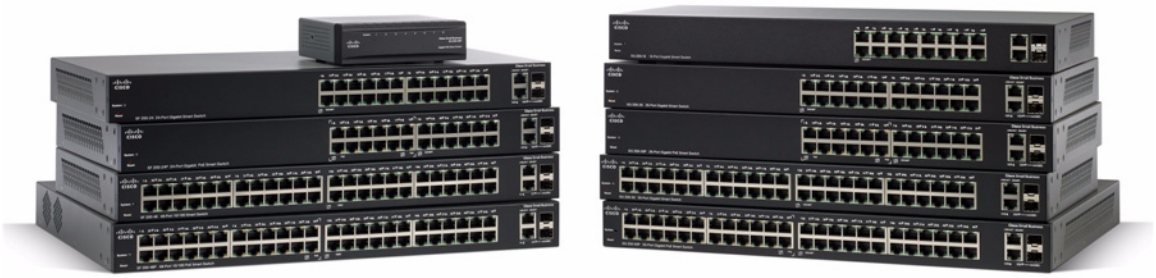

GUIDE D'ADMINISTRATION

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

Sommaire

1

Mise en route

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

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

Démarrage de l'utilitaire Web de configuration de commutateur

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

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

Les restrictions suivantes s'appliquent aux navigateurs :

- Si vous utilisez d'anciennes versions d'Internet Explorer, vous ne pouvez pas utiliser directement une adresse IPv6 pour accéder au commutateur. Vous pouvez néanmoins utiliser le serveur DNS (Domain Name System) 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 de configuration

Pour lancer l'utilitaire de configuration Web :

ÉTAPE 1 Ouvrez un navigateur Web.

ÉTAPE 2 Saisissez l'adresse IP du commutateur que vous configurez dans la barre d'adresse du navigateur puis appuyez sur **Entrée**. La page *Connexion* s'ouvre.

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

Connexion

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

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

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

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

ÉTAPE 1 Saisissez le nom d'utilisateur/le mot de passe. Le mot de passe peut comporter au maximum 64 caractères ASCII. Les règles de complexité du mot de passe sont

décrites à la section **Définition des règles de complexité du mot de passe** du chapitre **Configuration de la sécurité**.

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

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

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

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

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

Si vous avez saisi un nom d'utilisateur ou un mot de passe erroné, un message d'erreur apparaît et la page *Connexion* reste affichée sur la fenêtre.

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

HTTP/HTTPS

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

Pour savoir comment configurer HTTPS, reportez-vous à la section **Paramètres d'authentification de serveur SSL**.

Expiration du mot de passe

La page *Nouveau mot de passe* s'affiche :

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

Déconnexion

Par défaut, l'application se déconnecte au bout de dix minutes d'inactivité. Vous pouvez modifier cette valeur par défaut en suivant la procédure décrite à la section **Définition du délai d'expiration en cas de session inactive** du chapitre **Informations et opérations administratives générales**.

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

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

Lorsque le commutateur détecte automatiquement un périphérique, tel qu'un téléphone IP (voir **Chapitre 10, « Qu'est-ce qu'un port intelligent ? »**), il configure le port de manière adéquate pour ce périphérique. Ces commandes de configuration sont écrites dans le fichier de Configuration d'exécution. L'icône Enregistrer se met alors à clignoter lorsque vous vous connectez, même si vous n'avez apporté aucune modification à la configuration.

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

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

En cas d'expiration du délai ou si vous vous déconnectez intentionnellement du système, un message apparaît et la page *Connexion* s'ouvre avec un message spécifiant l'état de déconnexion. Une fois que vous vous êtes connecté, l'application retourne à la page initiale.

La page initiale qui s'affiche dépend de l'option « Ne pas afficher cette page au démarrage » de la page *Mise en route.* Si vous n'avez pas sélectionné cette option, la page initiale correspond à la page *Mise en route.* Si vous avez sélectionné cette option, la page initiale est la page *Récapitulatif système*.

Configuration du commutateur - Démarrage rapide

Pour simplifier la configuration du commutateur, vous pouvez accéder rapidement aux pages les plus fréquemment utilisées à l'aide des liens fournis à la page *Mise en route*.

Liens de la page Mise en route

Catégorie	Nom du lien (sur la page)	Page correspondante
	Applications et service de gestion des changements	Page *Services TCP/UDP*
	Modifier l'adresse IP de l'appareil	Page *Interface IPv4*
	Créer un VLAN	Page *Créer un VLAN*
	Configurer les paramètres de port	Page *Paramètres des ports*
État de l'appareil	Récapitulatif système	Page *Récapitulatif système*
	Statistiques des ports	Page *Interface*
	Statistiques RMON	Page *Statistiques*
	Afficher le journal	Page *Mémoire RAM*
Accès rapide	Modifier le mot de passe de l'appareil	Page *Comptes d'utilisateur*

Liens de la page Mise en route (Suite)

Catégorie	Nom du lien (sur la page)	Page correspondante
	Mettre à niveau le logiciel de l'appareil	Page *Mettre à niveau/ sauvegarder micrologiciel/ langue*
	Configuration de sauvegarde de l'appareil	Page *Télécharger/ sauvegarder configuration/ journal*
	Configurer la QoS	Page *Propriétés de QoS*
	Configurer la mise en miroir des ports	Page *Mise en miroir des ports et VLAN*

La page Mise en route comporte deux liens qui vous redirigent vers des pages Web Cisco. Vous y trouverez des informations supplémentaires. Cliquez sur le lien **Assistance** pour accéder à la page d'assistance produit du commutateur et cliquez sur le lien **Forums** pour accéder à la page de communauté d'assistance Cisco Small Business.

Conventions de nommage de l'interface

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

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

Navigation dans les fenêtres

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

En-tête d'application

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

Liens d'application

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

Liens d'application (Suite)

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

Boutons de gestion

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

Boutons de gestion

Nom du bouton	Description
	Servez-vous du menu déroulant pour configurer le nombre d'entrées par page.
	Indique un champ obligatoire.
Ajout	Cliquez sur ce bouton pour afficher la rubrique *Ajouter* correspondante et ajouter une entrée à une table. Saisissez les informations requises et cliquez sur **Appliquer** pour les enregistrer dans la Configuration d'exécution. Cliquez sur **Fermer** pour retourner à la page principale. Cliquez sur **Enregistrer** pour afficher la page *Copier/enregistrer la configuration* et enregistrer la Configuration d'exécution dans le type de fichier Configuration de démarrage sur le commutateur.
Appliquer	Cliquez pour appliquer des modifications à la Configuration d'exécution sur le commutateur. En cas de redémarrage du commutateur, la Configuration d'exécution est perdue, sauf si elle a été enregistrée dans le type de fichier Configuration de démarrage ou dans un autre type de fichier. Cliquez sur **Enregistrer** pour afficher la page *Copier/enregistrer la configuration* et enregistrer la Configuration d'exécution dans le type de fichier Configuration de démarrage sur le commutateur.
Annuler	Cliquez sur réinitialiser les modifications apportées à la page.
Effacer les compteurs de toutes les interfaces	Cliquez sur ce bouton pour effacer les compteurs de statistiques de toutes les interfaces.

Boutons de gestion (Suite)

Nom du bouton	Description
Effacer les compteurs de l'interface	Cliquez sur ce bouton pour effacer les compteurs de statistiques de l'interface sélectionnée.
Effacer les journaux	Efface les fichiers journaux.
Effacer la table	Efface les entrées de la table.
Fermer	Permet de revenir à la page principale. Un message s'affiche si des modifications n'ont pas été appliquées à la Configuration d'exécution.
Copier les paramètres	Une table comporte généralement une ou plusieurs entrées contenant des paramètres de configuration. Au lieu de modifier chaque entrée individuellement, il est possible de modifier une entrée, puis de la copier sur plusieurs autres, comme décrit ci-dessous : 1. Sélectionnez l'entrée à copier. Cliquez sur **Copier les paramètres** pour afficher la fenêtre contextuelle. 2. Saisissez les numéros des entrées de destination dans le champ de destination. 3. Cliquez sur **Appliquer** pour enregistrer les modifications et sur **Fermer** pour retourner à la page principale.
Suppr.	Après avoir sélectionné une entrée dans la table, cliquez sur **Supprimer** pour la supprimer.
Détails	Cliquez sur ce bouton pour afficher les détails de l'entrée sélectionnée.
Modif	Sélectionnez l'entrée et cliquez sur **Modifier**. La page *Modifier* s'ouvre et l'entrée peut être modifiée. 1. Cliquez sur **Appliquer** pour enregistrer les modifications dans la Configuration d'exécution. 2. Cliquez sur **Fermer** pour retourner à la page principale.
OK	Saisissez les critères de filtrage de requêtes et cliquez sur **OK**. Les résultats s'affichent sur la page.

Boutons de gestion (Suite)

Nom du bouton	Description
Test	Cliquez sur **Tester** pour effectuer les tests liés.

2

Affichage des statistiques

Cette section décrit comment afficher les statistiques du commutateur.

Elle couvre les rubriques suivantes :

- **Affichage des interfaces Ethernet**
- **Affichage des statistiques Etherlike**
- **Affichage des statistiques EAP 802.1X**
- **Gestion du contrôle à distance (RMON)**

Affichage des interfaces Ethernet

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

Cette page est utile pour analyser la quantité de trafic envoyé et reçu, ainsi que sa dispersion (Monodiffusion ou unicast, Multidiffusion ou multicast et Diffusion ou broadcast).

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

ÉTAPE 1 Cliquez sur **État et statistiques** > **Interface**. La page *Interface* s'affiche.

ÉTAPE 2 Saisissez les paramètres.

- **Interface** : sélectionnez le type d'interface et l'interface spécifique pour laquelle les statistiques Ethernet doivent être affichées.
- **Taux d'actualisation** : sélectionnez la durée qui s'écoule avant l'actualisation des statistiques Ethernet de l'interface. Les options disponibles sont les suivantes :
  - *Aucune actualisation* : les statistiques ne sont pas actualisées.
  - *15s* : les statistiques sont actualisées toutes les 15 secondes.

- *30s* : les statistiques sont actualisées toutes les 30 secondes.
- *60s* : les statistiques sont actualisées toutes les 60 secondes.

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

- **Total des octets :** octets reçus, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **Paquets de monodiffusion :** paquets de monodiffusion corrects reçus.
- **Paquets de multidiffusion :** paquets de multidiffusion corrects reçus.
- **Paquets de diffusion :** paquets de diffusion corrects reçus.
- **Paquets avec erreurs :** paquets avec erreurs reçus.

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

- **Total des octets :** octets transmis, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **Paquets de monodiffusion :** paquets de monodiffusion corrects transmis.
- **Paquets de multidiffusion :** paquets de multidiffusion corrects transmis.
- **Paquets de diffusion :** paquets de diffusion corrects transmis.

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs de l'interface affichée.
- Cliquez sur **Effacer les compteurs de toutes les interfaces** pour effacer les compteurs de l'ensemble des interfaces.

Affichage des statistiques Etherlike

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

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

ÉTAPE 1 Cliquez sur **État et statistiques** > **Etherlike**. La page *Etherlike* s'affiche.

ÉTAPE 2 Saisissez les paramètres.

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

Les champs sont affichés pour l'interface sélectionnée.

- **Erreurs FCS (Frame Check Sequence)** : trames reçues ayant échoué aux contrôles de redondance cyclique (CRC).
- **Trames de collisions individuelles** : trames impliquées dans une collision individuelle, mais ayant été transmises avec succès.
- **Collisions tardives** : collisions ayant été détectées après les 512 premiers octets de données.
- **Collisions excessives** : nombre de transmissions rejetées dues à des collisions excessives.
- **Paquets de taille excessive** : paquets de plus de 2 000 octets reçus.
- **Erreurs de réception MAC internes :** trames rejetées en raison d'erreurs de destination.
- **Trames de pause reçues** : trames de pause de contrôle de flux reçues.
- **Trames de pause transmises** : trames de pause de contrôle de flux transmises à partir de l'interface sélectionnée.

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs de l'interface sélectionnée.
- Cliquez sur **Effacer les compteurs de toutes les interfaces** pour effacer les compteurs de l'ensemble des interfaces.

Affichage des statistiques EAP 802.1X

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

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

ÉTAPE 1 Cliquez sur **État et statistiques** > **802.1x EAP**. La page *802.1x EAP* s'ouvre.

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

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

Les valeurs sont affichées pour l'interface sélectionnée.

- **Trames EAPOL reçues :** trames EAPOL valides reçues sur le port.
- **Trames EAPOL transmises :** trames EAPOL valides transmises par le port.
- **Trames EAPOL de début reçues :** affiche le nombre de trames EAPOL de début qui ont été reçues sur le port.
- **Trames EAPOL de déconnexion reçues :** affiche le nombre de trames EAPOL de déconnexion qui ont été reçues sur le port.
- **Trames ID/de réponse EAP reçues :** trames ID/de réponse EAP reçues sur le port.
- **Trames de réponse EAP reçues :** trames de réponse EAP reçues par le port (autres que les tramesID/de réponse).
- **Trames ID/de demande EAP transmises :** trames ID/de demande EAP transmises par le port.

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

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs de l'interface sélectionnée.
- Cliquez sur **Effacer les compteurs de toutes les interfaces** pour effacer les compteurs de l'ensemble des interfaces.

Gestion du contrôle à distance (RMON)

RMON (Remote Networking Monitoring, contrôle réseau à distance) permet au commutateur de surveiller les statistiques du trafic de manière proactive pendant une période donnée.

Grâce à cette fonctionnalité, vous pouvez afficher les statistiques actuelles (étant donné que les valeurs du compteur ont été effacées).

Affichage des statistiques RMON

La page *Statistiques* affiche des informations détaillées sur la taille des paquets, ainsi que des informations sur les erreurs de couche physique. Les informations affichées sont conformes à la norme RMON. Un paquet surdimensionné est défini en tant que trame Ethernet avec les critères suivants :

- La longueur du paquet est supérieure à la taille en octets MRU.
- Un événement de collision n'a pas été détecté.

- Un événement de collision tardive n'a pas été détecté.
- Un événement d'erreur de réception (Rx) n'a pas été détecté.
- Le paquet a un CRC valide.

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

ÉTAPE 1 Cliquez sur **État et statistiques > RMON** > **Statistiques**. La page *Statistiques* s'affiche.

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

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

Les statistiques sont affichées pour l'interface sélectionnée.

- **Octets reçus** : nombre d'octets reçus, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **Événements d'abandon** : nombre de paquets ayant été abandonnés.
- **Paquets reçus** : nombre de paquets corrects reçus, dont les paquets de multidiffusion et de diffusion.
- **Paquets de diffusion reçus** : nombre de paquets de diffusion corrects reçus. Ce nombre n'inclut pas les paquets de multidiffusion.
- **Paquets de multidiffusion reçus** : nombre de paquets de multidiffusion corrects reçus.
- **Erreurs d'alignement et CRC** : nombre d'erreurs d'alignement et CRC qui se sont produites.
- **Paquets de taille insuffisante** : nombre de paquets de taille insuffisante (moins de 64 octets) reçus.
- **Paquets de taille excessive** : nombre de paquets de taille excessive (plus de 2 000 octets) reçus.
- **Fragments :** nombre de fragments (paquets de moins de 64 octets, à l'exception des bits de synchronisation, mais incluant les octets FCS) reçus.
- **Jabotages** : nombre total de paquets reçus ayant une longueur supérieure à 1 632 octets. Ce nombre exclut les bits de synchronisation, mais inclut les octetsFCS qui comportaient une séquence FCS (Frame Check Sequence) erronée avec un nombre entier d'octets (Erreur FCS) ou une séquence FCS

erronée avec un nombre non entier d'octets (Erreur d'alignement). Un paquet de jabotage est défini en tant que trame Ethernet respectant les critères suivants :

- La longueur des données du paquet est supérieure à la MRU.
- Le paquet a un CRC non valide.
- Un événement d'erreur de réception (Rx) n'a pas été détecté.

- **Collisions :** nombre de collisions reçues. Si les trames Jumbo sont activées, le seuil des trames de jabotage est augmenté de façon à correspondre à la taille maximale des trames Jumbo.
- **Trames de 64 octets :** nombre de trames de 64 octets reçues.
- **Trames de 65 à 127 octets :** nombre de trames de 65 à 127 octets reçues.
- **Trames de 128 à 255 octets :** nombre de trames de 128 à 255 octets reçues.
- **Trames de 256 à 511 octets :** nombre de trames de 256 à 511 octets reçues.
- **Trames de 512 à 1 023 octets :** nombre de trames de 512 à 1 023 octets reçues.
- **Trames supérieures à 1 024 octets :** nombre de trames de 1 024 à 2 000 octets et de trames Jumbo reçues.

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs de l'interface sélectionnée.
- Cliquez sur **Effacer les compteurs de toutes les interfaces** pour effacer les compteurs de l'ensemble des interfaces.

3

Gestion des journaux système

Cette section décrit la fonction Journal système, qui permet au commutateur de générer plusieurs journaux indépendants. Chaque journal correspond à un ensemble de messages décrivant les événements système.

Le commutateur génère les journaux locaux suivants :

- Journal envoyé à l'interface de la console
- Journal enregistré dans une liste cyclique d'événements journalisés dans la mémoire RAM et effacé lors du redémarrage du commutateur
- Journal enregistré dans un fichier journal cyclique enregistré dans la mémoire Flash et conservé d'un redémarrage à l'autre

Vous pouvez en outre envoyer des messages à des serveurs SYSLOG distants sous la forme de messages SYSLOG.

Cette section contient les rubriques suivantes :

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

Définition des paramètres de journalisation système

Vous pouvez activer ou désactiver la journalisation sur la page *Paramètres des journaux* et indiquer si vous souhaitez ou non regrouper les messages de journaux.

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

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

- *Urgence* : le système n'est pas utilisable.
- *Alerte* : une action est requise.
- *Critique* : le système est dans un état critique.
- *Erreur* : le système subit une condition d'erreur.
- *Avertissement* : un avertissement système a été généré.
- *Remarque* : le système fonctionne correctement mais une remarque système a été générée.
- *Information* : informations du périphérique.
- *Débogage* : fournit des informations détaillées sur un événement.

