de sévérité se situe au-dessus du niveau critique. Cliquez pour ouvrir la page État et statistiques > Afficher le journal > Journal de la mémoire RAM . Une fois que vous aurez accédé à cette page, le bouton d'état d'alerte Syslog ne s'affichera plus.
	<p>L'icône X rouge qui s'affiche à gauche du bouton Enregistrer indique que des changements apportés à la configuration n'ont pas encore été enregistrés dans le fichier de Configuration de démarrage.</p> <p>Lorsque vous cliquez sur ce bouton, la page <i>Télécharger/sauvegarder configuration/journal</i> s'affiche. Enregistrez la Configuration d'exécution en la copiant dans le type de fichier Configuration de démarrage. Une fois cet enregistrement effectué, l'icône X rouge et le bouton Enregistrer ne s'affichent plus. Au redémarrage du commutateur, le type de fichier Configuration de démarrage est copié vers la configuration d'exécution et les paramètres du commutateur sont définis en fonction des données de configuration d'exécution.</p>
Utilisateur	Le nom de l'utilisateur connecté au commutateur. Le nom d'utilisateur par défaut est cisco .

Boutons (Suite)

Nom du bouton	Description
Menu Langue	Sélectionnez une langue ou chargez un nouveau fichier de langue dans l'appareil. Si la langue requise s'affiche dans le menu, sélectionnez-la. Dans le cas contraire, sélectionnez Download Language (Télécharger une langue) . Pour plus d'informations sur l'ajout d'une nouvelle langue, reportez-vous à la page <i>Mettre à niveau/sauvegarder micrologiciel/langue</i> .
Déconnexion	Cliquez sur ce bouton pour vous déconnecter de l'utilitaire Web de configuration du commutateur.
À propos de	Cliquez sur ce bouton pour afficher le type du commutateur et son numéro de version.
Aide	Cliquez sur ce bouton pour afficher l'aide en ligne.

Autres ressources

Vous pouvez utiliser les liens suivants de la page Avant de commencer pour obtenir des informations et une aide supplémentaires se rapportant à l'utilisation de votre commutateur :

- **Assistance** : affiche la page Web d'assistance des commutateurs gérés Cisco Small Business.
- **Forums** : affiche la page Web de la communauté d'assistance Cisco Small Business.

Fenêtre de navigation

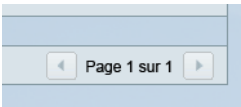


Une fenêtre de navigation est présente sur le côté gauche de chaque page. Cliquez sur une catégorie de niveau supérieur pour afficher des liens vers des pages connexes. Les liens précédés d'une flèche correspondent à des sous-catégories que vous pouvez développer pour afficher les liens vers les pages connexes.



Boutons de gestion

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

Boutons de gestion

Nom du bouton	Description
	Selon le nombre de pages et la page actuellement affichée, utilisez ces fonctions pour vous déplacer dans les pages de la table. Cliquez sur < pour accéder à la première page, sur < pour accéder à la page précédente, sur > pour accéder à la page suivante, et sur > pour accéder à la dernière page. Utilisez la liste déroulante Page <numéro> sur <numéro> pour choisir une page spécifique.
	Sélectionnez le nombre d'entrées de table à afficher sur chaque page.
	Indique un champ obligatoire.
Ajouter	<p>Cliquez sur ce bouton pour afficher la rubrique <i>Ajouter</i> correspondante et ajouter une entrée à une table. Saisissez les informations et cliquez sur Appliquer. Cliquez sur Fermer pour retourner à la page principale.</p> <p>Remarque : vos modifications sont uniquement appliquées à la Configuration d'exécution. En cas de redémarrage du commutateur, la Configuration d'exécution est perdue. Pour enregistrer vos modifications dans la Configuration de démarrage, cliquez sur Enregistrer. Pour plus d'informations, consultez la rubrique Copie et enregistrement des fichiers de configuration.</p>

Boutons de gestion (Suite)

Nom du bouton	Description
Appliquer	<p>Cliquez sur ce bouton pour appliquer les modifications que vous avez saisies sur la page sélectionnée.</p> <p>Remarque : vos modifications sont uniquement appliquées à la Configuration d'exécution. En cas de redémarrage du commutateur, la Configuration d'exécution est perdue. Pour enregistrer vos modifications dans la Configuration de démarrage, cliquez sur Enregistrer. Pour plus d'informations, consultez la rubrique Copie et enregistrement des fichiers de configuration.</p>
Annuler	Cliquez sur ce bouton pour annuler les modifications apportées à la page et réinitialiser les valeurs aux entrées précédemment appliquées.
Effacer les compteurs de toutes les interfaces	Cliquez sur ce bouton pour effacer les compteurs de statistiques de toutes les interfaces.
Effacer les compteurs de l'interface	Cliquez sur ce bouton pour effacer les compteurs de statistiques de l'interface sélectionnée.
Effacer les journaux	Cliquez sur ce bouton pour effacer les fichiers journaux.
Effacer la table	Cliquez sur ce bouton pour effacer les entrées de la table.
Fermer	Cliquez sur ce bouton pour retourner à la page principale. Un message s'affiche si des modifications n'ont pas été appliquées à la Configuration d'exécution.

Boutons de gestion (Suite)

Nom du bouton	Description
Copier les paramètres	<p>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 cela est décrit ci-dessous :</p> <ul style="list-style-type: none"> ▪ Sélectionnez l'entrée à copier. Cliquez sur Copier les paramètres. ▪ Saisissez les numéros d'entrées de destination. ▪ Cliquez sur Appliquer pour enregistrer les modifications dans la Configuration d'exécution. ▪ Cliquez sur Fermer pour retourner à la page principale.
Supprimer	Sélectionnez l'entrée à supprimer dans la table et cliquez sur Supprimer . L'entrée est supprimée.
Détails	Cliquez sur ce bouton pour afficher les détails de l'entrée sélectionnée sur la page principale.
Modifier	<p>Sélectionnez une entrée et cliquez sur Modifier pour l'ouvrir à des fins d'édition. La page <i>Modifier</i> s'ouvre et l'entrée peut être modifiée.</p> <ul style="list-style-type: none"> ▪ Cliquez sur Appliquer pour enregistrer les modifications dans la Configuration d'exécution. ▪ Cliquez sur Fermer pour retourner à la page principale.
Tester	Cliquez sur Tester pour effectuer les tests apparentés.
Effacer le filtre	Cliquez sur Effacer le filtre pour réafficher les données d'une page avec les critères par défaut.
OK	Cliquez sur OK pour filtrer les données s'affichant sur une page en utilisant les critères sélectionnés.

Boutons de gestion (Suite)

Nom du bouton	Description
Boutons de tri	Si le message <i>Cette table peut être triée</i> s'affiche en dessous d'une table, chaque en-tête de colonne correspond à un bouton de tri. Cliquez sur un en-tête de colonne pour trier les enregistrements dans l'ordre croissant, en fonction du contenu de la colonne sélectionnée. Une fois le tri appliqué, une flèche apparaît dans l'en-tête de la colonne. Vous pouvez cliquer sur cette flèche pour inverser l'ordre du tri.

État et statistiques

Ce chapitre explique comment afficher les statistiques du commutateur.

Il contient les rubriques suivantes :

- **Récapitulatif du système**
- **Statistiques relatives aux interfaces**
- **Statistiques relatives à Etherlike**
- **Statistiques EAP 802.1X**
- **Statistiques DHCP IPv6**
- **RMON**
- **Journaux**

Récapitulatif du système

La page *Récapitulatif du système* contient les principales informations, notamment la description du modèle du commutateur, la version du logiciel et le temps d'activité du système.

Affichage du récapitulatif du système

Pour afficher les informations relatives au système, cliquez sur **État et statistiques** > **Récapitulatif du système** dans la fenêtre de navigation, ou sur **Récapitulatif du système** sous **État de l'appareil** de la page *Prise en main*.

Cette page affiche les informations suivantes :

- **Description du système** : affiche une description du système.

- **Emplacement du système** : indique l'emplacement physique du commutateur. Cliquez sur **Modifier** pour accéder à la page *Paramètres système* et complétez ce champ.
- **Contact système** : indique le nom de la personne à contacter. Cliquez sur **Modifier** pour accéder à la page *Paramètres système* et complétez ce champ.
- **Nom d'hôte** : indique le nom du commutateur. Cliquez sur **Modifier** pour accéder à la page *Paramètres système* et complétez ce champ. Par défaut, le nom d'hôte du commutateur se compose du mot *switch* concaténé avec les trois octets les moins significatifs de l'adresse MAC du commutateur (les six chiffres hexadécimaux les plus à droite).
- **Temps utilisation syst.** : affiche le temps qui s'est écoulé depuis le dernier redémarrage.
- **Heure actuelle** : indique l'heure actuelle du système.
- **Adresse MAC de base** : indique l'adresse MAC du commutateur.

Informations sur la version du matériel et du micrologiciel

Les informations suivantes relatives à la version du matériel et du micrologiciel sont disponibles :

- **Numéro de série** : indique le numéro de série du commutateur.
- **PID VID** : affiche la référence et l'identifiant de la version.
- **Puissance maximale disponible (W)** : indique la puissance maximale disponible pouvant être fournie par les ports PoE (commutateurs PoE uniquement).
- **Consommation de l'alimentation principale (W)** : indique la puissance actuellement fournie aux périphériques PoE connectés au commutateur (commutateurs PoE uniquement).
- **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** : indique la version du code de démarrage.
- **Total de contrôle MD5 au démarrage** : affiche le total de contrôle MD5 au démarrage du code de démarrage.

En outre, la vue graphique du commutateur permet d'afficher les paramètres de chaque port du commutateur. Pour afficher la page *Paramètres des ports*, cliquez sur le port de votre choix.

Services TCP et UDP

Cette table répertorie les informations sur tous les services TCP et UDP :

- **Nom du service** : affiche le nom du service couramment utilisé, si disponible, tel que HTTP.
- **Type** : indique le protocole de transfert utilisé pour ce service (TCP ou UDP).
- **Port** : indique le numéro de port IANA (Internet Assigned Numbers Authority) utilisé pour ce service.
- **Adresse IP** : affiche l'adresse IP, si disponible, d'un appareil distant connecté à ce service du commutateur.
- **Port distant** : affiche le numéro de port IANA d'un appareil distant communiquant avec ce service.
- **État** : affiche l'état du service. Pour les services UDP, seules les connexions actives s'affichent dans la table. Lorsque l'état d'une connexion est défini sur Actif, une connexion est établie entre le commutateur et un client ou un serveur. Les états TCP suivants sont disponibles :
 - **Écouter** : le service écoute les requêtes de connexion.
 - **Actif** : une connexion est établie et les paquets sont transmis et reçus.
 - **Établi** : une connexion est établie entre le commutateur et un serveur ou un client, selon le rôle de l'appareil défini pour ce protocole.

Table des modules linguistiques

Cette table contient des informations sur les langues disponibles pour le commutateur. L'administrateur peut sélectionner une langue lors de la connexion à l'utilitaire de configuration.

L'anglais, défini en tant que langue par défaut, est intégré au logiciel. Pour télécharger d'autres modules linguistiques, accédez à la page *Mettre à niveau/sauvegarder micrologiciel/langue*. Les fichiers de langue sont disponibles sur la page de téléchargement de micrologiciels Cisco.

La table des modules linguistiques répertorie les informations suivantes pour toutes les langues disponibles :

- **Langue** : affiche le nom de la langue.
- **Paramètres régionaux** : affiche le code des paramètres régionaux IETF (Internet Engineering Task Force) qui identifie la langue, le pays et la région.
- **Version** : indique la version du fichier de langue.
- **Total de contrôle MD5** : affiche le code de hachage de 128 bits qui vérifie l'intégrité des fichiers.
- **Type de fichier** : ce champ peut prendre l'une des valeurs suivantes :
 - **Intégré** : affiche la langue du logiciel définie par défaut. Elle ne peut pas être téléchargée sous forme de fichier séparé.
 - **Externe** : définit le fichier de langue qui peut être téléchargé sur le commutateur et sélectionné lors de l'ouverture de la session.
- **Taille de fichier** : indique la taille du fichier (en Ko).
- **Langue par défaut** : si vous sélectionnez **Oui**, la page de connexion utilitaire Web de configuration du commutateur s'affichera dans cette langue à chaque redémarrage du commutateur.
- **État** : ce champ affiche la valeur **Actif** ou **Inactif**. Lors de l'ouverture de la session, l'utilisateur peut sélectionner la langue de son choix. La langue sélectionnée sera alors activée.

Configuration des paramètres système

Pour configurer les paramètres système :

ÉTAPE 1 Cliquez sur **État et statistiques > Récapitulatif du système**. L'écran *Paramètres système* s'ouvre.

ÉTAPE 2 Cliquez sur **Modifier** pour modifier les paramètres suivants :

- **Emplacement du système** : indiquez l'emplacement physique du commutateur.
- **Contact système** : saisissez le nom d'une personne à contacter.
- **Nom d'hôte** : sélectionnez 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 le précisent les normes RFC1033, RFC1034 et RFC1035). Le nom d'hôte par défaut inclut le mot *switch* suivi de trois premiers octets de l'adresse MAC principale. Par exemple, le nom d'hôte par défaut d'un commutateur avec une adresse MAC 010203040506 est *switch010203*.

ÉTAPE 3 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Statistiques relatives aux interfaces

La page *Interface* affiche les statistiques relatives aux paquets reçus et transmis. Pour accéder à cette page, cliquez sur **État et statistiques** > **Interface** dans la fenêtre de navigation, ou sur **Statistiques des ports** sous **État de l'appareil** de la page *Prise en main*.

Sélectionnez l'interface (un port ou un LAG) dont vous souhaitez afficher les statistiques, puis sélectionnez un taux d'actualisation des statistiques. Les informations suivantes s'affichent pour l'interface sélectionnée :

- **Total des octets** : indique le nombre total d'octets transmis ou reçus sur l'interface sélectionnée depuis la dernière actualisation du commutateur.
- **Paquets monodiffusion** : affiche le nombre total de paquets monodiffusion transmis ou reçus sur l'interface sélectionnée depuis la dernière actualisation du commutateur.
- **Paquets multidiffusion** : affiche le nombre total de paquets multidiffusion transmis ou reçus sur l'interface sélectionnée depuis la dernière actualisation du commutateur.
- **Paquets de diffusion** : affiche le nombre total de paquets de diffusion transmis ou reçus sur l'interface sélectionnée depuis la dernière actualisation du commutateur.
- **Paquets avec erreurs** : indique le nombre total de paquets avec erreurs transmis ou reçus sur l'interface sélectionnée depuis la dernière actualisation du commutateur.

- **BPDU STP** : affiche le nombre total d'unités BPDU (Bridge Protocol Data Units) STP (Spanning Tree Protocol) transmises ou reçues sur l'interface sélectionnée depuis la dernière actualisation du commutateur.
- **BPDU RSTP** : affiche le nombre total d'unités BPDU RSTP (Rapid Spanning Tree Protocol) transmises ou reçues sur l'interface sélectionnée depuis la dernière actualisation du commutateur.

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour remettre à zéro tous les compteurs de l'interface sélectionnée.
- Cliquez sur **Effacer les compteurs de toutes les interfaces** pour remettre à zéro tous les compteurs de toutes les interfaces.

Statistiques relatives à Etherlike

Le système collecte et génère les statistiques sur les ports et les LAG conformément à RFC2665.

Pour accéder à cette page, cliquez sur **État et statistiques** > **Etherlike** dans la fenêtre de navigation.

Sélectionnez l'interface (un port ou un LAG) dont vous souhaitez afficher les statistiques, puis sélectionnez un taux d'actualisation des statistiques. Ces statistiques peuvent être cumulées à compter de la dernière actualisation de la page. Les informations suivantes s'affichent pour l'interface sélectionnée :

- **Erreurs de séquence de contrôle de trame** : affiche le nombre d'erreurs de séquence de contrôle de trame reçues.
- **Trames de collision du signal** : affiche le nombre d'erreurs de trame de collision du signal reçues.
- **Collisions tardives** : affiche le nombre de trames de collisions tardives reçues.
- **Collisions excessives** : affiche le nombre de trames de collisions excessives reçues.
- **Collisions multiples** : affiche le nombre de trames de collisions multiples reçues.

- **Paquets de taille excessive** : affiche le nombre de paquets reçus dont la taille est supérieure à 1518 octets (en excluant les bits de trame, mais en incluant les octets de séquence de contrôle de trame) et, le cas échéant, sont bien formés.
- **Erreurs de réception MAC internes** : indique le nombre d'erreurs MAC internes qui ont été reçues sur le LAG ou l'interface.
- **Erreurs d'alignement** : indique le nombre de paquets reçus contenant des erreurs d'alignement.
- **Trames de pause reçues** : affiche le nombre de trames de pause qui ont été reçues sur le LAG ou l'interface.
- **Trames de pause transmises** : affiche le nombre de trames de pause transmises à partir du LAG ou de l'interface.

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour remettre à zéro tous les compteurs de l'interface sélectionnée.
- Cliquez sur **Effacer les compteurs de toutes les interfaces** pour remettre à zéro tous les compteurs de toutes les interfaces.

Statistiques EAP 802.1X

Vous pouvez configurer les ports du commutateur à l'aide du protocole EAP (Extensible Authentication Protocol) IEEE 802.1X afin de contrôler l'accès réseau (voir la rubrique [802.1X](#)). La page *EAP 802.1x* affiche les informations relatives aux paquets EAP reçus sur un port.

Pour accéder à cette page, cliquez sur **État et statistique** > **EAP 802.1X** dans la fenêtre de navigation.

ÉTAPE 1 Sélectionnez le **port** dont vous souhaitez afficher les statistiques.

ÉTAPE 2 Choisissez un **taux d'actualisation** des statistiques. Ces statistiques peuvent être cumulées à compter de la dernière actualisation de la page.

Les informations suivantes s'affichent pour l'interface sélectionnée :

- **Trames EAPOL reçues** : affiche le nombre de trames EAPOL (Extensible Authentication Protocol over LAN) valides qui ont été reçues sur le port.

- **Trames EAPOL transmises** : indique le nombre de trames EAPOL transmises via 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 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** : affiche le nombre de trames EAPOL avec une longueur de corps de paquet non valide reçues sur ce port.

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour remettre à zéro tous les compteurs de l'interface sélectionnée.
- Cliquez sur **Effacer les compteurs de toutes les interfaces** pour remettre à zéro tous les compteurs de toutes les interfaces.

Statistiques DHCP IPv6

Vous pouvez configurer le commutateur afin qu'il effectue la gestion via une interface IPv6 et reçoive son adresse de gestion IPv6 via le protocole DHCPv6 (Dynamic Host Configuration Protocol). Pour plus d'informations sur la configuration d'IPv6 et DHCP via l'interface de gestion, consultez la rubrique [Interface de gestion](#). La page *Statistiques DHCP IPv6* affiche les informations relatives aux paquets DHCPv6 transmis et reçus.

Pour accéder à cette page, cliquez sur **État et statistiques > Statistiques DHCP IPv6** dans la fenêtre de navigation.

Configurez un taux d'actualisation pour cette page. La page affiche les statistiques suivantes qui peuvent être cumulées depuis la dernière actualisation de la page.

- Paquets de publication DHCPv6 reçus
- Paquets de réponse DHCPv6 reçus
- Paquets de publication DHCPv6 reçus ignorés

- Paquets de réponse DHCPv6 reçus ignorés
- Paquets mal formés DHCPv6 reçus
- Total des paquets DHCPv6 reçus
- Paquets de sollicitation DHCPv6 transmis
- Paquets de requête DHCPv6 transmis
- Paquets de renouvellement DHCPv6 transmis
- Paquets de reconnexion DHCPv6 transmis
- Paquets de libération DHCPv6 transmis
- Total des paquets DHCPv6 transmis

Pour remettre tous les compteurs à zéro, cliquez sur **Effacer les compteurs**.

Statistiques RADIUS

Vous pouvez configurer le commutateur afin qu'il communique avec un serveur RADIUS lors de l'authentification des utilisateurs distants. Pour accéder à la page *Statistiques RADIUS*, cliquez sur **État et statistiques > Statistiques RADIUS** dans la fenêtre de navigation.

Sélectionnez un serveur RADIUS dans la liste, puis configurez un taux d'actualisation de la page. La page affiche les statistiques suivantes qui peuvent être cumulées depuis la dernière actualisation de la page.

- **Requêtes d'accès** : affiche le nombre de paquets de requête d'authentification transmis vers le serveur RADIUS.
- **Retransmissions d'accès** : affiche le nombre de paquets de requête d'authentification retransmis vers le serveur RADIUS.
- **Acceptations d'accès** : affiche le nombre de paquets de requête d'authentification acceptés par le serveur RADIUS.
- **Rejets d'accès** : indique le nombre de paquets de requête d'authentification rejetés par le serveur RADIUS.
- **Challenges d'accès** : affiche le nombre de paquets de challenge d'accès envoyés par le serveur RADIUS au commutateur.
- **Réponses d'accès mal formées** : affiche le nombre de paquets de réponse provenant du serveur RADIUS qui ont été mal formés.

- **Authentificateurs incorrects** : affiche le nombre de paquets de requête d'authentification contenant des attributs d'authentificateur de message incorrects.
- **Requêtes en attente** : affiche le nombre de paquets de requête d'authentification qui ont été envoyés au serveur et qui n'ont obtenu aucune réponse.
- **Délais d'expiration** : affiche le nombre de paquets de requête d'authentification qui ont expiré, car le serveur n'a renvoyé aucune réponse.
- **Types inconnus** : affiche le nombre de paquets RADIUS de type inconnu qui ont été reçus par le commutateur.
- **Paquets rejetés** : affiche le nombre de paquets RADIUS qui ont été rejetés par le commutateur.

Pour remettre tous les compteurs à zéro, cliquez sur **Effacer toutes les statistiques**.

RMON

La page *RMON Statistiques* affiche des informations détaillées sur la taille des paquets, ainsi que certaines informations sur les erreurs relatives aux couches physiques. Les informations affichées sont conformes à la norme RMON.

Pour afficher les statistiques :

-
- ÉTAPE 1** Cliquez sur **État et statistiques > RMON > RMON** dans la fenêtre de navigation.
 - ÉTAPE 2** Sélectionnez le port ou le LAG dont vous souhaitez afficher les statistiques.
 - ÉTAPE 3** Configurez un taux d'actualisation pour cette page.

Les informations suivantes s'affichent pour l'interface sélectionnée :

- **Octets reçus** : affiche le nombre d'octets reçus sur l'interface depuis la dernière actualisation du commutateur. Ce nombre inclut les paquets erronés et les octets de séquence de contrôle de trame, mais exclut les bits de trame.
- **Événements rejetés** : affiche le nombre de paquets rejetés au niveau de l'interface depuis la dernière actualisation du commutateur.

- **Paquets reçus** : affiche le nombre de paquets reçus sur l'interface, y compris les paquets erronés, les paquets multidiffusion et de diffusion, depuis la dernière actualisation du commutateur.
- **Paquets de diffusion reçus** : affiche le nombre de paquets de diffusion corrects qui ont été reçus sur l'interface depuis la dernière actualisation du commutateur. Ce nombre n'inclut pas les paquets multidiffusion.
- **Paquets multidiffusion reçus** : indique le nombre de paquets multidiffusion corrects qui ont été reçus sur l'interface depuis la dernière actualisation du commutateur.
- **Erreurs d'alignement et de CRC** : affiche le nombre d'erreurs d'alignement et de CRC qui se sont produites sur l'interface depuis la dernière actualisation du périphérique.
- **Paquets de taille insuffisante** : indique le nombre de paquets de taille insuffisante (inférieure à 64 octets) qui ont été reçus sur l'interface depuis la dernière actualisation du commutateur.
- **Paquets de taille excessive** : indique le nombre de paquets de taille excessive (supérieure à 1518 octets) qui ont été reçus sur l'interface depuis la dernière actualisation du commutateur.
- **Fragments** : affiche le nombre de fragments (paquets inférieurs à 64 octets, excluant les bits de trame, mais incluant les octets de séquence de contrôle de trame) reçus sur l'interface depuis la dernière actualisation du commutateur.
- **Jabotages** : affiche le nombre de paquets reçus qui dépassent 1518 octets et contiennent des erreurs de séquence de contrôle de trame détectées au cours de la session d'échantillonnage.
- **Collisions** : indique le nombre de collisions reçues sur l'interface depuis la dernière actualisation du commutateur.
- **Trames de 64 octets** : affiche le nombre de trames de 64 octets reçues sur l'interface depuis la dernière actualisation du commutateur.
- **Trames de 65 à 127 octets** : affiche le nombre de trames de 65 à 127 octets reçues sur l'interface depuis la dernière actualisation du commutateur.
- **Trames de 128 à 255 octets** : affiche le nombre de trames de 128 à 255 octets reçues sur l'interface depuis la dernière actualisation du commutateur.
- **Trames de 256 à 511 octets** : affiche le nombre de trames de 256 à 511 octets reçues sur l'interface depuis la dernière actualisation du commutateur.

- **Trames de 512 à 1023 octets** : affiche le nombre de trames de 512 à 1023 octets reçues sur l'interface depuis la dernière actualisation du commutateur.
- **Trames de 1024 à 1518 octets** : affiche le nombre de trames de 1024 à 1518 octets reçues sur l'interface depuis la dernière actualisation du commutateur.

Journaux

Le commutateur génère des messages pour identifier l'état du système et diagnostiquer les problèmes survenus lors du fonctionnement du commutateur. Ces messages sont générés en réponse aux événements, dysfonctionnements ou erreurs qui se sont produits sur la plate-forme, ainsi qu'aux modifications de la configuration.

Les journaux de ces messages sont stockés dans les mémoires RAM et flash. À la différence des entrées stockées dans la mémoire RAM, celles du journal flash sont conservées d'un redémarrage de la plate-forme à l'autre.

Pour accéder aux entrées de journal, cliquez sur **État et statistiques > Afficher le journal** dans la fenêtre de navigation. Le menu de journal comprend les pages suivantes :

- **Journal de la mémoire RAM**
- **Journal de la mémoire flash**

Journal de la mémoire RAM

L'écran *Mémoire RAM* affiche des informations sur les entrées de journal (cache) de mémoire RAM spécifiques, notamment l'heure à laquelle le journal a été créé, son niveau de gravité et sa description.

Pour accéder à cette page, cliquez sur **État et statistiques > Afficher le journal > Mémoire RAM** dans la fenêtre de navigation.

REMARQUE Lorsque le nombre maximal d'entrées est atteint, l'affichage de cette page peut prendre jusqu'à 45 secondes.

La table des journaux de mémoire RAM comprend les champs suivants :

- **Index du journal** : affiche l'identifiant numérique de l'entrée du journal.
- **Heure de journalisation** : indique l'heure à laquelle le journal a été créé dans la table des journaux de mémoire RAM.
- **Gravité** : ce champ peut prendre l'une des valeurs suivantes :
 - **Urgent (0)** : vous ne pouvez pas utiliser le système.
 - **Alerte (1)** : vous devez exécuter une action immédiatement.
 - **Critique (2)** : affiche les conditions critiques.
 - **Erreur (3)** : affiche les conditions d'erreur.
 - **Avertissement (4)** : affiche les conditions d'avertissement.
 - **Remarque (5)** : affiche les conditions normales, mais importantes.
 - **Informatif (6)** : affiche les messages d'information.
 - **Débogage (7)** : fournit des informations détaillées sur un événement.

La page *Paramètres de journal* permet de sélectionner les niveaux de gravité enregistrés dans le journal.

- **Composant** : affiche le composant ou le service logiciel qui a généré l'entrée de journal.
- **Description** : affiche la description du journal.

Pour supprimer toutes les entrées de journal de la mémoire RAM, cliquez sur **Effacer les journaux**.

Journal de la mémoire flash

Les fichiers journaux affichent des informations sur les entrées de journal spécifiques, notamment l'heure à laquelle le journal a été créé, son niveau de gravité et sa description. Le système prend en charge plusieurs types de journaux et stocke jusqu'à trois versions différentes de chaque type.

Pour afficher un journal de la mémoire flash :

ÉTAPE 1 Cliquez sur **État et statistiques** > **Afficher le journal** > **Mémoire flash** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez un type de journal dans la liste.

- **Par défaut** : à confirmer.
- **Démarrage** : inclut des entrées de journal créées lors des redémarrages du système.
- **Opérationnel** : inclut des entrées de journal créées lors du fonctionnement du système.

ÉTAPE 3 Sélectionnez la version du journal que vous souhaitez afficher.

Le journal Version 1 est le fichier actuel ou récemment créé. Le journal Version 2 est le fichier le plus récent suivant. Enfin, le journal Version 3 est le fichier le plus obsolète. Lorsqu'un nouveau journal du même type est créé, le journal Version 3 est supprimé, et les journaux Version 1 et Version 2 sont respectivement renommés en Version 2 et Version 3.

Si vous sélectionnez une autre version et un autre journal. Le nouveau journal s'affiche automatiquement dans la table des journaux de mémoire flash. Lorsque le nombre maximal d'entrées est atteint, l'affichage de cette page peut prendre jusqu'à 45 secondes.

La table des journaux de mémoire flash comprend les champs suivants :

- **Index du journal** : affiche l'identifiant numérique de l'entrée du journal.
- **Heure de journalisation** : indique l'heure à laquelle le journal a été créé dans la table des journaux de mémoire flash.
- **Gravité** : ce champ peut prendre l'une des valeurs suivantes :
 - **Alerte (1)** : vous devez exécuter une action immédiatement.
 - **Critique (2)** : affiche les conditions critiques.
 - **Erreur (3)** : affiche les conditions d'erreur.
 - **Avertissement (4)** : affiche les conditions d'avertissement.
 - **Remarque (5)** : affiche les conditions normales, mais importantes.
 - **Informatif (6)** : affiche les messages d'information.
 - **Débogage (7)** : fournit des informations détaillées sur un événement.

La page *Paramètres de journal* permet de sélectionner les niveaux de gravité enregistrés dans le journal.

- **Composant** : affiche le composant logiciel qui a généré l'entrée de journal.
- **Description** : affiche la description du journal.

REMARQUE Pour supprimer toutes les entrées de journal de la mémoire flash, cliquez sur **Effacer les journaux**. Cliquez sur **Sauvegarder les journaux** pour accéder à la page *Télécharger/sauvegarder configuration/journal*, et utilisez TFTP ou HTTP pour sauvegarder les fichiers journaux sur un serveur TFTP ou un emplacement réseau. Pour plus d'informations, consultez la rubrique **Sauvegarde du fichier de configuration et des journaux**.

Administration

Ce chapitre explique comment configurer les paramètres système globaux et effectuer des diagnostics.

Il contient les rubriques suivantes :

- **Configuration des paramètres système**
- **Interface de gestion**
- **Gestion des comptes d'utilisateurs**
- **Activation des services de gestion**
- **Configuration du délai d'expiration de session inactive**
- **Sessions de connexion**
- **Historique de connexion**
- **Paramètres de l'heure**
- **Journaux système**
- **Gestion de fichiers**
- **Redémarrage du commutateur**
- **Envoi de requêtes ping à des hôtes**
- **Configuration du transfert de paquets de contrôle**
- **Diagnostics**
- **Activation de Bonjour**
- **LLDP-MED**
- **Configuration des options de fournisseur de client DHCP**

Configuration des paramètres système

La page *Paramètres système* vous permet de configurer des informations qui identifient le commutateur au sein du réseau.

Pour configurer les paramètres système :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres système** dans la fenêtre de navigation.

La description du système est intégrée au micrologiciel.

ÉTAPE 2 Configurez les paramètres suivants :

- **Emplacement du système** : description de l'emplacement physique du commutateur.
- **Contact système** : personne à contacter pour le commutateur.
- **Nom d'hôte** : nom alloué de façon administrative pour ce nœud géré. Par convention, il s'agit du nom de domaine entièrement qualifié du nœud. Le nom d'hôte par défaut est « switch », concaténé avec les six derniers chiffres hexadécimaux de l'adresse MAC du commutateur. Les étiquettes de nom d'hôte comportent uniquement des lettres, des chiffres et des tirets. Elles ne peuvent pas être précédées ou suivies d'un tiret. Les autres symboles, les signes de ponctuation et les espaces ne sont pas autorisés.

ÉTAPE 3 Cliquez sur **Appliquer**. Les modifications sont enregistrées dans la configuration d'exécution.

Interface de gestion

L'interface de gestion du commutateur permet d'accéder à l'utilitaire Web de configuration du commutateur depuis une station de gestion du réseau. Le commutateur prend en charge la configuration d'un VLAN de gestion qui sépare le trafic de gestion du reste du trafic sur le commutateur.

L'interface de gestion peut être configurée avec une adresse IPv4 ou une adresse IPv6. Les adresses peuvent être configurées de manière statique ou être obtenues via des serveurs DHCP/BOOTP.

Consultez les rubriques suivantes pour plus d'informations sur les pages de configuration disponibles dans le menu **Administration** > **Interface de gestion** :

- **Configuration d'une interface de gestion IPv4**
- **Configuration d'une interface de gestion IPv6**
- **Affichage et ajout de voisins IPv6**

Configuration d'une interface de gestion IPv4

Vous pouvez utiliser la page *Interface IPv4* pour configurer le VLAN de gestion et l'adresse IPv4.

Pour configurer l'interface de gestion IPv4 :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion** > **Interface IPv4** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez un VLAN de gestion dans la liste.

Un port doit être membre du VLAN de gestion pour pouvoir accéder à l'utilitaire Web de configuration du commutateur. Par défaut, VLAN 1 est configuré comme VLAN de gestion et tous les ports de commutation sont configurés comme membres de VLAN 1.

Le VLAN de gestion doit comporter au minimum un port membre. La liste **Ports membres** affiche tous les membres actuels du VLAN de gestion sélectionné.

Notez que lorsque vous modifiez le VLAN de gestion, vous devez réaffecter tous les membres du VLAN de gestion précédent au nouveau VLAN pour qu'ils puissent continuer à bénéficier de leur accès de gestion.

ÉTAPE 3 Sélectionnez l'une des options suivantes pour le type d'adresse IP :

- **DHCP** : l'interface de gestion obtient son adresse IPv4 d'un serveur DHCP.
- **BOOTP** : l'interface de gestion obtient son adresse IPv4 d'un serveur BOOTP.
- **Statique** : adresse IPv4 de l'interface de gestion affectée dans le champ **Adresse IP**.

Par défaut, DHCP est activé et le commutateur demande une adresse IP à un serveur DHCP. Si le commutateur ne parvient pas à obtenir l'adresse IP d'un serveur, il utilise l'adresse IP statique d'usine par défaut. La LED système clignote alors en continu. Le commutateur continuera d'essayer d'obtenir son adresse IP depuis un serveur DHCP. L'adresse IP statique d'usine par défaut est 192.168.1.254/24, la passerelle par défaut étant 192.168.1.1.

Si le type d'adresse IP est défini sur Statique, spécifiez les éléments suivants :

- **Adresse IP** : saisissez une adresse IPv4.
- **Masque** : saisissez un masque de réseau 32 bits (par exemple, 255.255.255.0).
Sinon, sélectionnez **Longueur du préfixe** et spécifiez le nombre de bits (de 0 à 32) qui composent le préfixe du réseau (par exemple, 24).
- **Passerelle par défaut** : sélectionnez **Définie par l'utilisateur** et spécifiez l'adresse IP par défaut de la passerelle pour les paquets de gestion.
Sinon, sélectionnez **Aucune** pour que les paquets de gestion ne soient pas transmis en dehors du sous-réseau.
- **Passerelle par défaut opérationnelle** : la passerelle par défaut actuellement utilisée.

ÉTAPE 4 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.



ATTENTION La modification de l'adresse IP de gestion et du type d'adresse IP met fin à la session de gestion en cours. La modification du VLAN de gestion et de ses appartenances de port peut perturber vos communications avec le commutateur et ainsi mettre fin à la session de gestion en cours.

Configuration d'une interface de gestion IPv6

Utilisez la page *Interface IPv6* pour permettre l'accès à l'utilitaire Web de configuration du commutateur sur IPv6. Vous pouvez configurer le commutateur pour qu'il apprenne dynamiquement ses adresses IPv6 et configurer les adresses IPv6 de façon statique.

Pour permettre de l'accès de gestion IPv6 :

- ÉTAPE 1** Cliquez sur **Administration > Interface de gestion > Interface IPv6** dans la fenêtre de navigation.
- ÉTAPE 2** Configurez les paramètres suivants :
- **Mode IPv6** : sélectionnez cette option pour activer l'accès de gestion IPv6.
 - **Configuration automatique d'adresses IPv6** : sélectionnez cette option pour que le commutateur configure automatiquement son ou ses adresses de liaison locale au format EUI-64, en utilisant l'adresse MAC du ou des ports pour la partie liaison locale (link-local) de l'adresse. Le commutateur écoute les annonces du routeur pour détecter et configurer automatiquement la partie globale de l'adresse.
 - **DHCPv6** : sélectionnez ce paramètre pour permettre au commutateur d'obtenir son ou ses adresses IPv6 d'un serveur DHCPv6.
 - **Passerelle IPv6** : saisissez l'adresse de liaison locale du routeur IPv6 auquel le commutateur doit envoyer les paquets IPv6 destinés à un appareil situé en dehors du sous-réseau.
- ÉTAPE 3** Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution. Vous pouvez cliquer sur **Annuler** pour supprimer les modifications.

Ajout d'adresses IPv6

La Table des adresses IPv6 répertorie les adresses statiques actuellement configurées sur le commutateur. Elle contient les champs suivants :

- **Adresse** : adresse IPv6 au format d'adresse globale IPv6.

- **État DAD** : l'état de la détection des adresses en double. Lorsque vous configurez une adresse IPv6 sur le commutateur, celui-ci procède, préalablement à l'affectation proprement dite de l'adresse, à la découverte des voisins pour déterminer si cette adresse est déjà utilisée sur le réseau.
 - Si l'adresse est déjà utilisée, son état DAD est défini sur Vrai, et elle ne peut pas être utilisée pour un accès de gestion.
 - Si l'adresse est considérée comme unique, son état DAD est défini sur Faux, et elle peut être utilisée pour un accès de gestion.

Vous pouvez configurer plusieurs adresses IPv6. Chacune d'elles doit disposer d'un préfixe distinct afin que le commutateur puisse être géré depuis des stations situées sur des sous-réseaux différents. En cas de défaillance d'une route menant à un sous-réseau, le commutateur peut être géré depuis un autre sous-réseau.

Pour ajouter une adresse IPv6 statique :

ÉTAPE 1 Cliquez sur **Ajouter**.

ÉTAPE 2 Saisissez une adresse IPv6 suivie d'une barre oblique (/) et de la longueur du préfixe.

ÉTAPE 3 Sélectionnez **EUI-64** si l'adresse est conforme au format EUI-64, les trois à cinq premiers octets correspondant à l'OUI (Organizationally Unique Identifier) et les autres à une adresse affectée unique.

ÉTAPE 4 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Table des routeurs par défaut IPv6

Lorsque la gestion IPv6 est activée, le commutateur utilise le processus de découverte des voisins IPv6 afin d'identifier le routeur par défaut pour communiquer avec les appareils situés en dehors du sous-réseau IPv6 local. Le fonctionnement du routeur par défaut des réseaux IPv6 est similaire à celui du routeur par défaut des réseaux IPv4.

La Table des routeurs par défaut IPv6 répertorie l'adresse IP du routeur par défaut pour chaque adresse de gestion IPv6. Une adresse de routeur par défaut se compose de l'adresse de liaison locale de l'interface IPv6 sur le sous-réseau.

Affichage et ajout de voisins IPv6

Lorsque la gestion IPv6 est activée, le commutateur identifie les appareils IPv6 sur les liaisons établies. Le commutateur prend en charge la découverte d'un maximum 1 000 voisins IPv6 dynamiques et la configuration statique de voisins IPv6.

La page *Voisins IPv6* répertorie les voisins découverts de façon dynamique et ceux configurés de façon statique, et permet d'ajouter des hôtes statiques.

Pour afficher la Table des voisins IPv6, cliquez sur **Administration > Interface de gestion > Voisins IPv6** dans la fenêtre de navigation.

La Table des voisins IPv6 affiche les champs suivants pour chaque entrée dynamique :

- **Adresse IPv6** : adresse IPv6 du voisin.
- **Adresse MAC** : adresse MAC du voisin.
- **État** : état du voisin. Les états des entrées dynamiques sont présentés ci-dessous :
 - **Atteignable** : une confirmation indiquant que le chemin de transfert menant au voisin fonctionne correctement a été reçue dans un intervalle de temps préconfiguré. Lorsque l'état est Atteignable, l'appareil n'effectue aucune action particulière lors de l'envoi de paquets.
 - **Délai** : un délai supérieur à un intervalle de temps préconfiguré s'est écoulé depuis la réception de la dernière configuration indiquant que le chemin de transfert fonctionnait correctement.
- **Délai depuis mise à jour** : temps (en secondes) qui s'est écoulé depuis l'ajout d'une entrée au cache.
- **Type** : type de saisie des informations de cache de découverte des voisins (statique ou dynamique).

Vous pouvez cliquer sur **Effacer les voisins dynamiques** pour effacer le contenu de la table.

Ajout de voisins IPv6 statiques

Le commutateur peut prendre en charge jusqu'à 16 entrées de voisins IPv6 statiques. Pour ajouter un voisin statique :

-
- ÉTAPE 1** Cliquez sur **Ajouter**.
 - ÉTAPE 2** Saisissez une adresse IPv6 globale (n'incluant pas la longueur du préfixe).
 - ÉTAPE 3** Saisissez l'adresse MAC du voisin.
 - ÉTAPE 4** Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.
-

Gestion des comptes d'utilisateurs

Un utilisateur de gestion est par défaut configuré sur le commutateur :

- Nom d'utilisateur : **cisco**
- Mot de passe : **cisco**

Vous pouvez utiliser la page *Comptes d'utilisateurs* pour configurer jusqu'à cinq utilisateurs supplémentaires et modifier le mot de passe d'un utilisateur.

Ajout d'un utilisateur

Pour ajouter un nouvel utilisateur :

-
- ÉTAPE 1** Cliquez sur **Administration > Comptes d'utilisateurs** dans la fenêtre de navigation.

La Table des comptes d'utilisateurs affiche les utilisateurs actuellement configurés.
 - ÉTAPE 2** Cliquez sur **Ajouter**.
 - ÉTAPE 3** Saisissez un nom d'utilisateur comportant entre 1 et 32 caractères alphanumériques. Les noms d'utilisateur ne peuvent comporter que des chiffres (de 0 à 9) et des lettres (de a à z, majuscules et minuscules).
 - ÉTAPE 4** Saisissez un mot de passe comportant entre 1 et 64 caractères (en fonction du paramètre **Fiabilité du mot de passe**) et confirmez-le.

Une fois que vous avez saisi un mot de passe, le nombre et la couleur des barres verticales changent pour indiquer la robustesse du mot de passe, comme suit :

- Rouge : le mot de passe ne répond pas aux exigences minimales en termes de complexité. Le texte **Inférieur aux exigences minimales** s'affiche à droite de l'indicateur.
- Orange : le mot de passe répond aux exigences minimales en termes de complexité, mais il n'est pas très robuste. Le texte **Faible** s'affiche à droite de l'indicateur.
- Vert : le mot de passe est fort. Le texte **Fort** s'affiche à droite de l'indicateur.

Le bouton Appliquer ne s'affiche qu'une fois l'indicateur de robustesse orange et le mot de passe confirmé.

Lorsque vous ajoutez un utilisateur, vous pouvez désactiver de façon temporaire la fonction de vérification de la robustesse du mot de passe pour configurer un mot de passe qui ne répond pas aux critères de vérification de la robustesse. Cliquez sur **Ne pas appliquer la robustesse du mot de passe** puis sur **OK** lorsque l'avertissement s'affiche.

Pour désactiver la fonction de vérification de la robustesse du mot de passe pour l'ensemble des utilisateurs, ou pour configurer ses caractéristiques, utilisez la page *Fiabilité du mot de passe*.

ÉTAPE 5 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Modification d'un mot de passe utilisateur

Pour modifier un mot de passe utilisateur :

ÉTAPE 1 Cliquez sur **Administration > Comptes d'utilisateurs** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez l'utilisateur à configurer et cliquez sur **Modifier**.

ÉTAPE 3 Saisissez un mot de passe comportant entre 1 et 64 caractères (en fonction du paramètre **Fiabilité du mot de passe**) et confirmez-le.

Pendant la saisie du mot de passe, le nombre et la couleur des barres verticales changent pour en indiquer la robustesse. Les barres rouges indiquent un mot de passe plus faible. Les barres orange indiquent un mot de passe plus fort, et les barres vertes le niveau de mot de passe le plus robuste.

Lorsque vous modifiez un mot de passe, vous pouvez désactiver de façon temporaire la fonction de vérification de la robustesse du mot de passe pour configurer un mot de passe qui ne répond pas aux critères de vérification de la robustesse. Cliquez sur **Ne pas appliquer la robustesse du mot de passe** puis sur **OK** lorsque l'avertissement s'affiche.

Pour désactiver la fonction de vérification de la robustesse du mot de passe pour l'ensemble des utilisateurs, ou pour configurer ses caractéristiques, utilisez la page *Fiabilité du mot de passe*.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Suppression d'un utilisateur

Vous pouvez supprimer tous les utilisateurs, à l'exception de l'utilisateur par défaut, qui correspond généralement à l'ID utilisateur **cisco**.

Pour supprimer un utilisateur, sélectionnez son nom dans la Table des comptes d'utilisateurs et cliquez sur **Supprimer**.

Activation des services de gestion

Utilisez la page *Services de gestion* pour configurer le numéro de port TCP pour les connexions HTTP vers l'utilitaire Web de configuration du commutateur.

Le numéro de port par défaut pour les connexions HTTP correspond à un numéro de port IANA bien connu, à savoir le 80. Pour configurer un autre numéro de port HTTP :

ÉTAPE 1 Cliquez sur **Administration** > **Services de gestion** dans la fenêtre de navigation.

ÉTAPE 2 Saisissez le numéro de port logique à utiliser, compris entre 1 025 et 65 535. La valeur par défaut correspond au port 80.

ÉTAPE 3 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration du délai d'expiration de session inactive

Le logiciel déconnecte automatiquement les utilisateurs des interface de gestion en cas d'absence d'activité pendant une période spécifique. L'utilisateur doit se réauthentifier après une expiration de session.

Vous pouvez utiliser la page *Délai d'expiration de session inactive* pour configurer le délai d'expiration. Pour afficher cette page, cliquez sur **Administration > Délai d'expiration de session inactive** dans la fenêtre de navigation.

Le délai d'expiration des sessions HTTP inactives peut être compris entre 1 et 60 minutes. La valeur par défaut est de 10 minutes.

Si vous modifiez la valeur, cliquez sur **Appliquer** pour enregistrer votre modification dans la configuration d'exécution.

Sessions de connexion

La page *Sessions de connexion* affiche les sessions de connexion de gestion actives. Pour afficher cette page, cliquez sur **Administration > Sessions de connexion** dans la fenêtre de navigation.

Cette page répertorie les informations suivantes pour chaque utilisateur actuellement connecté :

- **Nom d'utilisateur** : nom dont s'est servi l'utilisateur pour se connecter.
- **Connexion depuis** : adresse IP de l'hôte.
- **Durée d'inactivité** : temps qui s'est écoulé depuis la dernière activité de cet utilisateur.
- **Durée de session** : temps qui s'est écoulé depuis la connexion de cet utilisateur.
- **Type de session** : protocole utilisé pour la session de gestion (HTTP).

Historique de connexion

Vous pouvez utiliser la page *Historique de connexion* pour afficher les données se rapportant aux précédentes connexions au logiciel de gestion. Pour afficher cette page, cliquez sur **Administration** > **Historique de connexion** dans la fenêtre de navigation.

Cette page affiche les champs suivants :

- **Temps de connexion** : durée pendant laquelle l'utilisateur est resté connecté.
- **Nom d'utilisateur** : nom dont s'est servi l'utilisateur pour se connecter.
- **Protocole** : protocole utilisé par l'utilisateur pour se connecter au logiciel de configuration. Les valeurs disponibles sont HTTP, Telnet, Série, SSH et SNMP.
- **Emplacement** : adresse IP de l'hôte.

Paramètres de l'heure

Une horloge système est utilisée pour fournir un service d'horodatage synchronisé sur le réseau pour les événements logiciels du commutateur tels que les journaux de messages. Vous pouvez configurer l'horloge système manuellement, ou configurer le commutateur en tant que client SNTP (Simple Network Time Protocol) qui obtient les données d'horloge d'un serveur.

Consultez les rubriques suivantes pour plus d'informations sur les pages de configuration disponibles dans le menu Administration > Paramètres de l'heure :

- **Définition de l'heure système**
- **Configuration des paramètres SNTP**
- **Configuration de l'authentification SNTP**

Définition de l'heure système

Utilisez la page *Heure système* pour définir l'heure système manuellement ou pour configurer le système afin qu'il récupère ses paramètres d'heure d'un serveur SNTP. Pour afficher cette page, cliquez sur **Administration** > **Paramètres de l'heure** > **Heure système** dans la fenêtre de navigation.

Par défaut, l'heure est configurée localement sur le commutateur.

REMARQUE Les informations actuelles d'heure, de date et de fuseau horaire du système, ainsi que le statut de l'heure d'été s'affichent en bas de la page.

Spécification locale des paramètres de l'horloge

Pour configurer localement les paramètres de l'heure :

ÉTAPE 1 Sur la page *Heure système*, sélectionnez **Utiliser les paramètres locaux**.

ÉTAPE 2 Sélectionnez **Source du fuseau horaire - DHCP** si vous souhaitez que le commutateur récupère son fuseau horaire d'un serveur DHCP.

ÉTAPE 3 Sélectionnez **Définir la date/l'heure de l'ordinateur** pour que le commutateur récupère les paramètres de l'heure de l'ordinateur que vous utilisez pour accéder au commutateur.

Vous pouvez également effacer ce champ et configurer les paramètres d'heure suivants :

- **Date** : saisissez la date au format mm/jj/aaaa, par exemple 01/01/2010 pour le 1er janvier 2010.
- **Heure locale** : saisissez l'heure actuelle au format HH:mm:ss, par exemple 22:00:00 pour 22 heures. (Le texte d'information indique **HH** si l'horloge est au format 24 heures ou **hh** si elle est au format 12 heures.)
- **Décalage fuseau horaire GMT** : sélectionnez la différence en nombre d'heures et de minutes entre le fuseau horaire local et l'heure GMT (Greenwich Mean Time).

ÉTAPE 4 Dans le champ **Acronyme du fuseau horaire**, vous pouvez si vous le souhaitez spécifier un acronyme de quatre caractères maximum, servant à identifier les paramètres configurés. Ce champ est uniquement utilisé à des fins de référence.

ÉTAPE 5 Sélectionnez **Heure d'été** pour configurer les paramètres d'heure d'été, si cela s'applique à votre fuseau horaire. Si vous sélectionnez cette option, configurez les champs suivants :

- **États-Unis/Europe/Autre** : sélectionnez États-Unis ou Europe pour que le décalage de l'heure d'été soit configuré en fonction des valeurs utilisées dans ces régions. Vous pouvez également sélectionner **Autre** pour configurer les paramètres manuellement. Lors d'une configuration manuelle, vous pouvez définir les paramètres se rapportant uniquement à la période d'heure d'été à venir, ou définir des paramètres récurrents.
- **Acronyme de fuseau horaire (heure d'été)** : spécifiez si vous le souhaitez un acronyme de quatre caractères maximum, servant à identifier les paramètres configurés. Ce champ est uniquement utilisé à des fins de référence.

- **Compensation d'heure définie** : indiquez de combien de minutes avancer l'horloge lors du passage à l'heure d'été.
- **De/À** : spécifiez la date et l'heure de début et de fin de l'heure d'été.
- **Récurrence** : sélectionnez cette option pour spécifier des périodes d'heure d'été récurrentes en choisissant le jour de la semaine et le numéro de semaine de l'année correspondant chaque année au début et à la fin de l'heure d'été.

ÉTAPE 6 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration du commutateur en tant que client SNTP

Vous pouvez également configurer le commutateur afin qu'il récupère l'heure depuis un serveur SNTP en définissant les paramètres SNTP du commutateur.

Pour configurer le commutateur afin qu'il récupère les paramètres de l'heure depuis un serveur SNTP :

ÉTAPE 1 Sur la page *Heure système*, sélectionnez **Utiliser le serveur SNTP**.

ÉTAPE 2 Configurez le mode de fonctionnement du client SNTP du commutateur :

- **Monodiffusion** : configure le commutateur pour qu'il envoie des requêtes SNTP uniquement aux serveurs SNTP de monodiffusion configurés. Vous devez ajouter au moins un serveur SNTP de monodiffusion pour activer cette fonction.
- **Diffusion** : configure le commutateur pour qu'il récupère ses paramètres d'heure de messages SNTP diffusés depuis des serveurs SNTP.

ÉTAPE 3 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

ÉTAPE 4 Utilisez les sections **Configuration des paramètres SNTP** et **Configuration de l'authentification SNTP** pour configurer des paramètres SNTP supplémentaires, tels que les intervalles d'interrogation, les adresses de serveurs de monodiffusion et les informations d'authentification dont a besoin le commutateur pour accéder aux serveurs SNTP.

Configuration des paramètres SNTP

Le commutateur prend en charge le protocole SNTP (Simple Network Time Protocol). SNTP garantit une synchronisation précise, à la milliseconde près, de l'heure des périphériques réseau. La synchronisation de l'heure est effectuée par un serveur SNTP réseau. Le commutateur fonctionne uniquement en tant que client SNTP et ne peut pas fournir de services d'heure à d'autres systèmes.

Pour afficher la page *Paramètres SNTP*, cliquez sur **Administration > Paramètres de l'heure > Paramètres SNTP** dans la fenêtre de navigation.

Configuration des paramètres SNTP

- ÉTAPE 1** Assurez-vous que l'option Utiliser le serveur SNTP est sélectionnée sur la page *Heure système*, et également que le mode Monodiffusion ou Diffusion est sélectionné, selon les besoins.
- ÉTAPE 2** Sur la page *Paramètres SNTP*, configurez les éléments suivants :
- **Port client** : numéro de port logique à utiliser pour le client SNTP sur le commutateur. La valeur par défaut correspond à un numéro de port IANA bien connu pour ce service, à savoir le 123.
 - **Intervalle d'interrogation de monodiffusion** : le rythme relatif auquel le commutateur envoie des messages de synchronisation au serveur SNTP. Ce champ n'est modifiable que lorsque la réception SNTP Monodiffusion est sélectionnée. Entrez une valeur comprise entre 3 et 16. L'intervalle réel, en secondes, correspond à la valeur spécifiée à la puissance 2. Par exemple, si vous entrez 4, l'intervalle d'interrogation sera de 16 secondes.
- ÉTAPE 3** Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Affichage des propriétés actives du serveur et des paramètres globaux

La page *Paramètres SNTP* affiche, le cas échéant, les propriétés suivantes pour le serveur SNTP depuis lequel le commutateur a le plus récemment obtenu ses paramètres d'heure. Cette page affiche également les paramètres globaux (non configurables).

Serveur actif :

- **Adresse hôte du serveur** : adresse IP du serveur SNTP.
- **Type du serveur** : version du protocole IP utilisée par le serveur (IPv4 ou IPv6).

- **Strate du serveur** : niveau hiérarchique du serveur SNTP qui identifie sa distance par rapport à une horloge de référence.
- **ID de référence du serveur** : code de 32 bits qui identifie l'horloge de référence utilisée par ce serveur.
- **Mode du serveur** : mode de fonctionnement du serveur :
 - **Monodiffusion** : le serveur SNTP écoute les requêtes de monodiffusion des clients SNTP.
 - **Diffusion** : le serveur SNTP envoie régulièrement des messages de diffusion aux clients SNTP.
 - **Réservé** : aucune réponse n'a été reçue d'un serveur SNTP. Lorsqu'une réponse est reçue d'un serveur, elle est remplacée par l'un des états valides (Diffusion ou Monodiffusion).

Paramètres globaux :

- **Version du client SNTP** : version la plus récente du protocole SNTP prise en charge par le commutateur.
- **Heure de la dernière mise à jour** : heure de réception de la dernière mise à jour SNTP.
- **Heure de la dernière tentative de monodiffusion** : heure de la dernière tentative de synchronisation du commutateur avec un serveur de monodiffusion SNTP.
- **Mode du client** : mode configuré du client SNTP (Monodiffusion ou Diffusion). Consultez la section [Définition de l'heure système](#) pour configurer ce mode.
- **Entrées maximales du serveur** : nombre maximum de serveurs que vous pouvez configurer sur le commutateur.
- **Entrées actuelles du serveur** : nombre de serveurs SNTP actuellement configurés sur le système, comme indiqué dans la Table des serveurs SNTP de monodiffusion
- **Nombre de diffusions** : nombre de paquets de diffusion SNTP que le commutateur a reçu de serveurs SNTP.

Ajout et modification de serveurs SNTP

La Table des serveurs SNTP de monodiffusion affiche les informations suivantes pour chaque serveur SNTP que vous configurez :

- **Serveur SNTP** : adresse IP ou nom d'hôte du serveur SNTP.
- **ID de clé d'authentification** : clé de cryptage requise pour communiquer avec le serveur SNTP.
- **Heure de la dernière tentative** : heure de la dernière tentative de synchronisation du commutateur avec un serveur de monodiffusion SNTP.
- **État** : état de fonctionnement du serveur SNTP. Ce champ peut prendre les valeurs suivantes :
 - **Réussite** : le client a pu obtenir l'heure de ce serveur.
 - **Expiration de la requête** : le délai de la requête du client a expiré.
 - **Date erronée** : un format de date erroné a été reçu du serveur.
 - **Version non prise en charge** : le serveur ne prend pas en charge la version SNTP configurée sur le commutateur.
 - **Non synchronisé** : l'heure du commutateur n'est pas synchronisée avec celle du serveur.
 - **Kiss of death** : le serveur SNTP a répondu avec un paquet « kiss of death », donnant pour instruction au commutateur d'arrêter d'envoyer des requêtes au serveur, en raison de pointes de trafic ou d'autres conditions d'erreur.
 - **Autre** : l'état n'a pas pu être déterminé.
- **Dernière réponse** : heure de la dernière réponse du serveur SNTP.
- **Version** : version du protocole SNTP utilisée par le serveur.
- **Port** : numéro de port du protocole (123 est un numéro de port bien connu pour SNTP).
- **Mode d'interrogation** : permet d'indiquer si le commutateur est configuré pour envoyer des requêtes SNTP à ce serveur (Activé ou Désactivé).
- **Demandes de monodiffusion totales** : nombre total de demandes de synchronisation envoyées par le commutateur au serveur de monodiffusion.

Pour modifier les paramètres d'un serveur, cochez la case pour le sélectionner, puis cliquez sur **Modifier**. Pour supprimer un serveur, cochez la case pour le sélectionner, puis cliquez sur **Supprimer**. Pour ajouter un nouveau serveur, cliquez sur **Ajouter**, puis saisissez les paramètres, comme décrit ci-dessous.

Pour ajouter un serveur SNTP :

ÉTAPE 1 Cliquez sur **Ajouter**.

ÉTAPE 2 Configurez les paramètres suivants :

- **Serveur SNTP** : saisissez une adresse IPv4 ou un nom de domaine. Pour utiliser un nom de domaine, assurez-vous que le service DNS est activé sur le commutateur (voir la section [Système de noms de domaine](#)).
- **Clé d'authentification** : cochez la case **Activer** si une authentification est requise pour communiquer avec le serveur SNTP.
- **ID de clé d'authentification** : si l'authentification est utilisée, sélectionnez l'ID de la clé d'authentification dans la liste. Consultez la section [Configuration de l'authentification SNTP](#) pour plus d'informations sur la configuration des clés d'authentification.
- **Mode d'interrogation** : cochez la case **Activer** pour autoriser le commutateur à envoyer des requêtes à ce serveur.
- **Port** : spécifiez le numéro de port UDP à indiquer dans l'en-tête des messages SNTP. Par défaut, le numéro de port correspond à une valeur IANA bien connue, à savoir le 123.
- **Version** : spécifiez la version SNTP la plus récente (de 1 à 4) prise en charge par le serveur.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration de l'authentification SNTP

Utilisez la page *Authentification SNTP* pour configurer les clés de cryptage, qui contiennent les informations d'identification utilisées par le commutateur pour s'authentifier auprès des serveurs SNTP. Vous pouvez également utiliser cette page pour activer le service d'authentification SNTP.

Lorsque vous définissez les serveurs SNTP que le commutateur peut utiliser, vous spécifiez si un serveur utilise l'authentification et quelle clé d'authentification il utilise.

REMARQUE Vous devez configurer au minimum une clé d'authentification validée avant d'activer l'authentification SNTP. Dans le cas contraire, le message **Échec de l'activation de l'authentification SNTP** s'affiche.

Pour configurer une clé d'authentification et activer ce service :

ÉTAPE 1 Cliquez sur **Administration > Paramètres de l'heure > Authentification SNTP** dans la fenêtre de navigation.

La Table des authentifications SNTP affiche chaque clé d'authentification actuellement configurée et indique si la clé peut actuellement être utilisée en tant que clé validée.

ÉTAPE 2 Cochez la case **Activer** pour demander que le commutateur s'authentifie auprès d'un serveur SNTP avant de synchroniser son horloge.

ÉTAPE 3 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

ÉTAPE 4 Dans la Table des authentifications SNTP, cliquez sur **Ajouter** pour ajouter une clé à la liste.

ÉTAPE 5 Configurez les paramètres suivants :

- **ID de clé d'authentification** : numéro de la clé. Lorsque vous définissez un serveur SNTP sur le système, vous spécifiez la clé qu'il utilise pour l'authentification.
- **Clé d'authentification** : valeur de la clé. La valeur correspond à la clé cryptographique utilisée pour crypter et décrypter les messages SNTP à destination et en provenance du serveur.

- **Clé validée** : indique si cette clé est validée. Seules les clés validées peuvent être utilisées. Au moins une clé validée doit être configurée pour activer le service d'authentification SNTP.

Les clés ne sont utilisées qu'avec les serveurs SNTP de monodiffusion. Une clé n'est utilisée pour authentifier un serveur SNTP que si elle est activée en tant que clé validée. Une clé configurée sur le commutateur mais spécifiée comme étant non validée ne sera pas utilisée. Un administrateur peut ajouter une clé non validée afin qu'elle puisse être ultérieurement utilisée.

ÉTAPE 6 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Journaux système

Le commutateur génère des messages en réponse à des événements, défaillances, erreurs, modifications de configuration et autres occurrences. Ces messages sont stockés localement dans la mémoire système et transmis à un ou plusieurs points centralisés de collecte pour des activités de surveillance ou un archivage à long terme.

Consultez les rubriques suivantes pour plus d'informations sur les pages de configuration disponibles dans le menu Administration > Journal système :

- **Configuration des paramètres de journal**
- **Configuration des serveurs de journalisation distants**

Configuration des paramètres de journal

Utilisez la page *Paramètres de journal* pour activer les journaux au niveau global, ainsi que pour définir les types d'événements qui sont journalisés dans la mémoire temporaire (RAM) et dans la mémoire persistante (flash). Les messages de journal stockés dans la mémoire flash sont conservés en cas de redémarrage. Une fois le journal plein, les événements les plus anciens sont automatiquement supprimés et remplacés par les nouvelles entrées.

Pour configurer les paramètres de journal :

ÉTAPE 1 Cliquez sur **Administration > Journal système > Paramètres de journal** dans la fenêtre de navigation.

ÉTAPE 2 Activez les types de journalisation à effectuer sur le système :

- **Agrégation des journaux** : lorsqu'elle est activée, cette fonction regroupe plusieurs journaux du même type dans un seul message de journal. Si plusieurs messages identiques sont reçus à la suite au cours d'un intervalle de temps configuré, ces messages sont agrégés dans un même message de journal.
- **Intervalle d'agrégation des journaux** : si l'Agrégation des journaux est activée, spécifiez l'intervalle en secondes. Les messages consécutifs reçus au cours de cet intervalle seront agrégés dans un seul message de journal. Cette valeur doit être comprise entre 15 et 120 secondes.
- **Journalisation de la mémoire RAM** : sélectionnez cette option pour activer la journalisation dans la RAM.
- **Journalisation de la mémoire flash** : sélectionnez cette option pour activer la journalisation dans la mémoire flash.
- **Taille du journal flash** : entrez le nombre maximum de messages de journal à stocker dans le journal de la mémoire flash.

ÉTAPE 3 Activez les niveaux de sévérité des événements à journaliser pour chaque type de journal. Les niveaux de sévérité sont répertoriés du niveau le plus élevé au plus faible, comme suit :

- **Emergency (Urgence)** : le système n'est pas utilisable.
- **Alert (Alerte)** : une action est requise.
- **Critical (Critique)** : le système est dans un état critique.
- **Error (Erreur)** : le système subit une condition d'erreur.
- **Warning (Avertissement)** : un avertissement système a été généré.
- **Notice (Remarque)** : le système fonctionne correctement mais une remarque système a été générée.
- **Informational (Informatif)** : information de l'appareil.
- **Debug (Débogage)** : fournit des informations détaillées sur un événement.

REMARQUE : lorsque vous choisissez un niveau de gravité, tous les événements de ce niveau ou d'un niveau plus élevé sont automatiquement sélectionnés pour être journalisés.

ÉTAPE 4 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration des serveurs de journalisation distants

Vous pouvez définir un ou plusieurs serveurs de journalisation distants auxquels le commutateur envoie des messages Syslog. Utilisez la page *Serveurs de journalisation distants* pour définir les serveurs de journalisation et configurer le niveau de sévérité des événements de journalisation à envoyer au serveur.

Pour activer le mode Syslog et configurer un serveur de journalisation distant :

ÉTAPE 1 Cliquez sur **Administration > Serveurs de journalisation distants** dans la fenêtre de navigation.

ÉTAPE 2 Pour activer le mode de Journalisation Syslog, cochez la case **Activer**, puis configurez les paramètres suivants :

- **Équipement** : sélectionnez dans la liste une valeur qui identifie la classification des messages syslog à partir de ce commutateur. La signification de ces valeurs (Local 0 à Local 7) est déterminée par l'administrateur réseau.
- **Port local** : spécifiez le numéro de port IANA du commutateur. La valeur par défaut correspond à un numéro de port IANA bien connu pour le protocole Syslog, à savoir le 514.

ÉTAPE 3 Dans la Table de serveurs de journalisation distants, cliquez sur **Ajouter**.

ÉTAPE 4 Configurez les paramètres suivants :

- **Serveur de journalisation** : adresse IPv4 ou nom d'hôte du serveur auquel envoyer les journaux.
- **Port UDP** : numéro de port UDP logique utilisé par le serveur distant pour le protocole Syslog. La valeur par défaut correspond à un numéro de port Syslog IANA bien connu, à savoir le 514.

- **Sévérité minimum** : seuls les éléments répondant à ce niveau de sévérité ou le dépassant sont envoyés au serveur distant. Consultez la section **Configuration des paramètres de journal** pour une description des niveaux de sévérité.

ÉTAPE 5 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Gestion de fichiers

Vous pouvez utiliser les fonctions de gestion de fichiers pour mettre à niveau ou sauvegarder le micrologiciel, mettre à jour les fichiers de langue, enregistrer les modifications apportées à la configuration, copier les fichiers de configuration dans le commutateur et mettre en place la fonction de configuration automatique.

REMARQUE Lorsqu'un téléchargement vers ou depuis le commutateur est en cours, tout accès de gestion à ce dernier est bloqué jusqu'à la fin du transfert, permettant ainsi de protéger le commutateur contre toute modification inconnue.

Consultez les rubriques suivantes pour plus d'informations sur les pages de configuration disponibles dans le menu Administration > Gestion de fichiers, ainsi que les tâches apparentées :

- **Mise à niveau et sauvegarde des fichiers de micrologiciel et de langue**
- **Téléchargement et sauvegarde des fichiers de configuration et journaux**
- **Supprimer la configuration**
- **Copie et enregistrement des fichiers de configuration**
- **Configuration automatique DHCP**
- **Récupération du micrologiciel via HTTP**

Fichiers et types de fichiers

Les types de fichiers de configuration et opérationnels suivants sont présents sur le commutateur :

- **Configuration d'exécution** : paramètres actuellement utilisés par le commutateur pour fonctionner. Il s'agit du seul type de fichier que vous pouvez modifier, en changeant des valeurs de paramètres via l'une des interfaces de configuration. Il doit en outre être enregistré manuellement dans un autre type de fichier, tel que la Configuration de démarrage, pour pouvoir être conservé après un redémarrage.

En cas de redémarrage du commutateur, la Configuration d'exécution est perdue. Lors du redémarrage du commutateur, la Configuration de démarrage stockée dans la mémoire flash est copiée dans la Configuration d'exécution stockée dans la mémoire vive (RAM).

- **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 du commutateur. Lors du redémarrage, la Configuration de démarrage est copiée dans la RAM et identifiée comme étant la Configuration d'exécution.

- **Configuration de secours** : copie manuelle des définitions de paramètres 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 secours. La Configuration de secours est conservée dans la mémoire flash et préservée en cas de redémarrage de l'appareil.
- **Configuration miroir** : copie de la Configuration de démarrage, créée par le commutateur si :
 - le commutateur a fonctionné de façon continue pendant 24 heures ;
 - des modifications de configuration ont été apportées à la Configuration d'exécution au cours des dernières 24 heures sans avoir été enregistrées.

Seul le commutateur peut copier la Configuration de démarrage dans la Configuration miroir. Vous pouvez toutefois copier la Configuration miroir dans d'autres types de fichiers ou sur un autre appareil.

- **Micrologiciel** : le système d'exploitation. Plus communément appelé *l'image*.
- **Code de démarrage** : contrôle le démarrage de base du système et lance l'image du micrologiciel.
- **Fichier de langue** : dictionnaire qui permet l'affichage des fenêtres dans la langue sélectionnée.
- **Journal flash** : messages SYSLOG stockés dans la mémoire flash.

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

Vous pouvez utiliser la page *Mettre à niveau/sauvegarder micrologiciel/langue* pour :

- mettre à niveau le micrologiciel en téléchargeant une nouvelle image d'un serveur ;
- mettre à niveau le code de démarrage en téléchargeant un nouveau fichier de démarrage d'un serveur ;
- mettre à jour les fichiers de langue en téléchargeant un nouveau fichier d'un serveur. Les fichiers de langue déterminent les options de langue proposées dans l'utilitaire Web de configuration du commutateur. Vous pouvez sélectionner la langue d'affichage à la connexion ;
- sauvegarder l'image du micrologiciel sur un serveur.

La langue par défaut est toujours l'anglais.

REMARQUE Vous pouvez également sauvegarder ou restaurer les fichiers de configuration. Consultez la section **Téléchargement et sauvegarde des fichiers de configuration et journaux** pour plus d'informations.