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

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

Par exemple, si **Avertissement** est sélectionné, tous les niveaux de sévérité de type **Avertissement** et plus élevés sont enregistrés dans le journal (Urgence, Alerte, Critique, Erreur et Avertissement). Aucun événement dont le niveau de sévérité est inférieur à **Avertissement** n'est enregistré (Remarque, Informatif et Débogage).

Pour définir des paramètres de journalisation globaux :

ÉTAPE 1 Cliquez sur **Administration** > **Journal système** > **Paramètres des journaux**. La page *Paramètres des journaux* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **Journalisation :** sélectionnez cette option pour activer la journalisation des messages.
- **Agrégateur Syslog :** sélectionnez cette option pour activer l'agrégation des messages « trap » et SYSLOG. Si elle est activée, les messages « trap » et les messages SYSLOG identiques et contigus sont agrégés pendant le temps d'agrégation max. spécifié et envoyés dans un même message. Les messages agrégés sont envoyés dans l'ordre de leur arrivée. Chaque message indique le nombre de fois où il a été agrégé.
- **Temps d'agrégation max.** : saisissez la période pendant laquelle les messages SYSLOG sont agrégés.
- **Journalisation de la mémoire RAM :** sélectionnez les niveaux de sévérité des messages à journaliser dans la RAM.
- **Journalisation de la mémoire Flash :** sélectionnez les niveaux de sévérité des messages à journaliser dans la mémoire Flash.

ÉTAPE 3 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Définition des paramètres de journalisation distante

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

Pour définir les serveurs SYSLOG :

ÉTAPE 1 Cliquez sur **Administration** > **Journal système** > **Serveurs de journalisation distants**. La page *Serveurs de journalisation distants* s'ouvre.

Cette page affiche la liste des serveurs de journalisation distants.

ÉTAPE 2 Cliquez sur **Ajouter**. La page *Ajouter serveur de journalis. distant* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

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

ÉTAPE 4 Cliquez sur **Appliquer**. La page *Ajouter serveur de journalis. distant* se ferme ; le serveur SYSLOG est ajouté et le fichier de Configuration d'exécution est mis à jour.

Affichage des journaux de la mémoire

Le commutateur peut enregistrer des informations dans les journaux suivants :

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

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

Mémoire RAM

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

Pour afficher les entrées du journal, cliquez sur **État et statistiques** > **Afficher le journal** > **Mémoire RAM**. La page *Mémoire RAM* s'ouvre.

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

Cette page affiche les champs suivants :

- **Index du journal :** numéro de l'entrée dans le journal.
- **Heure de journalisation :** heure à laquelle le message a été généré.
- **Sévérité**: niveau de sévérité de l'événement.
- **Description :** message texte décrivant l'événement.

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

Mémoire Flash

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

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

Cette page affiche les champs suivants :

- **Index du journal :** numéro de l'entrée dans le journal.
- **Heure de journalisation :** heure à laquelle le message a été généré.
- **Sévérité** : niveau de sévérité de l'événement.
- **Description :** message texte décrivant l'événement.

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

4

Gestion des fichiers système

Cette section se concentre sur la gestion des fichiers système.

Les sujets suivants sont traités :

- **Types de fichiers système**
- **Mettre à niveau/sauvegarder micrologiciel/langue**
- **Téléchargement ou sauvegarde d'une configuration ou d'un journal**
- **Affichage des propriétés des fichiers de configuration**
- **Copie des fichiers de configuration**
- **Configuration automatique DHCP**

Types de fichiers système

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

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

Les méthodes de transfert de fichiers disponibles sont les suivantes :

- Copie interne.
- HTTP/HTTPS qui utilise la structure fournie par le navigateur.
- Client TFTP, nécessitant un serveur TFTP.

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

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

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

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

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

Fichiers et types de fichiers

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

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

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

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

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

  La Configuration de démarrage est conservée dans la mémoire Flash et préservée à chaque redémarrage du commutateur. Lors du redémarrage, la Configuration de démarrage est copiée dans la RAM et identifiée comme étant la Configuration d'exécution.

- **Configuration miroir** : copie de la Configuration de démarrage, créée par le commutateur dans l'un des cas suivants :
  - le commutateur a fonctionné de façon continue pendant 24 heures ;
  - aucune modification n'a été apportée à la Configuration d'exécution au cours des dernières 24 heures ;
  - la Configuration de démarrage est identique à la Configuration d'exécution.

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

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

Actions des fichiers

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

- Mettre à niveau le micrologiciel ou le code de démarrage, ou remplacer une langue, comme décrit dans la section **Mettre à niveau/sauvegarder micrologiciel/langue**

- Enregistrer les fichiers de configuration présents dans le commutateur à un emplacement situé sur un autre appareil, comme décrit dans la section **Téléchargement ou sauvegarde d'une configuration ou d'un journal**
- Effacer les types de fichiers de Configuration de démarrage ou de Configuration de secours, comme décrit dans la section **Affichage des propriétés des fichiers de configuration**
- Copier un type de fichier de configuration dans un autre type de fichier de configuration, comme décrit dans la section **Copie des fichiers de configuration**
- Télécharger automatiquement un fichier de configuration depuis un serveur DHCP vers le commutateur, comme décrit dans la section **Configuration automatique DHCP**

Cette rubrique aborde les points suivants :

- **Mettre à niveau/sauvegarder micrologiciel/langue**
- **Téléchargement ou sauvegarde d'une configuration ou d'un journal**
- **Affichage des propriétés des fichiers de configuration**
- **Copie des fichiers de configuration**
- **Configuration automatique DHCP**

Mettre à niveau/sauvegarder micrologiciel/langue

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

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

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

- HTTP/HTTPS qui utilise la structure fournie par le navigateur
- TFTP qui nécessite un serveur TFTP

Si un nouveau fichier de langue a été chargé sur le commutateur, la langue correspondante peut être sélectionnée dans le menu déroulant. (Il n'est pas nécessaire de redémarrer le commutateur.)

Une seule image du micrologiciel est stockée sur le commutateur. Après le chargement d'un nouveau micrologiciel sur le commutateur, ce dernier doit être redémarré pour que le nouveau micrologiciel prenne effet. La page *Récapitulatif* continue à afficher l'image précédente tant que le commutateur n'a pas redémarré.

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

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

ÉTAPE 1 Cliquez sur **Administration** > **Gestion de fichiers** > **Mettre à niveau/sauvegarder micrologiciel/langue**. La page *Mettre à niveau/sauvegarder micrologiciel/langue* s'ouvre.

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

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

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

Sélectionnez l'une des actions suivantes :

- **Mode d'enregistrement Mettre à niveau** : spécifie que le type de fichier sur le commutateur doit être remplacé par une nouvelle version de ce type de fichier, qui est située sur un serveur TFTP.
- **Mode d'enregistrement Sauvegarder** : spécifie qu'une copie du type de fichier doit être enregistrée dans un fichier situé sur un autre appareil.

Renseignez les champs suivants :

- **Type de fichier** : sélectionnez le type de fichier de destination. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)
- **Définition du serveur TFTP** : indiquez si vous souhaitez spécifier le serveur TFTP par son adresse IP ou son nom de domaine.
- **Version IP** : indiquez si l'adresse utilisée est de type IPv4 oulPv6.

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

ÉTAPE 4 Si vous avez sélectionné **via HTTP/HTTPS**, vous pouvez uniquement procéder à la **mise à niveau**. Saisissez les paramètres décrits dans cette étape.

- **Type de fichier** : sélectionnez le type de fichier de configuration. Seuls les types de fichiers valides peuvent être sélectionnés. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.) Les types de fichiers suivants peuvent être mis à niveau :
  - *Image du micrologiciel* : sélectionnez cette option pour mettre à niveau l'image du micrologiciel.
  - *Langue* : sélectionnez cette option pour mettre à niveau le fichier de langue.
- **Nom du fichier** : cliquez sur **Parcourir** pour sélectionner un fichier ou saisissez le chemin et le nom du fichier source à utiliser pour le transfert.

ÉTAPE 5 Cliquez sur **Appliquer** ou sur **Terminé**. Le fichier est mis à niveau ou sauvegardé.

Téléchargement ou sauvegarde d'une configuration ou d'un journal

La page *Télécharger/sauvegarder configuration/journal* s'ouvre.

- Sauvegarde de fichiers de configuration ou de journaux depuis le commutateur vers un périphérique externe.
- Restauration de fichiers de configuration depuis un périphérique externe vers le commutateur.

REMARQUE

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

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

Lorsque vous procédez à une restauration vers la Configuration de démarrage, le commutateur doit être redémarré pour que cette Configuration puisse être utilisée en tant que Configuration d'exécution. Vous pouvez redémarrer le commutateur en utilisant le processus décrit dans la section **Redémarrage du commutateur**.

Pour sauvegarder ou restaurer le fichier de configuration système :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion de fichiers** > **Télécharger/sauvegarder configuration/journal**. La page *Télécharger/sauvegarder configuration/journal* s'ouvre.

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

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

Sélectionnez le **Mode d'enregistrement** Télécharger ou Sauvegarder.

Mode d'enregistrement Télécharger : spécifie que le fichier stocké sur un autre appareil remplace un type de fichier sur le commutateur. Renseignez les champs suivants :

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

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

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

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

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

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

e. **Serveur TFTP** : saisissez l'adresse IP du serveur TFTP.

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

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

Mode d'enregistrement Sauvegarder : spécifie qu'un type de fichier doit être copié vers un fichier situé sur un autre appareil. Renseignez les champs suivants :

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

b. **VersionIP** : indiquez si l'adresse utilisée est de type IPv4 oulPv6.

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

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

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

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

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

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

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

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

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

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

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

Sélectionnez l'**Enregistrement**.

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

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

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

c. Cliquez sur **Appliquer**. Le fichier est transféré de l'autre appareil vers le commutateur.

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

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

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

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

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

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

Affichage des propriétés des fichiers de configuration

La page *Propriétés des fichiers de configuration* vous permet de savoir quand les différents fichiers de configuration du système ont été créés. Elle permet également de supprimer les fichiers de Configuration de démarrage et de Configuration de secours. Vous ne pouvez en revanche pas modifier les autres types de fichiers de configuration.

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

ÉTAPE 1 Cliquez sur **Administration** > **Gestion de fichiers** > **Propriétés des fichiers de configuration**. La page *Propriétés des fichiers de configuration* s'ouvre.

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

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

Cette page contient les champs suivants :

- **Nom du fichier de configuration** : affiche le type de fichier.
- **Heure de création** : affiche la date et l'heure de la modification du fichier.

Copie des fichiers de configuration

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

ATTENTION Sauf si la Configuration d'exécution est copiée sur la Configuration de démarrage ou sur un autre fichier de configuration, toutes les modifications apportées depuis la dernière copie du fichier seront perdues lors du redémarrage du commutateur.

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

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

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

ÉTAPE 1 Cliquez sur **Administration** > **Gestion de fichiers** > **Copier/enregistrer la configuration**. La page *Copier/enregistrer la configuration* s'ouvre.

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

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

- Si vous sauvegardez un fichier de configuration, sélectionnez un des formats suivants.
  - **Exclure** : ne pas inclure les données sensibles à la sauvegarde.
  - **Chiffré** : inclure les données sensibles dans la sauvegarde, mais en les cryptant.
  - **Texte en clair** : inclure les données sensibles dans la sauvegarde sous forme de texte en clair.

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

ÉTAPE 4 Le champ **Clign. icône d'engistrement** indique si une icône clignote lorsque certaines données ne sont pas enregistrées. Pour activer/désactiver cette fonctionnalité, cliquez sur **Désactiver/Activer clignotement icône d'enr.**

ÉTAPE 5 Cliquez sur **Appliquer**. Le fichier est copié.

Configuration automatique DHCP

Le commutateur prend en charge la configuration automatique DHCP, qui permet de transmettre des informations de configuration (y compris l'adresse IP d'un serveur et un nom de fichier) aux hôtes d'un réseau TCP/IP. La fonctionnalité de configuration automatique permet à un commutateur de se baser sur ce protocole pour télécharger des fichiers de configuration depuis un serveur TFTP.

Par défaut, le commutateur est activé en tant que client DHCP lorsque la configuration automatique est activée.

Déclenchement de la configuration automatique DHCP

La configuration automatique se déclenche dans les cas suivants :

- Après un redémarrage quand une adresse IP est allouée ou renouvelée dynamiquement (via DHCP)
- Lors d'une demande explicite de renouvellement DHCP et si le commutateur et le serveur sont configurés pour agir ainsi
- Lors du renouvellement automatique du bail DHCP

Nom/adresse du serveur

Vous pouvez spécifier l'adresse IP ou le nom du serveur TFTP. Ce serveur est utilisé si aucune adresse IP de serveur n'a été spécifiée dans le message DHCP. Ce message DHCP correspond au message d'offre DHCP provenant du serveur DHCP. Les options possibles sont les options Bootp sname et siaddr, et les options DHCP 150 ou 66. Il s'agit d'un paramètre facultatif.

Nom du fichier de configuration de secours

Vous pouvez spécifier le nom du fichier de configuration de secours. Celui-ci est utilisé si aucun nom de fichier n'a été spécifié dans le message DHCP. Il s'agit d'un paramètre facultatif.

Processus de configuration automatique

Lorsque le processus de configuration automatique est déclenché, la séquence suivante d'événements se produit :

- Vous accédez au serveur DHCP pour obtenir l'adresse IP du serveur TFTP et le nom du fichier de configuration. Ces paramètres sont transférés dans les paramètres des options DHCP.
- Si une adresse IP n'a pas été fournie par le serveur DHCP, l'adresse du serveur de secours est utilisée (si l'utilisateur a choisi une telle action).
- Si une adresse IP n'a pas été fournie par le serveur DHCP et si l'adresse du serveur TFTP de secours n'est pas renseignée, le processus de configuration automatique est interrompu.

  REMARQUE Dans les deux puces précédentes, l'adresse IP fait référence à l'adresse IP ou au nom d'hôte du serveur TFTP.
- Si le nom du fichier de configuration a été fourni par le serveur DHCP, le protocole de copie (TFTP) est sélectionné comme décrit dans la section **Configuration automatique DHCP**.
- Si le nom du fichier de configuration n'a pas été fourni par le serveur DHCP, le nom du fichier de configuration de secours est utilisé.
- Si le nom du fichier de configuration n'a pas été fourni par le serveur DHCP et si le nom du fichier de configuration de secours n'est pas renseigné, le processus de configuration automatique est interrompu.

- Le fichier est téléchargé sur le serveur TFTP.

  Le téléchargement est réalisé seulement si le nouveau nom de fichier de configuration est différent du nom actuel (même si le fichier de configuration actuel est vide).

- Un message SYSLOG est généré pour confirmer que la configuration automatique a été effectuée avec succès.

Définition de la configuration automatique DHCP

La page *Configuration automatique DHCP* permet d'effectuer les actions suivantes si des informations ne sont pas fournies dans un message DHCP :

- Activer la configuration automatique DHCP.
- Spécifier le protocole de téléchargement.
- Configurer le commutateur pour qu'il récupère les informations de configuration dans un fichier spécifique sur un serveur donné.

Notez les considérations suivantes se rapportant au processus de configuration automatique DHCP :

- Un fichier de configuration placé sur le serveur TFTP doit correspondre aux exigences en termes de forme et de format du fichier de configuration pris en charge. La forme et le format du fichier sont vérifiés mais la validité des *paramètres* de configuration n'est pas contrôlée avant son chargement dans la Configuration de démarrage.
- Pour s'assurer que la configuration des appareils fonctionne comme prévu et en raison de l'allocation d'adresses IP différentes pour chaque cycle de renouvellement DHCP, il est conseillé de lier les adresses IP à des adresses MAC dans la table des serveurs DHCP. Cela permet de garantir que chaque appareil dispose de sa propre adresse IP réservée ainsi que d'autres informations appropriées.

Pour définir la configuration automatique de serveurs DHCP :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion de fichiers** > **Configuration automatique DHCP**. La page *Configuration automatique DHCP* s'ouvre.

ÉTAPE 2 Saisissez les valeurs appropriées.

- **Configuration automatique via DHCP** : sélectionnez cette option pour activer la configuration automatique DHCP.

- **Définition du serveur de secours** : sélectionnez **Par adresse IP** ou **Par nom** pour configurer le serveur TFTP.

ÉTAPE 3 Saisissez les informations facultatives suivantes à utiliser si la configuration automatique DHCP n'est pas activée, ou si elle est activée mais si aucun fichier de configuration n'a été fourni par le serveur DHCP.

- **AdresseIP/Nom du serveur de secours** : saisissez l'adresse IP ou le nom du serveur à utiliser si aucune adresse IP de serveur n'a été spécifiée dans le message DHCP.
- **Nom du fichier de configuration de secours** : saisissez le chemin et le nom du fichier à utiliser si aucun nom de fichier de configuration n'a été spécifié dans le message DHCP.

La fenêtre affiche les éléments suivants :

- **Adresse IP du dernier serveur pour configuration automatique** : affiche l'adresse IP du dernier serveur TFTP utilisé pour effectuer une configuration automatique.
- **Dernier nom du fichier de configuration automatique** : affiche le dernier nom de fichier utilisé par le commutateur pour effectuer une configuration automatique.

  REMARQUE Le **Dernier nom du fichier de configuration automatique** est comparé aux informations provenant d'un serveur DHCP si une adresse IP est obtenue pour le commutateur. Si cette valeur ne correspond pas, le commutateur transfère le fichier de configuration du serveur identifié par le serveur DHCP vers le fichier de Configuration de démarrage, puis initie un redémarrage. Si les valeurs correspondent, aucune action n'est initiée.

ÉTAPE 4 Cliquez sur **Appliquer**. La fonctionnalité de configuration automatique DHCP est mise à jour dans la Configuration d'exécution.

5

Informations administratives générales

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

Elle couvre les rubriques suivantes :

- **Modèles de commutateurs**
- **Informations système**
- **Redémarrage du commutateur**
- **Surveillance de l'état et de la température du ventilateur**
- **Définition du délai d'expiration en cas de session inactive**
- **Envoi d'une requête Ping à un hôte**

Modèles de commutateurs

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

En mode système Couche 2, le commutateur transfère les paquets en tant que pont tenant compte du VLAN. En mode Couche 3, le commutateur effectue à la fois un routage IPv4 et un pontage tenant compte du VLAN.

REMARQUE Les conventions de port suivantes sont utilisées :

- GE correspond aux ports Gigabit Ethernet (10/100/1 000).
- FE correspond aux ports Fast Ethernet (10/100).

La table suivante décrit les divers modèles, le nombre et le type de port qu'ils proposent, de même que des informations sur l'alimentation PoE (Power over Ethernet).

Modèles de commutateurs intelligents

Nom du modèle	ID du produit (PID)	Description des ports de l'appareil	Puissance dédiée auPoE	Nbre de ports gérant PoE
SG200-18	SLM2016T	16 ports GE + 2 ports GE combinés spécifiques		
SG200-26	SLM2024T	24 ports GE + 2 ports GE combinés spécifiques		
SG200-26P	SLM2024PT	24 ports GE + 2 ports GE combinés spécifiques	100 W	12 ports FE1-FE6, FE13 - FE18
SG200-50	SLM2048T	48 ports GE + 2 ports GE combinés spécifiques		
SG200-50P	SLM2048PT	48 ports GE + 2 ports GE combinés spécifiques	180 W	24 ports FE1-FE12, FE25 - FE36
SF200-24	SLM224GT	24 ports FE + 2 ports GE combinés spécifiques		
SF200-24P	SLM224PT	24 ports FE + 2 ports GE combinés spécifiques	100 W	12 ports FE1-FE6, FE13 - FE18
SF200-48	SLM248GT	48 ports FE + 2 ports GE combinés spécifiques		
SF200-48P	SLM248PT	FE1-FE48, GE1-GE4. 48 ports FE + 2 ports GE combinés spécifiques	180 W	24 ports FE1-FE12, FE25 - FE36

Informations système

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

Affichage du récapitulatif du système

Pour afficher les informations se rapportant au système, cliquez sur **État et statistiques** > **Récapitulatif du système**. La page *Récapitulatif du système* s'ouvre.

La page *Récapitulatif du système* affiche des informations se rapportant au système et au matériel.

Informations système :

- **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*, afin d'entrer cette valeur.
- **Contact système** : indique le nom de la personne à contacter. Cliquez sur **Modifier** pour accéder à la page *Paramètres système*, afin d'entrer cette valeur.
- **Nom d'hôte** : indique le nom du commutateur. Cliquez sur **Modifier** pour accéder à la page *Paramètres système*, afin d'entrer cette valeur. Par défaut, le nom d'hôte du commutateur se compose du mot *commutateur* concaténé avec les trois octets les moins significatifs de l'adresse MAC du commutateur (les six chiffres hexadécimaux les plus à droite).
- **Durée utilisation syst.** : affiche le temps de disponibilité qui s'est écoulé depuis le dernier redémarrage.
- **Heure actuelle** : indique l'heure actuelle du système.
- **AdresseMAC de base** : indique l'adresse MAC du commutateur.
- **Trames Jumbo** : état de prise en charge des trames Jumbo. Cette prise en charge peut être activée ou désactivée sur la page *Paramètres des ports* du menu Gestion des ports.

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

État des services TCP/UDP :

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

- **Description du modèle** : description du modèle de commutateur.
- **Numéro de série** : numéro de série.
- **PID VID** : affiche la référence et l'identifiant de la version.

Information d'alimentation PoE sur l'unité principale :

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

Configuration des paramètres système

Pour accéder aux paramètres système :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres système**. La page *Paramètres système* s'ouvre.

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

- **Description du système** : affiche une description du commutateur.
- **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 de ce commutateur. Voici ce qui est utilisé dans l'invite de l'interface de ligne de commande :
  - *Valeurs par défaut* : le nom d'hôte par défaut (Nom du système) de ces commutateurs est *commutateur123456*, où123456 représente les trois derniers octets de l'adresse MAC du commutateur au format hexadécimal.
  - *Défini par l'utilisateur* : saisissez le nom d'hôte. Utilisez uniquement des lettres, des chiffres et des tirets. Les noms d'hôte ne peuvent pas être précédés ni suivis d'un tiret. Les autres symboles, les signes de ponctuation et les espaces ne sont pas autorisés (comme cela est spécifié dans les normes RFC1033, 1034 et 1035).

- **Paramètres personnalisés de l'écran de connexion** : pour afficher du texte sur la page *Connexion*, entrez-le dans la zone de texte **Bannière de connexion**. Cliquez sur **Aperçu** pour afficher les résultats.

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

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

Redémarrage du commutateur

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

Vous pouvez sauvegarder la configuration en utilisant *Administration > Gestion de fichiers > Copier/enregistrer la configuration* ou en cliquant sur **Enregistrer** en haut de la fenêtre. Vous pouvez également charger la configuration depuis un périphérique distant. Consultez la section **Téléchargement ou sauvegarde d'une configuration ou d'un journal** dans la section **Gestion des fichiers système**.

Pour redémarrer le commutateur :

ÉTAPE 1 Cliquez sur **Administration** > **Redémarrer**. La page *Redémarrer* s'ouvre.

ÉTAPE 2 Cliquez sur l'un des boutons de **redémarrage** pour redémarrer le commutateur.

- **Effacer le fichier de configuration de démarrage** : choisissez cette option pour effacer la configuration du commutateur la prochaine fois qu'il démarrera.
- **Redémarrer :** redémarre le commutateur. Les informations non enregistrées de la Configuration d'exécution étant ignorées lors du redémarrage du commutateur, vous devez cliquer sur **Enregistrer** en haut à droite de

n'importe quelle fenêtre afin de conserver la configuration actuelle lors du processus de démarrage. Si l'option Enregistrer ne s'affiche pas, cela signifie que la Configuration d'exécution est identique à la Configuration de démarrage et qu'aucune action n'est nécessaire.

- **Redémarrer avec les paramètres d'origine** : redémarre le commutateur en utilisant sa configuration d'origine. Ce processus efface le fichier de Configuration de démarrage et le fichier de configuration de sauvegarde. Lorsque cette action est sélectionnée, tout paramètre non enregistré dans un autre fichier est perdu. Le fichier de configuration miroir n'est pas supprimé lorsque vous restaurez les paramètres d'origine.

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

Surveillance de l'état et de la température du ventilateur

La page *Santé* affiche l'état et la température du ventilateur du commutateur sur tous les appareils équipés de ventilateurs.

Pour afficher les paramètres de santé du commutateur, cliquez sur **État et statistiques** > **Santé.** La page *Santé* s'ouvre.

La page *Santé* affiche les champs suivants :

- **État du ventilateur**: état du ventilateur. Les valeurs suivantes sont possibles :
  - OK : le ventilateur fonctionne normalement.
  - Échec : le ventilateur ne fonctionne pas correctement.
  - S/O : l'ID du ventilateur n'est pas applicable au modèle en question.
- **Température (en degrés Celsius et Fahrenheit)** : la température interne du commutateur (sur les appareils équipés de capteurs de température).
- **Température d'alarme (en degrés Celsius et Fahrenheit)** : la température interne de l'unité (pour les appareils appropriés) à partir de laquelle une alarme se déclenche.

Définition du délai d'expiration en cas de session inactive

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

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

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

ÉTAPE 1 Cliquez sur **Administration** > **Expiration de la session inactive**. La page *Expiration de la session inactive* s'ouvre.

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

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

Envoi d'une requête Ping à un hôte

Ping est un utilitaire servant à déterminer si un hôte distant peut être atteint et à mesurer la durée aller-retour de transfert de paquets entre le commutateur et un périphérique de destination.

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

Pour envoyer une requête Ping à un hôte :

ÉTAPE 1 Cliquez sur **Administration > Ping**. La page *Ping* s'ouvre.

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

- **Définition de l'hôte** : indiquez si vous souhaitez spécifier les hôtes par leur adresse IP ou leur nom.

- **Version IP** : si l'hôte est identifié par son adresse IP, sélectionnez IPv4 ou IPv6 pour indiquer qu'il sera entré au format sélectionné.
- **Type d'adresse IPv6 :** sélectionnez Liaison locale ou Global comme type d'adresse IPv6 à saisir.
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut être routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPV6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresseIPv6 est Liaison locale, sélectionnez son lieu de réception.
- **Adresse IP/Nom hôte** : adresse ou nom d'hôte de l'appareil auquel la requête Ping est envoyée. C'est la définition de l'hôte qui détermine s'il s'agit d'une adresse IP ou d'un nom d'hôte.
- **Intervalle de Ping** : durée d'attente du système entre les paquets Ping. La requête Ping est réitérée autant de fois que configuré dans le champ Nombre de Pings, que la requête aboutisse ou non. Sélectionnez l'intervalle par défaut ou spécifiez votre propre valeur.
- **Nombre de Pings** : nombre de fois que l'opération Ping sera effectuée. Sélectionnez la valeur par défaut ou spécifiez votre propre valeur.
- **État** : indique si la requête Ping a réussi ou échoué.

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

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

6

Heure système

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

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

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

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

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

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

Options d'heure système

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

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

Time (Heure)

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

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

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

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

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

- time-c.timefreq.bldrdoc.gov

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

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

Fuseau horaire et heure d'été

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

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

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

Modes SNTP

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

- Réception de diffusion client (mode passif)

  Les serveurs SNTP diffusent l'heure et le commutateur écoute ces diffusions. Lorsque le commutateur est dans ce mode, il n'est pas nécessaire de définir un serveur SNTP monodiffusion.

- **Transmission de diffusion client (mode actif)** : le commutateur, en tant que client SNTP, demande périodiquement des mises à jour de l'heure SNTP. Ce mode fonctionne de l'une des manières suivantes :
  - **Mode client pluridiffusion SNTP** : le commutateur diffuse des paquets de demande d'heure à tous les serveurs SNTP du sous-réseau et attend une réponse.
  - **Mode Serveur SNTP monodiffusion** : le commutateur envoie des requêtes de monodiffusion à une liste de serveurs SNTP configurés manuellement et attend une réponse.

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

Configuration de l'heure système

Sélection de la source d'heure système

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

ATTENTION Si l'heure système est définie manuellement et que le commutateur est redémarré, les paramètres d'heure saisis manuellement doivent être ressaisis.

Pour définir l'heure système :

ÉTAPE 1 Cliquez sur **Administration**> **Paramètres d'heure** > **Heure système**. La page *Heure système* s'ouvre.

Les champs suivants sont affichés :

- **Heure actuelle (statique)** : heure système sur le périphérique.
- **Dernier serveur synchronisé** : adresse, strate et type du serveur SNTP à partir duquel l'heure a été extraite pour la dernière fois.

ÉTAPE 2 Saisissez les paramètres suivants :

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

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

  REMARQUE Le paramètre de source d'horloge doit être défini à l'une des valeurs ci-dessus pour que l'authentification MD5 RIP fonctionne. Cela sert également aux fonctionnalités qui sont associées à l'heure, par exemple : L'authentification de liste ACL, de port, de ports 802.1 basés sur l'heure et qui est prise en charge sur certains périphériques.

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

- **Date** : saisissez la date du système.
- **Heure locale** : saisissez l'heure système.

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

- **Obtenir le fuseau horaire de DHCP** : sélectionnez cette option pour activer la configuration dynamique du fuseau horaire et l'heure d'été à partir du serveur DHCP. Un seul ou les deux paramètres peuvent être configurés selon les informations trouvées dans le paquet DHCP. Si cette option est activée, *vous devez également activer le client DHCP sur le commutateur*. Pour ce faire, réglez le **Type d'adresse IP** sur **Dynamique** sur la page *Interface IPv4*.

  REMARQUE Le client DHCP prend en charge l'option 100 permettant le réglage dynamique du fuseau horaire. Le commutateur ne prend pas en charge le client DHCPv6.
- **Décalage du fuseau horaire** : sélectionnez la différence en heures entre le *temps du méridien de Greenwich* (GMT) et l'heure locale. Par exemple, le décalage de fuseau horaire pour Paris et GMT+1 et celui pour New York est GMT- 5.

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

- **Heure d'été** : sélectionnez cette option pour activer l'heure d'été.
- **Compensation d'heure définie** : entrez le nombre de minutes de décalage par rapport à l'heure GMT (entre 1 et 1 440). La valeur par défaut est 60.
- **Type d'heure d'été** : cliquez sur l'un des éléments suivants :
  - *États-Unis* : l'heure d'été est définie selon les dates utilisées aux États-Unis.
  - *Europe* : l'heure d'été est définie selon les dates utilisées par l'Union Européenne et d'autres pays qui appliquent cette norme.
  - *Par dates* : l'heure d'été est définie manuellement, généralement pour un autre pays que les États-Unis ou un pays européen. Saisissez les paramètres suivants :
  - *Récurrent* : l'heure d'été entre en vigueur à la même date chaque année.

  Sélectionnez *Par dates* pour personnaliser le début et la fin de l'heure d'été :
  - **De** : jour et heure de début de l'heure d'été.
  - **À** : jour et heure de fin de l'heure d'été.

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

- *Semaine* : semaine du mois au cours de laquelle l'heure d'été prend fin chaque année.
- *Mois* : mois de l'année au cours duquel l'heure d'été prend fin chaque année.
- *Heure* : heure à laquelle l'heure d'été prend fin chaque année.

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

Ajout d'un serveur de monodiffusion SNTP

Huit serveurs de monodiffusion SNTP maximum peuvent être configurés.

REMARQUE Pour spécifier un serveur de monodiffusion SNTP par son nom, vous devez d'abord configurer le ou les serveurs DNS sur le commutateur (reportez-vous à la section **Définition de serveurs DNS**). Pour ajouter un serveur de monodiffusion SNTP, activez la case à cocher **Client SNTP monodiffusion**.

Pour ajouter un serveur de monodiffusion SNTP :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres d'heure** > **Monodiffusion SNTP**. La page *Monodiffusion SNTP* s'ouvre.

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

- **Serveur SNTP** : adresse IP du serveur SNTP. Huit serveurs SNTP peuvent être définis au maximum. Le serveur ou nom d'hôte préféré est choisi selon son niveau de strate.
- **Intervalle d'interrogation** : indique si l'interrogation est activée ou désactivée.
- **ID de clé d'authentification** : l'identification de clé sert à communiquer entre le serveur SNTP et le commutateur.
- **Niveau de strate** : distance par rapport à l'horloge de référence, exprimée sous la forme d'une valeur numérique. Un serveur SNTP ne peut pas être le serveur principal (niveau de strate 1), sauf si l'intervalle d'interrogation est activé.

- **État** : état du serveur SNTP. Ce champ peut prendre les valeurs suivantes :
  - *Actif* : le serveur SNTP fonctionne actuellement normalement.
  - *Inactif* : le serveur SNTP n'est actuellement pas disponible.
  - *Inconnu* : le serveur SNTP est actuellement recherché par le commutateur.
  - *En cours* : se produit lorsque le serveur SNTP n'a pas entièrement approuvé son propre serveur de temps (c'est-à-dire lors du premier démarrage du serveur SNTP).
- **Dernière réponse** : date et heure de la dernière réponse reçue de la part de ce serveur SNTP.
- **Décalage** : décalage estimé entre l'horloge du serveur et l'horloge locale, en millisecondes. L'hôte détermine la valeur de ce décalage à l'aide de l'algorithme décrit au sein de la RFC 2030.
- **Écart** : temps estimé d'un aller-retour de transmission entre l'horloge du serveur et l'horloge locale sur le chemin du réseau, en millisecondes. L'hôte détermine la valeur de cet écart à l'aide de l'algorithme décrit au sein de la RFC 2030.

ÉTAPE 2 Pour ajouter un serveur de monodiffusion SNTP, activez **Client SNTP monodiffusion**.

ÉTAPE 3 Cliquez sur **Ajouter** pour afficher la page *Ajouter un serveur SNTP*.

ÉTAPE 4 Saisissez les paramètres suivants :

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

  REMARQUE Pour spécifier un serveur SNTP connu, le commutateur doit être connecté à Internet et configuré avec un serveur DNS ou configuré de manière à ce qu'un serveur DNS soit identifié en utilisant DHCP. (Voir la section **Définition de serveurs DNS**.)
- **Version IP** : sélectionnez la version de l'adresse IP : **Version 6** ou **Version 4**.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut être routée et ne peut servir à la communication

que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.

- *Global* : l'adresse IPv6 est de type global IPV6 monodiffusion, visible et joignable à partir d'autres réseaux.

- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée)
- **Adresse IP du serveur SNTP** : saisissez l'adresse IP du serveur SNTP. Le format dépend du type d'adresse sélectionné.
- **Serveur SNTP** : sélectionnez le nom du serveur SNTP à partir d'une liste de serveurs NTP connus. Si **autre** est choisi, saisissez le nom du serveur SNTP dans le champ adjacent.
- **Intervalle d'interrogation** : sélectionnez cette option afin d'activer l'interrogation du serveur SNTP pour les informations d'heure système. Tous les serveurs NTP enregistrés pour l'interrogation sont interrogés et l'horloge est sélectionnée à partir du serveur accessible qui dispose du niveau de strate le plus faible (distance par rapport à l'horloge de référence). Le serveur disposant de la strate la plus faible est considéré comme étant le serveur principal. Le serveur disposant de la strate la deuxième plus faible est un serveur secondaire et ainsi de suite. Si le serveur principal est inactif, le commutateur interroge tous les serveurs ayant leur paramètre d'interrogation activé et sélectionne celui disposant de la strate la plus faible comme le nouveau serveur principal.
- **Authentification** : cochez la case pour activer l'authentification.
- **ID de clé d'authentification** : si l'authentification est activée, sélectionnez la valeur de l'ID de clé. (Vous pouvez créer des clés d'authentification sur la page *Authentification SNTP*.)

ÉTAPE 5 Cliquez sur **Appliquer**. Le serveur SNTP est ajouté et vous retournez à la page principale.

Configuration du mode SNTP

Le commutateur peut être en mode actif et/ou passif (consultez **Modes SNTP** pour plus d'informations).

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

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

ÉTAPE 2 Sélectionnez l'une des options suivantes :

- **Mode client multidiffusion SNTP (réception de diffusion client)** : sélectionnez cette option pour recevoir l'heure système à partir de n'importe quel serveur SNTP du sous-réseau.
- **Mode client pluridiffusion SNTP (transmission de diffusion client)** : sélectionnez cette option pour transmettre des paquets de synchronisation de la diffusion SNTP demandant des informations d'heure système. Si des serveurs SNTP ont été définis, les paquets sont dirigés vers ces serveurs ; sinon, les paquets sont transmis à tous les serveurs SNTP du sous-réseau.