Pour mettre à niveau ou sauvegarder le micrologiciel ou pour mettre à jour le code de démarrage ou le fichier de langue :

ÉTAPE 1 Cliquez sur **Administration > Gestion de fichiers > Mettre à niveau/sauvegarder micrologiciel/langue** dans la fenêtre de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Méthode de transfert** : sélectionnez le protocole à utiliser pour le transfert de fichiers (TFTP ou HTTP), qui correspond au type de serveur sur lequel ou depuis lequel vous téléchargez.

- **Enregistrement** : sélectionnez **Mettre à niveau** pour télécharger un fichier sur le commutateur, ou **Sauvegarder** pour copier un fichier du commutateur au serveur.
- **Type de fichier** : sélectionnez le type de fichier à mettre à niveau ou à sauvegarder (vous pouvez uniquement sauvegarder l'image du micrologiciel) :
 - **Image du micrologiciel** : logiciel qui contrôle toutes les fonctions et interfaces du commutateur.
 - **Code de démarrage** : logiciel qui contrôle le démarrage initial du système.
 - **Pack linguistique** : les fichiers qui permettent à l'interface du système d'afficher la langue spécifiée par l'utilisateur sur la page de connexion.
- **Version IP** (TFTP uniquement) : sélectionnez la version du protocole Internet à utiliser pour la mise à niveau. Assurez-vous que le serveur prend en charge la version sélectionnée. Vous pouvez également sélectionner DNS pour saisir le nom du serveur plutôt que l'adresse IP. Pour utiliser un nom DNS, assurez-vous qu'un serveur DNS est configuré sur le commutateur (voir la page *Serveurs DNS*).
- **Serveur TFTP** (TFTP uniquement) : spécifiez l'adresse IP du serveur TFTP. Vous pouvez également spécifier le nom du serveur si DNS a été sélectionné en tant que Version IP.
- **Nom du fichier source** : pour les mises à niveau via TFTP, saisissez le nom du fichier, chemin compris. Pour les mises à niveau via HTTP, recherchez et sélectionnez le fichier depuis votre ordinateur.
- **Nom du fichier de destination** : pour les mises à jour via TFTP, saisissez le nom du fichier, chemin compris. Ce champ ne s'affiche pas pour les sauvegardes via HTTP.

ÉTAPE 3 Cliquez sur **Appliquer** pour commencer la mise à niveau ou la sauvegarde. Une barre de progression indique l'état du transfert de fichiers. Un transfert d'image typique peut prendre entre 5 et 6 minutes.



AVERTISSEMENT

Veillez à ce que le commutateur soit en permanence alimenté lors du téléchargement d'une image ou d'un fichier de code de démarrage. En cas de panne de courant lors du téléchargement d'un fichier sur le commutateur, le contenu du fichier enregistré dans la mémoire persistante est perdu.

En cas de panne d'alimentation au cours du téléchargement du fichier de code de démarrage, le commutateur ne pourra pas démarrer. Contactez le centre d'assistance Cisco Small Business pour obtenir de l'aide.

En cas de panne d'alimentation au cours du téléchargement d'une image, celle-ci ne se chargera pas, mais le programme d'amorçage sera néanmoins opérationnel. Consultez la section **Récupération du micrologiciel via HTTP** pour obtenir des instructions sur le téléchargement d'une image opérationnelle.

Téléchargement et sauvegarde des fichiers de configuration et journaux

Vous pouvez utiliser la page *Télécharger/sauvegarder configuration/journal* pour télécharger sur le commutateur un fichier de configuration enregistré afin de restaurer des paramètres précédemment enregistrés, ou sauvegarder le fichier de configuration actuel sur un emplacement réseau. Vous pouvez également utiliser cette page pour sauvegarder des fichiers journaux.

- *Téléchargement d'un fichier de configuration pour restaurer des paramètres*
- *Sauvegarde du fichier de configuration et des journaux*

Téléchargement d'un fichier de configuration pour restaurer des paramètres

Pour télécharger un fichier de configuration sur le commutateur afin de restaurer un fichier précédemment sauvegardé :

ÉTAPE 1 Cliquez sur **Administration > Gestion de fichiers > Télécharger/sauvegarder configuration/journal** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez la **Méthode de transfert** (HTTP ou TFTP).

ÉTAPE 3 Pour l'**Enregistrement**, sélectionnez **Mettre à niveau** pour télécharger le fichier que vous allez spécifier en dessous.

ÉTAPE 4 Saisissez les paramètres suivants :

- **Version IP** (TFTP uniquement) : sélectionnez la version du protocole Internet à utiliser pour la mise à niveau. Assurez-vous que le serveur prend en charge la version sélectionnée. Vous pouvez également sélectionner DNS pour saisir le nom du serveur plutôt que l'adresse IP. Pour utiliser un nom DNS, assurez-vous qu'un serveur DNS est configuré sur le commutateur (voir la page *Serveurs DNS*).
- **Serveur TFTP** (TFTP uniquement) : spécifiez l'adresse IP du serveur TFTP. Vous pouvez également spécifier le nom du serveur si DNS a été sélectionné en tant que Version IP.
- **Nom du fichier source** : pour TFTP, spécifiez le nom du fichier, chemin compris. Pour HTTP, recherchez et sélectionnez le fichier depuis votre ordinateur.
- **Type du fichier de destination** : sélectionnez l'une des options suivantes :
 - **Configuration de démarrage** : si le fichier de configuration spécifié est valide, il remplacera le fichier de Configuration de démarrage actuel. Il fera office de fichier de configuration actif lors du redémarrage du commutateur.
 - **Configuration de secours** : le fichier spécifié remplacera le fichier de Configuration de secours actuel.

ÉTAPE 5 Cliquez sur **Appliquer** pour commencer la mise à niveau. Une barre de progression indique l'état de l'opération.



ATTENTION Veillez à ce que le commutateur soit en permanence alimenté lors du téléchargement du fichier de configuration sur le commutateur. En cas de panne de courant lors du téléchargement du fichier de configuration, ce dernier est perdu et le processus doit être redémarré.

Sauvegarde du fichier de configuration et des journaux

Pour sauvegarder le fichier de configuration ou le journal :

- ÉTAPE 1** Cliquez sur **Administration > Gestion de fichiers > Télécharger/sauvegarder configuration/journal** dans la fenêtre de navigation.
- ÉTAPE 2** Sélectionnez la Méthode de transfert (HTTP ou TFTP).
- ÉTAPE 3** Pour l'**Enregistrement**, sélectionnez **Sauvegarder**.
- ÉTAPE 4** Configurez les paramètres suivants :
- **Version IP** (TFTP uniquement) : sélectionnez la version du protocole Internet à utiliser pour la mise à niveau. Assurez-vous que le serveur prend en charge la version sélectionnée. Vous pouvez également sélectionner DNS pour saisir le nom de domaine du serveur plutôt que l'adresse IP. Pour utiliser un nom DNS, assurez-vous qu'un serveur DNS est configuré sur le commutateur (voir la page *Serveurs DNS*).
 - **Serveur TFTP** (TFTP uniquement) : spécifiez l'adresse IP du serveur TFTP. Vous pouvez également spécifier le nom de domaine du serveur si DNS a été sélectionné en tant que Version IP.
 - **Nom du fichier de destination** (TFTP uniquement) : spécifiez un nom pour le fichier enregistré, chemin sur le serveur TFTP compris.
 - **Type du fichier source** : sélectionnez le type du fichier de configuration :
 - **Configuration d'exécution** : la configuration actuelle, incluant toute modification appliquée dans la session de gestion en cours.
 - **Configuration de démarrage** : le fichier de configuration enregistré dans la mémoire flash. Ce fichier n'inclut pas les modifications de configuration appliquées dans la RAM mais non encore enregistrées sur le commutateur.
 - **Configuration de secours** : un fichier de configuration supplémentaire enregistré sur le commutateur en vue d'une utilisation en tant que sauvegarde. L'administrateur peut copier le fichier de Configuration de secours dans le type de fichier de Configuration de démarrage, puis redémarrer le commutateur pour utiliser le fichier de Configuration de secours.
 - **Configuration miroir** : si la Configuration d'exécution ne subit aucune modification pendant au moins 24 heures, elle est automatiquement enregistrée dans un type de fichier de Configuration miroir, et un

message de journal avec une sévérité de niveau **Alerte** est généré pour indiquer qu'un nouveau fichier miroir est disponible. Cette fonction permet à l'administrateur d'afficher la version précédente de la configuration avant son enregistrement dans le type de fichier de Configuration de démarrage ou de copier le type de fichier de Configuration miroir dans un autre type de fichier de configuration. En cas de redémarrage du commutateur, les paramètres d'origine par défaut de la Configuration miroir sont restaurés.

- **Journal flash** : journal d'événements enregistré dans la mémoire flash.
- **Journal opérationnel** : journal d'événements stocké dans la RAM du commutateur, mais pas enregistré dans la mémoire flash.
- **Journal de démarrage** : journal des messages de démarrage.

ÉTAPE 5 Cliquez sur **Appliquer**.

Pour les sauvegardes HTTP, vous êtes invité à sélectionner un emplacement pour l'enregistrement du fichier. Une barre de progression indique l'état du transfert de fichiers.

Supprimer la configuration

La page *Supprimer la configuration* vous permet de supprimer la Configuration de démarrage ou la Configuration de secours. Si vous supprimez à la fois les fichiers de configuration de démarrage et de secours, le commutateur utilisera le fichier de configuration par défaut lorsqu'il redémarrera.

Pour supprimer le fichier de Configuration de démarrage ou de secours :

ÉTAPE 1 Cliquez sur **Administration > Gestion de fichiers > Supprimer la configuration** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez le type de fichier Configuration de démarrage ou Configuration de secours.

ÉTAPE 3 Cliquez sur **Appliquer**.

Copie et enregistrement des fichiers de configuration

La page *Copier/enregistrer la configuration* vous permet de copier des fichiers au sein du système de fichiers. Vous pouvez par exemple copier le fichier de Configuration de secours dans le fichier de Configuration de démarrage, afin qu'il soit utilisé lors du prochain redémarrage du commutateur.

Pour copier un fichier dans le fichier de Configuration de démarrage ou de secours :

ÉTAPE 1 Cliquez sur **Administration > Gestion de fichiers > Copier/enregistrer la configuration** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez le nom du fichier source :

- **Configuration d'exécution** : la configuration actuelle, incluant toute modification appliquée dans la session de gestion en cours.
- **Configuration de démarrage** : le type de fichier de configuration utilisé lors du dernier démarrage du commutateur. Ce fichier n'inclut pas les modifications de configuration appliquées mais non encore enregistrées sur le commutateur.
- **Configuration de secours** : le type de fichier de configuration de secours enregistré sur le commutateur.
- **Configuration miroir** : si la Configuration d'exécution ne subit aucune modification pendant au moins 24 heures, elle est automatiquement enregistrée dans le type de fichier de Configuration miroir, et un message de journal avec une sévérité de niveau **Alerte** est généré pour indiquer qu'un nouveau fichier de Configuration miroir est disponible. Le fichier de Configuration miroir peut être utilisé lorsque le commutateur rencontre des problèmes pour démarrer avec les types de fichiers de Configuration de démarrage ou de secours. L'administrateur peut alors copier la Configuration miroir dans le type de fichier de Configuration de démarrage ou de secours et redémarrer le commutateur.

ÉTAPE 3 Pour le Nom du fichier de destination, sélectionnez le type de fichier à remplacer par le fichier que vous copiez :

- **Configuration de démarrage** : le type de fichier de configuration utilisé lors du dernier démarrage du commutateur. Ce fichier n'inclut pas les modifications de configuration appliquées mais non encore enregistrées sur le commutateur.

- **Configuration de secours** : le type de fichier de configuration de secours enregistré sur le commutateur.

ÉTAPE 4 Cliquez sur **Appliquer** pour commencer la copie.

Le message Opération de copie réussie s'affiche une fois le processus terminé.

Configuration automatique DHCP

Le commutateur prend en charge la Configuration automatique via DHCP pour faciliter le déploiement et les mises à niveau de la configuration. Cette fonction permet de configurer automatiquement un commutateur lorsqu'aucun fichier de configuration n'a été trouvé dans le périphérique de stockage au cours du processus de démarrage, ou lorsqu'un fichier de configuration plus récent est disponible en téléchargement.

REMARQUE La fonction de Configuration automatique est subordonnée à une configuration appropriée des autres appareils du réseau, y compris un serveur DHCP ou BOOTP, un serveur TFTP et, si nécessaire, un serveur DNS.

Présentation

Au cours du démarrage, le commutateur essaie de communiquer avec un serveur DHCP pour obtenir son adresse IP ainsi que d'autres informations. Si la Configuration automatique est activée, le commutateur peut également télécharger un fichier de Configuration de démarrage, en fonction du nom du serveur TFTP et du fichier de Configuration de démarrage qu'il reçoit du serveur DHCP. La Configuration automatique est activée par défaut.

La Configuration automatique DHCP s'initialise lorsque le commutateur est redémarré avec Configuration automatique activé, et si l'une des conditions suivantes se produit :

1. Des informations sur le serveur TFTP et la Configuration de démarrage sont reçues du serveur DHCP, et la Configuration automatique n'a pas précédemment téléchargé le fichier de configuration.
2. Des informations sur le serveur TFTP et la Configuration de démarrage sont reçues du serveur DHCP, et le nom du fichier de configuration diffère du nom de fichier notifié dans un message DHCP précédent.
3. Le fichier de Configuration de démarrage n'est pas présent et aucune information sur le serveur TFTP ou la Configuration de démarrage n'a été reçue du serveur DHCP.

Lorsque les conditions 1 et 2 se produisent, le commutateur enregistre le fichier dans la mémoire flash. Lors des démarrages suivants, il compare le nom du fichier stocké au nom spécifié dans l'option 66/67 du message DHCP actuel. S'ils diffèrent, le nouveau fichier est téléchargé et enregistré dans la mémoire flash.

REMARQUE Lors du premier démarrage du système, le commutateur ne dispose d'aucun nom spécifique pour le fichier de configuration reçu du serveur DHCP, étant donné qu'il n'a pas encore téléchargé de fichier de Configuration de démarrage. Si ces options sont reçues dans le message DHCP, ce nom de fichier est enregistré et le téléchargement commence.

Lorsque l'option 3 se produit, le commutateur recherche le serveur TFTP et le fichier de Configuration de démarrage, comme décrit à la section **Fichier de configuration réseau par défaut**.

Détails des messages du serveur DHCP

Les différents champs suivants peuvent être renvoyés par un serveur BOOTP ou DHCP et traités par le commutateur :

- Le nom du fichier de configuration (fichier de démarrage ou option 67) à télécharger du serveur TFTP
- L'identification du serveur TFTP depuis lequel obtenir le fichier de démarrage.

L'adresse IP du serveur TFTP peut être déduite des différentes sources d'une réponse DHCP. Le commutateur fait son choix en fonction des critères suivants, du niveau de priorité le plus haut vers le plus bas :

1. Le champ **sname** d'une réponse DHCP ou BOOTP.
2. Le champ **Nom du serveur TFTP (option 66)** d'une réponse DHCP.
3. Le champ **Adresse du serveur TFTP (option 150)** d'une réponse DHCP.
4. Le champ **siaddr** d'une réponse DHCP ou BOOTP.

Si seules les valeurs **sname** ou option 66 sont renvoyées au commutateur, un serveur DNS est requis pour traduire l'adresse IP du serveur TFTP. Une fois qu'une adresse IP a été affectée au commutateur, et si aucun nom d'hôte n'a préalablement été affecté, la Configuration automatique envoie une requête DNS pour le nom d'hôte correspondant.

Serveur TFTP secondaire et nom de fichier

Sur la page *Configuration automatique DHCP*, vous pouvez configurer un serveur TFTP secondaire, ainsi que le nom de fichier à utiliser lorsque le nom de serveur ou de fichier fourni par le serveur DHCP est introuvable. La procédure ci-dessous est menée à bien :

1. Le commutateur envoie des messages de monodiffusion au serveur TFTP identifié via DHCP, s'il a été fourni.
2. Si les informations DHCP n'ont pas été fournies ou si le nom du serveur ou du fichier est introuvable, le serveur utilise les informations secondaires, si elles ont été configurées.
3. Si les informations secondaires ne sont pas configurées ou si le nom du serveur ou du fichier est introuvable, le commutateur envoie des messages de diffusion au serveur TFTP identifié via DHCP.

Détails de téléchargement du fichier de configuration

Le commutateur essaiera tout d'abord de télécharger un fichier de configuration spécifique à l'hôte. Si ce n'est pas possible, il téléchargera le fichier de configuration `<nom_hôte>.cfg` si le Mode de configuration réseau par défaut est activé.

Fichier de configuration spécifique à l'hôte

Le commutateur essaie de télécharger le fichier de configuration spécifique à l'hôte, dont le nom est spécifié en tant que nom de fichier de démarrage dans la réponse d'un serveur DHCP/BOOTP ou configuré en tant que fichier de Configuration de secours pour la Configuration automatique DHCP. Le commutateur émet trois requêtes TFTP de monodiffusion pour le fichier de démarrage spécifié. En cas d'échec des tentatives de monodiffusion, ou si aucune adresse de serveur TFTP n'a été fournie, le commutateur émet trois requêtes de diffusion vers tout serveur TFTP disponible pour le fichier de démarrage spécifié. Lorsque le commutateur obtient le fichier de configuration, la configuration est validée par rapport aux erreurs. Si la validation réussit, le commutateur copie la configuration dans le type de fichier de Configuration de démarrage, stocke le nom du fichier de configuration dans la mémoire non volatile et redémarre l'unité.

REMARQUE Pour le commutateur, le nom du fichier de démarrage doit porter l'extension `*.cfg`.

Fichier de configuration réseau par défaut

Si le Mode de configuration réseau par défaut est activé, le commutateur télécharge le fichier de configuration `<nom_hôte>.cfg` lorsqu'une des conditions suivantes se produit :

- Aucun fichier de configuration spécifique à l'hôte n'est spécifié ou configuré.
- Aucun fichier de configuration spécifique à l'hôte n'existe sur le serveur TFTP.
- Une défaillance se produit lors du téléchargement.

Pour traduire le nom d'hôte dans le fichier de configuration, le commutateur commence par télécharger `fp-net.cfg` du serveur TFTP. Le fichier `fp-net.cfg` est considéré comme le fichier de configuration réseau par défaut. Il contient un ou plusieurs mappages d'adresses IP aux noms d'hôte. Le commutateur détermine le nom d'hôte à partir des mappages se rapportant à cette adresse IP. S'il ne trouve aucun mappage, le commutateur utilise la recherche DNS inversée pour découvrir le nom d'hôte.

Un exemple de fichier `fp-net.cfg` vous est présenté ci-dessous :

```
config
...
ip host switch_to_setup 192.168.1.10
ip host another_switch 192.168.1.11
... <autres définitions de nom d'hôte>
exit
```

Lorsqu'un nom d'hôte a été déterminé, le commutateur émet une requête TFTP pour un fichier nommé « `<nom_hôte>.cfg` », où `<nom_hôte>` correspond aux huit premiers caractères du nom d'hôte du commutateur.

Le commutateur utilise l'adresse IP pour effectuer une recherche de noms DNS inversée. Par exemple, si l'adresse IP du commutateur est 192.168.1.10, le nom d'hôte devient **switch_t.cfg** (les huit premiers caractères dans l'exemple ci-dessus).

Le nom de commutateur par défaut est déterminé comme suit : *switch+six derniers chiffres de l'adresse hexadécimale*. Le fichier de mappage doit comporter les noms d'hôte, tels que **ip host switchD99FA5 192.168.1.10**. Ensuite, le nom d'hôte appris pour `<nom_hôte.cfg>` est **switchD9.cfg** pour le commutateur dont l'adresse IP est **192.168.1.10**.

Si le commutateur ne parvient pas à mapper son adresse IP à un nom d'hôte, la Configuration automatique envoie des requêtes TFTP pour le fichier de configuration par défaut **host.cfg**.

Lorsque le commutateur obtient le fichier de configuration par défaut, la configuration est validée par rapport aux erreurs. Si la validation réussit, le commutateur copie la configuration dans le type de fichier de Configuration de démarrage et redémarre. Dans ce cas, le nom du fichier de configuration par défaut n'est pas stocké dans la mémoire non volatile.

REMARQUE Si le commutateur ne parvient pas à obtenir le fichier de configuration valide, le processus décrit ci-dessus est répété toutes les 20 minutes jusqu'à ce que le commutateur l'obtienne. L'administrateur peut créer un fichier de Configuration de démarrage en enregistrant manuellement la Configuration d'exécution. Il peut également, s'il le souhaite, désactiver la Configuration automatique.

Le tableau suivant résume les fichiers de configuration pouvant être téléchargés et l'ordre dans lequel ils sont recherchés.

Ordre de recherche	Nom du fichier	Description	Fichier final recherché
1	<fichier_démarrage>.cfg	Fichier de configuration spécifique à l'hôte, portant l'extension *.cfg ¹	Oui
2	fp-net.cfg	Fichier de configuration réseau par défaut	Non
3	<nom_hôte>.cfg	Fichier de configuration spécifique à l'hôte, associé au nom d'hôte	Oui
4	host.cfg	Fichier de configuration par défaut	Oui

1. Le nom du fichier peut être appris via DHCP ou configuré manuellement, comme cela est décrit à la section **Serveur TFTP secondaire et nom de fichier**.

Un opérateur peut à tout moment, avant le téléchargement du fichier, mettre fin à la Configuration automatique. Cette opération doit s'effectuer alors que le commutateur est déconnecté du réseau, ou si les fichiers de configuration requis n'ont pas été configurés sur les serveurs TFTP.

Lorsqu'un fichier de configuration est téléchargé et enregistré dans le type de fichier de Configuration de démarrage, le commutateur journalise un message avec une sévérité de niveau Alerte avant de redémarrer.

Définition de la configuration automatique DHCP

Vous pouvez utiliser la page *Configuration automatique DHCP* pour activer et désactiver cette fonction, configurer les paramètres de serveur TFTP et de nom de fichier, et afficher les informations d'état.

Lorsque la Configuration automatique DHCP est activée, elle se trouve à l'état **En attente des options de démarrage**, jusqu'à ce qu'elle reçoive une notification du client DHCP. Le client DHCP déclenche le processus d'installation automatique lorsqu'il reçoit l'adresse IP du serveur DHCP, après quoi l'état passe à **Traitement des options DHCP/BOOTP, vérification des conditions préalables**.

Les messages supplémentaires suivants peuvent s'afficher :

- En attente des options de démarrage
- Traitement des options DHCP/BOOTP, vérification des conditions préalables
- Téléchargement de tftp://<adresse_tftp>/<nom_fichier>
- Application de la configuration téléchargée
- En attente de l'expiration du délai de redémarrage
- Enregistrement de la configuration téléchargée
- Arrêté
- L'installation automatique est terminée.
- Le processus d'installation automatique s'est arrêté : échec de la validation du fichier <nom_fichier>.
- Le processus d'installation automatique s'est arrêté : échec de l'enregistrement du fichier de configuration <fichier_démarrage> téléchargé dans la configuration de démarrage.
- Le processus d'installation automatique s'est arrêté : la configuration de démarrage est créée manuellement.
- Le processus d'installation automatique s'est arrêté : le fichier de démarrage correspondait au dernier fichier téléchargé.
- Le processus d'installation automatique s'est arrêté : échec de la traduction du nom du fichier de démarrage.

Pour définir la configuration automatique DHCP :

ÉTAPE 1 Cliquez sur **Administration > Configuration automatique DHCP** dans la fenêtre de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Configuration automatique via DHCP** : cochez la case **Activer** pour activer cette fonction sur le commutateur.
- **Mode de configuration réseau par défaut** : cochez la case Activer pour que le commutateur télécharge un fichier de configuration par défaut nommé *fp-net.cfg* lorsqu'il ne trouve aucun fichier spécifique à l'hôte. Consultez la section **Fichier de configuration réseau par défaut** pour plus d'informations.
- **Serveur TFTP secondaire** : spécifiez l'adresse IP d'un serveur TFTP qui fera office de serveur de secours. Un serveur TFTP secondaire est utilisé lorsque les requêtes de monodiffusion destinées au serveur TFTP spécifié dans l'option 66 échouent à trois reprises.
- **Fichier de configuration secondaire** : spécifiez le nom d'un fichier de configuration secondaire à utiliser comme fichier de secours. Si aucun fichier de configuration de démarrage n'a été identifié dans l'option 67 du serveur DHCP, ou si le fichier spécifié est introuvable sur le serveur TFTP, la Configuration automatique recherche le nom du fichier secondaire.
- **Dernier nom du fichier de configuration automatique** : nom du fichier de configuration utilisé lors de la dernière exécution du processus de Configuration automatique. Si un autre nom de fichier est identifié via DHCP, le téléchargement du fichier commence.
- **État actuel** : l'état du processus de Configuration automatique. Les valeurs possibles sont Terminé ou En cours.

ÉTAPE 3 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Récupération du micrologiciel via HTTP

Le commutateur dispose d'une fonction de récupération du micrologiciel qui permet de restaurer une image valide sur le commutateur après l'échec d'un téléchargement. En cas de panne de courant au cours du téléchargement d'une image, le commutateur pourrait ne pas être en mesure de démarrer. Dans ce cas,

bien que l'image ne soit pas utilisable, le fichier du programme d'amorçage qui charge l'image du micrologiciel depuis la mémoire flash vers la RAM continue d'être fonctionnel. Le fichier du programme d'amorçage intègre un serveur HTTP permettant à l'administrateur de se connecter au commutateur via un port de commutation et d'utiliser un navigateur Web pour télécharger et installer une nouvelle image de micrologiciel.

Le commutateur entre en mode de récupération HTTP de micrologiciel lorsque, au démarrage de l'appareil, le programme d'amorçage ne parvient pas à trouver d'image valide dans la mémoire flash. Dans ce mode, le programme d'amorçage définit le port réseau interne du commutateur sur l'adresse IP statique suivante :

- Adresse IP : 192.168.1.254
- Masque de réseau : 255.255.255.0
- Passerelle par défaut : 192.168.1.1

Un serveur HTTP démarre et écoute les connexions client sur le port 80.

Pour utiliser cette fonction afin de télécharger une nouvelle image de micrologiciel :

ÉTAPE 1 Connectez directement un PC de gestion à un port de commutation.

ÉTAPE 2 Configurez l'adresse IP et le masque sur le PC de gestion de telle façon qu'il se trouve sur le même sous-réseau que le commutateur.

REMARQUE : vous pouvez accéder au système à travers un réseau si l'adresse IP par défaut de la passerelle est 192.168.1.1.

ÉTAPE 3 Ouvrez un navigateur Web et saisissez l'adresse IP du commutateur dans la barre d'adresse (192.168.1.254).

REMARQUE : les fonctions de récupération HTTP du micrologiciel prennent en charge les navigateurs suivants :

- Firefox 3.0 et les versions ultérieures ;
- Internet Explorer 6 et les versions ultérieures.

Une page Récupération du micrologiciel s'affiche. Aucune authentification n'est requise.

La page Web affiche le PID/VID (ID du produit et ID du fournisseur), le numéro de série et l'adresse MAC du commutateur.

ÉTAPE 4 Sélectionnez **Parcourir** et choisissez une image de micrologiciel valide à télécharger.

Une barre de progression montre l'avancement du téléchargement du fichier. Le message suivant s'affiche une fois le téléchargement terminé :

Terminé à 100 %

Fichier téléchargé avec succès. Veuillez patienter pendant l'enregistrement du fichier en mémoire flash. Le système redémarrera automatiquement.

Le fichier sélectionné par l'administrateur est téléchargé dans la mémoire RAM et validé pour les conditions suivantes :

- Le CRC du fichier est bon.
- Le fichier STK est compatible avec cette plate-forme.
- La taille du fichier STK se situe dans les limites de la partition (4,5 Mo sont réservés pour ce fichier).

Si ces conditions sont remplies, le fichier est enregistré dans la mémoire flash et le système est redémarré avec le nouveau micrologiciel.

En cas d'échec d'une de ces vérifications, l'image n'est pas enregistrée dans la mémoire flash et le processus de récupération s'arrête. Vous pouvez redémarrer ce processus avec un fichier image correct.

En cas d'abandon du transfert suite à l'actualisation ou à la fermeture de la fenêtre du navigateur, la session est effacée et expire immédiatement. En cas d'abandon du transfert parce que le réseau est inaccessible, la session expire au bout de 45 secondes. Une fois la session expirée, vous pouvez relancer le processus de récupération.

Redémarrage du commutateur

Utilisez la page *Redémarrer* pour redémarrer le commutateur. Pour redémarrer le commutateur :

ÉTAPE 1 Cliquez sur **Administration** > **Redémarrer** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez l'une des options suivantes :

- **Redémarrer** : redémarre le commutateur en utilisant la dernière configuration enregistrée.

- **Redémarrer avec les paramètres d'origine** : redémarre le commutateur en utilisant le fichier de configuration par défaut d'origine. Tous les paramètres personnalisés sont perdus.

Une fenêtre s'affiche pour vous permettre de confirmer ou d'annuler le redémarrage. Il est possible que la session de gestion en cours soit arrêtée.

ÉTAPE 3 Confirmez ou annulez le redémarrage.

Envoi de requêtes ping à des hôtes

Utilisez la page *Ping* pour envoyer une requête ping du commutateur vers une adresse IP spécifique. Vous pouvez utiliser cette fonction pour vérifier si le commutateur peut communiquer avec un hôte de réseau particulier.

Pour envoyer une requête ping à un hôte de réseau :

ÉTAPE 1 Cliquez sur **Administration** > **Ping** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez **IPv4** ou **IPv6** comme Type d'adresse.

ÉTAPE 3 S'il s'agit d'une adresse IPv4, saisissez les paramètres suivants :

- **Adresse IP/Nom hôte** : saisissez l'adresse IP ou le nom d'hôte de la station à laquelle vous souhaitez que le commutateur envoie une requête ping.
- **Nombre** : spécifiez le nombre de requêtes ping à envoyer.
- **Intervalle** : spécifiez le nombre de secondes entre l'envoi de deux requêtes ping.
- **Taille du datagramme** : spécifiez la taille des données du paquet ping à envoyer.

S'il s'agit d'une adresse IPv6, saisissez les paramètres suivants :

- **Type ping** : sélectionnez **Global** pour envoyer une requête ping à une adresse située en dehors du sous-réseau local. Sélectionnez **Liaison locale** pour envoyer une requête ping à une adresse située sur le sous-réseau local.
- **Adresse/nom d'hôte IPv6** (Adresses globales uniquement) : saisissez l'adresse globale de 128 bits.

- **Adresse IPv6 de liaison locale** (Adresses de liaison locale uniquement) : saisissez l'adresse de liaison locale si l'adresse se trouve sur le même sous-réseau que le commutateur.
- **Taille du datagramme** : spécifiez la taille des données du paquet ping à envoyer (entre 48 et 2 048 octets).

ÉTAPE 4 Cliquez sur **Appliquer** pour envoyer la requête ping. Vous pouvez afficher l'état de la requête dans la fenêtre Ping.

Configuration du transfert de paquets de contrôle

Vous pouvez utiliser la page *Transfert de paquets de contrôle* pour configurer la façon dont le commutateur gère les paquets des types de protocole suivants :

- **CPD** : le protocole de découverte Cisco (CPD), pris en charge sur de nombreux types d'équipement réseau Cisco. CPD permet aux appareils directement connectés de partager des informations telles que leur adresse IP, leurs fonctionnalités et leurs versions logicielles. Bien que le commutateur ne prenne pas lui-même en charge le protocole CPD, il transfère par défaut les paquets CPD de la part des appareils connectés au sein d'un VLAN.
- **Dot1X** : le protocole IEEE 802.1X définit la manière dont les paquets EAP (Extensible Authentication Protocol, protocole d'authentification extensible) sont encapsulés sur un LAN. Dot1X offre un moyen d'authentifier les utilisateurs et de leur autoriser ou de leur refuser l'accès aux services proposés par les ports de commutation. Reportez-vous à 802.1X pour obtenir des informations sur la configuration de la fonction Dot1X sur le commutateur.
- Les périphériques réseau LLDP utilisent le protocole LLDP (Link Layer Discovery Protocol) pour notifier leurs fonctionnalités aux autres appareils. Reportez-vous à LLDP-MED pour obtenir des informations sur la configuration de la fonction LLDP sur le commutateur.

Pour configurer le transfert de paquets de contrôle :

ÉTAPE 1 Cliquez sur **Administration > Transfert de paquets de contrôle** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez le protocole à configurer (CPD, LLPD ou DOT 1x).

ÉTAPE 3 Sélectionnez l'action qu'un port mettra en œuvre lors de la réception de paquets du type spécifié :

- **Abandonner** : tous les paquets du type sélectionné sont abandonnés.
- **Transférer** : tous les paquets du type sélectionné sont transférés au sein du VLAN spécifié.
- **Terminer** : le paquet est accepté et traité sur le commutateur. Cette option n'est pas disponible pour les paquets CPD.

ÉTAPE 4 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Diagnostics

Vous pouvez utiliser les pages de diagnostics pour effectuer des tests virtuels des câbles en cuivre et à fibre optique, configurer une surveillance de diagnostic pour un port ou un VLAN, et afficher les données d'utilisation des CPU.

Consultez les rubriques suivantes pour plus d'informations sur les pages de configuration disponibles dans le menu Administration > Diagnostics :

- **Test des ports cuivre**
- **Configuration de la mise en miroir des ports**
- **Utilisation de la mémoire/des CPU**

Test des ports cuivre

Utilisez la page *Ports cuivre* pour effectuer des tests sur les câbles en cuivre. Ces diagnostics de la couche physique peuvent aider à déterminer si le câble est rompu et, si oui, à quel niveau.

La Table des ports cuivre répertorie chaque port ainsi que les données suivantes, acquises lors du test le plus récent (des données par défaut s'affichent si le port n'a pas été testé) :

- **Résultat de test** : résultats du dernier test effectué sur les câbles. Ce champ peut prendre les valeurs suivantes :
 - **Normal** : le câble fonctionne correctement.

- **Ouvert** : le câble est déconnecté ou le connecteur est défectueux.
- **Court-circuité** : il y a un court-circuit au niveau du câble.
- **Non testé** : aucun test n'a été effectué.
- **Échec du test du câble** : le test n'a pas permis de déterminer l'état du câble. Il est possible que le câble fonctionne correctement.
- **Distance au défaut** : distance en mètres depuis le port au niveau duquel l'erreur de câble a, le cas échéant, été détectée au cours du dernier test du câble.
- **Dernière mise à jour** : date et heure du dernier test du port.
- **Longueur de câble** : longueur du câble en mètres.

Pour lancer un test de port cuivre :

ÉTAPE 1 Cliquez sur **Administration > Diagnostics > Ports cuivre** dans la fenêtre de navigation.

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

Si une liaison est active sur le port lors de l'exécution d'un test de câble, cette liaison peut s'interrompre pendant la durée du test. L'exécution du test peut prendre plusieurs secondes. Une fois celui-ci terminé, une fenêtre apparaît et affiche les résultats.

Configuration de la mise en miroir des ports

Utilisez la fonction de mise en miroir des ports pour envoyer une copie du trafic réseau d'un port sur un autre port en vue de son analyse par un analyseur réseau.

Une session de mise en miroir se compose d'un *port de détection de destination* et d'au moins un *port* source. Une copie miroir du trafic sur le ou les ports source détectés est transmise depuis le port source vers le port de détection de destination. Un analyseur réseau peut être connecté à un port de détection de destination pour analyser le trafic réseau.

Un port configuré en tant que port de détection de destination fait office de port de mise en miroir tant que la session est opérationnellement active. Lorsque la session est inactive, le port transmet et reçoit du trafic en fonction des autres paramètres de configuration.

REMARQUE Lorsqu'un port est configuré en tant que port de détection, le commutateur ne transfère ou ne reçoit aucun trafic, et ne répond à aucune requête ping.