ÉTAPE 3 Si le système est en mode système Layer 3 , cliquez sur **Ajouter** pour saisir l'interface de réception/transmission SNTP. La page *Ajouter des paramètres d'interface SNTP* s'ouvre.

Sélectionnez une interface ainsi que les options de réception/transmission.

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

Définition de l'authentification SNTP

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

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

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

Workflow

ÉTAPE 1 Activez l'authentification à la page *Authentification SNTP*.

ÉTAPE 2 Créez une clé à la page *Authentification SNTP*.

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

Pour activer l'authentification SNTP et définir des clés :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres d'heure** > **Authentification SNTP**. La page *Authentification SNTP* s'ouvre.

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

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

ÉTAPE 4 Cliquez sur **Ajouter**. La page *Ajouter une authentification SNTP* s'ouvre.

ÉTAPE 5 Saisissez les paramètres suivants :

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

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

7

Gestion des diagnostics de l'appareil

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

Elle couvre les rubriques suivantes :

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

Test des ports cuivre

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

VCT réalise deux types de tests :

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

Conditions préalables à l'exécution du test des ports cuivre

Avant d'exécuter le test, procédez comme suit :

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

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

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

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

Pour tester les câbles en cuivre reliés aux ports :

ÉTAPE 1 Cliquez sur **Administration** > **Diagnostics** > **Test cuivre**. La page *Test cuivre* s'ouvre.

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

ÉTAPE 3 Cliquez sur **Test cuivre**.

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

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

- **Dernière mise à jour :** heure à laquelle a été effectué le dernier test sur le port.
- **Résultats de test** : résultats du test de câbles. Ce champ peut prendre les valeurs suivantes :
  - *OK :* le câble a réussi le test.
  - *Aucun câble* : le câble n'est pas connecté au port.
  - *Câble ouvert* : le câble n'est connecté que d'un côté.
  - *Câble court-circuité* : un court-circuit s'est produit au niveau du câble.

- *Résultat de test inconnu* : une erreur s'est produite.

- **Distance au défaut :** distance entre le port et l'emplacement du câble où le problème a été détecté.
- **État du port opérationnel** : indique si le port est actif ou inactif.

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

- **Longueur de câble :** propose une estimation de longueur.
- **Paire** : paire de fils de câble testée.
- **État** : état de la paire de fils. Rouge indique un défaut et Vert indique l'état OK.
- **Canal** : canal de câble indiquant si les fils sont droits ou croisés.
- **Polarité**: indique si la détection et la correction automatiques de la polarité ont été activées pour la paire de fils.
- **Déphasage entre paires** : différence de phase entre les paires de fils.

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

Affichage de l'état des modules optiques

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

SFP compatibles MSA

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

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

- MFELX1 : émetteur-récepteur SFP 100BASE-LX pour la fibre monomode, longueur d'onde de 1 310 nm, jusqu'à 10 km.

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

- MGBBX1 : émetteur-récepteur SFP 1000BASE-BX-20U pour la fibre monomode, longueur d'onde de 1 310 nm, jusqu'à 40 km.
- MGBLH1 : émetteur-récepteur SFP 1000BASE-LH pour la fibre monomode, longueur d'onde de 1 310 nm, jusqu'à 40 km.
- MGBLX1 : émetteur-récepteur SFP 1000BASE-LX pour la fibre monomode, longueur d'onde de 1 310 nm, jusqu'à 10 km.
- MGBSX1 : émetteur-récepteur SFP 1000BASE-SX pour la fibre multimode, longueur d'onde de 850 nm, jusqu'à 550 m.
- MGBT1 : émetteur-récepteur SFP 1000BASE-T pour le fil cuivre de catégorie5, jusqu'à 100 m.

Pour afficher les résultats des tests optiques, cliquez sur **Administration** > **Diagnostics** > **État des modules optiques**. La page *État des modules optiques* s'ouvre.

Cette page affiche les champs suivants :

- **Port :** numéro du port sur lequel le SFP est connecté.
- **Température** : température en degrés Celsius à laquelle le SFP fonctionne.
- **Tension** : tension de fonctionnement du SFP.
- **Intensité** : consommation de courant du SFP.
- **Puissance de sortie** : puissance optique transmise.
- **Puissance d'entrée** : puissance optique reçue.
- **Défaillance du transmetteur** : le SFP distant indique une perte de signal. Les valeurs sont Vrai, Faux et A/S (Aucun signal).
- **Perte de signal** : le SFP local indique une perte de signal. Les valeurs sont Vrai et Faux.
- **Données prêtes** : le SFP est opérationnel. Les valeurs sont Vrai et Faux.

Configuration de la mise en miroir des ports et de VLAN

La mise en miroir des ports est utilisée sur un commutateur réseau pour envoyer une copie des paquets réseau détectés sur un port commuté, plusieurs ports commutés ou l'intégralité d'un VLAN vers une connexion de surveillance réseau située sur un autre port du commutateur. Cette opération est souvent utilisée sur les équipements réseau qui requièrent une surveillance du trafic réseau, par exemple un système de détection des intrusions. Un analyseur réseau connecté au port de surveillance traite les paquets de données à des fins de diagnostic, débogage et contrôle des performances. Jusqu'à huit sources peuvent être mises en miroir. Il peut s'agir de n'importe quelle combinaison de huit ports et/ou VLAN individuels.

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

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

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

Pour activer la mise en miroir :

ÉTAPE 1 Cliquez sur **Administration** > **Diagnostics** > **Mise en miroir des ports et VLAN**. La page *Mise en miroir des ports et VLAN* s'ouvre.

Cette page affiche les champs suivants :

- **Port de destination :** port sur lequel le trafic doit être copié ; port de l'analyseur.
- **Interface source** : interface, port ou VLAN à partir duquel le trafic est envoyé au port de l'analyseur.
- **Type** : type de surveillance ; entrant sur le port (réception), sortant du port (émission) ou les deux.
- **État** : affiche l'une des valeurs suivantes :

- *Actif* : les interfaces source et de destination sont actives et transfèrent le trafic.
- *Pas prêt* : la source ou la destination est inactive (ou les deux) et ne transfère pas le trafic pour une raison quelconque.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un port ou un VLAN à mettre en miroir. La page *Ajouter la mise en miroir des ports et VLAN* s'ouvre.

ÉTAPE 3 Configurez les paramètres suivants :

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

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

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

Cette section décrit la fonction Secure Core Technology (SCT) et la façon d'afficher l'utilisation du CPU.

Le commutateur gère les types de trafic suivants en plus du trafic de l'utilisateur final :

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

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

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

Pour afficher l'utilisation du CPU :

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

La page *Utilisation du CPU* s'ouvre.

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

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

ÉTAPE 2 Sélectionnez le **Fréquence d'actualisation**, à savoir la durée en secondes qui s'écoule avant l'actualisation des statistiques. Un nouvel échantillon est créé pour chaque période.

8

Configuration de la détection

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

Elle couvre les rubriques suivantes :

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

Configuration de la détection Bonjour

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

Bonjour en mode système Layer2

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

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

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

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

Pour activer Bonjour globalement :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - Bonjour**. La page *Détection - Bonjour* s'ouvre.

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

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

LLDP et CDP

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

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

- CDP/LLDP peut être activé/désactivé globalement, ou activé/désactivé pour chaque port. La fonctionnalité CDP/LLDP d'un port ne s'applique que si CDP/LLDP est globalement activé.
- Si CDP/LLDP est globalement activé, le commutateur élimine les paquets CDP/LLDP entrants provenant des ports où CDP/LLDP est désactivé.
- Si CDP/LLDP est globalement désactivé, le commutateur peut être configuré pour ignorer l'inondation tenant compte du VLAN, ou l'inondation ne tenant pas compte du VLAN, de tous les paquets CDP/LLDP entrants. L'inondation tenant compte du VLAN transmet un paquet CDP/LLDP entrant au VLAN où le paquet est reçu, mais pas au port d'entrée. L'inondation ne

tenant pas compte du VLAN transmet un paquet CDP/LLDP entrant à tous les ports, sauf au port d'entrée. Par défaut, le système élimine les paquets CDP/LLDP lorsque CDP/LLDP est désactivé au niveau global. Vous pouvez configurer l'élimination/inondation des paquets CDP et LLDP entrants respectivement sur les pages Propriétés CDP et Propriétés LLDP.

- La fonction Port intelligent automatique requiert l'activation de CDP et/ou LLDP. La fonction Port intelligent automatique configure automatiquement une interface basée sur l'annonce CDP/LLDP reçue de l'interface.
- Les périphériques d'extrémité CDP et LLDP, tels que les téléphones IP, apprennent la configuration VLAN voix des annonces CDP et LLDP. Par défaut, le commutateur est activé pour envoyer une annonce CDP et LLDP basée sur le VLAN voix qui est configuré sur le commutateur. Pour plus d'informations, reportez-vous aux sections VLAN voix et VLAN voix automatique.

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

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

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

Si un port est la cible de la mise en miroir, il est considéré comme étant inactif conformément à CDP/LLDP.

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

Configuration de LLDP

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

- **Présentation de LLDP**
- **Configuration des propriétés LLDP**
- **Modification des paramètres de port LLDP**
- **LLDP MED**
- **Configuration des paramètres des ports LLDP MED**
- **Affichage de l'état des ports LLDP**
- **Affichage des informations LLDP locales**
- **Affichage des informations LLDP des voisins**
- **Accès aux statistiques LLDP**
- **Surcharge LLDP**

Présentation de LLDP

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

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

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

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

Flux de travail de configuration de LLDP

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

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

Configuration des propriétés LLDP

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

Pour saisir des propriétés LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Propriétés**. La page *Propriétés* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **État LLDP :** sélectionnez cette option pour activer LLDP sur le commutateur (activée par défaut).
- **Traitement des trames LLDP :** si LLDP n'est pas activé, sélectionnez l'action à réaliser en cas de réception d'un paquet correspondant aux critères sélectionnés :
  - *Filtrage* : supprime le paquet.

- *Inondation* : transfère le paquet à tous les membres du VLAN.

- **Intervalle d'annonce TLV** : définissez, en nombre de secondes, la fréquence d'envoi des mises à jour des annonces LLDP ou utilisez la valeur par défaut.
- **Intervalle de notification pour le journal syst. des changements de topologie** : saisissez le délai minimal entre deux notifications du journal système.
- **Multiplicateur de conservation** : saisissez la durée de conservation des paquets LLDP avant leur élimination, en multiples de l'intervalle d'annonce TLV. Par exemple, si l'intervalle d'annonceTLV est de 30 secondes et si le multiplicateur de conservation est4, les paquets LLDP seront éliminés après 120 secondes.
- **Délai de réinitialisation** : saisissez l'intervalle en secondes qui sépare la désactivation et la réactivation de LLDP, suite à un cycle d'activation ou de désactivation de LLDP.
- **Délai de transmission** : saisissez le délai en secondes qui séparera deux transmissions de trames LLDP successives en cas de modification dans la MIB de systèmes locaux LLDP.

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

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

Modification des paramètres de port LLDP

Utilisez la page *Paramètres des ports* pour activer LLDP et la notification de serveur de journalisation distant par port et pour sélectionner les TLV inclus dans les PDU LLDP.

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

Pour définir des paramètres de port LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Paramètres des ports**. La page *Paramètres des ports* s'ouvre.

Cette page affiche les informationsLLDP des ports.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier**. La page *Modifier les paramètres de port LLDP* s'ouvre.

Cette page contient les champs suivants :

- **Interface** : sélectionnez le port à modifier.
- **État administratif** : sélectionnez l'option de publication LLDP pour le port. Les valeurs disponibles sont les suivantes :
  - *Émission uniquement* : publication uniquement, pas de détection.
  - *Réception uniquement* : détection uniquement, pas de publication.
  - *Émission et réception* : publication et détection.
  - *Désactiver* : indique que LLDP est désactivé sur le port.
- **Notification du journal système** : sélectionnez **Activer** pour avertir les destinataires de notification d'une modification de la topologie.

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

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

Les champs suivants concernent l'adresse de gestion :

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

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

LLDP MED

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

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

Configuration d'une stratégie réseau LLDP MED

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

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

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

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

Pour définir une stratégie réseau LLDP MED :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Stratégie réseau LLDP MED**. La page *Stratégie réseau LLDP MED* s'ouvre.

Cette page affiche les stratégies réseau précédemment créées.

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

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

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

ÉTAPE 4 Pour définir une nouvelle stratégie, cliquez sur **Ajouter**. La page *Ajouter une stratégie réseau LLDP MED* s'ouvre.

ÉTAPE 5 Saisissez les valeurs appropriées :

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

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

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

Configuration des paramètres des ports LLDP MED

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

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

Pour configurer LLDP MED sur chaque port :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Paramètres des ports LLDP MED**. La page *Paramètres des ports LLDP-MED* s'ouvre.

Cette page affiche les paramètres LLDP MED, y compris les TLV activées, pour tous les ports.

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

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

ÉTAPE 4 Configurez les paramètres suivants :

- **Interface** : sélectionnez l'interface à configurer.
- **État LLDP MED** : Activez/désactivez LLDP MED sur ce port.
- **Notification du journal système** : indiquez si la notification du journal doit être envoyée port par port, lorsqu'une station de travail prenant en charge MED est détectée.

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

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

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

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

Affichage de l'état des ports LLDP

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

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

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

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

Informations globales d'état des ports LLDP

- **Sous-type de l'ID du châssis** : type d'ID de châssis (adresse MAC, par exemple).

- **ID du châssis** : identificateur du châssis. Si vous avez choisi l'adresse MAC comme sous-type d'ID de châssis, l'adresse MAC du commutateur est affichée.
- **Nom du système** : nom du commutateur.
- **Description du système** : description du commutateur, au format alphanumérique.
- **Fonctionnalités système prises en charge** : fonctions principales du périphérique, comme Pont, Point d'accès WLAN ou Routeur.
- **Fonctionnalités système activées** : fonctions principales activées sur le périphérique.
- **Sous-type de l'ID du port** : type d'ID de port affiché.

Table d'état des ports LLDP

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

Affichage des informations LLDP locales

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

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Informations locales LLDP**. La page *Informations locales LLDP* s'ouvre.

ÉTAPE 2 En bas de la page, cliquez sur **Table d'état des ports LLDP**.

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

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

ÉTAPE 3 Sélectionnez l'entrée voulue dans la liste **Port**.

Cette page contient les champs suivants :

Globale

- **Sous-type de l'ID du châssis** : type d'ID de châssis (adresse MAC, par exemple).
- **ID du châssis** : identificateur du châssis. Si vous avez choisi l'adresse MAC comme sous-type d'ID de châssis, l'adresse MAC du commutateur est affichée.
- **Nom du système** : nom du commutateur.
- **Description du système** : description du commutateur, au format alphanumérique.
- **Fonctionnalités système prises en charge** : fonctions principales du périphérique, comme Pont, Point d'accès WLAN ou Routeur.
- **Fonctionnalités système activées** : fonctions principales activées sur le périphérique.
- **Sous-type de l'ID du port** : type d'ID de port affiché.
- **ID du port** : identificateur du port.
- **Description du port** : informations sur le port, notamment son fabricant, son nom de produit et la version du matériel/logiciel.

Adresse de gestion

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

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

- **Numéro de l'interface** : interface spécifique associée à cette adresse de gestion.

Détails MAC/PHY

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

Détails 802.3

- **Taille de trame maximale 802.3** : taille maximale de trame IEEE802.3 possible.

Agrégation de liaisons 802.3

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

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

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

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

Détails MED

- **Fonctionnalités prises en charge** : fonctions MED prises en charge sur le port.
- **Fonctionnalités actuelles** : fonctions MED activées sur le port.
- **Classe de périphérique** : classe du périphérique d'extrémité LLDP MED. Les classes disponibles sont les suivantes :
  - *Classe de point de terminaison 1*: indique une classe de point de terminaison générique offrant des services LLDP de base.
  - *Classe de point de terminaison 2*: indique une classe de point de terminaison de média offrant des services de lecture multimédia en continu, en plus des services de classe 1.
  - *Classe de point de terminaison 3*: indique une classe de périphérique de communications offrant tous les services de classe 1 et de classe 2 ainsi que des fonctions de reconnaissance de l'emplacement, d'appel d'urgence, de prise en charge des commutateurs Layer2 et de gestion des informations de périphérique.
- **Type de périphérique PoE** : type PoE du port. Exemple : alimenté.
- **Source d'alimentation PoE** : source d'alimentation du port.
- **Priorité d'alimentation PoE** : priorité d'alimentation du port.
- **Valeur d'alimentation PoE** : valeur d'alimentation du port.
- **Révision du matériel** : version du matériel.
- **Révision du micrologiciel** : version du micrologiciel.
- **Révision du logiciel** : version du logiciel.
- **Numéro de série** : numéro de série du périphérique.
- **Nom du fabricant** : nom du fabricant du périphérique.
- **Nom du modèle** : nom de modèle du périphérique.
- **ID de ressource** : ID de la ressource.

Informations sur l'emplacement

- **Physique** : adresse postale.

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

Table des stratégies réseau

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

Affichage des informations LLDP des voisins

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

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

Pour afficher les informations LLDP des voisins :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Informations sur le voisin**. La page *Informations de voisinage LLDP* s'ouvre.

Cette page affiche les champs suivants :

- **Port local** : numéro du port local auquel le voisin est connecté.
- **Sous-type de l'ID du châssis** : type d'ID de châssis (adresse MAC, par exemple).

- **ID du châssis** : identificateur du châssis du périphérique de voisinage réseau (LAN) 802.
- **Sous-type de l'ID du port** : type d'ID de port affiché.
- **ID du port** : identificateur du port.
- **Nom du système** : nom publié du commutateur.
- **Durée de vie** : durée en secondes à l'issue de laquelle les informations concernant ce voisin sont supprimées.

ÉTAPE 2 Sélectionnez un port local puis cliquez sur **Détails**. La page *Informations sur le voisinage* s'ouvre.