Pour afficher la page *Mise en miroir de ports*, cliquez sur **Administration > Diagnostics > Mise en miroir de ports** dans la fenêtre de navigation.

Quatre sessions de mise en miroir, désactivées par défaut, sont disponibles pour être configurées. La Table des sessions de mise en miroir de ports affiche les champs suivants pour chaque session :

- **ID de session** : identifiant de la session de surveillance.
- **Mode administratif** : indique si la session de mise en miroir de ports est activée ou désactivée.
- **Interface de destination** : pour activer cette fonction, sélectionnez-la et choisissez le port sur lequel le trafic du port source est mis en miroir sur le port de détection de destination.
- **Interface source** : liste des interfaces source sélectionnés pour participer à cette session de mise en miroir.

La Table des interfaces source de mise en miroir de ports répertorie les interfaces source affectées à chaque session. Vous pouvez sélectionner Filtrer et choisir un ID de session pour n'afficher que les données d'une seule session.

Pour configurer la mise en miroir des ports, vous devez au préalable affecter des interfaces source à une session. Vous définissez ensuite un port de destination, et activez la session.

Pour configurer une session de mise en miroir :

ÉTAPE 1 Dans la Table des interfaces source de mise en miroir de ports , cliquez sur **Ajouter**.

ÉTAPE 2 Sélectionnez un ID de session.

ÉTAPE 3 Sélectionnez l'interface source et le type de trafic à mettre en miroir.

ÉTAPE 4 À l'aide de la case d'option Type, spécifiez le sens du trafic au niveau de l'interface source qui doit être surveillée :

- **Réception uniquement** : trafic entrant
- **Émission uniquement** : trafic sortant
- **Émission et réception** : trafic entrant et sortant

ÉTAPE 5 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Vous pouvez répéter le processus pour affecter plusieurs interfaces source à une même session. Veuillez toutefois noter qu'une interface source ne peut être utilisée que dans une seule session active à la fois.

ÉTAPE 6 Dans la Table des sessions de mise en miroir de ports, sélectionnez la session à activer et cliquez sur **Modifier**.

ÉTAPE 7 Pour le Mode administratif, cochez la case **Activer**.

ÉTAPE 8 Pour l'Interface de destination, cochez la case **Activer** et choisissez un port pour la mise en miroir des données.



ATTENTION Lorsqu'un port est configuré en tant que port de détection de destination, le commutateur ne transfère ou ne reçoit aucun trafic sur ce port, et ne répond à aucune requête ping reçue sur ce port. Tous les paramètres de configuration précédents de ce port sont effacés et le port doit être reconfiguré lorsque la mise en miroir est supprimée de la configuration du port.

ÉTAPE 9 Cliquez sur **Appliquer**, puis sur **Fermer**. La session de détection commence.

REMARQUE Pour mettre fin à une session de détection, sélectionnez la session dans la Table des sessions de mise en miroir de ports et cliquez sur **Modifier**. Décochez la case Mode administratif, cliquez sur **Appliquer**, puis cliquez sur **Fermer**.

Utilisation de la mémoire/des CPU

Utilisez la page *Utilisation de la mémoire/des CPU* pour contrôler l'utilisation des CPU et de la mémoire. Pour afficher cette page, cliquez sur **Administration** > **Diagnostics** > *Utilisation de la mémoire/des CPU* dans la fenêtre de navigation.

Cette page affiche les données suivantes :

- **Fréquence d'actualisation** : indiquez si la page doit s'actualiser avec les données les plus récentes toutes les 15, 30 ou 60 secondes ou laissez la valeur par défaut, Aucune actualisation.
- **Rapport d'utilisation des CPU** : pourcentage d'utilisation pour des intervalles de 5 secondes, 1 minute et 5 minutes.

- **Rapport d'utilisation de la mémoire** : ce rapport présente les données suivantes :
 - **Mémoire allouée** : quantité de mémoire dont dispose le système d'exploitation.
 - **Mémoire libre** : quantité de mémoire libre dont dispose le système d'exploitation.
 - **Mémoire totale** : mémoire totale du système, qui inclut la mémoire allouée, à laquelle s'ajoutent la mémoire libre ainsi que la mémoire réservée aux sections de code et de données de l'image logicielle.

Activation de Bonjour

Bonjour permet au commutateur et à ses services d'être détectés via le protocole mDNS (Multicast DNS). Bonjour notifie les services de commutation au réseau et répond aux demandes des types de services qu'il prend en charge, simplifiant de ce fait la configuration réseau dans les environnements de petites entreprises.

Le commutateur notifie les types de services suivants :

- **Description d'appareils spécifiques à Cisco** (cisco-sb) : ce service permet aux clients de détecter les commutateurs Cisco et d'autres produits déployés sur des réseaux de petites entreprises.
- **Interfaces utilisateur de gestion** : ce service identifie les interfaces de gestion disponibles sur le commutateur (HTTP).

Lorsqu'un commutateur compatible avec Bonjour est connecté à un réseau, tout client Bonjour peut détecter l'interface de gestion et y accéder sans configuration préalable.

Un administrateur système peut utiliser un module d'extension Internet Explorer installé pour détecter le commutateur. L'utilitaire Web de configuration du commutateur s'affiche sous la forme d'un onglet dans le navigateur.

Bonjour fonctionne sur les réseaux IPv4 et IPv6.

Pour activer la détection du commutateur via Bonjour :

-
- ÉTAPE 1** Cliquez sur **Administration > Détection - Bonjour** dans la fenêtre de navigation.
- ÉTAPE 2** Cochez la case Activer.
- ÉTAPE 3** Cliquez sur **Appliquer**.
-

LLDP-MED

La norme IEEE 802.1AB, le protocole LLDP (Link Layer Discovery Protocol), décrit une méthode permettant aux stations résidant sur un LAN de notifier des informations d'identification, des fonctions et des descriptions physiques. Les informations sont échangées en unités de données LLDP (LLDPDU, LLDP Data Units) qui comprennent des structures type-longueur-valeur (TLV). Les LLDPDU peuvent comporter différentes TLV, en fonction des informations configurées par l'administrateur sur le port à notifier.

Les informations apprises via des LLDPDU sont stockées dans des MIB, et peuvent être accessibles via un système de gestion du réseau (NMS, Network Management System) tel que SNMP. Ce cadre est extensible et permet une utilisation avancée dans des domaines tels que les réseaux VoIP.

REMARQUE Les LLDPDU se contentent de communiquer des informations ; elles ne configurent pas automatiquement le commutateur.

Le commutateur prend en charge les extensions LLDP-MED (LLDP Media Endpoint Discovery) du protocole LLDP. LLDP-MED permet la détection automatique des stratégies LAN, de l'emplacement des appareils et d'autres caractéristiques d'appareils, et automatise la gestion des terminaux PoE (Power-over-Ethernet).

Consultez les rubriques suivantes pour plus d'informations sur les pages de configuration disponibles dans le menu Administration > Détection - LLDP :

- **Configuration des propriétés LLDP-MED globales**
- **Configuration de LLDP-MED sur un port**
- **Détails sur l'état des ports LLDP-MED**
- **Informations sur le voisinage LLDP-MED**

Configuration des propriétés LLDP-MED globales

Utilisez la page *Propriétés LLDP-MED* pour spécifier les paramètres globaux de cette fonction.

Pour configurer les propriétés LLDP-MED globales :

-
- ÉTAPE 1** Cliquez sur **Administration > Détection - LLDP-MED > Propriétés** dans la fenêtre de navigation.
- ÉTAPE 2** Pour **ID de ressource**, saisissez l'ID de ressource du commutateur, notifié dans les TLV d'inventaire.
- ÉTAPE 3** Spécifiez les Paramètres d'emplacement afin d'identifier l'emplacement physique du commutateur pour les appels d'urgence :
- **Sous-type** : sélectionnez l'une des options suivantes pour spécifier le mode d'identification de l'emplacement du commutateur dans les TLV :
 - **Basé sur les coordonnées** : l'emplacement du commutateur est identifié à l'aide de coordonnées GPS au format hexadécimal.
 - **Adresse physique** : l'emplacement du commutateur est identifié à l'aide d'une description géographique du lieu, telle que la ville, le nom de la rue et le nom du bâtiment.
 - **ELIN** : l'emplacement du commutateur est identifié en utilisant le numéro ELIN (Emergency Location Identification Number, numéro d'identification de l'emplacement en cas d'urgence) du commutateur.
 - **Coordonnées** : coordonnées GPS du commutateur au format hexadécimal.
 - **Adresse ELIN** : numéro ELIN.
 - **Pays** : pays dans lequel se trouve la ville.
 - **Ville** : ville dans laquelle se trouve la rue.
 - **Rue** : rue dans laquelle se trouve le bâtiment.
 - **Bâtiment** : bâtiment dans lequel se trouve le commutateur.
- ÉTAPE 4** Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.
-

Configuration de LLDP-MED sur un port

Le protocole LLDP-MED (LLDP for Media Endpoint Discovery) fournit des extensions à la norme LLDP pour la configuration et la stratégie réseau, l'emplacement des appareils, la gestion de PoE (Power-over-Ethernet) et la gestion de l'inventaire.

Utilisez la page *Paramètres des ports LLDP-MED* pour afficher et configurer les opérations LLDP-MED sur les ports.

Pour configurer ces paramètres sur un port :

ÉTAPE 1 Cliquez sur **Administration > Détection - LLDP-MED > Paramètres des ports LLDP-MED** dans la fenêtre de navigation.

Chaque entrée de la Table des paramètres des ports LLDP-MED affiche la configuration LLDP-MED d'un port.

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

ÉTAPE 3 Spécifiez les éléments suivants pour le port sélectionné :

- **État LLDP-MED** : cochez la case Activer pour autoriser les opérations LLDP-MED sur le port.
- **Notification de configuration** : cochez la case Activer pour autoriser le commutateur à envoyer des notifications en cas de changement de topologie au niveau du réseau.

ÉTAPE 4 Sélectionnez les TLV disponibles que vous souhaitez que le port inclue dans les notifications LLDP :

- **Stratégie réseau** : ID du VLAN, la valeur de classe de service 802.1p et la valeur DCSP (Differentiated Services Code Point, point de code de services différenciés). Ces informations sont utilisées pour mettre en œuvre la fonction VLAN voix (voir la section **Trafic vocal et multimédia**).
- **Emplacement** : coordonnées GPS hexadécimales du commutateur.
- **PSE** : indique si le port se notifie comme étant un appareil PSE (Power Sourcing Equipment, équipement source d'alimentation) capable d'alimenter un appareil PoE (Power-over-Ethernet) connecté. Cette option n'apparaît que sur les appareils SG 200-08p.
- **PD** : indique si le port se notifie comme étant un appareil alimenté (PD, Powered Device) capable de recevoir le PoE (Power-over-Ethernet). Cette option ne peut être sélectionnée que pour le port g1 des appareils SG 200-08.

- **Inventaire** : informations sur les versions matérielles et logicielles.
- **Fonctionnalités système** : identifie la fonctionnalité de base du commutateur, telle que le pontage.

ÉTAPE 5 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

REMARQUE Vous pouvez cliquer sur **Configurer la stratégie réseau** pour afficher la page *VLAN multimédia*. (Vous pouvez également cliquer sur **Gestion des VLAN > Voix et multimédia > VLAN multimédia** dans la fenêtre de navigation.) Cette page vous permet d'affecter des applications LLDP-MED aux VLAN et de configurer les paramètres de priorité pour le trafic associé.

Détails sur l'état des ports LLDP-MED

La page *Détails sur l'état des ports LLDP-MED* affiche la configuration LLDP-MED de tous les ports sur lesquels la fonction est activée. Pour afficher cette page, cliquez sur **Administration > Détection - LLDP-MED > Détails sur l'état des ports LLDP-MED** dans la fenêtre de navigation.

Sélectionnez un port dans la liste des ports. La Table des stratégies réseau affiche les champs de chaque service ou stratégie notifié via LLDP :

- **Type d'application de stratégie multimédia** : type de service, tel que la voix, associé à la stratégie réseau LLDP.
- **ID VLAN** : ID de VLAN associé à la stratégie réseau.
- **Priorité** : valeur de classe de service 802.1p associée à la stratégie réseau.
- **DSCP** : valeur DSCP de la stratégie réseau.
- **Balisé** : la stratégie réseau est définie pour les VLAN balisés.

Les paramètres de commutateur suivants sont notifiés dans les TLV d'inventaire.

- **Révision du matériel** : ID de révision du matériel du commutateur.
- **Révision du micrologiciel** : numéro de révision du micrologiciel du commutateur.
- **Révision du logiciel** : numéro de révision du logiciel du commutateur.
- **Numéro de série** : numéro de série du commutateur.
- **Nom du fabricant** : nom du fabricant du commutateur.

- **Nom du modèle** : nom de modèle du commutateur.
- **ID de ressource** : ID de ressource LLDP-MED du commutateur.

Les paramètres de commutateur suivants sont notifiés dans les TLV système.

- **ID du châssis** : adresse matérielle du commutateur.
- **Sous-type de l'ID du châssis** : type d'adresse matérielle.
- **Description du système** : description préconfigurée du système.
- **Nom du système** : nom d'hôte configuré par l'utilisateur (voir la page *Paramètres système*).
- **Sous-type d'adresse de gestion** : version de protocole de l'adresse IP de gestion.
- **Adresse de gestion** : adresse IP du port de gestion (voir la page *Interface IPv4* ou *Interface IPv6*).
- **Sous-type de l'ID du port** : type de l'identifiant du port.
- **ID du port** : identifiant du port.
- **Description du port** : description du port.
- **Fonctionnalités système activées** : fonctionnalités activées sur le commutateur.
- **Fonctionnalités système prises en charge** : fonctionnalités actuellement notifiées comme étant prises en charge par le commutateur.

Les paramètres de commutateur suivants sont notifiés dans les TLV d'emplacement.

- **Sous-type** : le type d'informations d'emplacement pris en charge (civique, ELIN ou basé sur les coordonnées).
- **Coordonnées** : coordonnées GPS du commutateur au format hexadécimal, si le type d'informations d'emplacement basé sur les coordonnées est utilisé.
- **Adresse ELIN** : numéro ELIN, si ce type d'informations d'emplacement est utilisé.
- **Pays** : pays dans lequel se trouve la ville, si le type d'informations d'emplacement civique est utilisé.
- **Ville** : ville dans laquelle se trouve la rue, si le type d'informations d'emplacement civique est utilisé.

- **Rue** : rue dans laquelle se trouve le bâtiment, si le type d'informations d'emplacement civique est utilisé.
- **Bâtiment** : bâtiment dans lequel se trouve le commutateur, si le type d'informations d'emplacement civique est utilisé.

Informations sur le voisinage LLDP-MED

La page *Informations sur le voisinage* affiche les informations reçues d'autres appareils compatibles LLDP-MED du réseau. Pour afficher cette page, cliquez sur **Administration > Détection - LLDP-MED > Informations sur le voisinage** dans la fenêtre de navigation.

La Table d'informations sur le voisinage affiche les champs suivants pour chaque appareil de voisinage LLDP pour lequel une notification a été reçue :

- **Port local** : numéro de port de l'appareil local sur lequel la notification LLDP a été reçue.
- **ID distant** : adresse physique du port sur l'appareil voisin.
- **Classe de l'appareil** : classe notifiée de l'appareil distant.

Vous pouvez sélectionner une entrée et cliquer sur **Détails** pour afficher des informations supplémentaires de la notification LLDP-MED du voisin.

La page *Informations sur le voisinage - Détails* affiche les informations suivantes :

Fonctionnalités MED :

- **Fonctionnalités signalées** : fonctionnalités notifiées de l'appareil.
- **Fonctionnalités activées** : fonctionnalités notifiées qui sont activées sur l'appareil.
- **Classe de l'appareil** : classe notifiée de l'appareil distant.

Stratégies réseau :

- **Type d'application de stratégie multimédia** : type de service, tel que la voix, associé à la stratégie réseau LLDP.
- **ID VLAN** : ID de VLAN associé à la stratégie réseau.
- **Priorité** : valeur de classe de service 802.1p associée à la stratégie réseau.
- **DSCP** : valeur DSCP de la stratégie réseau.

- **Inconnu** : la valeur 802.1p et la valeur DSCP ne sont pas configurées pour cette stratégie réseau.
- **Balisé** : la stratégie réseau est définie pour les VLAN balisés.

Inventaire :

- **Révision du matériel** : ID de révision du matériel du commutateur.
- **Révision du micrologiciel** : numéro de révision du micrologiciel du commutateur.
- **Révision du logiciel** : numéro de révision du logiciel du commutateur.
- **Nom du fabricant** : nom du fabricant du commutateur.
- **Nom du modèle** : nom de modèle du commutateur.
- **ID de ressource** : ID de ressource LLDP-MED du commutateur.

Emplacement :

- **Sous-type** : sélectionnez l'une des options suivantes pour spécifier le mode d'identification de l'emplacement du commutateur dans les TLV :
 - **Basé sur les coordonnées** : l'emplacement du commutateur est identifié à l'aide de coordonnées GPS au format hexadécimal.
 - **Adresse physique** : l'emplacement du commutateur est identifié à l'aide d'une description géographique du lieu, telle que la ville, le nom de la rue et le nom du bâtiment.
 - **ELIN** : l'emplacement du commutateur est identifié en utilisant le numéro ELIN (Emergency Location Identification Number, numéro d'identification de l'emplacement en cas d'urgence) du commutateur.
- **Informations sur l'emplacement** : informations sur l'emplacement du commutateur, au format spécifié dans le champ Sous-type.

PoE étendu :

- **Type de l'appareil PoE** : si la fonctionnalité PoE est notifiée, ce champ indique si l'appareil est de type PD (Powered Device, appareil alimenté) ou PSE (Power Sourcing Equipment, équipement source d'alimentation).

PD PoE étendu :

Si l'appareil est alimenté par PoE, les propriétés suivantes peuvent être notifiées :

- **Valeur de puissance PoE** : puissance en watts requise par l'appareil.
- **Source d'alimentation PoE** : indique comment l'appareil est alimenté :
 - **Principal** : une alimentation est directement connectée à l'appareil.
 - **Secours** : l'appareil est alimenté depuis un appareil PSE PoE.
- **Priorité d'alimentation PoE** : affiche Haute, Faible ou Critique pour indiquer le niveau de priorité du port lorsque la puissance PoE pouvant être fournie est inférieure à celle demandée par tous les appareils alimentés.

Configuration des options de fournisseur de client DHCP

Vous pouvez configurer la fonctionnalité du client DHCP sur le commutateur de façon à inclure les informations sur le fournisseur dans ses requêtes DHCP (option 60 du serveur DHCP). Un serveur DHCP peut utiliser les informations sur le fournisseur pour différencier les clients en fonction de la fonctionnalité ou du type de matériel identifié.

Pour configurer la chaîne des options de fournisseur DHCP :

ÉTAPE 1 Cliquez sur **Administration** > **Options DHCP** dans la fenêtre de navigation.

Outre l'option et la chaîne d'options de fournisseur, la page affiche le format utilisé par le commutateur lorsqu'il obtient ses informations de fuseau horaire d'un serveur DHCP et indique où ces informations ont été reçues. Pour configurer le commutateur afin qu'il récupère son fuseau horaire depuis un serveur DHCP, consultez la section **Paramètres de l'heure**.

ÉTAPE 2 Cochez la case Activer d'Option du fournisseur.

ÉTAPE 3 Saisissez une valeur dans la zone de texte Chaîne d'options du fournisseur.

ÉTAPE 4 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Gestion des ports

Ce chapitre explique comment configurer les paramètres des ports de commutation, associer les ports en groupes d'agrégation de liaisons et configurer les fonctions d'alimentation des ports.

Il inclut les sujets suivants :

- **Configuration des paramètres des ports**
- **Agrégation de liaisons**
- **Configuration de PoE**
- **Green Ethernet**

Configuration des paramètres des ports

La page *Paramètres des ports* vous permet d'activer et de désactiver de façon administrative les ports et de configurer la négociation automatique du débit des ports et du mode duplex. Vous pouvez également utiliser cette page pour configurer le contrôle de flux sur le port.

Pour configurer les paramètres des ports :

-
- ÉTAPE 1** Cliquez sur **Gestion des ports > Paramètres des ports** dans la fenêtre de navigation.
- ÉTAPE 2** Sélectionnez l'interface à configurer, puis cliquez sur **Modifier**.
- ÉTAPE 3** Spécifiez les éléments suivants pour le port sélectionné :
- **État administratif** : sélectionnez Actif pour activer le port ou Inactif pour le désactiver.

- **Négociation automatique** : cochez la case Activer pour autoriser le commutateur à négocier automatiquement le débit des ports et le mode duplex avec l'appareil connecté. Si la négociation automatique est activée, les champs Débit de port administratif et Mode duplex administratif ne sont pas modifiables.
- **Débit de port administratif** : si la négociation automatique est désactivée, indiquez si le port peut fonctionner à 10 Mbit/s ou à 100 Mbit/s.
- **Mode duplex administratif** : si la négociation automatique est désactivée, sélectionnez Semi pour le semi-duplex ou Intégral pour le duplex intégral.
- **Annonce administrative** : si la négociation automatique est activée, sélectionnez le paramètre de débit de port et de duplex le plus élevé que vous souhaitez que le port négocie. Si vous sélectionnez Capacité maximale, le port négocie automatiquement jusqu'au paramètre de débit de port et de duplex le plus élevé pris en charge par le matériel.
- **Contrôle de flux** : sélectionnez cette option pour activer le contrôle de flux IEEE 802.3x. Le contrôle de flux permet d'empêcher la perte de données lorsque le port ne peut pas faire face au nombre de trames commutées. Lorsque cette option est activée, le commutateur peut envoyer une trame PAUSE pour arrêter le trafic sur un port si la quantité de mémoire utilisée par les paquets sur ce port dépasse un seuil préconfiguré. Le port en pause ne transfère pas les paquets pendant la période spécifiée dans la trame PAUSE. Une fois la durée de la trame PAUSE écoulée, ou une fois que l'utilisation revient à un seuil bas spécifié, le commutateur autorise à nouveau le port à transmettre des trames.
- **Membre dans LAG** : indique si le port est membre d'un groupe d'agrégation de liaisons (LAG, Link Aggregation Group). Consultez la section [Agrégation de liaisons](#) pour plus d'informations sur la configuration des LAG.
- **MTU** : spécifiez la taille maximale des unités de transmission, en octets. La valeur par défaut de l'unité MTU est 1 518 et la plage valide se situe entre 1 518 et 9 216 octets.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Agrégation de liaisons

L'agrégation de liaisons permet d'agréger une ou plusieurs liaisons Ethernet en duplex intégral de façon à former un groupe d'agrégation de liaisons (LAG, Link Aggregation Group). Le commutateur traite le LAG comme s'il s'agissait d'un seul port physique, avec une tolérance aux pannes accrue et une meilleure capacité de partage de charge.

Une interface LAG peut être statique ou dynamique :

- **LAG statique** : les ports sont directement affectés à un LAG par l'administrateur. Les ports restent des membres de LAG dédiés jusqu'à ce qu'ils soient configurés différemment.
- **LAG dynamique** : un LAG dynamique est configuré avec un ou plusieurs ports candidats. Le LAG est formé en échangeant des LACPDU (Link Aggregation Control Protocol Data Units, unités de données de protocole de contrôle de l'agrégation de liaisons) avec l'appareil distant se connectant aux ports candidats. Une fois formé, le LAG peut n'inclure qu'un sous-ensemble des ports éligibles, en fonction des limitations de numéros de port des LAG et d'autres facteurs. Les ports candidats qui ne sont pas sélectionnés en tant que ports membres actifs d'un LAG sont considérés comme des ports de réserve. Un port de réserve peut être sélectionné en tant que membre actif en cas de défaillance d'un port actif du même LAG.

Les rubriques suivantes fournissent des informations supplémentaires sur les pages de configuration disponibles dans le menu Gestion des ports > Agrégation de liaisons :

- [Configuration des LAG](#)
- [Configuration des paramètres des LAG](#)
- [Configuration des paramètres LACP](#)

Configuration des LAG

Le commutateur peut prendre en charge jusqu'à quatre LAG, avec huit ports par LAG. Utilisez la page *Gestion des LAG* pour affecter des ports aux LAG et LACP.

Pour afficher cette page, cliquez sur **Gestion des ports > Agrégation de liaisons > Gestion des LAG** dans la fenêtre de navigation.

Quatre LAG dynamiques nommés *ch1* à *ch4* sont préconfigurés par défaut. Ils ne comportent aucun port membre et sont désactivés.

Vous pouvez ajouter des ports à un LAG ou en supprimer sans perturber le trafic sur ce LAG.

Une appartenance peut être affectée aux LAG dans les VLAN ; toutefois, les ports individuels perdent leurs appartenances VLAN individuelles lorsqu'ils deviennent membres d'un LAG. Lorsqu'un port est supprimé d'un LAG, il rétablit la connexion avec les VLAN auxquels il appartenait précédemment, conformément à la Configuration de démarrage.

Pour configurer un LAG :

ÉTAPE 1 Sélectionnez un LAG à configurer, puis cliquez sur **Modifier**.

ÉTAPE 2 Spécifiez les paramètres suivants pour le LAG sélectionné :

- **Nom du LAG** : saisissez jusqu'à 15 caractères alphanumériques pour identifier le LAG.
- **Type** : sélectionnez Statique pour affecter manuellement des ports au LAG. Sélectionnez Dynamique pour permettre aux ports d'échanger des LACPDU pour former le LAG de façon dynamique.
- **Liste des ports/Membres du LAG** : pour ajouter ou supprimer des ports au niveau d'un LAG statique, sélectionnez chaque port et cliquez sur la flèche gauche ou droite pour le déplacer entre les listes des ports et des membres du LAG.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration des paramètres des LAG

Vous pouvez utiliser la page *Paramètres des LAG* pour activer ou désactiver un LAG de façon administrative et configurer les paramètres d'équilibrage de charge.

Pour configurer les paramètres des LAG :

ÉTAPE 1 Cliquez sur **Gestion des ports > Agrégation de liaisons > Paramètres des LAG** dans la fenêtre de navigation.

La Table des paramètres des LAG répertorie chaque LAG disponible.

ÉTAPE 2 Sélectionnez un LAG à configurer, puis cliquez sur **Modifier**.

ÉTAPE 3 Spécifiez les paramètres suivants pour le LAG sélectionné :

- **État administratif** : sélectionnez Actif ou Inactif pour activer ou désactiver le LAG de façon administrative. Lorsqu'un LAG est désactivé, ses ports membres fonctionnent comme des ports physiques autonomes.
- **Algorithme d'équilibrage de charge** : sélectionnez une des options pour permettre au commutateur d'équilibrer la charge des paquets sortants entre les ports membres d'un LAG. Le commutateur sélectionne une des liaisons du canal pour transmettre des paquets spécifiques. Le commutateur hiérarchise chaque critère d'équilibrage de charge dans l'ordre indiqué dans l'option. Les options sont les suivantes :
 - **MAC source/de dest, VLAN, EType, port entrant** : adresses MAC source et de destination, l'appartenance VLAN, le champ Ethertype et le port sur lequel le paquet a été reçu.
 - **Champs IP source/de dest et Port TCP/UDP** : adresse IP source et de destination, et le numéro de port TCP ou UDP dans le paquet IP.

Lorsque l'option de paquet IP est sélectionnée, les paquets non IP reçus sur le port sont équilibrés à l'aide de l'adresse MAC source et de destination.

- **MTU** : spécifiez la taille maximale des unités de transmission, en octets. La valeur par défaut de l'unité MTU est 1 518 et la plage valide se situe entre 1 518 et 9 216 octets.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration des paramètres LACP

Le commutateur utilise le protocole LACP (Link Aggregation Control Protocol, protocole de contrôle de l'agrégation de liaisons) pour automatiser la formation de LAG dynamiques. Les ports compatibles LACP envoient des unités de données de protocole LACP (LACPDU) pour se détecter les uns les autres sur un réseau et négocier un LAG.

Utilisez la page *LACP* pour afficher et configurer le fonctionnement du protocole.

Pour configurer les paramètres LACP sur des ports individuels :

ÉTAPE 1 Cliquez sur **Gestion des ports > Agrégation de liaisons > LACP** dans la fenêtre de navigation.

La Table des interfaces LACP affiche la configuration LACP locale (acteur) et distante (partenaire) pour chaque port du commutateur. Les paramètres d'acteur LACP incluent une Priorité du système pour le commutateur et une Clé d'administration qui identifie de façon unique le port dans les messages LACP. Ces valeurs ne sont pas configurables.

Pour modifier les paramètres LACP :

ÉTAPE 1 Sélectionnez le port que vous souhaitez configurer, puis cliquez sur **Modifier**.

ÉTAPE 2 Configurez les paramètres suivants pour le port sélectionné :

- **Mode** : cochez la case pour activer LACP sur le port.
- **Expiration de l'acteur** : les informations de l'acteur ne sont plus valides à expiration du délai.
 - **Court** : le délai d'expiration LACP court correspond à trois fois le temporisateur périodique court pour la transmission de paquets LACP. La valeur par défaut du délai LACP court est de 3 secondes.
 - **Long** : le délai d'expiration LACP long correspond à trois fois le temporisateur périodique long pour la transmission de paquets LACP. La valeur par défaut du délai LACP long est de 90 secondes.
- **Expiration du partenaire** : les informations du partenaire ne sont plus valides à expiration du délai.
 - **Court** : le délai d'expiration LACP court correspond à trois fois le temporisateur périodique court pour la transmission de paquets LACP. La valeur par défaut du délai LACP court est de 3 secondes.
 - **Long** : le délai d'expiration LACP long correspond à trois fois le temporisateur périodique long pour la transmission de paquets LACP. La valeur par défaut du délai LACP long est de 90 secondes.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration de PoE

Sur le SG 200E-08P, les ports 1 à 4 peuvent fonctionner en tant que PSE PoE. Un PSE peut alimenter des appareils PD (Powered Devices, appareils alimentés) PoE connectés.

Pour les commutateurs SG 200-08P, consultez les rubriques suivantes afin d'obtenir des informations sur les pages de configuration disponibles dans le menu Gestion des ports > PoE :

- **Configuration des propriétés PoE**
- **Configuration des paramètres des ports PoE**

REMARQUE Ces pages de configuration ne s'affichent pas sur les commutateurs qui ne prennent pas en charge la fonctionnalité PSE.

Configuration des propriétés PoE

Vous pouvez utiliser la page *Propriétés* pour définir si le commutateur génère des messages d'interruption sous certaines conditions et pour afficher les paramètres d'alimentation actuels :

Pour configurer les propriétés PoE :

ÉTAPE 1 Cliquez sur **Gestion des ports > PoE > Propriétés** dans la fenêtre de navigation.

ÉTAPE 2 Définissez les paramètres suivants :

- **Seuil des interruptions d'alimentation** : spécifiez un pourcentage de la puissance système disponible totale. Lorsque la puissance demandée sur les ports PoE dépasse le seuil, une interruption est enregistrée dans le journal.
- **Mode de gestion de l'alimentation** : sélectionnez la façon dont le commutateur hiérarchise la puissance qu'il fournit à plusieurs ports :
 - **Statique avec priorité du port** : gestion statique de la priorité de l'alimentation. Cet algorithme pré-affecte la puissance en fonction de la limite de puissance configurée et de la priorité du port.
 - **Dynamique avec priorité du port** : gestion dynamique de la priorité de l'alimentation. Cet algorithme alimente les appareils tant que la consommation se situe dans la limite et la priorité configurées. Il n'y a aucune pré-affectation de puissance.

Dans ces deux modes, lorsque le commutateur alimente plusieurs ports, la priorité est accordée à un port disposant d'une priorité plus haute. Si plusieurs ports disposent du même niveau de priorité, la priorité est accordée à celui dont le numéro de port est le plus faible.

- **Mode de réinitialisation** : cochez la case Activer pour permettre au commutateur d'initialiser toutes les machines à états des ports PoE.

ÉTAPE 3 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

REMARQUE Cette page contient les données suivantes se rapportant à la puissance PoE sur le commutateur :

- **Alimentation** : l'état actuel de l'alimentation. Si elle est définie sur *Activée*, le commutateur alimente un appareil connecté via PoE. Si elle est définie sur *Désactivée*, le commutateur n'alimente actuellement aucun appareil connecté via PoE.
- **Puissance nominale** : quantité totale (en watts) que le commutateur peut fournir à tous les ports compatibles PoE.
- **Seuil d'alimentation** : valeur d'alimentation de coupure au-dessus de laquelle aucun appareil PD supplémentaire n'est alimenté. Ce seuil est calculé à partir du paramètre Seuil des interruptions d'alimentation.
- **Consommation** : puissance totale (en watts) que le commutateur fournit actuellement aux ports PoE.

Configuration des paramètres des ports PoE

Vous pouvez utiliser la page *Paramètres des ports* pour afficher et configurer les paramètres des ports faisant office de PSE.

Pour configurer les paramètres PoE d'un port :

ÉTAPE 1 Cliquez sur **Gestion des ports > PoE > Paramètres des ports** dans la fenêtre de navigation.

La Table des paramètres PoE affiche les ports sur lesquels PoE est activé, leur priorité, l'affectation de puissance en milliwatts et d'autres paramètres pour chaque port.

ÉTAPE 2 Sélectionnez le port que vous souhaitez configurer, puis cliquez sur **Modifier**.

ÉTAPE 3 Configurez les paramètres suivants :

- **PoE** : cochez la case Activer pour configurer le port en tant que PSE.
- **Niveau de priorité d'alimentation** : sélectionnez Critique, Haute ou Faible pour configurer le niveau de priorité du port pour l'alimentation d'un appareil connecté.

Le commutateur pourrait ne pas être en mesure d'alimenter tous les appareils connectés qui le demandent. La priorité du port détermine les ports qui fournissent une alimentation lorsqu'une capacité de puissance adéquate n'est pas disponible pour tous les ports activés. Pour les ports disposant du même niveau de priorité, le port ayant le numéro le plus faible se voit affecter la priorité la plus élevée. Dans le cadre d'un système fournissant une puissance de crête à un certain nombre d'appareils, si un nouvel appareil est connecté à un port à haute priorité, l'alimentation d'un appareil connecté à un port à faible priorité est stoppée et le nouvel appareil est alimenté.

- **Type de limite de puissance** : sélectionnez une des méthodes suivantes pour limiter la puissance que le commutateur fournit à un appareil connecté.
 - **Dot3AF** : la puissance maximale pouvant être fournie par le port est limitée par la classe IEEE 802.3af détectée.
 - **Défini par l'utilisateur** : la puissance maximale pouvant être fournie par le port est spécifiée par l'utilisateur. Si vous sélectionnez cette option, spécifiez une valeur dans le champ Affectation de puissance.
 - **LLDP-MED** : la puissance maximale pouvant être fournie par le port est limitée par la valeur en TLV LLDP-MED reçue d'un appareil de port. La valeur spécifiée par l'appareil doit être comprise entre 3 et 16,2 watts. Si elle n'est pas comprise dans cette plage, la valeur par défaut de 16,2 watts sera utilisée.

Remarque : si le Type de limite de puissance sélectionné est LLDP-MED, le paramètre de priorité de l'appareil distant n'est pas respecté et le commutateur utilise le paramètre de Niveau de priorité d'alimentation configuré pour le port.

- **Dot3AF et LLDP-MED** : la puissance maximale pouvant être fournie par le port est limitée par la valeur en TLV LLDP-MED reçue d'un appareil de port. La valeur spécifiée par l'appareil doit être comprise entre 3 et 16,2 watts. Si elle n'est pas comprise dans cette plage, la puissance maximale est limitée par la classe IEEE 802.3AF.

- **Défini par l'utilisateur et LLDP-MED** : la puissance maximale pouvant être fournie par le port est limitée par la valeur en TLV LLDP-MED reçue d'un appareil de port. La valeur spécifiée par l'appareil doit être comprise entre 3 et 16,2 watts. Si elle n'est pas comprise dans cette plage, la puissance maximale est limitée par la valeur que vous spécifiez dans le champ Affectation de puissance.
- **Affectation de puissance** : si vous avez configuré une option définie par l'utilisateur pour Type de limite de puissance, entrez la puissance en milliwatts à affecter au port, comprise entre 3 000 et 16 200 milliwatts.
- **Type de détection** : sélectionnez une des méthodes suivantes pour détecter les appareils alimentés par PoE et connectés aux ports.
 - **Hérité uniquement** : seuls les appareils à signature capacitive sont détectés.
 - **802.3af 4point uniquement** : seuls les appareils à signature résistive sont détectés avec le premier algorithme.
 - **802.3af 4point et hérité** : les appareils à signature capacitive et résistive sont détectés avec le second algorithme.
 - **802.3af 2point uniquement** : seuls les appareils à signature résistive sont détectés avec le premier algorithme.
 - **802.3af 2point et hérité** : les appareils à signature capacitive et résistive sont détectés avec le premier algorithme.
- **Mode de réinitialisation** : cochez la case Activer pour permettre au commutateur d'initialiser les machines à états PoE.

Les statistiques suivantes s'affichent également :

- **Consommation électrique** : puissance actuellement consommée par le port.
- **Nombre de surcharges** : nombre total d'occurrences de surcharge de courant.
- **Nombre de courts-circuits** : nombre total d'occurrences de courts-circuits électriques sur un port.
- **Nombre de refus** : nombre de fois où l'alimentation a été bloquée sur l'appareil alimenté.
- **Nombre d'absences** : nombre de fois où l'alimentation de l'appareil alimenté a été arrêtée, l'appareil n'étant plus détecté.

- **Nombre de signatures non valides** : nombre de fois où une signature non valide a été reçue. L'appareil alimenté utilise des signatures pour s'identifier auprès du PSE. Une signature est générée lors de la détection, la classification ou la maintenance de l'appareil alimenté.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Green Ethernet

Le commutateur fournit les fonctions d'économie d'énergie Green Ethernet sur les ports cuivre Gigabit Ethernet. Les fonctions Green Ethernet incluent :

- **Mode Détection d'énergie** : contribue à réduire la consommation énergétique des puces en obligeant la couche PHY d'un port à passer en mode basse puissance en cas d'absence du signal d'un partenaire de liaison cuivre.

Lorsque le mode Détection d'énergie est activé, le commutateur passe automatiquement en mode basse puissance en cas de perte d'énergie sur la ligne, et reprend un fonctionnement normal lorsqu'il détecte de l'énergie. Lorsque la couche PHY du port est en mode basse puissance, cette couche se réactive au bout d'un certain temps, et envoie des impulsions de liaison pour surveiller l'énergie du partenaire de liaison. En cas de détection d'énergie alors que le port est en mode réveil, le commutateur rétablit le fonctionnement normal du port. Une fois la période de réveil expirée, le port retourne en mode basse puissance.

- **Mode Courte portée automatique** : lorsque ce mode est activé, un test de câble est automatiquement effectué en cas d'établissement d'une liaison. En cas de détection de câble de faible longueur, le port passe en mode basse puissance. En cas de défaillance de la liaison, le mode basse puissance est désactivé.

Le commutateur prend également en charge la configuration de la fonction Courte portée, qui effectue un test de la longueur du câble. Si la longueur du câble est inférieure à 10 mètres, la couche PHY passe en mode basse puissance, afin que seule la puissance nécessaire pour la prise en charge d'un câble de faible longueur soit utilisée. La Courte portée peut être configurée de deux manières :

- **Courte portée automatique** : le test du câble est automatiquement effectué lorsque la liaison est établie et, en cas de détection d'un câble de faible longueur, la couche PHY du port passe en mode basse puissance. En cas de défaillance de la liaison, le mode basse puissance est désactivé.
- **Forcer la courte portée** : le port est forcé de façon administrative à passer en mode basse puissance en cas d'utilisation de câbles à courte portée.

Les fonctions Green Ethernet sont opérationnelles que la négociation automatique soit ou non activée sur le port, et elles peuvent être activées ou désactivées par l'administrateur. Les propriétés du Mode Green Ethernet peuvent être configurées sur chacun des ports.

Configuration des propriétés Green Ethernet

Utilisez la page *Propriétés Green Ethernet* pour activer la fonctionnalité Green Ethernet au niveau global. Les paramètres globaux sont appliqués à tous les ports.

REMARQUE Vous pouvez remplacer les paramètres globaux en configurant ces fonctions sur des ports individuels (voir la section **Configuration des paramètres Green Ethernet des ports**) ; veuillez toutefois noter que toute modification apportée ultérieurement aux paramètres globaux remplacera les configurations de port individuelles.

Pour configurer les propriétés Green Ethernet globales :

ÉTAPE 1 Cliquez sur **Gestion des ports > Green Ethernet > Propriétés** dans la fenêtre de navigation.

Par défaut, les modes Détection d'énergie et Courte portée automatique sont activés globalement sur tous les ports.

ÉTAPE 2 Configurez les paramètres :

- **Détection d'énergie** : sélectionnez cette option pour activer le mode Détection d'énergie sur le commutateur. Le commutateur passe automatiquement en mode basse puissance en cas de perte d'énergie sur la ligne, et reprend un fonctionnement normal lorsqu'il détecte de l'énergie.

- **Courte portée automatique** : sélectionnez cette option pour que le test du câble soit automatiquement effectué lors de l'établissement de la liaison. En cas de détection de câble de faible longueur, le port passe en mode basse puissance. En cas de défaillance de la liaison, le mode basse puissance est désactivé.
- **Forcer la courte portée** : sélectionnez cette option pour forcer de façon administrative tous les ports à passer par défaut en mode basse puissance pour les câbles à courte portée. Ce paramètre peut être remplacé.

ÉTAPE 3 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration des paramètres Green Ethernet des ports

Utilisez la page *Paramètres Green Ethernet* pour afficher et configurer les paramètres Green Ethernet de ports individuels.

REMARQUE Les paramètres Green Ethernet des ports sont remplacés en cas de modification ultérieure des paramètres globaux (voir la section **Configuration des propriétés Green Ethernet**).

Pour configurer les paramètres Green Ethernet des ports :

ÉTAPE 1 Cliquez sur **Gestion des ports > Green Ethernet > Paramètres des ports** dans la fenêtre de navigation.

La Table des paramètres Green Ethernet affiche les informations suivantes, pour chaque port :

Champs Détection d'énergie :

- **Administratif** : indique si le mode Détection d'énergie est activé sur le port.
- **Opérationnel** : indique si le mode Détection d'énergie est actuellement opérationnel (« Activé ») sur le port.
- **Motif** : indique pourquoi l'état opérationnel est activé ou désactivé. Le motif suivant peut s'afficher lorsque l'état opérationnel du mode Détection d'énergie est Activé.
 - **Aucune énergie détectée** : aucune énergie n'est détectée sur la liaison.

Les motifs suivants peuvent s'afficher lorsque l'état opérationnel du mode Détection d'énergie est Désactivé.

- **Port en mode Fibre** : l'état administratif peut être actif, mais le port fonctionne en mode fibre. (La fonctionnalité Green Ethernet s'applique uniquement aux ports cuivre.)
- **Liaison active** : une activité a été détectée sur la liaison.
- **Mode administratif désactivé** : le mode Détection d'énergie est désactivé de façon administrative.

Champs de Courte portée :

- **Automatique** : indique si le mode Courte portée est activé de façon administrative sur le port.
- **Forcer** : indique si le mode Forcer la courte portée est activé sur le port.
- **Opérationnel** : indique si le mode Courte portée est opérationnel (activé) sur le port.
- **Motif** : indique pourquoi l'état opérationnel du mode Courte portée est actif ou inactif. Le motif suivant peut s'afficher lorsque l'état opérationnel du mode Courte portée est Activé.
 - **Longueur de câble < 10 m** : le port a été détecté comme ayant des câbles à Courte portée.
 - **Forcé** : le mode Courte portée a été forcé de façon administrative sur le port.

Les motifs suivants peuvent s'afficher lorsque l'état opérationnel du mode Courte portée est Désactivé.

- **Longueur de câble > 10 m** : le câble fait plus de 10 mètres.
- **Liaison inactive** : la liaison est inactive.
- **Fibre** : le port fonctionne en mode fibre et ne peut pas bénéficier du mode Green Ethernet.
- **Mode administratif désactivé** : la Courte portée est désactivée de façon administrative.
- **Pas à la vitesse GIG** : le port ne fonctionne pas en 1G et ne peut donc pas bénéficier du mode Green Ethernet.
- **Longueur de câble inconnue** : la longueur du câble n'a pas pu être déterminée.

ÉTAPE 2 Sélectionnez le port que vous souhaitez configurer, puis cliquez sur **Modifier**.

ÉTAPE 3 Configurez les paramètres suivants :

- **Détection d'énergie** : sélectionnez cette option pour activer de façon administrative le mode Détection d'énergie sur le port.
- **Courte portée automatique** : sélectionnez cette option pour activer le mode Courte portée sur le port.
- **Forcer la courte portée** : sélectionnez cette option pour activer le mode Forcer la courte portée sur le port.

ÉTAPE 4 Cliquez sur **Appliquer** pour enregistrer les modifications dans la Configuration d'exécution.

Gestion des VLAN

Ce chapitre décrit les étapes de configuration des VLAN (Virtual LAN, réseau local virtuel).

Il contient les rubriques suivantes :

- **Création d'un VLAN**
- **Configuration des paramètres d'interface VLAN**
- **Configuration d'une appartenance VLAN**
- **Configuration d'une appartenance VLAN des ports**
- **Définition du VLAN par défaut**
- **VLAN multimédia**
- **Trafic vocal et multimédia**

Le VLAN d'un commutateur de couche 2 offre des avantages de pontage et de routage à la fois. Tout comme un pont, un commutateur VLAN réachemine le trafic plus rapidement grâce à l'en-tête de couche 2. Tout comme un routeur, il divise le réseau en segments logiques et améliore l'administration, la sécurité et la gestion du trafic multidiffusion.

Un VLAN regroupe plusieurs stations terminales et ports du commutateur qui les relient. La division logique est nécessaire pour plusieurs raisons, notamment pour la participation à un projet ou à un service. La seule condition est que la station terminale et le port auquel elle est reliée appartiennent aux mêmes VLAN.

Tous les VLAN disposent d'un ID de VLAN qui s'affiche dans la balise IEEE 802.1Q, également appelée balise VLAN, de l'en-tête de couche 2 des paquets acheminés via un VLAN. Si une station terminale omet cette balise ou la partie VLAN de cette balise, le premier port du commutateur qui reçoit ce paquet le rejette ou y insère une balise correspondant à son ID de VLAN par défaut. Un port peut gérer le trafic provenant de plusieurs VLAN. Toutefois, il prend en charge le PVID (Port VLAN ID, ID de VLAN du port) uniquement.

L'ID de VLAN 1 est préconfiguré comme le VLAN par défaut sur le commutateur. Tous les ports sont membres de ce VLAN et utilisent son ID de VLAN (1) en tant que PVID.

Création d'un VLAN

La page *Création d'un VLAN* permet de créer et de configurer des VLAN d'un réseau. Pour accéder à cette page, cliquez sur **Gestion des VLAN > Créer un VLAN** dans la fenêtre de navigation.

La table des VLAN affiche l'ID de VLAN, le nom (si disponible) et le type du VLAN préconfiguré (ID de VLAN 1), ainsi que les VLAN que vous avez ajoutés. Vous devez configurer un port en tant que VLAN par défaut, puis définir tous les autres ports en tant que Statique. L'ID de VLAN 1 est préconfiguré comme le VLAN par défaut sur le commutateur. Tous les ports sont membres de ce VLAN et utilisent son ID de VLAN (1) en tant que PVID.

Si vous créez d'autres VLAN, configurez l'un d'entre eux en tant que VLAN par défaut. Pour plus d'informations, consultez la section **Définition du VLAN par défaut**. Vous ne pouvez pas supprimer le VLAN configuré par défaut. Toutefois, vous pouvez supprimer un VLAN statique. Vous ne pouvez pas également supprimer l'ID de VLAN 1, même si ce VLAN est configuré en tant que réseau statique.

Vous pouvez créer jusqu'à 16 VLAN et leur attribuer jusqu'à 4 094 ID de VLAN. Pour créer un ou plusieurs VLAN :

ÉTAPE 1 Cliquez sur **Ajouter**.

ÉTAPE 2 Sélectionnez un VLAN, puis saisissez un ID de VLAN.

Vous pouvez également créer plusieurs VLAN. Pour ce faire, cochez la case **Plage** et indiquez les ID de VLAN marquant le début et la fin de la plage.

ÉTAPE 3 Si vous créez un seul VLAN, vous pouvez saisir un nom de VLAN facultatif pour référence rapide.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration des paramètres d'interface VLAN

La page *Paramètres d'interface* permet d'afficher et de configurer les fonctions de tagging des VLAN. Pour accéder à cette page, cliquez sur **Gestion des VLAN** > **Paramètres d'interface** dans la fenêtre de navigation.

La table des paramètres d'interface affiche la configuration des VLAN de tous les ports. Pour afficher la configuration VLAN des groupes LAG, sélectionnez LAG dans la liste Type d'interface.

Pour configurer les paramètres d'interface VLAN :

ÉTAPE 1 Sélectionnez le port ou le LAG que vous souhaitez configurer, puis cliquez sur **Modifier**.

ÉTAPE 2 Configurez les paramètres suivants sur le port ou le LAG sélectionné :

- **Mode VLAN de l'interface** : sélectionnez l'une des options pour configurer le type de port par rapport au tagging et à l'appartenance VLAN.
 - **Général** : le port appartient à un ou plusieurs VLAN balisés ou non balisés. Ce mode permet d'activer toutes les fonctions décrites dans les caractéristiques techniques IEEE 802.1Q, « Tagging des VLAN ».
 - **Accès** : le port n'accepte que les trames non balisées. Un port d'accès peut appartenir à un VLAN uniquement et utilise l'ID de VLAN en tant que PVID. En général, les ports d'accès permettent de relier des hôtes qui deviennent membres du VLAN, car ils sont physiquement connectés au port.
 - **Liaison** : le port est membre d'un seul VLAN non balisé, appelé *VLAN natif*, et à plusieurs VLAN balisés (voir à aucun). En général, les ports de liaison permettent d'acheminer le trafic de plusieurs VLAN en provenance du commutateur vers d'autres périphériques réseau, tels qu'un routeur en amont ou un commutateur secondaire.
- **PVID** : l'ID de VLAN du port désigne le VLAN par défaut dont l'interface est membre. Pour les ports en mode Liaison, le PVID est défini sur l'ID de VLAN natif défini. Pour les ports en mode Général, vous pouvez configurer le PVID en tant que tout ID de VLAN valide du commutateur. Pour les ports en mode Accès, le PVID est défini sur l'ID de VLAN d'accès.
- **VLAN natif** (ports en mode Liaison uniquement) : le VLAN natif identifie l'appartenance d'un port de liaison à un VLAN non balisé. Cochez la case VLAN par défaut pour définir cette valeur à celle du VLAN par défaut du port, ou cochez la case Personnalisé pour définir un autre ID de VLAN.

- **PVID** (ports en mode Général uniquement) : cet ID est identique à l'ID du VLAN dont le port est membre non balisé.
- **VLAN d'accès** (ports en mode Accès uniquement) : un port d'accès ne peut être membre que d'un seul VLAN, appelé VLAN d'accès. L'ID de VLAN d'accès désigne l'ID de VLAN d'un port d'accès.
- **Type de trame** : indique le type de trame pris en charge par le port :
 - **Admettre non balisées uniquement** : seules les trames non balisées sont acceptées sur le port. Les trames balisées sont ignorées.
 - **Admettre balisées uniquement** : seules les trames balisées sont acceptées sur le port. Les trames non balisées sont ignorées.
 - **Tout admettre** : les trames balisées et non balisées sont acceptées sur le port.

Les ports d'accès peuvent accepter les trames non balisées uniquement. Les ports de liaison ne peuvent appartenir qu'à un seul VLAN non balisé, ainsi qu'à un ou plusieurs VLAN balisés. Si les ports de liaison sont à la fois membres des VLAN balisés et non balisés, ils acceptent tous les types de trames. Si les ports de liaison sont membres des VLAN balisés uniquement, ils n'acceptent que des trames balisées.

- **Filtrage en entrée** : cochez la case en regard de cette option pour activer le filtrage en entrée sur le port. Lorsque cette option est activée, le commutateur accepte les trames provenant uniquement des VLAN dont il est membre. Il ignore les trames provenant d'autres VLAN. Cette option de filtrage est toujours activée pour l'ensemble des ports définis en mode Accès ou Liaison. Vous pouvez activer ou désactiver cette option uniquement pour les ports définis en mode Général.
- **Priorité de VLAN** : indique la valeur de priorité 802.1p par défaut du port. Cette valeur est appliquée aux paquets entrants selon le mode de confiance QoS configuré sur le port et selon les types de paquets. Pour plus d'informations sur la configuration du mode de confiance des ports, consultez la rubrique [Propriétés de QoS](#).

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Modification du mode VLAN de l'interface

Lorsque le mode VLAN d'un port est modifié, le commutateur gère automatiquement la configuration d'appartenance au VLAN concerné comme suit :

Basculement du mode Accès en mode Liaison

La configuration VLAN reste la même. Le VLAN du port en mode Accès devient le VLAN natif pour le port en mode Liaison. Le port doit répondre aux exigences des ports en mode Liaison.

Basculement du mode Liaison en mode Accès

Si le port d'origine en mode Liaison a un membre VLAN non balisé sur le port, il est supprimé de tous ses VLAN sauf du VLAN non balisé configuré sur le port. Le PVID est défini sur l'ID de VLAN non balisé.

Si le port d'origine en mode Liaison n'a aucun membre VLAN non balisé sur le port, il est supprimé de tous ses VLAN et devient membre du VLAN défini par défaut. Son PVID est défini sur l'ID de VLAN par défaut. Le port n'accepte désormais que des paquets non balisés ou ceux contenant des balises de priorité. Il est non balisé sur le VLAN configuré par défaut.

Basculement du mode Accès en mode Général

La configuration VLAN reste la même, excepté que le port peut désormais accepter toutes les trames. En mode Général, un port peut être membre balisé ou non balisé d'un VLAN.

Basculement du mode Général en mode Accès

Si le port d'origine en mode Général a un membre VLAN non balisé sur le port, il est supprimé de tous ses VLAN sauf du VLAN dont le port est membre non balisé. Le port est alors configuré en tant que membre non balisé de ce VLAN.

Si le port d'origine en mode Général n'a aucun membre VLAN non balisé sur le port, il est supprimé de tous ses VLAN et devient membre du VLAN défini par défaut. Son PVID est défini sur l'ID de VLAN par défaut. Le port n'accepte désormais que des paquets non balisés ou ceux contenant des balises de priorité. Il est non balisé sur le VLAN configuré par défaut.

Basculement du mode Liaison en mode Général

La configuration VLAN reste la même. En mode Général, un port peut être membre balisé ou non balisé d'un VLAN.

Basculement du mode Général en mode Liaison

La configuration VLAN reste la même. Le PVID du port en mode Général permet de configurer le VLAN natif du port en mode Liaison. Ce port doit répondre aux exigences du port en mode Liaison.

Supposons par exemple qu'un port en mode Général est un membre non balisé des VLAN 1, 10 et 20 et que le PVID du port est 1.

Lorsque le port est mis en mode Liaison, le VLAN 1 devient le VLAN natif. Le port en mode Liaison est toujours membre des VLAN 10 et 20, et le tagging est désormais activé.

Suppression d'un VLAN

La suppression d'un VLAN entraîne les actions suivantes :

- Si le VLAN supprimé était un VLAN natif du port en mode Liaison, le VLAN natif et le PVID sont définis sur le VLAN par défaut.
- Si un port en mode Accès était membre du VLAN supprimé, il devient membre du VLAN défini par défaut et son PVID est configuré sur l'ID de VLAN par défaut.
- Si un port en mode Général utilisait l'ID de VLAN en tant que son PVID, le PVID de ce port est défini sur l'ID de VLAN par défaut. Aucune autre appartenance VLAN n'est modifiée.

Configuration d'une appartenance VLAN

Ces pages permettent d'afficher et de configurer des appartenances VLAN :

- Sur la page *Port vers VLAN*, sélectionnez un VLAN, puis configurez ses ports membres. Reportez-vous à [Configuration de ports vers un VLAN](#).
- Sur la page *Appartenance VLAN des ports*, sélectionnez un port, puis configurez-le en tant que membre d'un ou plusieurs VLAN. Reportez-vous à [Configuration d'une appartenance VLAN des ports](#).

Par défaut, tous les ports sont membres du VLAN 1. Vous pouvez modifier l'appartenance VLAN de tous les ports. Les appartenances VLAN peuvent être définies en tant que balisées ou non balisées.

- Si le commutateur reçoit une trame non balisée d'un VLAN, il insère une balise VLAN avant de réacheminer cette trame vers les ports de sortie configurés en tant que membres balisés du VLAN.

- Si le commutateur reçoit une trame non balisée d'un VLAN, il réachemine cette trame telle quelle vers les ports de sortie configurés en tant que membres non balisés du VLAN.
- Si le commutateur reçoit une trame balisée d'un VLAN, il supprime la balise VLAN avant de réacheminer cette trame vers les ports de sortie configurés en tant que membres non balisés du VLAN.
- Si le commutateur reçoit une trame balisée d'un VLAN, il réachemine cette trame telle quelle vers les ports de sortie configurés en tant que membres balisés du VLAN.

Configuration de ports vers un VLAN

La page *Port vers VLAN* permet d'attribuer des ports aux VLAN.

ÉTAPE 1 Cliquez sur **Gestion des VLAN > Port vers VLAN** dans la fenêtre de navigation.

Pour le PVID, le port ou le LAG sélectionné, cette page affiche la configuration d'administration du mode de port d'interface (Accès, Liaison et Général), l'appartenance, la fonction de tagging et le PVID de tous les ports membres du VLAN. Pour plus d'informations sur la configuration de ce paramètre, consultez la rubrique **Configuration des paramètres d'interface VLAN**.

ÉTAPE 2 Sélectionnez l'ID de VLAN que vous souhaitez configurer et utilisez la liste Type d'interface pour afficher les ports ou les LAG.

ÉTAPE 3 Pour chaque interface, configurez les paramètres suivants :

- **Membre** : cochez cette case si le port doit être membre du VLAN. Le cas échéant, décochez cette case. Par défaut, le port n'est pas membre du VLAN.
- **Balisés** : cochez cette case si tous les paquets du VLAN envoyés vers le port doivent être balisés. Le cas échéant, cochez la case Non balisés. Les ports en mode Liaison sont balisés par défaut. Cette option est uniquement pertinente, si le port est membre du VLAN.
- **Non balisés** : cochez cette case si tous les paquets du VLAN envoyés vers le port doivent être non balisés. Le cas échéant, cochez la case Balisés. Les ports en mode Accès sont toujours non balisés. Les ports en mode Général sont non balisés par défaut. Cette option est uniquement pertinente, si le port est membre du VLAN.

- **PVID** : cochez cette case si l'ID de VLAN sélectionné pour le port doit être utilisé en tant que son PVID (ID de VLAN du port). Le cas échéant, décochez cette case. Si cette case est cochée pour un port en mode Accès ou Liaison, ce port doit être membre non balisé du VLAN. Les paquets non balisés provenant du port sont attribués au VLAN correspondant.

ÉTAPE 4 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration d'une appartenance VLAN des ports

Pour configurer les paramètres VLAN des ports :

ÉTAPE 1 Cliquez sur **Gestion des VLAN > Appartenance VLAN des ports** dans la fenêtre de navigation.

Cette page affiche par défaut des informations sur le VLAN de tous les ports. Utilisez les paramètres de filtre pour afficher ces informations pour les ports LAG. Cette page affiche le mode VLAN d'interface (Liaison ou Accès), le PVID et les appartenances VLAN. Si un port est membre de plusieurs VLAN, sélectionnez-le, puis cliquez sur **Détails** pour afficher ces informations pour un seul port.

ÉTAPE 2 Sélectionnez le port ou le LAG que vous souhaitez configurer, puis cliquez sur **Modifier**.

ÉTAPE 3 Pour attribuer ou supprimer une appartenance VLAN, utilisez les flèches comme décrit ci-après.

- Pour ajouter une appartenance VLAN : cliquez sur un VLAN de la liste Disponibles, modifiez ses propriétés de tagging si nécessaire (voir ci-après), puis cliquez sur la flèche de droite pour le déplacer vers la liste Sélectionnés.
- Pour supprimer une appartenance VLAN : cliquez sur un VLAN dans la liste Sélectionnés, puis sur la flèche de gauche pour le déplacer vers la liste Disponibles.

Propriétés de PVID et de balisage

En fonction du mode VLAN sélectionné (Liaison, Accès ou Général), lorsque vous sélectionnez un VLAN dans la liste Disponibles, vous pouvez définir les propriétés suivantes pour l'interface, avant de déplacer ce VLAN vers la liste Sélectionnés.

- **Appartenance** : configurez l'interface en tant que membre balisé ou non balisé du VLAN sélectionné.

- **Balisé** : lorsque cette case est cochée, le port est un membre balisé du VLAN sélectionné. Lorsque le commutateur réachemine des paquets qu'il reçoit pour ce VLAN via l'interface, il leur ajoute un ID de VLAN.
- **Non balisé** : lorsque cette case est cochée, le port est un membre non balisé du VLAN sélectionné. Lorsque le commutateur réachemine des paquets qu'il reçoit pour ce VLAN via l'interface, il ne leur ajoute aucun ID de VLAN.

Si vous sélectionnez le mode VLAN d'interface Général, vous pouvez sélectionner l'option de votre choix pour les VLAN. Si vous configurez le mode Accès, vous ne pouvez sélectionner qu'un seul VLAN. Vous devez également cocher la case Non balisé. Si vous sélectionnez le mode Liaison, vous pouvez configurer l'interface en tant que membre non balisé d'un VLAN et en tant que membre balisé pour d'autres VLAN.

- **PVID** : lorsque cette case est cochée, le port utilise l'ID de VLAN sélectionné en tant que son PVID (ID de VLAN du port). Le port attribue le PVID à toutes les trames non balisées reçues avant de les réacheminer. Les règles de configuration suivantes s'appliquent :
 - Si vous configurez le mode VLAN Général, vous pouvez sélectionner tous les VLAN dont l'interface est membre balisé ou non balisé pour définir le PVID.
 - Si vous sélectionnez le mode VLAN Liaison, le PVID est défini sur l'ID de VLAN dont le port est membre balisé.
 - Si vous sélectionnez le mode VLAN Accès, le PVID est défini sur l'ID de VLAN d'accès et vous ne pourrez plus modifier le contenu de ce champ.

Lorsque vous cochez les cases Non balisé, Balisé et PVID et déplacez le VLAN vers la liste Sélectionnés, les lettres N, B et P sont ajoutées à l'ID de VLAN.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Définition du VLAN par défaut

Par défaut, le commutateur définit automatiquement le VLAN 1 en tant que VLAN par défaut pour tous les ports et LAG. Si le port n'a aucune appartenance VLAN, le commutateur le configure automatiquement en tant que membre du VLAN par défaut.

La page *Paramètres VLAN par défaut* permet de modifier le VLAN configuré par défaut.

Lorsque l'ID du VLAN par défaut est modifié :

- Les ports qui sont membres du VLAN d'origine par défaut sont supprimés en tant que membres de ce VLAN et définis en tant que membres du nouveau VLAN par défaut.
- Le PVID des ports membres du VLAN d'origine par défaut est remplacé par l'ID de VLAN du nouveau VLAN par défaut.
- Si le VLAN de gestion était le même que le VLAN par défaut d'origine, il est mis à jour vers le nouveau VLAN par défaut.
- Le type du VLAN d'origine par défaut est mis en mode Statique et peut désormais être supprimé. La seule exception est le VLAN 1. Même s'il n'est plus défini en tant que VLAN par défaut, il ne peut pas être supprimé.

Pour sélectionner un VLAN par défaut :

-
- ÉTAPE 1** Cliquez sur **Gestion des VLAN > Paramètres VLAN par défaut** dans la fenêtre de navigation.
- ÉTAPE 2** Sélectionnez le VLAN dans la liste.
- ÉTAPE 3** Cliquez sur **Appliquer**.
-

Trafic vocal et multimédia

Le protocole VoIP (Voice-over-Internet-Protocol) permet d'accéder à un réseau de données facilitant les appels téléphoniques vocaux. En raison du déploiement croissant d'applications coûteuses en temps, telles que les VoIP déployés au sein des réseaux modernes, une configuration QoS appropriée est nécessaire pour améliorer la qualité des performances. La fonctionnalité Trafic vocal et multimédia fournit un mécanisme de classification simplifiée des paquets vocaux qui les définit comme prioritaires par rapport aux paquets de données.

Cette fonctionnalité identifie les flux VoIP sur les commutateurs Ethernet et leur offre une meilleure classe de service (Class-of-Service, CoS) qu'au trafic normal. Le commutateur prend en charge deux fonctions vocales et multimédia :

- **Basé sur le protocole** : identifie une session VoIP à l'aide du protocole d'initiation de session (Session Initiation Protocol, SIP) et le trafic de contrôle H.323, et attribue ensuite à ces paquets la priorité la plus élevée sur le VLAN vocal.
- **Basé sur OUI** : les ports pour lesquels cette option est activée automatiquement, deviennent membres du VLAN vocal configuré. Le commutateur détecte les valeurs OUI (Organizationally Unique Identifier) dans les trois premiers octets des adresses MAC des paquets clients pour les classer sur le VLAN VoIP et définir leur priorité sur les ports prenant en charge le VoIP automatique.

Pour plus d'informations sur les pages de configuration disponibles dans le menu Gestion des VLAN > Trafic vocal et multimédia, consultez les rubriques suivantes :

- [Affichage et ajout des OUI de téléphonie](#)
- [Configuration de la fonctionnalité Trafic vocal et multimédia basé sur OUI](#)
- [Configuration de la fonctionnalité Trafic vocal et multimédia basé sur les protocoles SIP/H323](#)

Affichage et ajout des OUI de téléphonie

La page *OUI de téléphonie* répertorie les OUI (Organizationally Unique Identifiers) associés aux différents VLAN vocaux.

Pour accéder à cette page, cliquez sur **Gestion des VLAN > VOIP automatique > OUI de téléphonie** dans la fenêtre de navigation.

La table des OUI de téléphonie contient des identifiants des appareils de téléphonie fréquemment utilisés. L'administrateur peut ajouter ou supprimer les OUI. Lorsque la fonctionnalité Trafic vocal et multimédia est activée, les ports utilisent les chiffres OUI des adresses MAC de destination et/ou sources figurant dans les paquets entrants afin d'attribuer automatiquement le trafic vocal à un VLAN vocal. Pour plus d'informations sur l'attribution d'une priorité IEEE 802.1p au VLAN et sur l'activation de la fonctionnalité Trafic vocal et multimédia pour les ports, consultez la rubrique **Configuration de la fonctionnalité Trafic vocal et multimédia basé sur OUI**.

Pour ajouter une nouvelle description OUI :

ÉTAPE 1 Cliquez sur **Ajouter**.

ÉTAPE 2 Configurez les champs suivants :

- **OUI de téléphonie** : saisissez un identifiant de 3 octets pour l'application de téléphonie.
- **Description** : saisissez une description du service telle que le nom du fournisseur ou le produit de téléphonie.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**.

Configuration de la fonctionnalité Trafic vocal et multimédia basé sur OUI

La page VoIP automatique basé sur OUI de téléphonie permet d'effectuer les actions suivantes :

- Configurer un niveau de priorité IEEE 802.1p pour le trafic vocal et multimédia identifié à l'aide des chiffres OUI des adresses MAC.
- Définir le VLAN pour les paquets VoIP basés sur OUI. Même si vous pouvez attribuer des ID de VLAN qui n'ont pas encore été créés sur le commutateur, vous devez ensuite créer le VLAN afin que la fonctionnalité puisse être activée (voir la rubrique **Création d'un VLAN**).
- Activez les ports pour l'exécution de cette fonctionnalité. Lorsque cette fonctionnalité est activée sur un port, ce dernier devient automatiquement membre du VLAN vocal configuré. Ainsi, l'administrateur n'a pas besoin d'ajouter ce port manuellement en tant que membre du VLAN.

Pour configurer la fonctionnalité Trafic vocal et multimédia basé sur OUI :

- ÉTAPE 1** Cliquez sur **Gestion des VLAN > Trafic vocal et multimédia > Basé sur OUI** dans la fenêtre de navigation.
- ÉTAPE 2** Cochez la case VLAN pour pouvoir modifier le contenu des champs ID de VLAN et Priorité.
- ÉTAPE 3** Dans le champ ID de VLAN, indiquez le VLAN pour l'acheminement du trafic vocal. Ce VLAN doit déjà être configuré sur le commutateur (voir la rubrique [Création d'un VLAN](#)).
- ÉTAPE 4** Dans le champ Priorité, saisissez le niveau de priorité CoS IEEE 802.1p pour le trafic VoIP.
- ÉTAPE 5** Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.
- ÉTAPE 6** Dans la table des paramètres d'interface basée sur OUI de téléphonie, sélectionnez l'interface que vous souhaitez configurer, puis cliquez sur **Modifier**.
- ÉTAPE 7** Cochez la case Activer en regard de l'option Mode VoIP automatique. Le port est automatiquement ajouté en tant que membre du VLAN vocal.
- ÉTAPE 8** Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration de la fonctionnalité Trafic vocal et multimédia basé sur les protocoles SIP/H323

La page *VoIP automatique SIP/H323* permet de configurer le commutateur afin qu'il identifie le trafic VoIP à l'aide de son protocole, tel que le protocole d'initiation de session (SIP) et le protocole H.323. La priorité du trafic est automatiquement définie en fonction de la classe du trafic VoIP configuré sur les ports.

Pour configurer la fonctionnalité Trafic vocal et multimédia basé sur les protocoles SIP/H323 :

- ÉTAPE 1** Cliquez sur **Gestion des VLAN > Trafic vocal et multimédia > VoIP automatique SIP/H323** dans la fenêtre de navigation.
- ÉTAPE 2** Le menu Type d'interface affiche les ports ou les LAG dans la table des paramètres d'interface basée sur le protocole.

-
- ÉTAPE 3** Sélectionnez l'interface (le port ou le LAG) que vous souhaitez configurer, puis cliquez sur **Modifier**.
- ÉTAPE 4** Cochez la case Activer en regard de l'option Mode VoIP automatique.
- ÉTAPE 5** Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.
-

VLAN multimédia

La fonctionnalité VLAN multimédia permet aux ports du commutateur d'acheminer le trafic vocal, vidéo et de signalisation en fonction de leur valeur de priorité attribuée. L'attribution des différentes priorités permet de séparer le trafic multimédia du trafic de données sur le port d'entrée. La fonctionnalité VLAN multimédia permet de prévenir toute détérioration de la qualité vidéo ou audio d'un dispositif vidéo ou d'un téléphone IP lorsque le trafic de données sur le port est élevé.

L'isolation du trafic assurée par les VLAN gère le trafic inter-VLAN et empêche aux clients connectés au réseau de lancer une attaque directe sur les composants vocaux. Le commutateur utilise la valeur IP-DSCP ou 802.1p dans les paquets provenant des périphériques multimédia et attribue ainsi ce trafic aux files d'attente de priorité élevée.