Cette page affiche les champs suivants :

Détails du port

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

Détails de base

- **Sous-type de l'ID du châssis** : type d'ID de châssis (adresse MAC, par exemple).
- **ID du châssis** : identificateur du châssis du périphérique de voisinage réseau (LAN) 802.
- **Sous-type de l'ID du port** : type d'ID de port affiché.
- **ID du port** : identificateur du port.
- **Description du port** : informations sur le port, notamment son fabricant, son nom de produit et la version du matériel/logiciel.
- **Nom du système** : nom du système publié.
- **Description du système** : description de l'entité réseau, au format alphanumérique. Inclut le nom du système et la version du matériel, le système d'exploitation et les logiciels réseau pris en charge par le périphérique. Cette valeur est identique à l'objet sysDescr.

- **Fonctionnalités système prises en charge** : fonctions principales du périphérique. Les fonctionnalités sont indiquées par deux octets. Les bits 0 à 7 indiquent respectivement Autres, Répéteur, Pont, Point d'accès WLAN, Routeur, Téléphone, Système de câble DOCSIS et Station. Les bits 8 à 15 sont réservés.
- **Fonctionnalités système activées** : fonctions principales activées sur le périphérique.

Table des adresses de gestion

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

Détails MAC/PHY

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

Alimentation 802.3 via MDI

- **Classe de port de prise en charge de l'alimentation MDI** : classe de port annoncée pour la prise en charge de l'alimentation.
- **Prise en charge de l'alimentation MDI PSE** : indique si l'alimentation MDI est prise en charge sur le port.
- **État de l'alimentation MDI PSE** : indique si l'alimentation MDI est activée sur le port.

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

Détails 802.3

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

Agrégation de liaisons 802.3

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

802.3 Energy Efficient Ethernet (EEE)

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

Détails MED

- **Fonctionnalités prises en charge** : fonctions MED activées sur le port.
- **Fonctionnalités actuelles** — TLV MED annoncées par le port.
- **Classe de périphérique** : classe du périphérique d'extrémité LLDP MED. Les classes disponibles sont les suivantes :
  - *Classe de point de terminaison 1* : indique une classe de point de terminaison générique offrant des services LLDP de base.

- *Classe de point de terminaison 2* : indique une classe de point de terminaison de média offrant des services de lecture multimédia en continu, en plus des services de classe 1.
- *Classe de point de terminaison 3* : indique une classe de périphérique de communications offrant tous les services de classe 1 et de classe 2, ainsi que des fonctions de reconnaissance de l'emplacement, d'appel d'urgence, de prise en charge des commutateurs Layer 2 et de gestion des informations de périphérique.

- **Type de périphérique PoE** : type PoE du port. Exemple : alimenté.
- **Source d'alimentation PoE** : source d'alimentation du port.
- **Priorité d'alimentation PoE** : priorité d'alimentation du port.
- **Valeur d'alimentation PoE** : valeur d'alimentation du port.
- **Révision du matériel** : version du matériel.
- **Révision du micrologiciel** : version du micrologiciel.
- **Révision du logiciel** : version du logiciel.
- **Numéro de série** : numéro de série du périphérique.
- **Nom du fabricant** : nom du fabricant du périphérique.
- **Nom du modèle** : nom de modèle du périphérique.
- **ID de ressource** : ID de la ressource.

VLAN et protocole 802.1

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

Table PPVID

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

ID VLAN

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

ID de protocole

- **Table des ID de protocole** : ID de protocole annoncés.

Informations sur l'emplacement

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

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

Stratégies réseau

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

Accès aux statistiques LLDP

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

Pour afficher les statistiques LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Statistiques LLDP**. La page *Statistiques LLDP* s'ouvre.

Pour chaque port, les champs suivants sont affichés :

- **Interface :** identificateur d'interface.

- **Total de trames émises** : nombre des trames transmises.
- **Trames reçues**
  - *Total* : nombre des trames reçues.
  - *Éliminé* : nombre des trames reçues qui ont été éliminées.
  - *Erreurs* : nombre total des trames reçues comportant des erreurs.
- **TLV reçues**
  - *Éliminé* : nombre total de TLV reçues qui ont été éliminées.
  - *Non reconnu* : nombre total de TLV reçues non reconnues.
- **Nombre de suppressions d'informations du voisin** : nombre d'expirations du délai maximal du voisin sur l'interface.

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

Surcharge LLDP

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

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

Pour afficher les informations de surcharge LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Surcharge LLDP**. La page *Surcharge LLDP* s'ouvre.

Cette page contient les champs suivants, pour chaque port :

- **Interface** : identificateur de port.
- **Total (octets)** : nombre total d'octets d'informations LLDP dans chaque paquet.
- **Restant à envoyer (octets)** : nombre total d'octets disponibles restants pour des informations LLDP supplémentaires dans chaque paquet.

- **État** : indique si des TLV sont en cours de transmission ou si une surcharge est intervenue.

ÉTAPE 2 Pour afficher les détails de surcharge d'un port, sélectionnez-le et cliquez sur **Détails**. La page *Détails des surcharges LLDP* s'ouvre.

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

- **TLV LLDP obligatoires**
  - *Taille (octets)* : taille totale des TLV obligatoires, en octets.
  - *État* : indique si un groupe de TLV obligatoires est en cours de transmission ou si une surcharge est intervenue.
- **Fonctionnalités LLDP MED**
  - *Taille (octets) :* taille totale des paquets de fonctionnalités LLDP MED, en octets.
  - *État* : indique si les paquets de fonctionnalités LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **Emplacement LLDP MED**
  - *Taille (octets)* : taille totale des paquets d'emplacement LLDP MED, en octets.
  - *État* : indique si les paquets d'emplacement LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **Stratégie réseau LLDP MED**
  - *Taille (octets)* : taille totale des paquets de stratégie réseau LLDP MED, en octets.
  - *État* : indique si les paquets de stratégie réseau LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **Alimentation LLDP MED étendue via MDI**
  - *Taille (octets)* : taille totale des paquets d'alimentation LLDP MED étendue via MDI, en octets.
  - *État* : indique si les paquets d'alimentation LLDP MED étendue via MDI ont été envoyés ou si une surcharge est intervenue.

- **TLV 802.3**
  - *Taille (octets)* : taille totale des paquets de TLV 802.3 LLDP MED, en octets.
  - *État* : indique si les paquets de TLV 802.3 LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **TLV LLDP facultatives**
  - *Taille (octets)* : taille totale des paquets de TLV LLDP MED facultatives, en octets.
  - *État* : indique si les paquets de TLV LLDP MED facultatives ont été envoyés ou si une surcharge est intervenue.
- **Inventaire LLDP MED**
  - *Taille (octets)* : taille totale des paquets de TLV d'inventaire LLDP MED, en octets.
  - *État* : indique si les paquets de TLV d'inventaire LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **Total (octets)** : nombre total d'octets d'informations LLDP dans chaque paquet.
- **Restant à envoyer (octets)** : nombre total d'octets disponibles restants pour des informations LLDP supplémentaires dans chaque paquet.

Configuration de CDP

Cette section explique comment configurer CDP.

Elle couvre les rubriques suivantes :

- **Définition des propriétés CDP**
- **Modification des paramètres d'interface CDP**
- **Affichage des informations locales CDP**
- **Affichage des informationsde voisinage CDP**
- **Affichage des statistiques CDP**

Définition des propriétés CDP

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

Workflow de configuration de CDP

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

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

ÉTAPE 2 Configurez CDP sur chaque interface à l'aide de la page *Paramètres d'interface*.

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

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

Pour saisir les paramètres généraux CDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - CDP** > **Propriétés**. La page *Propriétés* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **État CDP** : sélectionnez cette option pour activer CDP sur le commutateur.
- **Traitement des trames CDP** : si CDP n'est pas activé, sélectionnez l'action à réaliser en cas de réception d'un paquet correspondant aux critères sélectionnés :
  - *Pontage* : transfère le paquet basé sur le VLAN.
  - *Filtrage* : supprime le paquet.
  - *Inondation* : inondation ne tenant pas compte du VLAN qui transmet les paquets CDP entrants à tous les ports, sauf aux ports d'entrée.

- **Annonce VLAN voix CDP** : sélectionnez cette option pour permettre au commutateur d'annoncer le VLAN voix dans CDP sur tous les ports activés pour CDP et membres du VLAN voix. Vous pouvez configurer le VLAN voix sur la page Propriétés du VLAN voix.
- **Validation CDP des TLV obligatoires** : si cette option est sélectionnée, les paquets CDP entrants qui ne contiennent pas de TLV obligatoires sont éliminés et le compteur d'erreurs non valides est incrémenté.
- **Version CDP** : sélectionnez la version du protocole CDP à utiliser.
- **Délai d'attente CDP** : durée de conservation des paquets CDP avant leur élimination, en multiples de l'intervalle d'annonceTLV. Par exemple, si l'intervalle d'annonce TLV est de 30 secondes et si le multiplicateur de conservation est 4, les paquets LLDP seront éliminés après 120 secondes. Les options suivantes sont disponibles :
  - *Valeurs par défaut* : utilisez la durée par défaut (180 secondes)
  - *Défini par l'utilisateur :* saisissez la durée en secondes.
- **Niveau de transmission CDP** : fréquence (en secondes) d'envoi des mises à jour d'annonces CDP. Les options suivantes sont disponibles :
  - *Valeurs par défaut* : utilisez la fréquence par défaut (60 secondes).
  - *Défini par l'utilisateur :* saisissez la fréquence en secondes.
- **Format d'ID de périphérique** : sélectionnez le format de l'ID de périphérique (adresse MAC ou numéro de série).
- **Interface source** : adresse IP à utiliser dans la TLV des trames. Les options suivantes sont disponibles :
  - *Valeurs par défaut* : utilisez l'adresse IP de l'interface sortante.
  - *Défini par l'utilisateur* : utilisez l'adresse IP de l'interface (dans le champ **Interface**) dans la TLV d'adresse.
- **Interface** : si vous avez sélectionné *Défini par l'utilisateur* pour **Interface source**, sélectionnez l'interface.
- **Non-concordance VLAN voix Syslog** : cochez cette option pour envoyer un message SYSLOG lorsqu'une non-concordance VLAN voix est détectée. Cela signifie que les informations de VLAN voix dans la trame entrante ne correspondent pas à l'élément annoncé par le périphérique local.

- **Non-concordance VLAN natif Syslog** : cochez cette option pour envoyer un message SYSLOG lorsqu'une non-concordance VLAN natif est détectée. Cela signifie que les informations de VLAN natif dans la trame entrante ne correspondent pas à l'élément annoncé par le périphérique local.
- **Non-concordance duplex Syslog** : cochez cette option pour envoyer un message SYSLOG lorsque les informations duplex ne correspondent pas. Cela signifie que les informations duplex dans la trame entrante ne correspondent pas à l'élément annoncé par le périphérique local.

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

Modification des paramètres d'interface CDP

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

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

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

Pour définir les paramètres d'interface LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - CDP** > **Paramètres d'interface**. La page *Paramètres d'interface* s'ouvre.

Cette page affiche les informations CDP suivantes pour chaque interface.

- **État CDP** : option de publication CDP pour le port.
- **Signalisation des conflits avec les voisins CDP** : affiche l'état des options de rapport qui sont activées/désactivées sur la page **Modifier** (VLAN voix/ VLAN natif/Duplex).
- **Nombre de voisins** : nombre de voisins détectés.

Quatre boutons sont disponibles en bas de la page :

- **Copier les paramètres** : sélectionnez ce bouton pour copier une configuration d'un port vers un autre.

- **Modifier** : les différents champs sont décrits à l'étape 2 ci-dessous.
- **Détails des informations locales CDP** : ouvre la page *Administration > Détection - CDP > Informations locales CDP*.
- **Détails des informations de voisinage CDP** : ouvre la page *Administration > Détection - CDP > Informations de voisinage CDP*.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier**. La page *Modifier les paramètres d'interface CDP* s'ouvre.

Cette page contient les champs suivants :

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

  REMARQUE Les trois champs suivants sont opérationnels si le commutateur a été configuré pour envoyer des messages « trap » à la station de gestion.
- **Non-concordance VLAN voix Syslog** : sélectionnez cette option pour activer l'envoi d'un message SYSLOG lorsqu'une non-concordance VLAN voix est détectée. Cela signifie que les informations de VLAN voix dans la trame entrante ne correspondent pas à l'élément annoncé par le périphérique local.
- **Non-concordance VLAN natif Syslog** : sélectionnez cette option pour activer l'envoi d'un message SYSLOG lorsqu'une non-concordance VLAN natif est détectée. Cela signifie que les informations de VLAN natif dans la trame entrante ne correspondent pas à l'élément annoncé par le périphérique local.
- **Non-concordance duplex Syslog** : sélectionnez cette option pour activer l'envoi d'un message SYSLOG lorsqu'une non-concordance des informations duplex est détectée. Cela signifie que les informations duplex dans la trame entrante ne correspondent pas à l'élément annoncé par le périphérique local.

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

Affichage des informations locales CDP

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

ÉTAPE 1 Cliquez sur **Administration** > **Détection - CDP** > **Informations locales CDP**. La page *Informations locales CDP* s'ouvre.

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

- **Interface** : numéro du port local.
- **État CDP** : indique si CDP est activé.
- **TLV d'ID de périphérique**
  - **Type d'ID de périphérique** : type d'ID de périphérique annoncé dans la TLV d'ID de périphérique.
  - **ID de périphérique** : ID de périphérique annoncé dans la TLV d'ID de périphérique.
- **Durée de vie du nom du système**
  - **Nom du système** : nom système de l'appareil.
- **TLV de l'adresse**
  - **Adresses 1-3** : adresses IP (annoncées dans la TLV d'adresse de périphérique).
- **TLV du port**
  - **ID du port** : identificateur du port annoncé dans la TLV de port.
- **TLV des fonctionnalités**
  - **Fonctionnalités** : fonctionnalités annoncées dans la TLV de port.
- **TLV de la version**
  - **Version** : informations sur la version logicielle sous laquelle le périphérique fonctionne.
- **TLV de la plateforme**
  - **Plate-forme** : identificateur de la plate-forme annoncée dans la TLV de plate-forme.

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

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

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

L'interface passe à l'état Désactivé.

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

Affichage des informationsde voisinage CDP

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

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

Pour afficher les informations de voisinage CDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - CDP** > **Informations de voisinage CDP**. La page *Informations de voisinage CDP* s'ouvre.

Cette page contient les champs suivants pour le partenaire de liaison (voisin) :

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

ÉTAPE 2 Sélectionnez un périphérique, puis cliquez sur **Détails**. La page *Détails de voisinage CDP* s'ouvre.

Cette page contient les champs suivants relatifs au voisin :

- **ID de périphérique** : ID du périphérique de voisinage.
- **Interface locale** : numéro d'interface du port via lequel la trame a été reçue.
- **Version d'annonce** : version du protocole CDP.
- **Durée de vie** : durée en secondes à l'issue de laquelle les informations concernant ce voisin sont supprimées.
- **Fonctionnalités** : fonctions principales du périphérique. Les fonctionnalités sont indiquées par deux octets. Les bits 0 à 7 indiquent respectivement Autres, Répéteur, Pont, Point d'accès WLAN, Routeur, Téléphone, Système de câble DOCSIS et Station. Les bits 8 à 15 sont réservés.
- **Plate-forme** : identificateur de la plate-forme du voisin.
- **Interface de voisinage** : numéro d'interface du voisin via lequel la trame a été reçue.
- **VLAN natif** : VLAN natif du voisin.
- **Duplex** : indique si l'interface de voisinage est semi-duplex ou duplex intégral.
- **Adresses** : adresses du voisin.
- **Alimentation prélevée** : puissance consommée par le voisin sur l'interface.
- **Version** : version logicielle du voisin.

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

Affichage des statistiques CDP

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

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

Pour afficher les statistiques CDP :

ÉTAPE 1 Cliquez sur **Administration > Détection - CDP > Statistiques CDP**. La page *Statistiques CDP* s'ouvre.

Les champs suivants sont affichés pour chaque interface :

Paquets reçus/transmis :

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

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

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

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

9

Gestion des ports

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

Elle couvre les rubriques suivantes :

- **Configuration des ports**
- **Définition de la configuration de base des ports**
- **Configuration de l'agrégation de liaisons**
- **Configuration de Green Ethernet**

Configuration des ports

Pour configurer des ports, procédez comme suit :

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

Définition de la configuration de base des ports

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

Pour configurer les paramètres des ports :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Paramètres des ports**. La page *Paramètres des ports* s'ouvre.

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

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

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

ÉTAPE 4 Pour mettre à jour les paramètres des ports, sélectionnez le port voulu et cliquez sur **Modifier**. La page *Modifier les paramètres de port* s'ouvre.

ÉTAPE 5 Modifiez les paramètres suivants :

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

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

- **Description du port** : saisissez le nom défini par l'utilisateur pour ce port ou un commentaire.
- **État administratif** : indiquez si le port doit être démarré ou arrêté au redémarrage du commutateur.
- **État opérationnel :** indique si le port est actuellement actif ou inactif.
- **Réactiver le port suspendu :** sélectionnez cette option pour réactiver un port précédemment suspendu. Vous pouvez suspendre un port de diverses manières, notamment via l'option de sécurité de verrouillage des ports, de violation d'hôte unique dot1x, de détection de bouclage, de garde de bouclage STP. L'opération de réactivation permet de réactiver le port sans tenir compte du motif de suspension du port.
- **Négociation automatique** : sélectionnez cette option pour activer la négociation automatique sur le port. La négociation automatique permet à un port d'annoncer sa vitesse de transmission, son mode duplex et ses fonctions de contrôle de flux à son partenaire de liaison.
- **Négociation automatique opérationnelle** : affiche l'état actuel de la négociation automatique sur le port.
- **Débit de port administratif** : configurez la vitesse du port. Le type de port détermine les vitesses disponibles. Vous ne pouvez choisir *Vitesse administrative* que si la négociation automatique est désactivée pour le port.
- **Débit de port opérationnel** : affiche le débit actuel du port, obtenu par négociation.
- **Mode duplex administratif** : sélectionnez le mode duplex du port. Ce champ ne peut être configuré que lorsque la négociation automatique est désactivée et que le débit du port est réglé sur 10M ou 100M. Lorsque le port a un débit de 1G, le mode est toujours Duplex intégral. Les options disponibles sont les suivantes :
  - *Duplex intégral* : l'interface prend en charge la transmission entre le commutateur et le client dans les deux directions simultanément.
  - *Semi-duplex* : l'interface prend en charge la transmission entre le commutateur et le client dans une seule direction à la fois.
- **Mode duplex opérationnel** : affiche le mode duplex actuel du port.