Grâce aux VLAN multimédia, le commutateur prend en charge les applications LLDP-MED. Pour plus d'informations sur ce protocole, consultez la rubrique **LLDP-MED**. Chaque VLAN multimédia correspond à une application LLDP-MED pour un type précis de trafic multimédia. Les applications LLDP-MED comprennent les paramètres suivants : la voix, la signalisation vocale, la voix d'invité, la signalisation de voix d'invité, la voix de téléphone logiciel, la vidéoconférence, la lecture vidéo en continu et la signalisation vidéo. Les VLAN multimédia comprennent les paramètres suivants :

- un VLAN avec le tagging de VLAN facultatif ;
- une valeur de priorité IEEE 802.1p ;
- une valeur DSCP.

Lorsqu'une stratégie réseau est associée au port prenant en charge le protocole LLDP-MED, le commutateur indique ses VLAN multimédia dans les TLV de stratégie réseau LLDP-MED en dehors du port. Lorsque le commutateur détecte une extrémité multimédia LLDP, il installe le VLAN multimédia sur le port correspondant. Les pages Administration, Détection - LLDP, permettent d'activer le protocole LLDP-MED et des stratégies réseau.

Vous pouvez activer ou désactiver cette fonctionnalité au niveau global du commutateur. Chaque application et son VLAN multimédia sont configurables au niveau du port. Par exemple, l'option Voix d'invité peut se trouver sur le VLAN multimédia 1 de l'interface g1, mais aussi sur le VLAN multimédia 10 de l'interface g2.

La table des paramètres des VLAN multimédia affiche tous les types de trafic multimédia disponibles, ainsi que leur état et leurs paramètres définis sur le port sélectionné.

Pour configurer les applications VLAN multimédia :

ÉTAPE 1 Cliquez sur **Gestion des VLAN > Trafic vocal et multimédia > VLAN multimédia** dans la fenêtre de navigation.

ÉTAPE 2 Cochez la case Activer en regard de l'option Mode d'administration pour activer cette fonctionnalité globalement sur le commutateur, puis cliquez sur **Appliquer**.

ÉTAPE 3 Dans la liste Interface, sélectionnez l'interface que vous souhaitez configurer.



ATTENTION Vous ne pouvez pas activer les ports qui sont membres d'un LAG pour les applications VLAN multimédia (voir la rubrique [Configuration des LAG](#)).

ÉTAPE 4 Cliquez sur **Modifier**.

ÉTAPE 5 Dans la liste Application, sélectionnez le type de trafic multimédia que vous souhaitez configurer :

- Voix
- Signalisation vocale
- Voix d'invité
- Signalisation de voix d'invité
- Voix de téléphone logiciel

- Vidéoconférence
- Lecture vidéo en continu
- Signalisation vidéo

ÉTAPE 6 En regard de l'option État d'application, cochez la case Activer pour attribuer un niveau de priorité à l'application sélectionnée. Pour désactiver cette fonctionnalité, décochez cette case.

ÉTAPE 7 Lorsque vous activez l'option État d'application, vous devez activer ou désactiver les fonctionnalités suivantes :

- **Non balisés** : cochez la case Activer si le périphérique multimédia (extrémité LLDP-MED) doit envoyer des paquets non balisés. La TLV de stratégie réseau du commutateur doit également préciser cette condition. Vous devez autoriser l'utilisation des trames non balisées sur le périphérique multimédia. Pour désactiver cette fonctionnalité, décochez cette case.
- **VLAN et ID de VLAN** : cochez la case Activer pour définir un VLAN, puis sélectionnez un ID de VLAN dans la liste. Pour désactiver cette fonctionnalité, décochez cette case.
- **Priorité et Valeur de priorité** : cochez la case Activer pour définir la priorité des paquets de l'application sélectionnée. Saisissez ensuite une valeur de tagging de priorité CoS IEEE 802.1p pour le trafic VLAN multimédia. La plage des balises de priorité est comprise entre 0 et 7.
- **DSCP et Valeur DSCP** : cochez la case Activer pour définir un point DSCP pour l'application sélectionnée. Saisissez ensuite une valeur DSCP du port. La plage valide est comprise entre 0 et 63.

ÉTAPE 8 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

ÉTAPE 9 Assurez-vous que le protocole LLDP-MED est activé sur l'interface sélectionnée. Pour plus d'informations, consultez la rubrique **LLDP-MED**.

Sessions VoIP automatique

La page *Sessions VoIP automatique* affiche les informations sur la source, la destination et le protocole de toutes les sessions VoIP (Voice over IP).

Arbre recouvrant

Ce chapitre décrit les étapes de configuration du protocole d'arbre recouvrant (Spanning Tree Protocol, STP) sur le commutateur.

Il contient les rubriques suivantes :

- **Description du protocole d'arbre recouvrant**
- **Configuration de l'état et des paramètres globaux du protocole d'arbre recouvrant**
- **Configuration des paramètres d'interface STP**
- **Paramètres d'interface RSTP**

Description du protocole d'arbre recouvrant

Ce protocole optimise les communications sur des réseaux comprenant plusieurs ponts. Les dispositifs connectés à ces réseaux peuvent apprendre plusieurs chemins vers la même extrémité, ce qui crée une redondance. Cette redondance permet notamment de maintenir le flux de trafic lorsque certaines liaisons sont interrompues. Toutefois, elle peut générer des boucles de commutation qui réduisent les performances du réseau et perturbent les algorithmes de réacheminement.

Chaque pont prenant en charge le protocole d'arbre recouvrant échange des unités BPDU (Bridge Protocol Data Units) avec d'autres ponts. Ces unités identifient les adresses MAC des ports, ainsi que la priorité et le coût associé à chaque port. Le protocole d'arbre recouvrant utilise ensuite ces informations pour générer une topologie qui établit un chemin actif entre deux stations quelconques du réseau. Les chemins dupliqués entre ces stations sont mis en état d'attente et sont utilisés uniquement lorsque le chemin actif n'est plus disponible.

Par ailleurs, les échanges des unités BPDU facilitent la sélection d'un pont racine et d'un port racine du réseau. Le pont racine représente un point de référence que les autres ponts utilisent pour déterminer le chemin au coût le plus bas en additionnant le coût des ports de chaque chemin et en sélectionnant celui dont le total est le plus bas. Le port qui relie un pont au chemin au coût le plus bas est appelé *port racine*.

Lorsque le pont racine est sélectionné et que tous les ports racines sont configurés, les segments du réseau déterminent le pont qui fournit le chemin au coût le plus bas vers le port racine. Le port qui fournit ce chemin est appelé *port désigné*. Le protocole d'arbre recouvrant désactive les autres ports de ce segment de réseau ou les spécifie en tant que ports secondaires ou de sauvegarde.

Le commutateur prend en charge d'autres versions du protocole d'arbre recouvrant, telles que le protocole d'arbre recouvrant commun (Common Spanning Tree, CST) le protocole d'arbre recouvrant rapide (Rapid Spanning Tree Protocol, RSTP).

- Le protocole d'arbre recouvrant commun (IEEE 802.1D) est la version d'origine qui fournit un seul chemin entre les stations, sans créer de boucles de commutation.
- Le protocole d'arbre recouvrant rapide (IEEE 802.1w) comprend des améliorations qui permettent aux réseaux de créer rapidement une topologie d'arbre recouvrant optimale.

Configuration de l'état et des paramètres globaux du protocole d'arbre recouvrant

La page *État et paramètres globaux STP* permet d'activer le protocole d'arbre, de sélectionner son mode de fonctionnement et de configurer les paramètres de priorité des ponts. Vous pouvez également afficher les informations relatives à l'état de la topologie d'arbre recouvrant. Pour accéder à cette page, cliquez sur **Arbre recouvrant > État et paramètres globaux STP** dans la fenêtre de navigation.

Sur cette page, vous pouvez configurer les paramètres globaux et les paramètres des ponts, ainsi qu'afficher les informations sur les racines désignées.

Configuration des paramètres globaux et des ponts

Pour configurer les paramètres globaux du protocole d'arbre recouvrant et les paramètres des ponts :

ÉTAPE 1 Définissez les paramètres globaux suivants :

- **État d'arbre recouvrant** : sélectionnez cette option pour activer le protocole d'arbre recouvrant sur le commutateur. Vous devez également activer ce protocole pour chaque port individuel (voir la rubrique **Configuration des paramètres d'interface STP**).
- **Mode de fonctionnement d'arbre recouvrant** : sélectionnez le mode d'arbre recouvrant classique ou d'arbre recouvrant rapide. Le protocole d'arbre recouvrant rapide représente une version évoluée du protocole d'arbre recouvrant (norme 802.1D) et fournit une convergence de l'arbre recouvrant plus rapide suite aux modifications apportées à la topologie.
- **Gestion BPDU** : les unités BPDU sont des messages échangés entre les commutateurs permettant de déterminer la topologie d'arbre recouvrant. Sélectionnez la méthode de gestion des paquets BPDU lorsque le protocole d'arbre recouvrant est désactivé sur une interface :
 - **Filtrage** : le port ignore les paquets BPDU reçus lorsque le protocole d'arbre recouvrant est désactivé sur les interfaces.
 - **Inondation** : inonde les paquets BPDU (qui ont été reçus sur les ports sans protocole d'arbre recouvrant) sur tous les autres ports sans protocole d'arbre recouvrant.

ÉTAPE 2 Définissez le paramètre de pont suivant :

- **Priorité** : définit la valeur de priorité du pont. Lorsque des commutateurs ou des ponts exécutent le protocole d'arbre recouvrant, ils se voient attribuer un niveau de priorité. Après l'échange des unités BPDU, le commutateur portant la priorité la moins élevée devient le pont racine. La valeur de priorité du pont doit être un multiple de 4096. Si vous spécifiez toute autre valeur, la priorité du pont est automatiquement définie sur le plus petit multiple de 4096. Par exemple, si vous essayez de définir la priorité sur une valeur comprise entre 0 et 4095, elle sera définie sur 0. La valeur de priorité par défaut est 32768. La plage valide est comprise entre 0 et 61440.

La section de cette page affiche les informations suivantes :

- **Hello Time** : indique l'intervalle auquel un pont envoie des messages de configuration.

- **Délai d'attente maximal** : indique le délai d'attente (en secondes) d'un pont avant l'implémentation d'un changement de topologie.
- **Sauts max.** : indique le nombre maximal de sauts avant qu'une unité BPDU soit ignorée et les informations du port expirent. Ce nombre limite est défini sur 20 et ne peut être modifié.
- **Délai avant réacheminement** : indique la durée (en secondes) pendant laquelle un pont est à l'état d'écoute et d'apprentissage avant le réacheminement de paquets.
- **Délai d'attente** : indique le délai maximal (en secondes) qui s'écoule avant le réacheminement des unités BPDU de configuration via un port du pont.

La section Racine désignée affiche les informations suivantes :

- **ID de pont** : affiche l'identifiant du pont qui est une concaténation de la priorité et de l'adresse MAC de base du pont.
- **ID de pont racine** : affiche l'identifiant du pont racine. Le pont dont l'identifiant porte la priorité la moins élevée devient le pont racine.
- **Port racine** : indique le numéro de port proposant le chemin au coût le plus faible entre ce pont et le pont racine. Cet aspect est d'autant plus important, car il ne s'agit pas du pont racine. La valeur par défaut est zéro.
- **Coût du chemin racine** : affiche le coût d'acheminement entre ce pont et le pont racine.
- **Nombre de changements de topologie** : affiche le nombre total des changements de topologie d'arbre recouvrant effectués.
- **Dernier changement de topologie** : indique le délai écoulé depuis le dernier changement de topologie.

ÉTAPE 3 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration des paramètres d'interface STP

La page *Paramètres d'interface STP* attribue des propriétés d'arbre recouvrant à chaque port ou LAG. Ces paramètres s'appliquent quel que soit le mode défini (protocole d'arbre recouvrant classique ou rapide).

Pour modifier les paramètres d'un port ou LAG :

ÉTAPE 1 Cliquez sur **Arbre recouvrant** > **Paramètres d'interface STP** dans la fenêtre de navigation.

La table des paramètres d'interface STP affiche les informations sur la configuration de chaque port et LAG. Le protocole d'arbre recouvrant est activé par défaut sur tous les ports.

REMARQUE : La liste des ports ou des LAG peut s'étendre sur plusieurs pages. Utilisez la liste des pages pour afficher les entrées suivantes.

ÉTAPE 2 Sélectionnez le port ou le LAG que vous souhaitez configurer, puis cliquez sur **Modifier**.

ÉTAPE 3 Configurez les paramètres suivants :

- **Protocole d'arbre recouvrant** : sélectionnez cette option pour activer le protocole d'arbre recouvrant sur le port ou le LAG.
- **Détection aut. de port secondaire** : cochez la case Activer afin que le commutateur puisse déterminer automatiquement s'il s'agit d'un port secondaire. Un port est appelé port secondaire lorsqu'il n'est relié à aucun pont. La détection automatique accélère la transition du port vers l'état de réacheminement. Lorsque les ports sont mis en état de réacheminement, ils peuvent transférer le trafic et apprendre des adresses MAC.
- **Port secondaire** : cochez la case Activer pour configurer manuellement le port en tant que port secondaire.
- **Gestion BPDU** : les unités BPDU sont des messages échangés entre les commutateurs permettant de déterminer la topologie d'arbre recouvrant. Sélectionnez la méthode de gestion des paquets BPDU lorsque le protocole d'arbre recouvrant est désactivé sur une interface :
 - **Filtrage** : le port ignore les paquets BPDU reçus lorsque le protocole d'arbre recouvrant est désactivé sur les interfaces.

- **Inondation** : inonde les paquets BPDU (qui ont été reçus sur les ports sans protocole d'arbre recouvrant) sur tous les autres ports sans protocole d'arbre recouvrant.
- **Coût du chemin** : indiquez le coût d'acheminement vers un port. Ce coût représente la contribution du port au coût d'acheminement vers le pont racine. Le coût d'acheminement permet de réacheminer le trafic lorsqu'un chemin est redirigé. Cochez la case Valeur par défaut pour définir le coût d'acheminement en fonction de la vitesse du port, ou Personnalisé pour définir une valeur personnalisée comprise entre 0 et 200 000 000. La valeur nulle signifie que le coût d'acheminement est défini en fonction de la vitesse du port.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

La table des interfaces STP affiche désormais la nouvelle configuration, ainsi que les informations suivantes sur le port ou le LAG.

- **État opérationnel secondaire** : précise si le port en fonctionnement est un port secondaire. Ce champ indique la valeur Activé lorsque le port est mis en état de réacheminement selon l'une des configurations suivantes :
 - Le port est configuré en tant que port secondaire et par conséquent, est mis automatiquement en état de réacheminement.
 - Le port est configuré automatiquement en tant que port secondaire et, étant donné qu'il n'a reçu aucune unité BPDU, a est mis en état de réacheminement.
- **État du port** : affiche l'état d'arbre recouvrant actuel d'un port. S'il est activé, l'état du port détermine l'action de réacheminement de trafic. Ce champ peut prendre les valeurs suivantes :
 - **Désactivé** : le protocole d'arbre recouvrant est actuellement désactivé sur le port. Par conséquent, le port ne participe pas à l'arbre recouvrant, mais est en état opérationnel pour l'apprentissage des adresses MAC et le réacheminement du trafic.
 - **Blocage** : le port est actuellement bloqué et ne peut ni réacheminer de trafic, ni apprendre d'adresses MAC.
 - **Écoute** : le port est actuellement en mode d'écoute. Il ne peut ni réacheminer de trafic, ni apprendre d'adresses MAC.

- **Apprentissage** : le port est actuellement en mode d'apprentissage. Il ne peut pas réacheminer de trafic, mais il peut apprendre de nouvelles adresses MAC.
- **Réacheminement** : le port est actuellement en mode de réacheminement. Il peut réacheminer du trafic et apprendre de nouvelles adresses MAC.
- **ID de pont désigné** : affiche l'identifiant du pont qui propose le coût d'acheminement racine le plus faible vers un réseau local. Cet identifiant est une concaténation de la priorité et de l'adresse MAC de base du pont.
- **ID de port désigné** : affiche l'identifiant de port pour le pont désigné qui propose le coût d'acheminement racine le plus faible vers un réseau local. Cet identifiant est une concaténation de la priorité et du numéro d'interface du port.
- **Coût désigné** : indique le coût d'acheminement racine entre le pont désigné et le pont racine. Les ports présentant des coûts inférieurs sont peu susceptibles d'être bloqués lorsque le protocole d'arbre recouvrant détecte des boucles.
- **Vitesse** : indique la vitesse du port.
- **LAG** : affiche le LAG dont le port est membre (si disponible).

Paramètres d'interface RSTP

Le protocole d'arbre recouvrant rapide (Rapid Spanning Tree Protocol, RSTP) assure une convergence plus rapide de l'arbre recouvrant sans création de boucles pour tout réseau local relié par un pont. Pour accéder à la page *Paramètres d'interface RSTP*, cliquez sur **Arbre recouvrant** > **Paramètres d'interface RSTP** dans la fenêtre de navigation.

Une topologie arbre recouvrant rapide est créée automatiquement lorsqu'un protocole arbre recouvrant rapide est sélectionné en tant que mode d'arbre recouvrant. La page *État et paramètres globaux STP* permet d'activer le mode d'arbre recouvrant rapide.

La table des paramètres d'interface RSTP affiche par défaut les informations sur chaque port. La liste Type d'interface affiche les ports ou les LAG sous forme d'une table. La table d'interface RSTP affiche les informations suivantes sur chaque port :

- **État opérationnel point à point** : un port physique est connecté point à point à un réseau local lorsqu'il fonctionne en duplex intégral.
- **Rôle de port** : indique le rôle de port attribué par l'algorithme d'arbre recouvrant aux chemins d'arbre recouvrant. Ce champ peut prendre les valeurs suivantes :
 - **Racine** : fournit le coût d'acheminement racine le plus bas vers le pont racine parmi tous les ports du commutateur.
 - **Désigné** : fournit le coût d'acheminement racine le plus bas vers le pont racine à partir d'un réseau local. Le commutateur est le pont désigné du réseau local.
 - **Secondaire** : indique un autre chemin vers le pont racine à partir de l'interface racine.
 - **Sauvegarde** : fournit un chemin de sauvegarde pour le chemin de port désigné vers les nœuds terminaux d'arbre recouvrant. Les ports de sauvegarde sont activés uniquement lorsque deux ports sont connectés en boucle via une liaison point à point, ou lorsqu'un réseau local dispose d'au moins deux connexions vers un segment partagé.
 - **Désactivé** : le port ne participe pas à l'arbre recouvrant.
- **Mode** : indique si le mode d'administration d'arbre recouvrant rapide est activé ou désactivé sur le port.
- **État de fonctionnement du port secondaire** : si vous activez cette option sur un port ou un LAG, le port (ou le LAG) est mis en état de réacheminement. Pour plus d'informations sur la modification de ce paramètre, consultez la rubrique **Configuration des paramètres d'interface STP**.
- **État du port** : affiche l'état de fonctionnement du port.

Sélectionnez un port, puis cliquez sur **Activer la migration des protocoles** afin que le commutateur envoie les unités BPDU RSTP au port sélectionné. Cette action permet de vérifier si tous les ponts hérités du réseau local ont été supprimés.

Tables d'adresses MAC

Ce chapitre décrit la configuration statique et l'apprentissage dynamique des adresses MAC (Media Access Control, contrôle d'accès au support) dans la base de données de filtrage du commutateur. Le commutateur consulte sa base de données de filtrage pour déterminer sur quel port un paquet doit être transmis. Dans le présent document, la base de données de filtrage est également appelée table des ponts. La recherche est basée sur le VLAN et l'adresse MAC de destination du paquet. Si la recherche ne renvoie aucune entrée correspondante, le commutateur transmet les paquets au VLAN en inondant les ports, à l'exception du port d'entrée.

Il contient les rubriques suivantes :

- **Configuration d'adresses MAC statiques**
- **Configuration du délai d'expiration des adresses dynamiques**
- **Adresses MAC dynamiques**

Configuration d'adresses MAC statiques

La page *Adresses statiques* affiche une liste d'adresses MAC qui sont configurées manuellement dans la table des ponts du commutateur. Une adresse MAC statique est également associée à un VLAN ainsi qu'à un port.

Pour ajouter des entrées d'adresses MAC statiques :

-
- ÉTAPE 1** Cliquez sur **Tables d'adresses MAC > Adresses statiques** dans la fenêtre de navigation.
- ÉTAPE 2** Cliquez sur **Ajouter**.

ÉTAPE 3 Configurez les paramètres suivants :

- **ID VLAN** : sélectionnez le VLAN dans lequel réside l'appareil doté de l'adresse MAC statique.
- **Interface** : spécifiez le port/LAG sur lequel l'appareil doté des adresses MAC statiques peut être joint.
- **Adresse MAC** : saisissez l'adresse MAC statique.
- **État** : sélectionnez un état pour cette adresse MAC statique :
 - **Permanent** : lorsque cet état est sélectionné, l'adresse MAC statique n'expire pas. Veuillez toutefois noter qu'en cas de redémarrage du commutateur, l'entrée n'est restaurée que si le type de fichier de Configuration d'exécution a été copié dans le type de fichier de Configuration de démarrage. Reportez-vous à [Copie et enregistrement des fichiers de configuration](#).
 - **Sécurisé** : lorsque cet état est sélectionné, l'adresse MAC est sécurisée et utilisée conjointement avec la fonctionnalité Sécurité des ports. Lorsqu'une adresse MAC est sécurisée au niveau d'un port, les paquets qui proviennent de cette adresse ne peuvent entrer qu'à partir du port sécurisé. Dans le cas contraire, les paquets sont éliminés. Si la sécurité des ports est désactivée sur le port, l'adresse MAC est supprimée de la liste des adresses MAC statiques. Lorsque la sécurité des ports est activée sur un port, ce dernier peut prendre en charge un maximum de 256 adresses MAC statiques et dynamiques. (Pour plus d'informations, consultez la section [Activation de la sécurité des ports](#).)
 - **Supprimer à l'expiration** : lorsque cet état est sélectionné, l'adresse MAC statique reste statique mais peut expirer en cas d'inactivité. Elle est de ce fait traitée comme une adresse MAC apprise dynamiquement. Consultez la section *Paramètres des adresses dynamiques* pour définir le délai d'expiration.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

REMARQUE Pour supprimer une adresse MAC statique, sélectionnez-la dans la table et cliquez sur **Supprimer**.

Configuration du délai d'expiration des adresses dynamiques

La page *Paramètres des adresses dynamiques* vous permet de définir un délai d'expiration au bout duquel le système supprime de la table des adresses MAC dynamiques les adresses n'ayant pas été actualisées. Le délai d'expiration s'applique aux adresses apprises dynamiquement ainsi qu'aux adresses statiques configurées sur Supprimer à l'expiration. Le délai d'expiration par défaut est de 300 secondes.

Pour configurer le délai d'expiration :

- ÉTAPE 1** Cliquez sur **Tables d'adresses MAC > Paramètres des adresses dynamiques** dans la fenêtre de navigation.
- ÉTAPE 2** Spécifiez un délai d'expiration compris entre 10 et 1 000 000 secondes.
- ÉTAPE 3** Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Adresses MAC dynamiques

Lorsque le commutateur ne parvient pas à trouver dans sa table de ponts d'entrées qui correspondent au VLAN et à l'adresse MAC de destination d'un paquet entrant, le commutateur apprend l'adresse MAC, le VLAN et le port d'entrée du paquet, et ajoute une entrée à la Table des adresses dynamiques.

Pour éviter le débordement de la table des ponts et libérer de l'espace pour les nouvelles adresses, une adresse MAC dynamique est supprimée de cette table si aucun trafic n'est reçu de cette adresse avant l'expiration du délai configuré (voir la section [Configuration du délai d'expiration des adresses dynamiques](#)).

Pour afficher la page *Adresses dynamiques*, cliquez sur **Tables d'adresses MAC > Adresses dynamiques** dans la fenêtre de navigation.

REMARQUE L'affichage de la page peut prendre jusqu'à 45 secondes lorsque la Table des adresses dynamiques contient le nombre d'entrées maximum.

Par défaut, la Table des adresses dynamiques affiche toutes les adresses MAC apprises dynamiquement. Vous pouvez saisir des critères de filtrage et cliquer sur **OK** pour filtrer l'affichage. Utilisez le filtre *ID VLAN* pour afficher les entrées de table d'un VLAN spécifique. Utilisez le filtre *Adresse MAC* pour afficher les entrées d'une adresse MAC spécifique. Utilisez le filtre *Interface* pour afficher les entrées d'un port ou LAG spécifique. Cliquez sur **Effacer le filtre** pour afficher toutes les entrées.

La Table des adresses dynamiques affiche les champs suivants pour chaque entrée qu'elle apprend :

- **ID VLAN** : VLAN sur lequel l'adresse MAC a été apprise. Les trames ne sont transmises vers l'interface que si elles sont associées à ce VLAN.
- **Adresse MAC** : les adresses MAC apprises dynamiquement.
- **Interface** : le port sur lequel l'adresse MAC a été apprise dynamiquement. Les trames spécifiant cette adresse MAC et ce VLAN comme destination sont transmises vers ce port.

Cliquez sur **Effacer la table** pour effacer toutes les entrées d'adresses MAC dynamiques de la table.

Multidiffusion

Ce chapitre indique comment configurer les protocoles de multidiffusion qui transfèrent les paquets d'une source vers plusieurs destinations.

Il contient les rubriques suivantes :

- **Propriétés de multidiffusion**
- **Configuration d'adresses MAC de groupe**
- **Configuration de la surveillance de trafic IGMP**
- **Configuration de la surveillance de trafic MLD**
- **Configuration d'interfaces de routeur de multidiffusion IGMP**
- **Configuration d'interfaces de routeur de multidiffusion MLD**

Les protocoles de multidiffusion transfèrent les paquets d'une source vers plusieurs destinataires. Ils améliorent l'utilisation de la bande passante et contribuent à réduire la charge de traitement des hôtes et des routeurs, faisant de ces protocoles des outils parfaitement adaptés pour des applications telles que la conférence audio et vidéo, les outils de tableau blanc et les messages de distribution d'actions.

Le commutateur gère une table de transfert multidiffusion pour prendre des décisions de transfert pour les paquets qui arrivent avec une adresse MAC de destination de multidiffusion. Lorsque les multidiffusions sont limitées à des ports spécifiques, le trafic ne peut pas accéder aux parties du réseau dans lesquelles ne se trouve aucun destinataire. Lorsqu'un paquet entre dans le commutateur, l'adresse MAC de destination est associée à l'ID du VLAN et une recherche est effectuée dans la table de transfert multidiffusion. Si aucune correspondance n'est trouvée, le paquet est envoyé à tous les ports du VLAN ou supprimé, en fonction de la configuration du commutateur. En cas de correspondance, le paquet est uniquement transféré vers les ports qui font partie de ce groupe de multidiffusion.

Les entrées de multidiffusion peuvent être apprises en *surveillant le trafic* (écoutant) des protocoles de couche 3 qui gèrent les appartenances de multidiffusion :

- Les adresses des groupes de multidiffusion IPv4 peuvent être apprises via le protocole IGMP (Internet Group Management Protocol).
- Les adresses des groupes de multidiffusion IPv6 peuvent être apprises via le protocole MLD (Multicast Listener Discovery).

Les interfaces avec des routeurs de multidiffusion IGMP et MLD pour un VLAN spécifique peuvent être configurées de manière statique ou dynamique. Les routeurs de multidiffusion utilisent IGMP et MLD pour gérer l'appartenance des groupes de multidiffusion. Un routeur de multidiffusion est également requis pour que le commutateur puisse prendre correctement en charge la surveillance de trafic IGMP/MLD dans un VLAN.

Propriétés de multidiffusion

Vous pouvez utiliser la page *Propriétés de multidiffusion* pour indiquer le mode de transfert des paquets de multidiffusion au sein de VLAN.

Configuration d'un mode de transfert multidiffusion sur tous les VLAN

Vous pouvez configurer pour chaque VLAN la façon dont le commutateur transfère les paquets de multidiffusion. Lorsque vous créez un VLAN, une option de transfert multidiffusion par défaut est affectée. Vous pouvez utiliser le paramètre Mode de multidiffusion global pour définir tous les VLAN actuellement configurés sur le commutateur sur un mode de transfert donné. Le paramètre global ne crée pas de paramètre par défaut pour les VLAN créés ultérieurement ; il permet simplement de garantir que tous les VLAN existants seront configurés avec le mode spécifié.

Pour configurer tous les VLAN existants avec un mode de transfert multidiffusion spécifique :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Propriétés** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez un Mode de multidiffusion global à appliquer à tous les VLAN. Si un VLAN a été configuré avec un autre mode, il est réinitialisé sur le mode suivant :

- **Transférer non enregistrés** : si un paquet est reçu d'un VLAN avec une adresse de destination multidiffusion et qu'aucun port du VLAN n'est enregistré pour recevoir des paquets de multidiffusion pour cette adresse, le paquet est envoyé à tous les ports du VLAN. La responsabilité d'accepter ou de rejeter les paquets appartient aux hôtes. Si un paquet de multidiffusion est reçu et que des ports sont enregistrés pour le recevoir, le paquet est uniquement envoyé aux ports enregistrés.
- **Transférer tout** : tous les paquets de multidiffusion reçus d'un VLAN sont envoyés à tous les ports du VLAN, indépendamment des enregistrements des ports sur des adresses de multidiffusion.
- **Filtrer non enregistrés** : si un paquet est reçu d'un VLAN pour une adresse de destination multidiffusion et qu'aucun port du VLAN n'est enregistré pour recevoir des paquets de multidiffusion pour cette adresse, le paquet est abandonné.

ÉTAPE 3 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration de propriétés de multidiffusion sur un VLAN

Pour configurer un VLAN afin qu'il dispose d'un mode de transfert différent du paramètre de Mode de multidiffusion global :

ÉTAPE 1 Sélectionnez le VLAN dans le menu ID VLAN et cliquez sur **Modifier**.

ÉTAPE 2 Sélectionnez le Mode de multidiffusion comme le décrit la section **Configuration d'un mode de transfert multidiffusion sur tous les VLAN**.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration d'adresses MAC de groupe

La page *Adresse MAC de groupe* vous permet d'afficher et de configurer les associations entre des adresses MAC de groupes de multidiffusion et des VLAN sur le commutateur. Vous pouvez configurer des associations statiques, mais elles peuvent également être apprises dynamiquement via la surveillance de trafic IGMP ou MLD. Lorsqu'un paquet est reçu pour une adresse de groupe de multidiffusion qui correspond à une entrée dans la Table des adresses MAC de groupes, le paquet est uniquement envoyé aux ports qui sont membres du VLAN.

Le commutateur peut prendre en charge jusqu'à 32 entrées statiques et dynamiques de la table des adresses MAC de groupes. Une entrée dynamique expire si aucun paquet n'est reçu pour l'adresse MAC de groupe pendant une durée configurable (voir la page *Surveillance IGMP* pour configurer l'intervalle d'appartenance à des groupes IGMP).

Affichage de la Table des adresses MAC de groupes

Pour afficher la Table des adresses MAC de groupes, cliquez sur **Multidiffusion > Adresse MAC de groupe** dans la fenêtre de navigation.

Par défaut, toutes les entrées s'affichent dans la table. Vous pouvez utiliser les filtres ID VLAN et Adresse MAC de groupe pour afficher uniquement les entrées qui correspondent aux valeurs spécifiées. Les champs suivants s'affichent :

- **Type** : indique si l'entrée est configurée de façon statique ou apprise dynamiquement.
- **ID VLAN** : ID du VLAN vers lequel les paquets de multidiffusion sont transférés lorsqu'ils correspondent à l'adresse MAC de multidiffusion spécifiée.
- **Adresse MAC de groupe** : adresse MAC du groupe de multidiffusion, au format hexadécimal, qui est comparée à l'adresse MAC de destination d'un paquet entrant.

Ajout d'une entrée statique à la Table des adresses MAC de groupes

Pour ajouter une adresse MAC de multidiffusion statique et l'associer à un VLAN :

ÉTAPE 1 Cliquez sur **Ajouter** sur la page *Adresse MAC de groupe*.

ÉTAPE 2 Configurez les paramètres suivants :

- **ID VLAN** : sélectionnez un VLAN dans la liste.
- **Type d'adresse** : sélectionnez IPv4 pour spécifier une adresse en notation IPv4 32 bits (xxx.xxx.xxx.xxx), ou MAC pour spécifier l'adresse au format hexadécimal à 6 octets (xx.xx.xx.xx.xx.xx).
- **Adresse MAC de groupe** : saisissez l'adresse au format sélectionné. S'il s'agit d'une adresse IPv4, les 23 bits les moins significatifs sont mappés à une adresse MAC Ethernet.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**. L'entrée s'affiche dans la Table des adresses MAC de groupes.

Configuration de l'appartenance des ports à des groupes d'adresses MAC

Par défaut, les paquets destinés à une adresse MAC de multidiffusion sont envoyés à tous les ports. Des ports peuvent devenir membres d'un groupe d'adresses MAC spécifique de façon dynamique, via l'échange de paquets IGMP, mais vous pouvez également configurer cette appartenance de manière statique.

Pour afficher les détails et configurer les ports membres d'une adresse de groupe de multidiffusion :

ÉTAPE 1 Sélectionnez une entrée sur la page *Adresse MAC de groupe* et cliquez sur **Détails**.

La page identifie les membres de l'adresse de groupe de multidiffusion sur tous les ports. L'état Aucun signifie que le port ne compte aucun membre.

ÉTAPE 2 Cliquez sur **Statique** pour configurer un port en tant que membre statique de l'adresse MAC de multidiffusion.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration de la surveillance de trafic IGMP

Le protocole IGMP (Internet Group Management Protocol) est un protocole Internet de couche 3 permettant aux réseaux IPv4 de gérer les appartenances aux groupes de multidiffusion. (Le trafic de multidiffusion IPv6 est géré via le protocole MLD, comme le décrit la section [Configuration de la surveillance de trafic MLD](#).) La communication IGMP se produit entre les routeurs IGMP et les hôtes compatibles IGMP (clients). Bien que le commutateur ne déclenche pas de paquets IGMP et n'y réponde pas, il peut être configuré pour écouter les communications IGMP entre les routeurs et les clients qui sont reliés par le commutateur, et pour prendre des décisions de transfert qui contribuent à réduire le trafic réseau inutile. Ce comportement d'écoute est appelé surveillance de trafic IGMP. Il s'avère particulièrement bénéfique pour le trafic réseau de multidiffusion à bande passante élevée.

D'ordinaire, lorsque le commutateur reçoit des paquets de diffusion ou de multidiffusion, il en transfère une copie dans chacun des segments réseau restants. Cette approche est bien adaptée aux paquets de diffusion qui sont destinés à être traités par tous les nœuds connectés. En revanche, pour les paquets de multidiffusion, cette approche peut entraîner une utilisation moins efficace de la bande passante, notamment lorsque le paquet n'est destiné qu'à un petit nombre de nœuds ; les paquets inondent des segments du réseau dans lesquels aucun nœud n'a intérêt à les recevoir.

La surveillance de trafic IGMP permet au commutateur d'intercepter les rapports d'appartenance des clients IGMP et les requêtes des routeurs. Si les communications interceptées indiquent qu'aucun client IGMP n'existe sur une liaison pour une adresse de destination de multidiffusion spécifique au sein d'un VLAN, le commutateur n'envoie pas de copies de ces paquets de multidiffusion à ce segment du réseau.

La surveillance de trafic IGMP peut être activée ou désactivée sur chaque VLAN. Lorsqu'elle est activée sur un VLAN, elle est appliquée à toutes les interfaces membres de ce VLAN.