- **Annonce automatique** : sélectionnez les fonctionnalités annoncées par la négociation automatique lorsqu'elle est activée. Les options sont les suivantes :
  - *Capacité maximale* : tous les débits de port et paramètres de mode duplex sont acceptés.
  - *10 Semi-duplex* : débit de 10Mbits/s et mode Semi-duplex.
  - *10 Duplex intégral* : débit de 10Mbits/s et mode Duplex intégral.
  - *100 Semi-duplex* : débit de 100Mbits/s et mode Semi-duplex.
  - *100 Duplex intégral* : débit de 100Mbits/s et mode Duplex intégral.
  - *1 000 Duplex intégral* : débit de 1 000Mbits/s et mode Duplex intégral.
- **Annonce opérationnelle** : affiche les fonctionnalités actuellement publiées à l'attention du voisin du port. Les options disponibles sont celles spécifiées dans le champ *Annonce administrative*.
- **Annonce de voisin** : affiche les fonctionnalités publiées par le périphérique de voisinage réseau (partenaire de liaison).
- **Contre-pression** : sélectionnez le mode de contre-pression du port (utilisé en mode Semi-duplex) à appliquer pour ralentir la vitesse de réception des paquets en cas de surcharge du commutateur. Cela désactive le port distant, ce qui l'empêche d'envoyer des paquets en engorgeant le signal.
- **Contrôle de flux** : activez ou désactivez le contrôle de flux802.3x ou activez la négociation automatique du contrôle de flux sur le port (uniquement en mode Duplex intégral).
- **MDI/MDIX :** état MDI (*Media Dependent Interface*, interface dépendant du support)/MDIX (*Media Dependent Interface with Crossover*, interface dépendant du support avec croisement) sur le port.

  Les options sont les suivantes :
  - *MDIX* : sélectionnez cette option pour permuter les paires d'émission et de réception.
  - *MDI* : sélectionnez cette option pour relier ce commutateur à une station de travail via un câble droit.
  - *Auto* : sélectionnez cette option pour configurer le commutateur afin qu'il détecte automatiquement le brochage correct pour la connexion à un autre périphérique.

- **MDI/MDIX opérationnel** : affiche le paramètre MDI/MDIX actuel.

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

Configuration de l'agrégation de liaisons

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

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

Présentation de l'agrégation de liaisons

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

Deux types de LAG sont pris en charge :

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

membres actifs. Les ports candidats non actifs sont des ports *de réserve* prêts à remplacer n'importe quel port membre actif défaillant.

Équilibrage de charge

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

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

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

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

Gestion des LAG

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

Le commutateur peut prendre en charge quatre LAG.

Chaque LAG possède les caractéristiques suivantes :

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

- Les divers protocoles, comme Spanning Tree, considèrent tous les ports d'un LAG comme étant un port unique.

Flux de travail des LAG statiques et dynamiques

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

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

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

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

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

Définition de la gestion des LAG

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

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

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Agrégation de liaisons** > **Gestion des LAG**. La page *Gestion des LAG* s'ouvre.

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

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

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

Pour définir les ports membres ou candidats dans un LAG :

ÉTAPE 1 Sélectionnez le LAG à configurer et cliquez sur **Modifier**. La page *Modifier l'appartenance du LAG* s'ouvre.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

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

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

Configuration des paramètres des LAG

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

Pour configurer les paramètres des LAG ou réactiver un LAG suspendu :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Agrégation de liaisons** > **Paramètres des LAG**. La page *Paramètres des LAG* s'ouvre.

ÉTAPE 2 Sélectionnez un LAG et cliquez sur **Modifier**. La page *Modifier les paramètres des LAG* s'ouvre.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **LAG** : sélectionnez l'ID du LAG.
- **Description** : saisissez le nom du LAG ou un commentaire.
- **Type de LAG** : affiche le type de port inclus dans le LAG.
- **État administratif** : définissez le LAG sélectionné comme étant démarré ou arrêté.
- **État opérationnel** : indique si le LAG est actuellement opérationnel.
- **Réactiver le LAG suspendu** : sélectionnez cette option pour réactiver un port si le LAG a été désactivé via l'option de sécurité de verrouillage des ports ou .
- **Négociation automatique administrative** : permet d'activer ou de désactiver la négociation automatique sur le LAG. La négociation automatique est un protocole établi entre deux partenaires de liaison qui permet à un LAG d'annoncer sa vitesse de transmission et son contrôle de flux à son partenaire (la valeur par défaut pour le contrôle de flux est *Désactivé*). Il est recommandé de maintenir la négociation automatique activée des deux côtés d'une liaison agrégée (ou de la désactiver des deux côtés), tout en s'assurant que les débits de liaison sont identiques.
- **Négociation automatique opérationnelle** : affiche le paramètre de négociation automatique.
- **Débit administratif** : sélectionnez le débit du LAG.
- **Débit de LAG opérationnel** : affiche le débit actuel de fonctionnement du LAG.

- **Annonce administrative** : sélectionnez les fonctionnalités que le LAG doit annoncer. Les options sont les suivantes :
  - *Capacité maximale* : tous les débits de LAG et modes duplex sont acceptés.
  - *10 Duplex intégral* : le LAG annonce un débit de 10Mbits/s et le mode est Duplex intégral.
  - *100 Duplex intégral* : le LAG annonce un débit de 100Mbits/s et le mode est Duplex intégral.
  - *1 000 Duplex intégral* : le LAG annonce un débit de 1 000Mbits/s et le mode est Duplex intégral.
- **Annonce opérationnelle** : affiche l'état d'annonce administrative. Le LAG annonce ses fonctions à son voisin pour lancer le processus de négociation. Les options disponibles sont celles spécifiées dans le champ *Annonce administrative*.
- **Contrôle de flux administratif** : définissez le contrôle de flux à **Activer** ou **Désactiver**, ou activez la **négociation automatique** du contrôle de flux sur le LAG.
- **Contrôle de flux opérationnel** : affiche le paramètre de contrôle de flux actuel.

ÉTAPE 4 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Configuration de LACP

Un LAG dynamique est un LAG où LACP est activé ; le protocole LACP (Link Aggregation Control Protocol, protocole de contrôle de l'agrégation de liaisons) est exécuté sur chaque port candidat défini dans le LAG.

Priorité et règles LACP

Les options Priorité du système LACP et Priorité des ports LACP déterminent les ports candidats qui deviennent des ports membres actifs d'un LAG dynamique configuré avec plus de huit ports candidats.

Les ports candidats sélectionnés pour le LAG sont tous connectés au même périphérique distant. Les commutateurs locaux et distants disposent d'une priorité du système LACP.

L'algorithme suivant permet de déterminer si les priorités des ports LACP doivent être obtenues du périphérique local ou du périphérique distant : la priorité du système LACP du périphérique local est comparée à la priorité du système LACP du périphérique distant. Le périphérique ayant la priorité la plus basse contrôle la sélection de port candidat vers le LAG. Si les deux priorités sont identiques, les adresses MAC locale et distante sont comparées. La priorité du périphérique ayant l'adresse MAC la plus basse contrôle la sélection de port candidat vers le LAG.

Un LAG dynamique peut comporter jusqu'à 16 ports Ethernet du même type. Huit ports (maximum) peuvent être actifs et jusqu'à huit ports peuvent être en mode de réserve. Si un LAG dynamique comprend plus de huit ports, le commutateur situé du côté qui contrôle la liaison applique les priorités de port pour déterminer les ports agrégés dans le LAG et ceux qui restent en mode de réserve à chaud. Les priorités des ports de l'autre commutateur (du côté de la liaison qui n'a pas le contrôle) sont ignorées.

Les règles supplémentaires permettant de sélectionner des ports actifs ou de réserve dans un LACP dynamique sont les suivantes :

- Toute liaison fonctionnant avec un débit différent de celui du membre actif ayant le débit le plus élevé ou fonctionnant en mode half-duplex est désignée comme étant celle de réserve. Tous les ports actifs d'un LAG dynamique fonctionnent avec le même débit en bauds.
- Si la priorité LACP du port de la liaison est inférieure à celle des membres de liaison actuellement actifs et si le nombre maximal de membres actifs a déjà été atteint, la liaison devient inactive et placée en mode de réserve.

Configuration des paramètres LACP des ports

La page *LACP* affiche et active la configuration des paramètres Priorité du système LACP, Délai LACP et Priorité des ports LACP. La valeur de délai LACP est définie pour chaque port. Il s'agit de l'intervalle qui sépare l'envoi et la réception de deux PDU LACP consécutives. Lorsque tous les facteurs sont égaux, si le LAG est configuré avec davantage de ports candidats que le maximum de ports actifs autorisé, le commutateur sélectionne des ports et les marque comme actifs à partir du LAG dynamique dont la priorité est la plus élevée.

REMARQUE Le paramètre LACP ne s'applique pas aux ports qui ne sont pas membres d'un LAG dynamique.

Pour définir les paramètres LACP :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Agrégation de liaisons** > **LACP**. La page *LACP* s'ouvre.

ÉTAPE 2 Saisissez la priorité du système LACP. Reportez-vous à la section **Configuration de LACP**.

ÉTAPE 3 Sélectionnez un port et cliquez sur **Modifier**. La page *Modifier LACP* s'ouvre.

ÉTAPE 4 Saisissez les valeurs pour les champs suivants :

- **Interface** : sélectionnez le numéro du port auquel s'appliquent les valeurs de délai et de priorité.
- **Priorité des ports LACP** : saisissez la valeur de priorité LACP du port. Reportez-vous à la section **Configuration des paramètres LACP des ports**.
- **Délai LACP** : sélectionnez les transmissions périodiques des PDU LACP, qui s'effectuent à une vitesse de transmission longue ou courte, selon la préférence de délai LACP définie.

ÉTAPE 5 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Configuration de Green Ethernet

Cette section décrit la fonction Green Ethernet qui est conçue pour réduire la consommation d'énergie du commutateur.

Elle contient les sections suivantes :

- **Présentation de la fonction Green Ethernet**
- **Définition des propriétés Green Ethernet globales**
- **Définition des propriétés Green Ethernet des ports**

Présentation de la fonction Green Ethernet

Green Ethernet est le nom d'usage d'un ensemble de fonctions conçues pour respecter l'environnement et réduire la consommation électrique d'un périphérique. La fonction Green Ethernet est différente de EEE, puisque la détection d'énergie Green Ethernet est activée sur tous les périphériques alors qu'avec EEE, seuls les ports Giga-octets sont activés.

La fonction Green Ethernet réduit la consommation énergétique globale comme suit :

- **Mode Détection d'énergie** : sur une liaison inactive, le port passe en mode inactif, ce qui permet d'économiser l'énergie tout en maintenant le port à l'état administratif Démarré. La sortie de ce mode et le retour au mode entièrement opérationnel sont rapides, transparents et sans aucune perte de trame. Ce mode est pris en charge sur les ports GE comme sur les ports FE.
- **Mode Courte portée** : cette fonction permet d'économiser de l'énergie sur une courte longueur de câble. Une fois que la longueur du câble a été analysée, la consommation d'énergie est ajustée en fonction de cette longueur. Si la longueur de câble est inférieure à 50 mètres, le commutateur a besoin de moins de puissance pour envoyer des trames sur ce câble, ce qui représente une économie d'énergie. Ce mode n'est pris en charge que sur les ports GE RJ45 ; il ne s'applique pas aux ports mixtes.

  Par défaut, ce mode est désactivé au niveau global. Il ne peut pas être activé si le mode EEE est activé (voir ci-dessous).

Outre les fonctions Green Ethernet ci-dessus, la fonction **802.3az Energy Efficient Ethernet (EEE)** est disponible sur les périphériques prenant en charge les ports GE. EEE réduit la consommation électrique lorsqu'il n'y a pas de trafic sur le port. Pour plus d'informations, reportez-vous à **Fonction 802.3az Energy Efficient Ethernet** (uniquement sur les modèles GE).

EEE est activé par défaut au niveau global. Sur un port donné, si EEE est activé, le mode Courte portée est désactivé. Si le mode Courte portée est activé, EEE apparaît en grisé.

Ces modes peuvent être configurés pour chaque port, sans tenir compte de l'appartenance au LAG des ports.

Les LED des périphériques consomment de l'énergie. Étant donné que les périphériques se situent la plupart du temps dans une pièce inoccupée, le fait de maintenir ces LED allumées est un gaspillage d'énergie. La fonction Green Ethernet permet de désactiver les LED des ports (liaison, vitesse et PoE) lorsqu'elles ne sont pas nécessaires et de les activer lorsqu'elles le sont (débogage, raccordement de périphériques supplémentaires, etc.).

Sur la page *Récapitulatif système*, les LED qui sont représentées sur les illustrations des cartes des périphériques ne sont pas affectées par la désactivation des LED.

Il est possible de contrôler les économies d'énergie, la consommation électrique actuelle et l'énergie totale économisée. La quantité totale d'énergie économisée est affichée sous la forme d'un pourcentage de l'énergie qu'auraient consommé les interfaces physiques sans le mode Green Ethernet.

L'énergie économisée s'affiche uniquement si elle est liée à la fonction Green Ethernet. La quantité d'énergie économisée par EEE n'apparaît pas.

Fonction 802.3az Energy Efficient Ethernet

Cette section décrit la fonction 802.3az Energy Efficient Ethernet (EEE).

Elle couvre les rubriques suivantes :

- **Présentation de 802.3az EEE**
- **Négociation des fonctionnalités d'annonce**
- **Découverte de niveau de liaison pour 802.3az EEE**
- **Disponibilité de 802.3az EEE**
- **Configuration par défaut**
- **Interactions entre les fonctions**
- **Workflow de configuration de 802.3az EEE**

Présentation de 802.3az EEE

802.3az EEE est conçue pour réduire la consommation énergétique lorsqu'il n'y a pas de trafic sur la liaison. Dans Green Ethernet, la consommation est réduite lorsque le port est inactif. Avec 802.3az EEE, la consommation est réduite lorsque le port est actif, mais qu'il n'y a pas de trafic sur celui-ci.

La fonction 802.3az EEE est uniquement prise en charge sur les périphériques utilisant des ports GE.

Lorsque vous utilisez la fonction 802.3az EEE, les systèmes situés aux deux extrémités de la liaison peuvent désactiver une partie de leurs fonctionnalités et économiser de l'énergie au cours des périodes sans trafic.

802.3az EEE prend en charge le fonctionnement IEEE 802.3 MAC à 100 Mbits/s et 1 000 Mbits/s :

LLDP permet de sélectionner un ensemble optimal de paramètres pour les deux périphériques. Si LLDP n'est pas pris en charge par le partenaire de liaison ou s'il est désactivé, la fonction 802.3az EEE reste opérationnelle, mais n'utilise peut-être pas le mode opérationnel optimal.

La fonction 802.3az EEE est implémentée via le mode de port LPI (Low Power Idle). Lorsqu'il n'y a pas de trafic et que cette fonction est activée sur le port, ce dernier passe en mode LPI, ce qui réduit de manière importante la consommation énergétique.

Les deux extrémités d'une connexion (le port de commutateur et le périphérique en cours de connexion) doivent prendre en charge 802.3az EEE pour qu'elle fonctionne. Lorsqu'il n'y a aucun trafic, les deux extrémités envoient des signaux indiquant que la consommation va être réduite. Lorsque les signaux provenant des deux extrémités sont reçus, le signal Maintenir actif indique que les ports ont l'état LPI (et non l'état Inactif) et que la consommation est réduite.

Pour que les ports restent en mode LPI, le signal Maintenir actif doit être reçu en continu des deux extrémités.

Négociation des fonctionnalités d'annonce

La prise en charge de la fonction 802.3az EEE est annoncée lors de le phase de négociation automatique. La négociation automatique permet au périphérique lié de détecter les fonctionnalités (modes de fonctionnement) prises en charge par le périphérique situé à l'autre extrémité de la liaison, de déterminer les fonctionnalités communes et de se configurer lui-même pour un fonctionnement conjoint. La négociation automatique s'effectue au moment de la connexion, lors d'une commande exécutée par le système de gestion ou lors de la détection d'une erreur de liaison. Au cours du processus d'établissement de la liaison, les deux partenaires de liaison échangent leurs fonctionnalités 802.3az EEE. La négociation automatique fonctionne automatiquement sans interaction de l'utilisateur lorsqu'elle est activée sur le périphérique.

> **REMARQUE** Si la négociation automatique n'est pas activée sur un port, la fonction EEE est désactivée. La seule exception est que si la vitesse de la liaison est de 1Go ; la fonction EEE est toujours activée même si la négociation automatique est désactivée.

Découverte de niveau de liaison pour 802.3az EEE

Outre les fonctionnalités décrites ci-dessus, les fonctionnalités et paramètres 802.3az EEE sont également annoncés par le biais de trames qui sont basées sur les TLV spécifiques à l'organisation et définies dans l'annexe G du protocole IEEE Std 802.1AB (LLDP). LLDP permet d'optimiser encore davantage le fonctionnement de 802.3az EEE une fois que la négociation automatique est terminée. La TLV 802.3az EEE permet de définir précisément le réveil et les durées d'actualisation du système.

Disponibilité de 802.3az EEE

Reportez-vous aux notes de version pour obtenir la liste complète des produits qui prennent en charge EEE.

Configuration par défaut

Par défaut, les fonctions 802.3az EEE et EEE LLDP sont activées au niveau global et pour chaque port.

Interactions entre les fonctions

Les interactions de 802.3az EEE avec les autres fonctions sont décrites ci-après :

- Si la négociation automatique n'est pas activée sur le port, l'état opérationnel de la fonction 802.3az EEE est désactivé. L'exception à cette règle est que si la vitesse de la liaison est de 1Go, la fonction EEE est toujours activée même si la négociation automatique est désactivée.
- Si la fonction 802.3az EEE est activée et que le port est actif, elle commence à fonctionner immédiatement conformément à la valeur de réveil maximale du port.
- Sur l'interface utilisateur graphique (GUI), le champ EEE du port n'est pas disponible lorsque l'option Mode Courte portée est cochée.
- Si la vitesse du port sur le port GE passe à 10 Mbit, la fonction 802.3az EEE est désactivée. Cette fonctionnalité est uniquement prise en charge sur les modèles GE.

Workflow de configuration de 802.3az EEE

Cette section explique comment configurer la fonction 802.3az EEE et afficher ses compteurs.

ÉTAPE 1 Assurez-vous que la négociation automatique est activée sur le port en ouvrant la page **Gestion des ports > Paramètres des ports**.

a. Sélectionnez un port et ouvrez la page *Modifier le paramètre de port*.

b. Sélectionnez le champ **Négociation automatique** pour vérifier qu'elle est bien activée.

ÉTAPE 2 Assurez-vous que la fonction **802.3 Energy Efficient Ethernet (EEE)** est activée au niveau global sur la page Gestion des ports > Green Ethernet > *Propriétés* (elle est activée par défaut). Cette page indique également la quantité d'énergie qui a été économisée.

ÉTAPE 3 Assurez-vous que la fonction 802.3az EEE est activée sur un port en ouvrant la page Green Ethernet > *Paramètres des ports*.

a. Sélectionnez un port et ouvrez la page *Modifier le paramètre de port*.

b. Activez le mode **802.3 Efficient Energy Ethernet (EEE)** sur le port (il est activé par défaut).

c. Indiquez si vous souhaitez activer ou désactiver l'annonce des fonctionnalités 802.3az EEE via LLDP dans **LLDP 802.3 Energy Efficient Ethernet (EEE)** (elle est activée par défaut).

ÉTAPE 4 Pour consulter les informations associées à 802.3 EEE sur le périphérique local, ouvrez la page *Administration > Détection LLDP > Informations locales LLDP*, puis affichez les informations disponibles dans le bloc 802.3 Energy Efficient Ethernet (EEE).

ÉTAPE 5 Pour consulter les informations associées à 802.3az EEE sur le périphérique distant, ouvrez les pages *Administration > Détection - LLDP > Informations de voisinage LLDP*, puis affichez les informations contenues dans le bloc 802.3 Energy Efficient Ethernet (EEE).

Définition des propriétés Green Ethernet globales

La page *Propriétés* affiche et active la configuration du mode Green Ethernet pour le commutateur. Les économies d'énergie actuelles sont également affichées.

Pour activer Green Ethernet et EEE, et afficher les économies d'énergie :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Green Ethernet** > **Propriétés**. La page *Propriétés* s'ouvre.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **Mode Détection d'énergie :** désactivé par défaut. Activez la case à cocher.
- **Courte portée** : permet d'activer ou de désactiver globalement le mode Courte portée s'il existe des ports GE sur le commutateur.

  REMARQUE Si le mode Courte portée est activé, EEE doit être désactivé.
- **Économies d'énergie** : affiche le pourcentage d'énergie économisé grâce aux modes Green Ethernet et Courte portée. Les économies d'énergie affichées ne concernent que l'énergie économisée grâce aux modes Courte portée et Détection d'énergie. Les économies d'énergie EEE sont de nature dynamique, étant donné qu'elles sont basées sur l'utilisation des ports et qu'elles ne sont par conséquent pas prises en compte.
- **Énergie totale économisée** : affiche la quantité d'énergie économisée depuis le dernier redémarrage du commutateur. Cette valeur est mise à jour à chaque événement qui affecte l'économie d'énergie.
- **802.3 Energy Efficient Ethernet (EEE)** : permet d'activer ou de désactiver globalement le mode EEE.
- **LED des ports :** sélectionnez cette option pour activer les LED des ports. Lorsque les LED des ports sont désactivés, ils n'affichent pas l'état des liaisons, l'activité, etc.

ÉTAPE 3 Cliquez sur **Appliquer**. Les propriétés Green Ethernet sont écrites dans le fichier de Configuration d'exécution.

Définition des propriétés Green Ethernet des ports

La page *Paramètres des ports* affiche les modes Green Ethernet et EEE actuels de chaque port, et permet de configurer la fonction Green Ethernet sur un port par l'intermédiaire de la page *Modifier le paramètre de port*. Pour que les modes Green Ethernet fonctionnent sur un port, vous devez avoir activé ces modes globalement sur la page *Propriétés*.

Notez que les paramètres EEE s'affichent uniquement pour les périphériques qui disposent de ports GE. EEE fonctionne uniquement lorsque les ports sont activés pour la négociation automatique. Seule exception : EEE fonctionne encore même si la négociation automatique est désactivée, mais que le port a un débit de 1 Go minimum.

Pour définir les paramètres Green Ethernet de chaque port :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Green Ethernet** > **Paramètres des ports**. La page *Paramètres des ports* s'ouvre.

La page *Paramètres des ports* affiche les éléments suivants :

- **État des paramètres globaux :** décrit les fonctionnalités activées.

Pour chaque port, les champs suivants sont décrits :

- **Port** : numéro du port.
- **Détection d'énergie** : état du mode Détection d'énergie sur le port :
  - *Administratif* : indique si le mode Détection d'énergie est activé.
  - *Opérationnel* : indique si le mode Détection d'énergie est actuellement opérationnel.
  - *Motif* : si le mode Détection d'énergie n'est pas opérationnel, indique le motif.
- **Courte portée** : état du mode Courte portée sur le port :
  - *Administratif* : indique si le mode Courte portée est activé.
  - *Opérationnel* : indique si le mode Courte portée est actuellement opérationnel.
  - *Motif* : si le mode Courte portée n'est pas opérationnel, indique le motif.
  - *Longueur de câble* : indique la longueur de câble détectée par VCT, en mètres.

REMARQUE Le mode Courte portée n'est pris en charge que sur les ports GE RJ45 ; il ne s'applique pas aux portsmixtes.

- **802.3 Energy Efficient Ethernet (EEE)** : état du port concernant la fonction EEE :
  - *Administratif* : indique si la fonction EEE est activée.
  - *Opérationnel* : indique si la fonction EEE est actuellement opérationnelle sur le port local. Vous savez ainsi si elle a été activée (État administratif), si elle a été activée sur le port local et si elle est opérationnelle sur le port local.
  - *LLDP administratif* : indique si l'annonce des compteurs EEE via LLDP est activée.
  - *LLDP opérationnel* : indique si l'annonce des compteurs EEE via LLDP est actuellement opérationnelle.
  - *Support EEE sur la distance* : indique si la fonction EEE est prise en charge sur le partenaire de liaison. La fonction EEE doit être prise en charge sur les partenaires de liaison local et distant.

REMARQUE Cette fenêtre affiche les paramètres Courte portée, Détection d'énergie et EEE de chaque port. Pour autant, vous ne pouvez pas les activer sur un port s'ils ne sont pas aussi activés globalement via la page *Propriétés*. Pour activer globalement les modes Courte portée et EEE, consultez **Définition des propriétés Green Ethernet globales**.

ÉTAPE 2 Sélectionnez un **port** puis cliquez sur **Modifier**. *La page Modifier le paramètre de port* s'ouvre.

ÉTAPE 3 Choisissez d'activer ou de désactiver le mode Détection d'énergie pour le port.

ÉTAPE 4 Activez ou désactivez le mode Courte portée sur le port si le périphérique comporte des ports GE.

ÉTAPE 5 Activez ou désactivez le mode 802.3 Energy Efficient Ethernet (EEE) sur le port si le périphérique comporte des ports GE.

ÉTAPE 6 Activez ou désactivez le mode LLDP 802.3 Energy Efficient Ethernet (EEE) sur le port (annonce des fonctionnalités EEE via LLDP) si le périphérique comporte des ports GE.

ÉTAPE 7 Cliquez sur **Appliquer**. Les paramètres des ports Green Ethernet sont écrits dans le fichier de Configuration d'exécution.

10

Ports intelligents

Ce document décrit la fonction Port intelligent.

Il contient les rubriques suivantes :

Vue d'ensemble

La fonction Port intelligent constitue un moyen pratique d'enregistrer et de partager des configurations communes. En appliquant la même macro Port intelligent à plusieurs interfaces, ces dernières partagent un ensemble commun de configurations.

Il est possible d'appliquer une macro Port intelligent à une interface par Type de port intelligent associé à la macro.

Il existe deux moyens d'appliquer une macro Port intelligent par Type de port intelligent à une interface :

- **Port intelligent statique** : vous attribuez manuellement un Type de port intelligent à une interface. La macro Port intelligent correspondante est alors appliquée à l'interface.
- **Port intelligent automatique** : le Port intelligent automatique attend qu'un appareil soit associé à l'interface avant d'appliquer une configuration. Lorsqu'un appareil est détecté à partir d'une interface, la macro Port intelligent (si elle est attribuée) qui correspond au Type de port intelligent de l'appareil en cours d'association est automatiquement appliquée.

La fonction Port intelligent est constituée de plusieurs composants et opère conjointement avec d'autres fonctions du commutateur. Ces composants et fonctions sont décrits dans les sections suivantes :

- Port intelligent, Types de port intelligent et Macros Port intelligent, décrits dans cette section.
- VLAN vocal et Port intelligent, décrits dans la section **VLAN voix**.
- LLDP/CDP pour port intelligent, décrits respectivement dans les sections **Configuration de LLDP** et **Configuration de CDP**.

Les workflows classiques sont également décrits dans la section **Tâches courantes de port intelligent**.

Qu'est-ce qu'un port intelligent ?

Un port intelligent est une interface à laquelle une macro intégrée peut être appliquée. Ces macros sont conçues pour permettre de configurer rapidement le commutateur, afin de répondre aux exigences de communication et d'utiliser les fonctions des différents types de périphériques réseau. Les exigences d'accès réseau et de qualité de service (QoS) varient si l'interface est connectée à un téléphone IP, une imprimante, ou un routeur et/ou un point d'accès (AP).

Types de port intelligent

Les Types de port intelligent se réfèrent aux types d'appareils associés ou devant être associés aux ports intelligents. Le commutateur prend en charge les Types de port intelligent suivants :

- Imprimante
- Bureau
- Invité
- Serveur
- Hôte
- Caméra IP
- Téléphone IP
- Téléphone IP + Bureau
- Commutateur
- Routeur
- Point d'accès sans fil

Les Types de port intelligent sont nommés pour décrire le type d'appareil connecté à une interface. Chaque Type de port intelligent est associé à deux macros Port intelligent. La première, appelée « la macro », permet d'appliquer la configuration souhaitée. La deuxième, appelée « l'anti-macro », permet d'annuler toutes les configurations effectuées par « la macro » lorsque cette interface devient un autre Type de port intelligent.

Le tableau suivant décrit la relation entre les Types de port intelligent et le Port intelligent automatique.

Types de port intelligent et port intelligent automatique

Type de port intelligent	Pris en charge par le Port intelligent automatique	Pris en charge par le Port intelligent automatique par défaut
Inconnu	Non	Non
Valeur par défaut	Non	Non
Imprimante	Non	Non
Bureau	Non	Non
Invité	Non	Non
Serveur	Non	Non
Hôte	Oui	Non
Caméra IP	Non	Non
Téléphone IP	Oui	Oui
Téléphone IP Bureau	Oui	Oui
Commutateur	Oui	Oui
Routeur	Oui	Non
Point d'accès sans fil	Oui	Oui

Types de port intelligent spéciaux

Il existe deux Types de port intelligent spéciaux : *par défaut* et *inconnu*. Ces deux types ne sont pas associés à des macros, mais servent à indiquer l'état de l'interface par rapport au port intelligent.

Les Types de port intelligent spéciaux sont décrits ci-dessous :

- **Valeur par défaut**

  Une interface à laquelle un Type de port intelligent n'est pas (encore) attribué a l'état Port intelligent par défaut.

Si le Port intelligent automatique attribue un Type de port intelligent à une interface et que l'interface n'est pas configurée pour être persistante au Port intelligent automatique, alors son Type de port intelligent est réinitialisé aux valeurs par défaut dans les cas suivants :

- Une opération de désactivation/activation de la liaison est effectuée sur l'interface.
- Le commutateur est redémarré.
- Tous les appareils associés à l'interface ont vu leur délai expirer, ce qui est défini par l'absence d'annonce CDP et/ou LLDP en provenance de l'appareil pour une durée spécifiée.

- **Inconnu**

  Si une macro Port intelligent est appliquée à une interface et qu'une erreur se produit, l'état Inconnu est attribué à l'interface. Dans ce cas, les fonctions Port intelligent et Port intelligent automatique ne sont pas actives sur l'interface tant que vous n'avez pas corrigé l'erreur et appliqué l'action Réinitialiser (sur les pages *Paramètres d'interface*) qui réinitialise l'état Port intelligent.

  Pour obtenir des conseils de dépannage, reportez-vous à la zone de workflow dans **Tâches courantes de port intelligent**.

REMARQUE Dans cette section, l'expression « délai expiré » sert à décrire les messages LLDP et CDP via leur TTL. Si la fonction Port intelligent automatique est activée, que l'État persistant est désactivé et qu'aucun message CDP ou LLDP n'est plus reçu sur l'interface avant que les deux TTL des paquets CDP et LLDP les plus récents ne diminuent à 0, l'anti-macro est exécutée et le Type de port intelligent est réinitialisé à ses valeurs par défaut.

Macros Port intelligent

Une macro Port intelligent est un script de qui configure une interface de manière appropriée pour un appareil réseau spécifique.

Ne confondez pas les macros Port intelligent avec les macros globales. Les macros globales configurent le commutateur de manière globale, alors que l'étendue d'une macro Port intelligent est limitée à l'interface à laquelle elle s'applique.

Pour trouver la source de la macro, vous devez cliquant sur le bouton **Afficher la source de la macro** de la page *Paramètres de type de port intelligent*.

Une macro et l'anti-macro correspondante sont couplées en association avec chaque Type de port intelligent. La macro applique la configuration et l'anti-macro la supprime.

Deux macros Port intelligent sont couplées par leurs noms de la manière suivante :

- macro_name (par exemple : printer)
- no_macro_name (par exemple : no_printer, l'anti-macro Port intelligent inverse de la macro Port intelligent printer)

Pour afficher la liste des macros Port intelligent intégrées pour chaque type d'appareil, reportez-vous à la section **Macros Port intelligent intégrées**.

Application d'un Type de port intelligent à une interface

Lorsque des Types de port intelligent sont appliqués aux interfaces, les Types de port intelligent et la configuration dans les macros Port intelligent associées sont enregistrés dans le fichier de Configuration d'exécution. Si l'administrateur enregistre le fichier de Configuration d'exécution dans le fichier de Configuration de démarrage, le commutateur applique les Types de port intelligent et les macros Port intelligent aux interfaces après le redémarrage du système, comme suit :

- Si le fichier de Configuration de démarrage ne spécifie pas de Type de port intelligent pour une interface, son Type de port intelligent est défini sur Par défaut.
- Si le fichier de Configuration de démarrage spécifie un Type de port intelligent statique, le Type de port intelligent de l'interface est défini sur ce type statique.
- Si le fichier de Configuration de démarrage spécifie un Type de port intelligent qui a été dynamiquement attribué par la fonction Port intelligent automatique.
  - Si l'état Port intelligent automatique opérationnel global, l'état Port intelligent automatique de l'interface et l'état Persistant sont tous **activés**, le Type de port intelligent est défini sur ce type dynamique.
  - Sinon, l'anti-macro correspondante est appliquée et l'état de l'interface est défini sur Par défaut.

Échec de la macro et opération de réinitialisation

Une macro Port intelligent peut échouer s'il y a un conflit entre la configuration existante de l'interface et une macro Port intelligent.

Lorsqu'une macro Port intelligent échoue, un message SYSLOG contenant les paramètres suivants est envoyé :

- Numéro de port
- Type de port intelligent
- Numéro de ligne de la commande CLI ayant échoué dans la macro

Lorsqu'une macro Port intelligent échoue sur une interface, l'état de l'interface est défini sur *Inconnu*. La raison de l'échec peut être affichée sur la page *Paramètres d'interface*, dans la fenêtre contextuelle **Afficher les diagnostics**.

Une fois que la source du problème a été identifiée et que la configuration existante ou la macro Port intelligent a été corrigée, vous devez effectuer une opération de réinitialisation pour réinitialiser l'interface avant de pouvoir la réappliquer avec un Type de port intelligent (sur les pages *Paramètres d'interface*). Pour obtenir des conseils de dépannage, reportez-vous à la zone de workflow dans **Tâches courantes de port intelligent**.

Fonctionnement de la fonction Port intelligent

Il est possible d'appliquer une macro Port intelligent à une interface par Type de port intelligent associé à la macro.

Puisque le système prend en charge les Types de port intelligent correspondant aux appareils qui ne peuvent pas être découverts via CDP et/ou LLDP, ces Types de port intelligent doivent être attribués de manière statique aux interfaces souhaitées. Pour ce faire, accédez à la page *Paramètres d'interface de port intelligent*, sélectionnez la case d'option correspondant à l'interface souhaitée, puis cliquez sur **Modifier**. Sélectionnez ensuite le Type de port intelligent que vous souhaitez attribuer, puis définissez les paramètres appropriés avant de cliquer sur **Appliquer**.

Il existe deux moyens d'appliquer une macro Port intelligent par Type de port intelligent à une interface :

- **Port intelligent statique**

  Vous attribuez manuellement un Type de port intelligent à une interface. La macro Port intelligent correspondante est appliquée à l'interface. Sur la page *Paramètres d'interface de port intelligent*, vous pouvez attribuer manuellement un Type de port intelligent à une interface.

- **Port intelligent automatique**

  Lorsqu'un appareil est détecté à partir d'une interface, la macro Port intelligent (si elle est présente) qui correspond au Type de port intelligent de l'appareil en cours d'association est automatiquement appliquée. La fonction Port intelligent automatique est activée par défaut au niveau global et au niveau de l'interface.

Dans les deux cas, l'anti-macro associée est exécutée lorsque le Type de port intelligent est supprimé de l'interface, et l'anti-macro est exécutée exactement de la même manière, supprimant ainsi toute la configuration de l'interface.