Bien que le protocole IGMP soit basé sur les adresses de multidiffusion IP, le commutateur réalise le transfert de multidiffusion effectif en se basant sur les adresses MAC équivalentes.

Pour configurer la surveillance de trafic IGMP :

- ÉTAPE 1** Cliquez sur **Multidiffusion > Surveillance IGMP** dans la fenêtre de navigation.
- ÉTAPE 2** Cochez la case Activer correspondant à État de la surveillance IGMP.
- ÉTAPE 3** Cliquez sur **Ajouter** dans la Table de surveillance IGMP.
- ÉTAPE 4** Pour **ID VLAN**, sélectionnez le VLAN qui devra prendre en charge la surveillance de trafic IGMP.
- ÉTAPE 5** Configurez les paramètres suivants :
- **Sortie rapide IGMP** : cochez la case Activer pour permettre au commutateur de supprimer immédiatement un port (ou LAG) de sa table de transfert de multidiffusion lorsqu'il reçoit un message de sortie IGMP pour ce groupe de multidiffusion. Lorsque cette option est activée, le commutateur supprime le port sans envoyer au préalable de requêtes générales à l'interface. Activez le mode Sortie rapide uniquement sur les VLAN sur lesquels un seul hôte est connecté à chaque port. Cela permet d'éviter l'abandon inopiné des autres hôtes qui sont connectés au même port et qui souhaitent continuer à recevoir le trafic de multidiffusion dirigé vers ce groupe.
 - **Intervalle d'appartenance à des groupes IGMP** : spécifiez la durée en secondes pendant laquelle le commutateur attend un rapport d'appartenance IGMP d'un groupe spécifique sur une interface donnée avant de supprimer cette interface de l'entrée dans la base de données de transfert de multidiffusion. Sélectionnez Par défaut pour spécifier 260 secondes, ou sélectionnez Défini par l'utilisateur et saisissez une valeur comprise entre 2 et 3 600 secondes.
 - **Délai de réponse max. IGMP** : spécifiez la durée en secondes pendant laquelle le commutateur attend une réponse après avoir envoyé une requête sur une interface parce qu'il n'avait pas reçu de rapport pour un groupe spécifique de cette interface. Cette valeur doit être inférieure à celle de l'Intervalle d'appartenance à des groupes IGMP. Sélectionnez Par défaut pour spécifier 10 secondes, ou sélectionnez Défini par l'utilisateur et saisissez une valeur comprise entre 1 et 25 secondes.
 - **Délai d'expiration mrouter IGMP** : spécifiez la durée en secondes pendant laquelle le commutateur attend la réception d'une requête sur une interface de routeur mrouter dynamique avant de supprimer cette interface du VLAN. Une valeur égale à 0 indique un délai infini (pas d'expiration). Sélectionnez Par défaut pour spécifier 0 seconde, ou sélectionnez Défini par l'utilisateur et saisissez une valeur comprise entre 0 et 3 600 secondes.

ÉTAPE 6 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

La nouvelle entrée VLAN apparaît dans la Table de surveillance IGMP.

ÉTAPE 7 Assurez-vous qu'une interface de routeur mrouter IGMP a été configurée pour ce VLAN (ou pour tous les VLAN). Reportez-vous à [Configuration d'interfaces de routeur de multidiffusion IGMP](#).

Configuration de la surveillance de trafic MLD

MLD est un protocole utilisé par les routeurs de multidiffusion IPv6 pour détecter la présence d'écouteurs de multidiffusion (nœuds souhaitant recevoir des paquets de multidiffusion IPv6) sur ses liaisons directes, et pour savoir quels paquets de multidiffusion présentent un intérêt pour les nœuds voisins. MLD provient d'IGMP, qui effectue une fonction similaire pour le trafic de multidiffusion IPv4 (voir la section [Configuration de la surveillance de trafic IGMP](#)).

Lorsque la surveillance de trafic MLD est activée, le commutateur transfère de manière sélective les paquets de multidiffusion IPv6 à une liste de ports qui souhaitent recevoir les données, au lieu de les envoyer à tous les ports du VLAN. Cette liste est établie en surveillant le trafic des paquets de contrôle de multidiffusion IPv6.

REMARQUE Le commutateur prend en charge la surveillance de trafic MLD des paquets MDL de version 1 et de version 2. Le commutateur peut être configuré pour effectuer simultanément la surveillance de trafic MLD et IGMP.

La surveillance de trafic MLD peut être activée ou désactivée séparément sur chaque VLAN. Bien que le protocole MLD soit basé sur les adresses IPv6, le commutateur réalise le transfert de multidiffusion effectif en se basant sur les adresses MAC équivalentes.

Pour activer et configurer la surveillance de trafic MLD :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Surveillance MLD** dans la fenêtre de navigation.

La Table de surveillance MLD répertorie chaque VLAN sur lequel cette fonction est activée.

ÉTAPE 2 Cochez la case Activer correspondant à État de la surveillance MLD.

ÉTAPE 3 Cliquez sur **Ajouter** dans la Table de surveillance MLD.

ÉTAPE 4 Pour **ID VLAN**, sélectionnez le VLAN qui devra prendre en charge la surveillance de trafic MLD.

ÉTAPE 5 Configurez les paramètres suivants :

- **Sortie rapide MLD** : cochez la case Activer pour permettre au commutateur de supprimer immédiatement un port (ou LAG) de sa table de transfert de multidiffusion lorsqu'il reçoit un message de sortie MLD pour ce groupe de multidiffusion. Lorsque cette option est activée, le commutateur supprime le port sans envoyer au préalable à l'interface de requêtes générales basées sur MAC. Activez le mode Sortie rapide uniquement sur les VLAN sur lesquels un seul hôte est connecté à chaque port. Cela permet d'éviter l'abandon inopiné des autres hôtes qui sont connectés au même port et qui souhaitent continuer à recevoir le trafic de multidiffusion dirigé vers ce groupe.
- **Intervalle d'appartenance à des groupes MLD** : spécifiez la durée en secondes pendant laquelle le commutateur attend un rapport d'appartenance MLD d'un groupe spécifique sur une interface donnée avant de supprimer cette interface de l'entrée dans la base de données de transfert de multidiffusion. Sélectionnez Par défaut pour spécifier 260 secondes, ou sélectionnez Défini par l'utilisateur et saisissez une valeur comprise entre 2 et 3 600 secondes.
- **Délai de réponse max. MLD** : spécifiez la durée en secondes pendant laquelle le commutateur attend une réponse après avoir envoyé une requête sur une interface parce qu'il n'avait pas reçu de rapport pour un groupe spécifique de cette interface. Cette valeur doit être inférieure à celle de l'Intervalle d'appartenance à des groupes MLD. Sélectionnez Par défaut pour spécifier 10 secondes, ou sélectionnez Défini par l'utilisateur et saisissez une valeur comprise entre 1 et 65 secondes.

- **Délai d'expiration mrouter MLD** : spécifiez la durée en secondes pendant laquelle le commutateur attend la réception d'une requête sur une interface avant de supprimer cette interface de la liste des interfaces reliées à un routeur de multidiffusion MLD. Une valeur égale à 0 indique un délai infini (pas d'expiration). Sélectionnez Par défaut pour spécifier 0 seconde, ou sélectionnez Défini par l'utilisateur et saisissez une valeur comprise entre 0 et 3 600 secondes.

ÉTAPE 6 Cliquez sur **Appliquer**, puis sur **Fermer**.

La nouvelle entrée VLAN apparaît dans la Table de surveillance MLD.

ÉTAPE 7 Assurez-vous qu'une interface de routeur mrouter MLD a été configurée pour ce VLAN. Reportez-vous à [Configuration d'interfaces de routeur de multidiffusion MLD](#).

Configuration d'interfaces de routeur de multidiffusion IGMP

Un routeur IGMP est nécessaire pour gérer les clients IGMP d'un VLAN. Pour chaque VLAN prenant en charge la surveillance de trafic IGMP, le commutateur doit être configuré de façon statique avec une ou plusieurs interfaces comportant un routeur IGMP ou apprendre ces interfaces dynamiquement. Une interface comportant un routeur IGMP est appelée interface de routeur de multidiffusion IGMP. Un VLAN sur lequel la surveillance de trafic IGMP est activée doit disposer d'une ou de plusieurs interfaces de routeur de multidiffusion IGMP. Un routeur de multidiffusion IGMP peut servir un ou plusieurs VLAN.

Pour activer un LAG ou port de commutation en tant qu'interface mrouter IGMP et configurer les paramètres s'y rapportant :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Mrouter IGMP** dans la fenêtre de navigation.

Par défaut, la Table mrouter IGMP répertorie chaque port de commutation. Pour afficher les LAG, sélectionnez LAG dans la liste Type d'interface.

ÉTAPE 2 Sélectionnez le port ou LAG à configurer, puis cliquez sur **Modifier**.

ÉTAPE 3 Cochez la case **Activer** située en regard de Mode.

ÉTAPE 4 Pour spécifier les VLAN qui utilisent cette interface en tant qu'interface mrouter IGMP, déplacez le VLAN vers la liste Sélectionnés, comme cela est décrit ci-dessous.

- Pour sélectionner un VLAN : cliquez sur un VLAN dans la liste Disponibles, puis cliquez sur la flèche droite pour le déplacer vers la liste Sélectionnés.
- Pour supprimer un VLAN : cliquez sur un VLAN dans la liste Sélectionnés, puis sur la flèche de gauche pour le déplacer vers la liste Disponibles.

ÉTAPE 5 Cliquez sur **Appliquer**, puis sur **Fermer**.

Dans la Table mrouter IGMP, l'interface affiche *Activer* dans la colonne Mode et répertorie les VLAN sélectionnés.

Configuration d'interfaces de routeur de multidiffusion MLD

Un routeur de multidiffusion MLD est nécessaire pour gérer les clients MLD d'un VLAN. Pour chaque VLAN prenant en charge la surveillance de trafic MLD, le commutateur doit être configuré de façon statique avec une ou plusieurs interfaces comportant un routeur de multidiffusion MLD ou apprendre ces interfaces dynamiquement. Une interface comportant un routeur MLD est appelée interface de routeur de multidiffusion MLD. Un VLAN sur lequel la surveillance de trafic MLD est activée doit disposer d'une ou de plusieurs interfaces de routeur de multidiffusion MLD. Un routeur de multidiffusion MLD peut servir un ou plusieurs VLAN.

Pour activer un LAG ou port de commutation en tant qu'interface mrouter MLD :

ÉTAPE 1 Cliquez sur **Multidiffusion > Mrouter MLD** dans la fenêtre de navigation.

Par défaut, la Table mrouter MLD répertorie chaque port de commutation. Pour afficher les LAG, sélectionnez LAG dans la liste Type d'interface.

ÉTAPE 2 Sélectionnez le port ou le LAG que vous souhaitez configurer, puis cliquez sur **Modifier**.

ÉTAPE 3 Cochez la case **Activer** située en regard de Mode.

ÉTAPE 4 Utilisez la flèche gauche ou droite pour déplacer les ID de VLAN entre les listes Disponibles et Sélectionnés. Les VLAN de la liste Sélectionnés utiliseront ce port ou LAG en tant qu'interface mrouter MLD.

ÉTAPE 5 Cliquez sur **Appliquer**, puis sur **Fermer**.

Dans la Table mrouter MLD, l'interface affiche Activer dans la colonne Mode et répertorie les VLAN inclus.

Configuration IP

Ce chapitre décrit les fonctions de protocole de résolution d'adresse (ARP) et de système de noms de domaine (DNS) du client.

Il contient les rubriques suivantes :

- **Table ARP**
- **Système de noms de domaine**

Table ARP

Le commutateur gère une Table ARP (Address Resolution Protocol, protocole de résolution d'adresse). Chaque entrée de la table inclut l'adresse IP et les adresses MAC d'un appareil ayant récemment communiqué avec le commutateur.

Vous pouvez utiliser la page *ARP* pour afficher les entrées ARP apprises par le VLAN de gestion. Pour afficher cette page, cliquez sur **Configuration IP > ARP** dans la fenêtre de navigation.

Vous pouvez cliquer sur **Effacer ARP** pour supprimer toutes les entrées de la table, à l'exception de l'adresse IP et de l'adresse MAC du port de gestion.

Système de noms de domaine

Le commutateur prend en charge la fonctionnalité de client DNS IPv4. Lorsqu'il est activé en tant que client DNS, le commutateur fournit un service de recherche de noms d'hôte à d'autres applications du commutateur, telles que ping, RADIUS, syslog, Configuration automatique et TFTP. Le commutateur peut être configuré avec des serveurs DNS qui traduisent les noms d'hôte en adresses IP. Le commutateur peut également être configuré avec des mappages de noms d'hôte aux adresses IP qui contournent le serveur DNS.

Consultez les rubriques suivantes pour plus d'informations sur les pages de configuration disponibles dans le menu Configuration IP > Système de noms de domaine.

- [Configuration de serveurs DNS](#)
- [Mappage des noms d'hôte](#)

Configuration de serveurs DNS

Pour traduire un nom d'hôte en adresse IP, le client contacte un ou plusieurs serveurs DNS. Ces derniers peuvent être appris dynamiquement si l'interface de gestion est également configurée en tant que client DHCP (voir la section [Interface de gestion](#)). Vous pouvez également utiliser la page *Serveurs DNS* pour configurer des serveurs DNS de façon statique.

La fonctionnalité de client DNS est activée par défaut.

Configuration des paramètres DNS globaux

Pour configurer les paramètres globaux et de mode des serveurs DNS :

- ÉTAPE 1** Cliquez sur **Configuration IP > Système de noms de domaine > Serveurs DNS** dans la fenêtre de navigation.
- ÉTAPE 2** Cochez la case Activer pour mettre en œuvre la fonctionnalité de client DNS sur le commutateur, si ce n'est pas déjà fait.
- ÉTAPE 3** Saisissez les paramètres suivants :
 - **Nom de domaine par défaut** : spécifiez un nom de domaine à utiliser pour compléter un nom d'hôte. Par exemple, *finance.yahoo.com* est un nom de domaine complet. Si seul le nom d'hôte incomplet, *finance*, est spécifié, le nom de domaine par défaut *yahoo.com* est ajouté en incluant un point entre

les deux. Dans votre entrée, n'incluez pas le point qui sépare le nom d'hôte incomplet du nom de domaine. La plage valide est de 1 à 255 caractères alphanumériques.

- **Nouvelles tentatives** : spécifiez le nombre de tentatives d'envoi de requêtes DNS. La plage valide est comprise entre 0 et 100 et la valeur par défaut est de 2 fois.
- **Délai du domaine** : spécifiez la durée en secondes pendant laquelle le commutateur attend une réponse à une requête DNS. La plage valide est comprise entre 0 et 3 600 secondes et la valeur par défaut est de 3 secondes.

Remarque : si les noms de domaine par défaut sont appris à partir des messages de réponse DHCP, ces noms s'affichent dans la Liste des noms de domaine par défaut.

ÉTAPE 4 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Ajout de serveurs DNS

La Table des serveurs DNS répertorie les serveurs configurés.

Pour ajouter un serveur DNS :

ÉTAPE 1 Cliquez sur **Ajouter**.

ÉTAPE 2 Spécifiez l'adresse IPv4 ou IPv6 du serveur DNS.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**. Vos modifications sont enregistrées dans la Configuration d'exécution et le serveur s'affiche dans la Table des serveurs DNS.

Mappage des noms d'hôte

Utilisez la page *Mappage d'hôtes* pour afficher et configurer les associations entre les noms d'hôte et les adresses IP. Vous pouvez associer de manière statique un nom d'hôte à une adresse IP. Vous pouvez également afficher les noms d'hôte ayant été appris dynamiquement via des applications qui utilisent le service de recherche DNS.

Configuration des mappages DNS statiques

La Table de mappage des hôtes répertorie les noms d'hôte affectés de façon statique à des adresses IP sur le commutateur. Pour configurer un mappage de noms d'hôte statique :

- ÉTAPE 1** Cliquez sur **Configuration IP > Système de noms de domaine > Mappage d'hôtes** dans la fenêtre de navigation.
- ÉTAPE 2** Cliquez sur **Ajouter**.
- ÉTAPE 3** Saisissez un nom d'hôte comportant entre 1 et 255 caractères alphanumériques. Le nom d'hôte doit commencer par une lettre.
- ÉTAPE 4** Saisissez une adresse IPv4 ou IPv6 à associer au nom d'hôte.
- ÉTAPE 5** Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Affichage et suppression d'entrées DNS dynamiques

La table Entrées DNS dynamiques affiche les noms d'hôte ayant été appris par des applications qui utilisent des services de recherche DNS. Par exemple, si vous envoyez une requête ping à un nom d'hôte, le service de recherche DNS est appelé et une adresse IP associée est apprise et ajoutée à la table.

La table Entrées DNS dynamiques contient les champs suivants :

- **Nom hôte** : nom d'hôte affecté à l'adresse IP (ou à un nom d'hôte officiel).
- **Total** : nombre de minutes pendant lesquelles le nom d'hôte a été réservé pour cette affectation.
- **Écoulé** : nombre de minutes qui se sont écoulées depuis l'affectation du nom d'hôte.
- **Type** : identifie le nom d'hôte comme étant d'un des types suivants :
 - **IP** : le nom d'hôte affecté est associé à une adresse IP.
 - **Canonique** : le nom d'hôte affecté est l'alias ou le surnom d'un nom d'hôte officiel. Par exemple, *www.google.com* peut être l'alias de nom d'hôte associé au nom d'hôte officiel *www.l.google.com*.

- **Adresses** : si le Type est IP, ce champ affiche l'adresse IPv4 ou IPv6 associée au nom d'hôte. Si le Type est Canonique, ce champ affiche le nom d'hôte canonique auquel l'alias est associé. Plusieurs alias de nom d'hôte peuvent être associés à une adresse DNS canonique.

Pour supprimer une entrée dynamique, sélectionnez-la et cliquez sur **Supprimer**. Pour supprimer toutes les entrées dynamiques de la table, cliquez sur **Supprimer toutes les entrées dynamiques**.

Sécurité

Ce chapitre décrit les fonctions de sécurité configurables au niveau du port, de l'utilisateur et du serveur.

Il contient les rubriques suivantes :

- **RADIUS**
- **Fiabilité du mot de passe**
- **Règles du profil d'accès de gestion**
- **Méthodes d'authentification**
- **Contrôle des tempêtes**
- **Sécurité des ports**
- **802.1X**

RADIUS

Le commutateur prend en charge la fonction client RADIUS (Remote Authorization Dial-In User Service, service d'authentification à distance des utilisateurs). Les administrateurs de réseaux de grande taille utilisent de plus en plus le protocole RADIUS lors de l'authentification des utilisateurs à distance. Un mot de passe ou un *secret* partagé identique, configuré pour le client RADIUS et le serveur RADIUS, permet d'authentifier les utilisateurs en toute sécurité. Cette clé secrète génère des authenticateurs cryptés à sens unique figurant dans tous les paquets RADIUS. Si l'utilisateur malveillant ignore la clé secrète, la probabilité qu'il puisse usurper correctement l'identité des paquets est suffisamment réduite.

Le client RADIUS du commutateur est utilisé pour l'authentification d'accès de gestion du commutateur et le contrôle d'accès au port IEEE 802.1X (« dot1X ») (voir les sections **Règles du profil d'accès de gestion** et **802.1X**).

La page *RADIUS* permet de configurer les paramètres RADIUS globaux et d'ajouter des serveurs RADIUS.

Configuration des paramètres RADIUS globaux

Pour configurer les paramètres globaux :

ÉTAPE 1 Cliquez sur **Sécurité > RADIUS** dans la fenêtre de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Tentatives** : affiche le nombre maximal de requêtes transmises par le client RADIUS au serveur RADIUS. La plage est comprise entre 1 et 10. La valeur par défaut est 3.
- **Délai de réponse** : indique le nombre de secondes pendant lesquelles le commutateur attend une réponse du serveur RADIUS avant d'envoyer une autre requête. La plage est comprise entre 1 et 30. La valeur par défaut est 3.
- **Délai d'inactivité** : affiche le délai qui s'écoule avant qu'un serveur RADIUS soit contourné après que le commutateur a déterminé que le serveur n'est plus disponible. Le contournement des serveurs non disponibles améliore le délai de réponse du commutateur. La plage est comprise entre 0 et 2000. La valeur par défaut est 0.
- **Attribut 4 RADIUS** (adresse IP NAS) : lorsque cette option est activée, le commutateur inclut l'attribut NAS (Network Access Server, serveur d'accès réseau) aux paquets de requêtes d'accès du serveur RADIUS. Si cette option est désactivée, le client RADIUS utilise l'adresse du port de gestion du commutateur en tant que l'adresse IP NAS.
- **Adresse IP NAS** : affiche l'adresse IP que vous devez inclure dans les paquets de requêtes d'accès. Vous pouvez modifier le contenu de ce champ uniquement après avoir coché la case Attribut 4 RADIUS. Cette adresse doit être unique par rapport au système NAS compris dans l'étendue du serveur RADIUS.

ÉTAPE 3 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Ajout d'un serveur RADIUS

Vous pouvez configurer plusieurs serveurs RADIUS, ainsi que les niveaux de priorité qui définissent l'ordre dans lequel ils sont contactés.



ATTENTION

Tous les utilisateurs gestionnaires créés disposent des autorisations de lecture-écriture. Assurez-vous que tous les utilisateurs du serveur RADIUS que vous avez configurés disposent des mêmes niveaux de privilèges. Le cas échéant, ils ne pourront pas accéder au commutateur.

Pour ajouter un serveur RADIUS à la table RADIUS :

ÉTAPE 1 Cliquez sur **Ajouter**

ÉTAPE 2 Configurez les paramètres suivants :

- **Adresse IP/Nom d'hôte RADIUS** : affiche l'adresse IP ou le nom d'hôte du serveur.
- **Priorité** : plus la valeur de priorité est basse, plus le niveau de priorité réel du serveur est élevé. Par exemple, un serveur dont la valeur de priorité est configurée sur 1, a une priorité plus élevée que celui dont la valeur de priorité est définie sur 2. Si tous les serveurs ont la même valeur de priorité (configurée par défaut), le commutateur contacte en premier les serveurs RADIUS en tête de la file. La plage est comprise entre 1 et 65535. La valeur par défaut est 8.
- **Chaîne de clé** : indique la chaîne de clé secrète partagée, utilisée pour l'authentification et le cryptage de toutes les communications RADIUS entre le commutateur et le serveur RADIUS. Cette clé doit correspondre à celle configurée sur le serveur RADIUS. Pour modifier la clé secrète, supprimez l'ancienne saisie et indiquez la nouvelle clé secrète de votre choix. Cette chaîne doit comprendre entre 32 et 176 caractères alphanumériques (ASCII).
- **Port d'authentification** : affiche le numéro de port utilisé pour l'envoi de requêtes et réponses d'authentification RADIUS. Le port 1812, défini par défaut et également appelé port IANA, est utilisé par les services d'authentification RADIUS. La plage est comprise entre 1025 et 65535. La valeur par défaut est 1812.

- **Authentificateur de message** : cette option est activée par défaut. Une fois activé, l'attribut d'authentificateur de message est inclus dans les messages de requêtes RADIUS envoyés au serveur. Cet attribut protège les messages RADIUS contre toute tentative d'usurpation et de falsification. Le secret partagé est utilisé en tant que clé. Si un paquet contient l'attribut d'authentificateur de message RADIUS, il est vérifié par le serveur. En cas d'échec de la vérification, le serveur rejette le paquet de la requête.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Fiabilité du mot de passe

La page *Fiabilité du mot de passe* permet de définir les caractéristiques des mots de passe des utilisateurs gestionnaires.

Pour configurer les paramètres de fiabilité du mot de passe :

ÉTAPE 1 Cliquez sur **Sécurité > Fiabilité du mot de passe** dans la fenêtre de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Longueur minimale du mot de passe** : affiche le nombre minimum de caractères requis pour les mots de passe d'utilisateur gestionnaire. Saisissez 0 pour définir la longueur du mot de passe entre 1 et 7 caractères. Vous pouvez également définir cette longueur à une valeur comprise entre 8 et 64 caractères.
- **Délai d'expiration du mot de passe** : cochez cette case et saisissez le délai (en jours) au bout duquel le mot de passe expire (entre 1 et 365 jours). À l'expiration du mot de passe, l'utilisateur doit saisir un nouveau mot de passe avant de poursuivre.

ÉTAPE 3 Cochez la case **Activer** en regard du champ Fiabilité du mot de passe afin de configurer les différentes vérifications à exécuter :

- **Vérification des mots clés à exclure** : une fois activée, cette option permet au commutateur de vérifier si les mots clés prédéfinis figurent dans le mot de passe créé ou modifié par l'utilisateur. Il s'agit des mots clés suivants : *cisco* et *ocsic*.

- **Nom d'utilisateur saisi comme mot de passe** : une fois activée, cette option empêche l'utilisateur d'utiliser son nom lors de la création ou de la modification des mots de passe.
- **Répétition successive d'un caractère 3 fois au maximum** : une fois activée, cette option permet au commutateur de vérifier si un caractère du mot de passe est répété successivement plus de trois fois.
- **Nombre minimal de classes de caractères** : cochez cette case, puis saisissez le nombre minimal de classes de caractères que doit contenir une chaîne de mot de passe. Les quatre classes de caractères autorisées sont : les majuscules, les minuscules, les chiffres et les caractères spéciaux d'un clavier standard.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Règles du profil d'accès de gestion

La page *Règles du profil d'accès de gestion* permet de configurer un profil et des règles d'accès à l'appareil à des fins de gestion.

Vous pouvez limiter l'accès aux noms d'utilisateur, aux ports d'entrée, aux LAG et aux adresses IP sources spécifiques.

Pour accéder à cette page, cliquez sur **Sécurité** > **Règles du profil d'accès de gestion** dans la fenêtre de navigation.

La table des profils d'accès contient le nom du profil actuellement configuré (si disponible). Elle affiche également les règles définies pour ce profil. Le commutateur ne contient aucun profil, ni aucune règle d'accès configurée par défaut. Vous pouvez créer et activer un seul profil à la fois. Toutes les règles créées sont attribuées à ce profil.

Configuration du profil et des règles d'accès

Pour créer un profil d'accès et lui attribuer des règles :

ÉTAPE 1 Dans la section Table des profils d'accès, cliquez sur **Ajouter**.

ÉTAPE 2 Spécifiez le nom du profil d'accès, puis cliquez sur Activer.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**.

Le nouveau profil s'affiche dans la table des profils d'accès. Vous pouvez désormais y ajouter des règles.

ÉTAPE 4 Dans la section Table des règles de profil, cliquez sur **Ajouter**.

ÉTAPE 5 Pour restreindre ou accorder l'accès, configurez les paramètres suivants :

- **Priorité des règles** : les règles sont validées en fonction de la requête de gestion entrante dans l'ordre croissant de leur priorité. Si une règle correspond à la requête, l'action spécifiée est exécutée et les règles suivantes sont ignorées. Par exemple, si vous configurez l'adresse IP source 10.10.10.10 avec la priorité 1 sur Autoriser, et avec la priorité 2 sur Refuser, l'accès à cette adresse IP est autorisé lorsque le profil est actif. La deuxième règle est ignorée. La plage est comprise entre 1 et 16, 1 désignant la priorité la plus élevée.
- **Méthode de gestion** : indique la méthode utilisée pour accéder à la configuration du commutateur. L'accès HTTP est autorisé par défaut afin que tous les utilisateurs puissent exécuter l'utilitaire Web de configuration du commutateur. Par exemple, pour accorder l'accès à certains utilisateurs uniquement, vous pouvez créer une règle interdisant l'accès HTTP à tous les utilisateurs, puis une autre accordant cet accès à certains utilisateurs. Vous devez définir une priorité plus élevée pour la règle autorisant l'accès à certains utilisateurs que pour la règle interdisant l'accès à tous les utilisateurs.

REMARQUE : étant donné que HTTP est la seule méthode d'accès de gestion disponible, cette option est équivalente à l'option Toutes.

- **Action** : sélectionnez l'action à exécuter lorsque les critères de règles correspondent à la requête.
 - **Autoriser** : l'interface, l'utilisateur ou l'adresse IP spécifiée bénéficie d'un accès autorisé au commutateur qui serait, le cas échéant, explicitement interdit par une règle de refus.

- **Refuser** : l'accès au commutateur est refusé à l'interface, à l'utilisateur ou à l'adresse IP spécifiée.
- **S'applique à l'interface** : sélectionnez Toutes pour appliquer cette règle à toutes les interfaces (les ports et les LAG). Vous pouvez également activer l'option Personnalisé, puis sélectionner un port ou un LAG auquel la règle s'applique.
- **S'applique à l'utilisateur** : sélectionnez Activer, puis choisissez l'utilisateur configuré auquel cette règle s'applique. Vous pouvez ainsi conserver les utilisateurs gestionnaires dans le système et leur empêcher d'accéder au commutateur en appliquant cette règle au profil d'accès.
- **S'applique à l'adresse IP source** : sélectionnez Toutes afin d'appliquer la règle à toutes les adresses IP sources. Vous pouvez également activer l'option Personnalisé, puis définir une adresse IPv4 source et un masque auxquels cette règle s'applique.

ÉTAPE 6 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

La nouvelle règle s'affiche dans la table des règles de profil. Sélectionnez la règle et cliquez sur **Modifier** pour la modifier, ou sur **Supprimer** pour la supprimer du profil d'accès.

REMARQUE L'accès de gestion ne sera pas refusé à l'utilisateur **cisco**.



ATTENTION Si vous avez activé un profil interdisant l'accès à l'intranet ou au domaine sur lequel une session de gestion Web actuelle est active, cette session restera active jusqu'à sa déconnexion ou son expiration. Le profil bloquera les sessions suivantes. Afin que les sessions actives exécutées sous Internet Explorer 8 ne soient pas immédiatement interrompues, ajoutez l'adresse IP de gestion du commutateur à la liste Sites Internet locaux sous Internet Explorer. Pour plus d'informations, consultez la rubrique [Démarrage de l'utilitaire Web de configuration du commutateur](#).

Modification et suppression des profils et des règles d'accès

Avant de supprimer un profil d'accès ou de modifier ses règles, vous devez désactiver ce profil.

Pour désactiver un profil d'accès :

ÉTAPE 1 Sélectionnez le profil dans la table des profils d'accès, puis cliquez sur **Modifier**.

ÉTAPE 2 Décochez la case Activer.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**.

Après avoir terminé les modifications, réactivez le profil d'accès.

Pour supprimer un profil d'accès (après l'avoir désactivé) :

ÉTAPE 1 Sélectionnez le profil dans la table des profils d'accès.

ÉTAPE 2 Cliquez sur **Supprimer**.

Pour supprimer une règle de profil (après avoir désactivé le profil d'accès) :

ÉTAPE 1 Sélectionnez la règle dans la table des règles de profil.

ÉTAPE 2 Cliquez sur **Supprimer**.

Pour modifier une règle de profil (après avoir désactivé le profil d'accès) :

ÉTAPE 1 Sélectionnez la règle dans la table des règles de profil, puis cliquez sur **Modifier**.

ÉTAPE 2 Saisissez les nouveaux paramètres.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**.

Pour activer un profil d'accès (après avoir effectué toutes les modifications) :

ÉTAPE 1 Sélectionnez le profil dans la table des profils d'accès, puis cliquez sur **Modifier**.

ÉTAPE 2 Cochez la case Activer.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**.

Méthodes d'authentification

Sur la page *Cliquez sur* **Sécurité > Méthodes d'authentification** dans la fenêtre de navigation. *Méthodes d'authentification*, vous pouvez configurer les méthodes d'authentification via lesquelles les utilisateurs sont autorisés à accéder aux ports du commutateur.

Pour sélectionner une méthode d'authentification :

ÉTAPE 1 Cliquez sur **Sécurité > Méthodes d'authentification** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez une méthode d'authentification dans la liste Méthodes :

- **Locale** : la combinaison nom d'utilisateur/mot de passe du demandeur est comparée à la base de données des utilisateurs du commutateur stockée en local.
- **Aucune** : aucune méthode d'authentification n'est utilisée.
- **RADIUS** : le commutateur envoie des requêtes d'authentification à un serveur RADIUS, qui renvoie des trames RADIUS d'accès accordé ou d'accès refusé.
- **RADIUS, aucune** : le commutateur envoie les requêtes d'authentification à un serveur RADIUS. S'il ne parvient pas à se connecter au serveur, aucune méthode d'authentification n'est utilisée.
- **RADIUS, locale** : le commutateur envoie les requêtes d'authentification à un serveur RADIUS. S'il ne parvient pas à atteindre le serveur, il utilisera la base de données des utilisateurs locale.

ÉTAPE 3 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Contrôle des tempêtes

Une tempête de trafic résulte d'un afflux simultané excessif de messages de diffusion, de multidiffusion ou de monodiffusion inconnue sur un réseau par l'intermédiaire d'un seul port. Les réponses des messages redirigés peuvent surcharger les ressources du réseau et entraîner l'expiration de ce dernier.

Le commutateur mesure le taux de paquets de diffusion/multidiffusion/monodiffusion entrants par port et ignore les paquets lorsque ce taux dépasse la valeur définie. Vous pouvez activer ou désactiver le contrôle des tempêtes pour chaque interface.

Sur la page *Contrôle des tempêtes*, vous pouvez activer et configurer la fonction de contrôle des tempêtes dans les interfaces du commutateur. Pour accéder à cette page, cliquez sur **Sécurité** > **Contrôle des tempêtes** dans la fenêtre de navigation.

Cette option est désactivée par défaut sur tous les ports et pour tous les paquets. Pour modifier les paramètres du contrôle des tempêtes pour un port :

ÉTAPE 1 Sélectionnez le port que vous souhaitez configurer, puis cliquez sur **Modifier**.

ÉTAPE 2 Pour éviter le trafic de diffusion, de multidiffusion et de monodiffusion non sollicité, définissez les paramètres suivants pour le port sélectionné :

- **Contrôle des tempêtes** : cochez la case Activer pour activer la protection contre les tempêtes pour tout type de trafic.
- **Type de seuil de débit** : sélectionnez la méthode qui permet au commutateur de déterminer si le trafic dépasse le seuil défini :
 - **Pourcentage** : le trafic est interrompu lorsqu'il dépasse le pourcentage de débit sur la liaison.
 - **pps** : paquets par seconde. Le trafic est interrompu lorsqu'il dépasse le seuil de paquets par seconde sur la liaison.
- **Seuil de débit de contrôle des tempêtes** : saisissez le débit maximal auquel les paquets sont redirigés. Si le type de seuil de débit est défini sur Pourcentage, saisissez un pourcentage (entre 0 et 100 %) pour le débit total du port. S'il est défini sur pps, saisissez un taux de paquets par seconde (entre 0 et 14880000). Les ports fonctionnant à 10 Mbits/s, à 100 Mbits/s et à 1000 Mbits/s présentent respectivement un débit maximal de 14880, de 148800 et de 1488000 paquets par seconde.

REMARQUE : le taux actuel du trafic entrant requis pour l'activation du contrôle des tempêtes est basé sur la taille des paquets entrants, ainsi que sur la taille moyenne des paquets codés de manière irréversible (512 octets). Le taux de paquets par seconde est calculé lorsque le matériel requiert une valeur en pps par rapport à un taux absolu en Kbits/s. Par exemple, si le seuil configuré est de 10 %, il est converti en ~25 000 pps (pour un port 100M) et défini pour le matériel.

ÉTAPE 3 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Sécurité des ports

Vous pouvez activer la sécurité pour chaque port individuellement. Lorsqu'un port est sécurisé (verrouillé), le commutateur redirige uniquement les paquets dont l'adresse MAC source est sécurisée sur le port en question. Tous les autres paquets sont ignorés. Le commutateur ignore également les paquets provenant d'un port dont l'adresse Mac source est sécurisée sur un autre port.

Les adresses MAC sécurisées peuvent être configurées de manière statique ou apprises de façon dynamique. Le nombre maximal d'adresses MAC sécurisées sur un port sécurisé s'élève à 256. La configuration des adresses Mac sécurisées statiques est décrite à la page *Adresses statiques*. Les adresses MAC sécurisées statiques et dynamiques sont soumises aux délais d'expiration (voir la section [Configuration du délai d'expiration des adresses dynamiques](#)).

Pour accéder à la page *Sécurité des ports*, cliquez sur **Sécurité** > **Sécurité des ports** dans la fenêtre de navigation.

La table de sécurité des ports affiche la configuration de sécurité actuelle de tous les ports. Pour afficher les données des LAG uniquement, sélectionnez LAG dans la liste *Type d'interface*. Par défaut, la sécurité des ports est désactivée globalement et pour chaque interface.

Activation de la sécurité des ports

Pour configurer la sécurité des ports :

- ÉTAPE 1** Dans la page *Sécurité des ports*, cochez la case Activer en regard de l'option Mode d'administration, puis cliquez sur **Appliquer**.
- ÉTAPE 2** Sélectionnez le port ou le LAG que vous souhaitez configurer, puis cliquez sur **Modifier**.
- ÉTAPE 3** Configurez les paramètres suivants :
- **État de l'interface** : cochez la case Verrouiller pour activer la sécurité des ports pour cette interface. Lorsque l'état d'une interface est configuré sur Verrouillé, toutes les adresses apprises de manière dynamique par le commutateur sur ce port sont supprimées de la liste des adresses MAC du commutateur.
 - **Nb max d'adresses MAC statiques** : indique le nombre maximal d'adresses MAC sécurisées statiques sur le port ou le LAG. Vous pouvez configurer les adresses MAC sécurisées statiques à partir de l'écran *Adresses statiques*. Le nombre total d'adresses sécurisées est limité à 256.
 - **Nb max d'adresses MAC dynamiques** : indique le nombre maximal d'adresses MAC sécurisées dynamiques qui peuvent être apprises sur le port ou le LAG. Le nombre total d'adresses sécurisées est limité à 256.

Lorsque la sécurité des ports a été activée sur un port et que de nouvelles valeurs ont été définies pour les seuils statiques ou dynamiques, les règles suivantes s'appliquent :

- Si la nouvelle valeur est supérieure à l'ancienne, aucune action n'est exécutée ni pour les adresses statiques, ni pour les adresses dynamiques.
- Si la nouvelle valeur est inférieure à l'ancienne, les actions suivantes sont exécutées :

Adresses dynamiques : le commutateur déclenche une purge de toutes les adresses apprises sur le port.

Adresses statiques : le commutateur conserve les adresses statiques (jusqu'à la limite autorisée) quelle que soit leur configuration : sécurisée, permanente ou supprimée à l'expiration. Il supprime ensuite les adresses statiques restantes de la liste des adresses MAC.

- **Action en cas de violation** : sélectionnez la manière dont le commutateur traite les paquets entrants non autorisés sur le port verrouillé :
 - **Ignorer** : les paquets sont rejetés.
 - **Rediriger** : les paquets sont redirigés, mais les adresses MAC sources ne sont pas ajoutées à la base de données de redirection.
 - **Fermer** : les paquets sont ignorés et le port est fermé.
- **Convertir les adresses dynamiques en statiques** : cochez la case Activer afin de convertir toutes les adresses MAC sécurisées dynamiques en adresses MAC sécurisées statiques.
- **Réinitialiser le port** : sélectionnez cette option pour réinitialiser le port lorsque ce dernier a été fermé par la fonction Sécurité des ports.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Affichage et configuration des adresses MAC sécurisées

Pour afficher la liste actuelle des adresses MAC sécurisées, ainsi que les ports et les VLAN associés, cliquez sur **Table des adresses sécurisées** dans la page *Sécurité des ports*.

Pour chaque interface, la table des adresses sécurisée répertorie toutes les adresses MAC configurées de façon statique, que le port soit verrouillé ou non. Cette table comprend également des adresses MAC apprises de manière dynamique sur les ports verrouillés. Les entrées dynamiques d'un port sont effacées lorsque l'état du port est configuré sur Déverrouillé ou lorsque la liaison n'est plus utilisable.

Cliquez sur **Table des adresses statiques** afin d'afficher la page de configuration des adresses statiques. Reportez-vous à **Configuration d'adresses MAC statiques**. Assurez-vous que le champ État est configuré sur Sécurisé.

Cliquez sur **Table de sécurité des ports** pour afficher de nouveau la page *Sécurité des ports*.

802.1X

En général, les réseaux locaux (LAN) sont déployés dans les environnements au sein desquels les appareils non autorisés peuvent être physiquement reliés à l'infrastructure LAN ou les utilisateurs non autorisés peuvent tenter d'accéder au réseau local par l'intermédiaire du matériel déjà relié. Pour ce type d'environnements, il est conseillé de restreindre l'accès aux services du réseau local aux utilisateurs et appareils autorisés.

La fonction de contrôle d'accès de port permet aux réseaux de vérifier si les hôtes peuvent accéder aux services fournis par un port connecté. Vous pouvez configurer le commutateur afin qu'il exécute le contrôle d'accès de port en utilisant le protocole IEEE 802.1x.

Le protocole 802.1x définit trois types d'entités :

- **Demandeur** : désigne une entité qui demande l'accès à un port à l'extrémité distante de la liaison. Le demandeur fournit les informations d'identification au réseau qui sont utilisées par l'autre nœud du réseau, l'authentificateur, lors des requêtes d'authentification à partir d'un serveur.
- **Authentificateur** : désigne une entité qui simplifie l'authentification du demandeur à l'extrémité distante d'une liaison. L'authentificateur accorde au demandeur l'accès au port lorsque l'authentification est validée.
- **Serveur d'authentification** : désigne un serveur, tel que serveur RADIUS, qui effectue l'authentification au nom de l'authentificateur et indique si le demandeur est autorisé à accéder aux services fournis via le port d'authentification.

Au cours de l'authentification, 802.1X prend en charge le protocole EAP (Extensible Authentication Protocol) pour des échanges de messages (EAPOL) sur les réseaux locaux entre les demandeurs et les authentificateurs.

Le port du commutateur peut être configuré soit comme authentificateur, soit comme demandeur, mais pas les deux.

Définition des propriétés 802.1X

L'écran *Propriétés 802.1X* permet de configurer le mode d'administration 802.1X général du commutateur.

Pour activer globalement la sécurité 802.1X :

-
- ÉTAPE 1** Cliquez sur **Sécurité > 802.1X > Propriétés** dans la fenêtre de navigation.
- ÉTAPE 2** Cochez la case Activer en regard de l'option État d'authentification par port pour activer l'authentification par port 802.1X globalement au niveau du commutateur.
- ÉTAPE 3** Sélectionnez une méthode d'authentification dans la liste des méthodes d'authentification :
- **Aucune** : aucune méthode d'authentification n'est utilisée.
 - **Locale** : le commutateur effectue une authentification locale d'un demandeur distant en utilisant le port EAP-MD5. Les informations d'identification du demandeur doivent correspondre à celles des utilisateurs configurés sur le commutateur (voir [Gestion des comptes d'utilisateurs](#)).
 - **RADIUS** : le commutateur fait appel à un ou plusieurs serveurs RADIUS externes pour effectuer l'authentification. Configurez l'authentification et les informations d'identification des demandeurs directement sur les serveurs. Pour plus d'informations, consultez la section [RADIUS](#).
 - **RADIUS, aucune** : le commutateur fait appel à un ou plusieurs serveurs RADIUS externes pour effectuer l'authentification (voir la description de RADIUS ci-dessus). Si le commutateur ne parvient pas à se connecter au serveur, aucune méthode d'authentification n'est utilisée.
 - **RADIUS, locale** : le commutateur fait appel à un ou plusieurs serveurs RADIUS externes pour effectuer l'authentification (voir la description de RADIUS ci-dessus). Si le commutateur ne parvient pas à se connecter au serveur, il effectue une authentification locale (voir la description de la méthode d'authentification Locale ci-dessus).
- ÉTAPE 4** Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.
-

REMARQUE Consultez la section [Modification des fonctionnalités des extensions d'adresse physique des ports](#) pour plus d'informations sur la sélection du rôle pour chaque port, et la section [Configuration de l'authentification des ports](#) pour en savoir plus sur la configuration de l'authentification sur les ports individuels.

Modification des fonctionnalités des extensions d'adresse physique des ports

L'écran *Fonctionnalités des extensions d'adresse physique des ports* permet d'afficher et de configurer le rôle 802.1X de chaque port en tant qu'authentificateur ou demandeur.

Pour définir le rôle d'un port en tant qu'authentificateur ou demandeur :

ÉTAPE 1 Cliquez sur **Sécurité > 802.1X > Propriétés** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez le port que vous souhaitez configurer, puis cliquez sur **Modifier**.

ÉTAPE 3 Sélectionnez le rôle du port :

- **Authentificateur** : lorsque cette option est sélectionnée, le port effectue l'authentification du demandeur distant avant d'autoriser l'accès à un port local.
- **Demandeur** : lorsque cette option est sélectionnée, le port envoie une requête d'autorisation à l'authentificateur distant avant d'accéder à un port distant.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration de l'authentification des ports

L'écran *Authentification des ports* permet de configurer le contrôle d'accès de port sur les ports qui servent d'authentificateurs. Pour activer un port en tant qu'authentificateur, consultez la rubrique [Modification des fonctionnalités des extensions d'adresse physique des ports](#).

Pour modifier les paramètres d'un authentificateur de port :

ÉTAPE 1 Cliquez sur **Sécurité > 802.1X > Authentification des ports** dans la fenêtre de navigation.

La table d'authentification des ports affiche la configuration actuelle de chaque port.

ÉTAPE 2 Sélectionnez le port que vous souhaitez configurer, puis cliquez sur **Modifier**.

ÉTAPE 3 Configurez les paramètres suivants :

- **Nom d'utilisateur de la base de données locale** : les flèches de gauche et de droite permettent de déplacer les utilisateurs gestionnaires vers la liste Disponibles ou Sélectionnés. Seuls les utilisateurs de la liste Sélectionnés ont accès au port soumis à l'authentification. Cette liste s'applique uniquement lorsque l'authentification s'effectue en local, et non via un serveur RADIUS.
- **État actuel du contrôle de port** : affiche l'état d'autorisation actuel du port (Autorisé ou Non autorisé).
- **Contrôle du port** : sélectionnez le mode d'autorisation du port. Ce champ peut prendre les valeurs suivantes :
 - **Non-autorisation forcée** : si vous sélectionnez cette option, l'accès au port sera toujours refusé aux demandeurs tentant de se connecter à ce port, et l'état de contrôle du port sera défini sur Non autorisé.
 - **Automatique** : si vous sélectionnez cette option, le contrôle du port s'effectuera en fonction du résultat de l'authentification. Lorsque le demandeur est authentifié, l'état de contrôle du port est défini sur Autorisé, indiquant ainsi que le demandeur peut désormais accéder au port. Lorsque le demandeur n'est pas authentifié, l'état de contrôle du port est défini sur Non autorisé, indiquant ainsi que le demandeur ne dispose d'aucun accès au port.
 - **Autorisation forcée** : si vous sélectionnez cette option, l'accès aux ports sera toujours autorisé si l'authentification des demandeurs distants n'est pas requise, et l'état de contrôle du port sera défini sur Autorisé.

- **Réauthentification régulière** : sélectionnez cette option afin que le port effectue régulièrement une réauthentification de son demandeur. Le port effectue la réauthentification aux intervalles définis, même s'il est resté authentifié.
- **Durée de réauthentification** : affiche l'intervalle compris entre les tentatives de réauthentification. La plage est comprise entre 300 et 4294967295 secondes. La valeur par défaut est de 3600 secondes.
- **Réauthentifier maintenant** : sélectionnez cette option pour forcer la réauthentification des ports immédiate.
- **État de l'authentificateur** : affiche l'état actuel de l'autorisation du port. Ce champ peut prendre les valeurs suivantes : Initialisé, Déconnecté, Connexion, Authentification, Authentifié, Abandon, En attente, Authentification forcée et Non-authentification forcée.
- **État du terminal** : affiche l'état actuel de la machine d'état d'authentification du terminal. Ce champ peut prendre les valeurs suivantes : Requête, Réponse, Succès, Échec, Expiré, Inactif et Initialiser.
- **Période silencieuse** : affiche le délai pendant lequel le commutateur reste en état silencieux après l'échec d'un échange d'authentification. Au cours de cette période, le commutateur ne peut pas accepter, ni initialiser les requêtes d'authentification. Modifiez la valeur par défaut de cette commande uniquement lors des circonstances particulières, telles que les liaisons non fiables ou les problèmes de comportement spécifiques survenant pour certains clients et serveurs d'authentification. Afin d'améliorer le délai de réponse, saisissez un nombre plus petit que celui défini par défaut (60 secondes). La plage est comprise entre 0 et 65535 secondes.
- **Renvoi d'EAP** : indique la durée écoulée avant que les demandes EAP soient renvoyées. La plage est comprise entre 1 et 65535 secondes. La valeur par défaut est de 30 secondes.
- **Délai pour demandeur** : indique la durée écoulée avant que les demandes EAP soient renvoyées aux demandeurs. Modifiez la valeur par défaut de cette commande (30 secondes) uniquement lors des circonstances particulières, telles que les liaisons non fiables ou les problèmes de comportement spécifiques survenant pour certains clients et serveurs d'authentification. Afin d'améliorer le délai de réponse, saisissez un nombre plus petit que celui défini par défaut. La plage est comprise entre 1 et 65535 secondes.

- **Délai pour serveur** : affiche le nombre de secondes qui s'écoulent avant que le commutateur renvoie une demande au serveur d'authentification. La plage est comprise entre 1 et 65535 secondes. La valeur par défaut est de 30 secondes.
- **Demandes EAP max** : affiche le nombre maximal prédéfini des demandes EAP que le commutateur envoie avant de redémarrer l'authentification lorsqu'il ne reçoit aucune réponse.
- **Cause d'arrêt** : affiche la raison pour laquelle l'authentification du port a été arrêtée.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Configuration de l'authentification des ports du demandeur

L'écran *Authentification des ports du demandeur* permet de configurer le contrôle d'accès de port qui ont été définis en tant que demandeurs. Pour activer un port en tant que demandeur, consultez la rubrique **Modification des fonctionnalités des extensions d'adresse physique des ports**.

Pour configurer l'authentification des ports du demandeur :

ÉTAPE 1 Cliquez sur **Sécurité > 802.1X > Authentification des ports du demandeur** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez le port que vous souhaitez configurer, puis cliquez sur **Modifier**.

Le champ Contrôle du port actuel affiche le mode d'autorisation du port actuellement défini.

ÉTAPE 3 Configurez les options suivantes :

- **Contrôle du port d'administration** : sélectionnez le mode d'autorisation du port. Ce champ peut prendre les valeurs suivantes :
 - **Non-autorisation forcée** : refuse l'accès au système d'interface sélectionné en mettant ce dernier en mode non autorisé.
 - **Automatique** : le commutateur détecte le mode de l'interface en fonction du résultat des échanges d'authentification effectués entre le demandeur, l'authentificateur et le serveur d'authentification.

- **Autorisation forcée** : le port est défini en mode Autorisé sans requérir d'authentification avec le serveur d'authentification. L'interface envoie et reçoit un trafic normal sans effectuer d'authentification par port client.
- **Nom d'utilisateur** : sélectionnez l'utilisateur que le port utilisera pour s'identifier en tant que demandeur. L'utilisateur doit faire partie des utilisateurs gestionnaires définis au préalable sur le commutateur. Le mot de passe défini pour cet utilisateur sera utilisé lors de l'authentification. En tant que demandeur, le commutateur prend en charge la méthode d'authentification par port EAP-MD5. Pour configurer les utilisateurs, consultez la rubrique [Gestion des comptes d'utilisateurs](#).

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Affichage des hôtes authentifiés

Pour afficher les ports dont les utilisateurs ont été authentifiés à la page *Hôtes authentifiés*, cliquez sur **Sécurité > 802.1X > Hôtes authentifiés** dans la fenêtre de navigation.

La table des hôtes authentifiés affiche les informations suivantes sur chaque hôte :

- **Port** : désigne le port utilisé pour l'authentification.
- **Nom d'utilisateur** : indique le nom d'utilisateur de l'hôte.
- **Adresse MAC du demandeur** : correspond à l'adresse MAC de l'appareil du demandeur.
- **Durée de la session** : indique le délai de connexion (en secondes) du demandeur.
- **Délai de la session** : indique la durée pendant laquelle une session donnée est valide. Ce délai (mesuré en secondes) est renvoyé par le serveur RADIUS pour l'authentification du port.

Qualité de service

Ce chapitre offre un aperçu de la qualité de service (QoS) et explique les fonctionnalités de QoS disponibles depuis le menu Qualité de service.

- **Propriétés de QoS**
- **Définition de files d'attente**
- **Mappage de priorités CoS/802.1p aux files d'attente**
- **Mappage de la priorité IP aux files d'attente**
- **Mappage de valeurs DSCP aux files d'attente**
- **Définition de profils de limitation de débit**
- **Application de profils de limitation de débit à des interfaces**
- **Mise en forme du trafic**

Dans un commutateur typique, chaque port physique se compose d'une ou de plusieurs files d'attente pour la transmission de paquets sur le réseau connecté. Plusieurs files d'attente par port sont souvent configurées pour accorder la préférence à certains paquets plutôt qu'à d'autres, en fonction de critères définis par l'utilisateur. Lorsqu'un paquet est mis en file d'attente en vue d'une transmission dans un port, la vitesse à laquelle il sera traité dépend du mode de configuration de la file d'attente, voire de la quantité de trafic présent dans les autres files d'attente du port. Si un délai est nécessaire, les paquets sont conservés en attente dans la file jusqu'à ce que le planificateur autorise cette dernière à effectuer la transmission. À mesure que les files d'attente se remplissent, les paquets ne peuvent plus être conservés en attente en vue de leur transmission et peuvent être abandonnés par le commutateur.

QoS permet d'assurer une livraison régulière et prévisible des données en distinguant les paquets ayant des exigences temporelles strictes de ceux qui tolèrent davantage les retards. Sur un réseau compatible QoS, un traitement spécial est accordé aux paquets ayant des exigences temporelles strictes.

Sur les réseaux bénéficiant de la QoS, tous les éléments du réseau doivent être compatibles QoS. La présence d'un ou de plusieurs nœuds non compatibles QoS provoque une déficience au niveau du chemin du réseau et compromet la performance de l'ensemble du flux de paquets.

Le commutateur prend en charge quatre files d'attente de sortie pour chaque port ou LAG. La file d'attente 1 est celle qui dispose de la priorité la plus basse, tandis que la priorité la plus haute est affectée à la file d'attente 4.

Les pages du menu Qualité de service vous permettent de définir les propriétés des files d'attente, et de les associer au trafic ayant des caractéristiques spécifiques ou arrivant sur des interfaces particulières. Vous pouvez également créer des profils de limitation de débit qui définissent des critères permettant de déterminer si un port reçoit plus de trafic qu'il ne peut en gérer. Vous pouvez alors affecter ces profils de limitation de débit aux ports.

Propriétés de QoS

Vous pouvez configurer les ports de commutation afin d'affecter le trafic à des files d'attente de sortie en fonction des informations de priorité encodées dans les trames Ethernet ou les en-têtes de paquets IP. Le trafic peut également utiliser une valeur de priorité par défaut configurée sur le port sur lequel il arrive. Lorsqu'un port est configuré pour utiliser la valeur de priorité encodée (telle que la valeur 802.1p, de priorité IP ou DSCP), il est considéré comme *validé*. Un port configuré pour utiliser sa propre valeur de priorité, plutôt que celle encodée dans la trame ou le paquet, pour décider de l'affectation de files d'attente est considéré comme *non validé*.

Si un port est configuré en tant que port validé, mais que la trame ou le paquet ne dispose d'aucune information de priorité, la priorité de port par défaut est affectée au paquet. Cette priorité de port par défaut est de zéro.

Vous pouvez utiliser la page *Gestion des VLAN > Paramètres d'interface* pour modifier la valeur de la priorité VLAN.

Vous pouvez utiliser la page *Propriétés de QoS* pour définir un port comme étant validé ou non validé et pour configurer les valeurs de priorité auxquelles il fait confiance.

Pour configurer le mode de confiance d'un port ou d'un LAG :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Propriétés de QoS** dans la fenêtre de navigation.

ÉTAPE 2 Utilisez le menu Type d'interface pour afficher les ports ou LAG dans la table Configuration du mode de confiance.

ÉTAPE 3 Sélectionnez l'interface à configurer et cliquez sur **Modifier**.

ÉTAPE 4 Pour spécifier le type de valeurs de priorité à utiliser pour déterminer les files d'attente de sortie des paquets, sélectionnez un des modes de confiance suivants :

- **untrusted** : le port affecte sa propre priorité 802.1p par défaut (0).
- **trust dot1p** : le port utilise la valeur de priorité 802.1p dans les trames Ethernet balisées VLAN. La priorité par défaut du port est affectée aux trames non balisées.
- **trust ip-precedence** : le port utilise la valeur de priorité IP dans l'en-tête du paquet IP. Si aucune valeur n'est fournie, la priorité par défaut du port est affectée. Cette priorité par défaut est en outre affectée aux trames balisées et non balisées VLAN non IP.
- **trust ip-dscp** : le port utilise le marquage DSCP dans l'en-tête des paquets IP balisés et non balisés VLAN. La priorité par défaut du port est affectée aux trames balisées et non balisées VLAN non IP.
- **trust all** : pour les paquets IP, le port utilise le marquage DSCP afin de déterminer la priorité. Pour les trames non IP, le port utilise la priorité 802.1p si la trame est balisée VLAN, et la priorité par défaut du port dans le cas contraire.

ÉTAPE 5 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Définition de files d'attente

Vous pouvez utiliser la page *File d'attente* pour configurer la façon dont le planificateur de trafic détermine quelle file d'attente a accès au port de sortie. Une file d'attente peut être configurée en mode de priorité stricte (SP, Strict Priority) ou en mode « Round Robin » pondéré (WRR, Weighted Round-Robin). Par défaut, toutes les files d'attente sont des files d'attente de priorité stricte.

Les paquets sont transmis conformément aux principes suivants :

- Les paquets émanant de la file d'attente à haute priorité sont transmis en premier.
- Si une file d'attente est en mode de priorité stricte, elle est autorisée à transmettre jusqu'à ce qu'elle n'ait plus de paquets ou jusqu'à ce qu'une file d'attente de priorité plus haute ait des paquets à envoyer.
- Si une file d'attente est en mode WRR, elle est autorisée à transmettre un nombre de paquets proportionnel à sa valeur de pondération configurable. La pondération est exprimée en pourcentage de la bande passante totale de chaque port.

Il est possible de configurer une combinaison de file d'attente stricte et de files d'attente WRR au niveau d'un port.

Recommandations en matière de configuration des files d'attente

Il est recommandé de configurer les files d'attente dont le numéro est le plus élevé avec des paramètres de priorité, de pondération et de bande passante minimale plus élevés.

Des scénarios recommandés pour la priorité stricte (SP, Strict Priority) et WRR sur les files d'attente (Q) 1 à 4 vous sont présentés ci-dessous :

- **Les quatre files d'attente en mode SP** ($Q4 > Q3 > Q2 > Q1$). De la bande passante est allouée à Q4 tant qu'il y a des paquets à traiter dans Q4. Q3 est ensuite traitée, suivie de Q2 et de Q1 dans cet ordre.
- **Les quatre files d'attente en mode WRR** ($Q4:Q3:Q2:Q1 = A:B:C:D$). Dans ce mode, chaque file d'attente se voit allouer sa bande passante minimale, conformément aux pondérations configurées.

- **Une file d'attente en mode SP et trois en mode WRR** ($Q4 > Q3/Q2/Q1$; $Q3:Q2:Q1 = A:B:C$). Dans ce scénario, il est conseillé que Q4 soit configurée en mode SP et Q3, Q2 et Q1 en mode WRR.
- **Deux files d'attente en mode SP et deux en mode WRR** ($q4 > q3 > q2/q1$; $q2:q1 = A:B$). Dans ce scénario, il est conseillé que Q4 et Q3 soient configurées en mode SP, et Q2 et Q1 en mode WRR.

Ces scénarios illustrent le fait que lorsqu'il y a davantage de ports d'entrée avec un trafic destiné à des files d'attente différentes sur des ports de sortie, un système peut rencontrer une condition de blocage Head of Line (HOL, Head of Line Blocking). HOL peut provoquer l'allocation d'une bande passante plus élevée aux files d'attente ayant des numéros plus élevés, alors même que ces files d'attente sont configurées avec une bande passante et une pondération minimales plus faibles. On recommande toujours de configurer en mode SP les files d'attente dont le numéro est le plus élevé, afin que même en cas de condition HOL, la répartition de sortie souhaitée soit assurée entre les files d'attente.

Configuration des files d'attente

Pour configurer les propriétés de QoS :

- ÉTAPE 1** Cliquez sur **Qualité de service** > **File d'attente** dans la fenêtre de navigation.
- ÉTAPE 2** Sélectionnez le port ou LAG à configurer.
- ÉTAPE 3** Sélectionnez un des modes suivants pour chaque file d'attente de l'interface sélectionnée :
 - **Priorité stricte** : le planificateur réachemine le trafic en se basant strictement sur les niveaux de priorité des files d'attente. La file d'attente disposant du trafic avec la priorité la plus haute aura accès au port de sortie jusqu'à ce que tout le trafic soit réacheminé. Le mode de priorité stricte peut être utilisé pour fournir un service à faible latence aux classes de trafic de priorité plus haute.
 - **WRR** : le planificateur traite la file d'attente à tour de rôle avec les autres files d'attente WRR, en fonction de son pourcentage de bande passante par rapport à ces autres files d'attente WRR. Les files d'attente strictes continuent d'être traitées pendant la durée au cours de laquelle elles disposent d'un trafic à priorité plus haute.

ÉTAPE 4 Si vous sélectionnez le mode WRR pour une file d'attente, entrez un pourcentage de bande passante dans le champ Pourcentage de bande passante WRR. Le total de tous les pourcentages de bande passante pour l'ensemble des files d'attente ne peut pas dépasser 100 %.

ÉTAPE 5 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Pour appliquer ces propriétés de file d'attente à toutes les autres interfaces du commutateur, cliquez sur **Copier les paramètres dans toutes les interfaces**.

Mappage de priorités CoS/802.1p aux files d'attente

La priorité d'un paquet arrivant sur une interface peut être identifiée par une valeur de priorité IEEE 802.1p dans l'en-tête des trames Ethernet. 802.1p spécifie huit niveaux de priorité (de 0 à 7). Utilisez la page *CoS/802.1p vers file d'attente* pour mapper ces niveaux de priorité aux quatre files d'attente CoS afin de *guider* les paquets vers la file d'attente de sortie appropriée. La file d'attente 1 est celle qui dispose de la priorité la plus basse, tandis que la priorité la plus haute est affectée à la file d'attente 4.

REMARQUE Le mappage des niveaux de priorité CoS/802.1p aux files d'attente est configuré pour chaque interface. Configurez ces valeurs de mappage sur l'interface entrante.

Pour mapper des valeurs de priorité 802.1p aux files d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service > CoS/802.1p vers file d'attente** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez le port ou LAG à configurer.

ÉTAPE 3 Pour chaque classe de service 802.1p, sélectionnez une file d'attente dans la liste File d'attente de sortie. La file d'attente 1 est celle qui dispose de la priorité la plus basse, tandis que la priorité la plus haute est affectée à la file d'attente 4.

ÉTAPE 4 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

ÉTAPE 5 Pour appliquer ces mappages à toutes les autres interfaces du commutateur, cliquez sur **Copier les paramètres dans toutes les interfaces**.

REMARQUE Si vous cliquez sur **Restaurer les valeurs par défaut**, les mappages suivants sont appliqués à toutes les interfaces.

Priorité 802.1p	File d'attente de sortie
0	1
1	1
2	2
3	3
4	3
5	4
6	4
7	4

Mappage de la priorité IP aux files d'attente

La priorité d'un paquet arrivant sur une interface peut être identifiée par le champ Type de service (ToS) d'un en-tête de paquet IP. Huit niveaux de priorité sont définis (de 0 à 7). Vous pouvez utiliser la page *Priorité IP sur file d'attente* pour mapper ces valeurs aux quatre files d'attente CoS afin de guider les paquets vers la file d'attente de sortie appropriée. La file d'attente 1 est celle qui dispose de la priorité la plus basse, tandis que la priorité la plus haute est affectée à la file d'attente 4.

REMARQUE Le mappage de la priorité IP aux files d'attente est configuré par interface. Configurez ces valeurs de mappage sur l'interface entrante.

Pour mapper des valeurs de priorité IP aux files d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service > Priorité IP sur file d'attente** dans la fenêtre de navigation.

ÉTAPE 2 Sélectionnez le port ou LAG à configurer.

ÉTAPE 3 Pour chaque valeur de priorité IP, sélectionnez une file d'attente dans la liste File d'attente de sortie. La file d'attente 1 est celle qui dispose de la priorité la plus basse, tandis que la priorité la plus haute est affectée à la file d'attente 4.

ÉTAPE 4 Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Pour appliquer ces mappages à toutes les autres interfaces du commutateur, cliquez sur **Copier les paramètres dans toutes les interfaces**.

REMARQUE Si vous cliquez sur **Restaurer les valeurs par défaut**, les mappages suivants sont appliqués à toutes les interfaces.

Priorité IP	File d'attente de sortie
0	1
1	1
2	2
3	3
4	3
5	4
6	3
7	3

Mappage de valeurs DSCP aux files d'attente

La priorité d'un paquet arrivant sur une interface peut être identifiée par la valeur DSCP (Differentiated Services Code Point) d'un en-tête de paquet IP. Le champ DSCP IP peut contenir une des 64 valeurs possibles, comprises entre 0 et 63. Vous pouvez utiliser la page *DSCP vers file d'attente* pour mapper ces valeurs aux quatre files d'attente de sortie. La file d'attente 1 est celle qui dispose de la priorité la plus basse, tandis que la priorité la plus haute est affectée à la file d'attente 4.

Les paramètres de mappage DSCP sont appliqués globalement à l'ensemble des ports.

Pour mapper des valeurs DSCP aux files d'attente :

-
- ÉTAPE 1** Cliquez sur **Qualité de service > DSCP vers file d'attente** dans la fenêtre de navigation.
 - ÉTAPE 2** Pour chaque valeur DSCP d'entrée, sélectionnez une file d'attente dans la liste File d'attente de sortie. La file d'attente 1 est celle qui dispose de la priorité la plus basse, tandis que la priorité la plus haute est affectée à la file d'attente 4.
 - ÉTAPE 3** Cliquez sur **Appliquer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.
-

REMARQUE Si vous cliquez sur **Restaurer les valeurs par défaut**, les mappages suivants sont appliqués à toutes les interfaces.

Valeur DSCP	File d'attente de sortie
00-07	1
08-15	1
16-23	2
24-31	3
32-39	3
40-47	4
48-55	3
56-63	3

Définition de profils de limitation de débit

La fonction de limitation de débit vous permet de définir un débit de trafic entrant maximal pour un port. Lorsque le débit de données dépasse le débit configuré, le commutateur abandonne tout trafic supplémentaire en provenance du port. Les limites de débit sont appliquées par port.

Pour appliquer des limites de débit, commencez par utiliser cette page pour créer un ou plusieurs profils de limitation de débit. Les profils spécifient les critères qui déterminent à quel moment la limite de débit est dépassée. Vous affectez ensuite des profils de limitation de débit aux interfaces (consultez la section [Application de profils de limitation de débit à des interfaces](#)).

Pour ajouter une entrée à la table Profil de limitation de débit :

- ÉTAPE 1** Cliquez sur **Qualité de service > Profil de limitation de débit** dans la fenêtre de navigation.
- ÉTAPE 2** Cliquez sur **Ajouter**.
- ÉTAPE 3** Configurez les paramètres suivants :
 - **ID de profil** : spécifiez un nombre compris entre 1 et 64 pour identifier le profil.

- **CIR** : spécifiez le débit minimum garanti, qui correspond au débit de transmission des données. La moyenne du débit est établie au-dessus d'un incrément de temps minimal. La plage est comprise entre 64 et 1 048 576 Kbit/s.
- **CBS** : spécifiez une taille de rafale garantie, qui correspond à la quantité garantie de bande passante pour le trafic par rafale sur le port. La plage est comprise entre 4 et 16 384 Kbit/s.

ÉTAPE 4 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Application de profils de limitation de débit à des interfaces

Si vous avez créé un ou plusieurs profils de limitation de débit, vous pouvez utiliser cette page pour les affecter à des interfaces. Consultez la section [Définition de profils de limitation de débit](#) pour obtenir des instructions sur la création de profils.

Pour appliquer un profil de limitation de débit à une interface.

ÉTAPE 1 Cliquez sur **Qualité de service > Limitation de débit de l'interface** dans la fenêtre de navigation.

ÉTAPE 2 Utilisez la liste Type d'interface pour afficher les ports ou LAG dans la table Limitation de débit de l'interface.

ÉTAPE 3 Sélectionnez l'interface à configurer et cliquez sur **Modifier**.

ÉTAPE 4 Ajoutez ou supprimez un profil :

- Pour affecter un profil à cette interface, cliquez sur l'ID de profil dans la liste Disponibles, puis cliquez sur la flèche droite pour le déplacer vers la liste Sélectionnés. Un seul profil pouvant être affecté à un port, tous les profils disparaissent de la liste Disponibles.
- Pour supprimer un profil, cliquez sur l'ID de profil dans la liste Sélectionnés, puis cliquez sur la flèche gauche pour le déplacer vers la liste Disponibles. Tous les profils s'affichent dans la liste Sélectionnés.

ÉTAPE 5 Cliquez sur **Appliquer**, puis sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Mise en forme du trafic

Vous pouvez utiliser la page *Mise en forme du trafic* pour lisser le débit de sortie des paquets. Vous pouvez configurer le débit de sortie maximal de chaque port et LAG, exprimé en pourcentage de la bande passante. Lorsque le débit du trafic atteint cette limite, les paquets excédentaires sont conservés dans une file d'attente, puis programmés en vue d'une transmission ultérieure sur des incréments de temps.

Pour configurer la mise en forme du trafic sur un port ou un LAG :

- ÉTAPE 1** Cliquez sur **Qualité de service** > **Mise en forme du trafic** dans la fenêtre de navigation.
- ÉTAPE 2** Utilisez le menu **Type d'interface** pour afficher les ports ou LAG dans la table Paramètres de mise en forme du trafic.
- ÉTAPE 3** Sélectionnez l'interface à configurer et cliquez sur **Modifier**.
- ÉTAPE 4** Pour le port ou LAG sélectionné, entrez la limite de débit de sortie en pourcentage de la bande passante totale. Cliquez sur **Appliquer**.
- ÉTAPE 5** Répétez si nécessaire l'étape précédente pour affecter l'utilisation de la bande passante à d'autres ports et LAG.
- ÉTAPE 6** Une fois que vous avez terminé, cliquez sur **Fermer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration d'exécution.

Cisco, Cisco Systems et les logos Cisco et Cisco Systems sont des marques commerciales ou déposées de Cisco et/ou de ses succursales aux États-Unis et dans d'autres pays. Toutes les autres marques commerciales mentionnées dans ce document ou sur ce site Web appartiennent à leurs propriétaires respectifs. L'utilisation du mot « partenaire » n'implique pas de relation de partenariat entre Cisco et une autre société. (1002R)