Port intelligent automatique

Pour que le Port intelligent automatique attribue automatiquement des Types de port intelligent aux interfaces, la fonction Port intelligent automatique doit être activée au niveau global et sur les interfaces pertinentes que le port intelligent automatique doit être autorisé à configurer. Par défaut, le Port intelligent automatique est activé et autorisé à configurer toutes les interfaces. Le Type de port intelligent attribué à chaque interface est déterminé par les paquets CDP et LLDP reçus respectivement sur chaque interface.

- Si plusieurs appareils sont associés à une interface, un profil de configuration adapté à tous les appareils est si possible appliqué à l'interface.
- Si un appareil est arrivé à expiration (ne reçoit plus d'annonces des autres appareils), la configuration de l'interface est modifiée conformément à son État persistant. Si l'État persistant est activé, la configuration de l'interface est conservée. Sinon, le Type de port intelligent revient à ses valeurs par défaut.

Activation du Port intelligent automatique

Le Port intelligent automatique peut être activé au niveau global sur la page *Propriétés* en procédant comme suit :

- **Activé** : active manuellement le Port intelligent automatique et le rend opérationnel immédiatement.
- **Activer par VLAN voix automatique** : permet au Port intelligent automatique de fonctionner si la fonction VLAN voix automatique est activée et opérationnelle. Activer par VLAN voix automatique est la valeur par défaut.

REMARQUE Outre l'activation du Port intelligent automatique au niveau global, vous devez aussi activer le Port intelligent automatique sur l'interface souhaitée. Par défaut, le Port intelligent automatique est activé sur toutes les interfaces.

Pour plus d'informations sur l'activation du VLAN voix automatique, reportez-vous à la section **VLAN voix**.

Identification du Type de port intelligent

Si le Port intelligent automatique est activé au niveau global (sur la page *Propriétés*) et sur une interface (sur la page *Paramètres d'interface*), le commutateur applique une macro Port intelligent à l'interface conformément au Type de port intelligent de l'appareil en cours d'association. Le Port intelligent automatique détecte les Types de port intelligent des appareils en cours d'association, sur la base des fonctionnalités CDP et/ou LLDP notifiées par les appareils.

Par exemple, si un téléphone IP est associé à un port, il transmet des paquets CDP ou LLDP qui annoncent ses fonctionnalités. Après réception de ces paquets CDP et/ou LLDP, le commutateur détecte le Type de port intelligent approprié au téléphone et applique la macro Port intelligent correspondante à l'interface à laquelle le téléphone IP est associé.

Excepté si le Port intelligent automatique persistant est activé sur une interface, le Type de port intelligent et la configuration générée qui est appliquée par le Port intelligent automatique sont supprimés si le ou les appareils en cours d'association arrivent à expiration, passent en liaison inactive, redémarrent, ou si des fonctionnalités conflictuelles sont reçues. Les délais d'expiration sont déterminés par l'absence d'annonces CDP et/ou LLDP en provenance de l'appareil pour une durée spécifiée.

Utilisation des informations CDP/LLDP pour identifier les Types de port intelligent

Le commutateur détecte le type d'appareil associé au port, sur la base des fonctionnalités CDP/LLDP.

Ce mappage est présenté dans les tableaux suivants :

Mappage des fonctionnalités CDP au Type de port intelligent

Nom de la fonctionnalité	Bit CDP	Type de port intelligent
Routeur	0x01	Routeur
Pont TB	0x02	Point d'accès sans fil
Pont SR	0x04	Ignorer
Commutateur	0x08	Commutateur
Hôte	0x10	Hôte
Filtrage conditionnel IGMP	0x20	Ignorer
Répéteur	0x40	Ignorer
Téléphone VoIP	0x80	ip_phone
Appareil géré à distance	0x100	Ignorer
Port de téléphone CAST	0x200	Ignorer
Relais MAC à deux ports	0x400	Ignorer

Mappage des fonctionnalités LLDP au Type de port intelligent

Nom de la fonctionnalité	Bit LLDP	Type de port intelligent
Autres	1	Ignorer
Répéteur IETF RFC 2108	2	Ignorer
Pont MAC IEEE Std. 802.1D	3	Commutateur
Point d'accès WLAN IEEE Std. 802.11 MIB	4	Point d'accès sans fil

Mappage des fonctionnalités LLDP au Type de port intelligent (Suite)

Nom de la fonctionnalité	Bit LLDP	Type de port intelligent
Routeur IETF RFC 1812	5	Routeur
Téléphone IETF RFC 4293	6	ip_phone
Système de câble DOCSIS IETF RFC 4639 et IETF RFC 4546	7	Ignorer
Station uniquement IETF RFC 4293	8	Hôte
Composant C-VLAN d'un pont VLAN IEEE Std. 802.1Q	9	Commutateur
Composant S-VLAN d'un pont VLAN IEEE Std. 802.1Q	10	Commutateur
Relais MAC à deux ports (TPMR) IEEE Std. 802.1Q	11	Ignorer
Réservé	12-16	Ignorer

REMARQUE Si seul le téléphone IP et les bits hôtes sont définis, le Type de port intelligent est ip_phone_desktop.

Plusieurs appareils associés au port

Le commutateur détecte le Type de port intelligent d'un appareil connecté via les fonctionnalités que l'appareil annonce dans ses paquets CDP et/ou LLDP.

Si plusieurs appareils sont connectés au commutateur par le biais d'une seule interface, le Port intelligent automatique utilise chaque annonce de fonctionnalité qu'il reçoit via cette interface pour attribuer le Type de port intelligent correct. L'attribution est basée sur l'algorithme suivant :

- Si tous les appareils présents sur une interface annoncent la même fonctionnalité (il n'y a pas de conflit), le Type de port intelligent correspondant est appliqué à l'interface.
- Si l'un des appareils est un commutateur, le Type de port intelligent *Commutateur* est utilisé.
- Si l'un des appareils est un point d'accès, le Type de port intelligent *Point d'accès sans fil* est utilisé.

- Si l'un des appareils est un téléphone IP et qu'un autre appareil est un hôte, le Type de port intelligent *ip_phone_desktop* est utilisé.
- Si l'un des appareils est un téléphone IP Bureau et que l'autre est un téléphone IP ou un hôte, le Type de port intelligent *ip_phone_desktop* est utilisé.
- Dans tous les autres cas, le Type de port intelligent par défaut est utilisé.

Pour plus d'informations sur LLDP/CDP, reportez-vous respectivement aux sections **Configuration de LLDP** et **Configuration de CDP**.

Interface du Port intelligent automatique persistant

Si l'État persistant d'une interface est activé, son Type de port intelligent et la configuration qui est déjà appliquée dynamiquement par le Port intelligent automatique sont conservés sur l'interface, même si l'appareil en cours d'association est arrivé à expiration, l'interface a été désactivée et le commutateur a été redémarré (si l'on part du principe que la configuration a été enregistrée). Le Type de port intelligent et la configuration de l'interface ne sont pas modifiés, sauf si le Port intelligent automatique détecte un appareil en cours d'association avec un autre Type de port intelligent. Si l'État persistant d'une interface est désactivé, l'interface rétablit le Type de port intelligent par défaut lorsque l'appareil en cours d'association arrive à expiration, l'interface est désactivée ou le commutateur est redémarré. L'activation de l'État persistant sur une interface élimine le retard de détection de l'appareil.

REMARQUE La persistance des Types de port intelligent appliqués aux interfaces est effective entre les redémarrages uniquement si la configuration d'exécution avec le Type de port intelligent appliqué aux interfaces est enregistrée dans le fichier de Configuration de démarrage.

Gestion des erreurs

Lorsque l'application d'une macro Port intelligent à une interface échoue, vous pouvez examiner le point d'échec sur la page *Paramètres d'interface*, réinitialiser le port et réappliquer la macro une fois que l'erreur a été corrigée à partir des pages *Paramètres d'interface* et *Modifier les paramètres d'interface*.

Configuration par défaut

Le port intelligent est toujours disponible. Par défaut, le Port intelligent automatique est activé par le VLAN voix automatique, se base sur CDP et LLDP pour détecter le Type de port intelligent de l'appareil en cours d'association, et détecte le Type de port intelligent Téléphone IP, Téléphone IP + Bureau, Commutateur et Point d'accès sans fil.

Pour obtenir une description des valeurs de voix par défaut, reportez-vous à la section **VLAN voix**.

Relations avec les autres fonctions et compatibilité descendante

La fonction Port intelligent automatique est activée par défaut. Vous avez la possibilité de la désactiver. Les OUI de téléphonie ne peuvent actuellement pas fonctionner avec les fonctions Port intelligent automatique et VLAN voix automatique. Le Port intelligent automatique doit être désactivé avant d'activer le OUI de téléphonie.

Tâches courantes de port intelligent

Cette section décrit quelques tâches courantes permettant de configurer le Port intelligent et le Port intelligent automatique.

Workflow 1 : *pour activer globalement le Port intelligent automatique sur le commutateur et configurer un port avec la fonction Port intelligent automatique, procédez comme suit :*

ÉTAPE 1 Pour activer la fonction Port intelligent automatique sur le commutateur, ouvrez la page *Port intelligent > Propriétés*. Définissez **Port intelligent automatique administratif** sur **Activer** ou **Activer par VLAN voix**.

ÉTAPE 2 Spécifiez si le commutateur doit traiter les annonces CDP et/ou LLDP des appareils connectés.

ÉTAPE 3 Sélectionnez le type d'appareils à détecter dans le champ **Détection périphérique de port intelligent auto.**.

ÉTAPE 4 Cliquez sur **Appliquer**.

ÉTAPE 5 Pour activer la fonction Port intelligent automatique sur une ou plusieurs interfaces, ouvrez la page *Port intelligent > Paramètres d'interface*.

ÉTAPE 6 Sélectionnez l'interface et cliquez sur **Modifier**.

ÉTAPE 7 Sélectionnez Port intelligent automatique dans le champ **Application de port intelligent**.

ÉTAPE 8 Cochez ou décochez **État persistant**.

ÉTAPE 9 Cliquez sur **Appliquer**.

Workflow 2 : *pour configurer une interface en tant que port intelligent statique, procédez comme suit :*

ÉTAPE 1 Pour activer la fonction Port intelligent sur l'interface, ouvrez la page *Port intelligent > Paramètres d'interface*.

ÉTAPE 2 Sélectionnez l'interface et cliquez sur **Modifier**.

ÉTAPE 3 Sélectionnez le type de port intelligent que vous souhaitez attribuer à l'interface dans le champ **Application de port intelligent**.

ÉTAPE 4 Définissez les paramètres de macro souhaités.

ÉTAPE 5 Cliquez sur **Appliquer**.

Workflow 3 : *pour définir les valeurs par défaut des paramètres de macro Port intelligent, procédez comme suit :*

Cette procédure vous permet d'effectuer les tâches suivantes :

- Afficher la source de la macro.
- Modifier les valeurs par défaut des paramètres.
- Restaurer les paramètres d'usine.

1. Ouvrez la page *Port intelligent > Paramètres de type de port intelligent*.
2. Sélectionnez le Type de port intelligent.
3. Cliquez sur **Afficher la source de la macro** pour afficher la macro Port intelligent actuelle qui est associée au Type de port intelligent sélectionné.

4. Cliquez sur **Modifier** pour ouvrir une nouvelle fenêtre Les valeurs par défaut de ces paramètres sont utilisées lorsque le Port intelligent automatique applique le Type de port intelligent sélectionné (le cas échéant) à une interface.
5. Sur la page *Modifier*, modifiez les champs.
6. Cliquez sur **Appliquer** pour réexécuter la macro si les paramètres ont été modifiés ou sur **Restaurer les valeurs par défaut** pour restaurer si nécessaire les valeurs par défaut des paramètres dans les macros intégrées.

Workflow 4 : *pour réexécuter une macro Port intelligent si celle-ci a échoué, procédez comme suit :*

ÉTAPE 1 Sur la page *Paramètres d'interface*, sélectionnez une interface avec le Type de port intelligent Inconnu.

ÉTAPE 2 Cliquez sur **Afficher les diagnostics** pour visualiser le problème.

ÉTAPE 3 Lancez la procédure de dépannage, puis corrigez le problème. Reportez-vous au conseil de dépannage ci-dessous.

ÉTAPE 4 Cliquez sur **Modifier.** Une nouvelle fenêtre s'ouvre. Cliquez sur **Réinitialiser** pour réinitialiser l'interface.

ÉTAPE 5 Revenez à la page principale et réappliquez la macro en utilisant **Réappliquer** (pour les appareils qui ne sont ni des commutateurs, ni des routeurs ni des points d'accès) ou **Réappliquer la macro de port intelligent** (pour les commutateurs, routeurs ou points d'accès) afin d'exécuter la macro Port intelligent sur l'interface.

Il existe une deuxième méthode de réinitialisation des interfaces uniques ou multiples inconnues :

ÉTAPE 1 Sur la page *Paramètres d'interface*, activez la case à cocher *Type de port est égal à*.

ÉTAPE 2 Sélectionnez *Inconnu* et cliquez sur **OK**.

ÉTAPE 3 Cliquez sur **Réinitialiser tous les ports intelligents inconnus**. Réappliquez ensuite la macro comme indiqué ci-dessus.

ASTUCE L'échec de la macro peut être dû à un conflit avec une configuration de l'interface qui a été effectuée avant l'application de la macro (le plus souvent rencontré dans les paramètres de sécurité et de contrôle des tempêtes), un type de port incorrect, une typo ou une commande incorrecte dans la macro définie par l'utilisateur ou encore une valeur de paramètre non valide. Les paramètres sont contrôlés, sans prise en compte du type ou de la limite, avant la tentative d'application de la macro. Par conséquent, une entrée incorrecte ou non valide pour une valeur de paramètre se soldera presque assurément par un échec lors de l'application de la macro.

Configuration de port intelligent à l'aide de l'interface Web

Vous pouvez configurer la fonction Port intelligent sur les pages *Port intelligent > Propriétés*, *Paramètres de type de port intelligent* et *Paramètres d'interface*.

Pour la configuration du VLAN vocal, reportez-vous à la section **VLAN voix**.

Pour la configuration de LLDP/CDP, reportez-vous respectivement aux sections **Configuration de LLDP** et **Configuration de CDP**.

Propriétés de port intelligent

Pour configurer la fonction Port intelligent de façon globale :

ÉTAPE 1 Cliquez sur **Port intelligent > Propriétés**. La page *Propriétés* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **Port intelligent automatique administratif** : sélectionnez cette option pour activer ou désactiver globalement le Port intelligent automatique. Les options suivantes sont disponibles :
  - *Désactiver* : sélectionnez cette option pour désactiver le Port intelligent automatique sur l'appareil.
  - *Activer* : sélectionnez cette option pour activer le Port intelligent automatique sur l'appareil.
  - *Activer par VLAN voix automatique* : cette option active le Port intelligent automatique, mais ne le rend opérationnel que lorsque le VLAN voix automatique est aussi activé et opérationnel. Activer par VLAN voix automatique est la valeur par défaut.

- **Méthode de détection périphérique de port intelligent auto.** : indiquez si les types de paquets entrants CDP et/ou LLDP doivent être utilisés pour détecter le Type de port intelligent des appareils en cours d'association. Vous devez cocher au moins un type pour que le Port intelligent automatique puisse identifier les appareils.
- **État CDP opérationnel** : affiche l'état opérationnel du CDP. Activez CDP si le Port intelligent automatique doit détecter le Type de port intelligent à partir de l'annonce CDP.
- **État LLDP opérationnel** : affiche l'état opérationnel du LLDP. Activez LLDP si le Port intelligent automatique doit détecter le Type de port intelligent à partir de l'annonce LLDP/LLDP-MED.
- **Détection périphérique de port intelligent auto.** : sélectionnez chaque type d'appareil pour lequel le Port intelligent automatique peut attribuer des Types de port intelligent aux interfaces. Si vous ne cochez pas cette option, le Port intelligent automatique n'attribue ce Type de port intelligent à aucune interface.

ÉTAPE 3 Cliquez sur **Appliquer**. Vous appliquez ainsi les paramètres de Port intelligent globaux sur le commutateur.

Paramètres de type de port intelligent

Utilisez la page *Paramètres de type de port intelligent* pour modifier les paramètres de type de port intelligent et afficher la source de la macro.

Par défaut, chaque Type de port intelligent est associé à une paire de macros Port intelligent intégrées. Pour plus d'informations sur la macro et l'anti-macro, reportez-vous à la section **Types de port intelligent**. Les macros intégrées ou définies par l'utilisateur peuvent comporter des paramètres. Les macros intégrées peuvent intégrer jusqu'à trois paramètres.

La modification de ces paramètres pour les Types de port intelligent qui sont appliqués par le Port intelligent automatique sur la page *Paramètres de type de port intelligent* configure les valeurs par défaut de ces paramètres. Ces valeurs par défaut sont utilisées par le Port intelligent automatique.

REMARQUE Une fois les modifications apportées aux types Port intelligent automatique, les nouveaux paramètres sont appliqués aux interfaces auxquelles le Port intelligent automatique a déjà attribué ce type. Dans ce cas, si vous liez une macro non valide ou définissez une valeur par défaut non valide pour un paramètre, tous les ports de ce Type de port intelligent deviennent inconnus.

ÉTAPE 1 Cliquez sur **Port intelligent > Paramètres de type de port intelligent**. La page *Paramètres de type de port intelligent* s'ouvre.

ÉTAPE 2 Pour afficher la macro Port intelligent associée à un Type de port intelligent, sélectionnez un Type de port intelligent, puis cliquez sur **Afficher la source de la macro**.

ÉTAPE 3 , sélectionnez un Type de port intelligent, puis cliquez sur **Modifier**. La page *Modifier les paramètres de type de port intelligent* s'ouvre.

ÉTAPE 4 Renseignez les champs.

- **Type de port** : sélectionnez un Type de port intelligent.
- **Nom de la macro** : affiche le nom de la macro Port intelligent actuellement associée au Type de port intelligent.
- **Paramètres de macro** : affiche les champs suivants pour trois paramètres dans la macro :
  - *Nom du paramètre* : nom du paramètre dans la macro.
  - *Valeur du paramètre* : valeur actuelle du paramètre dans la macro. Vous pouvez la modifier ici.
  - *Description du paramètre* : description du paramètre.

  Vous pouvez restaurer les valeurs par défaut des paramètres en cliquant sur **Restaurer les valeurs par défaut**.

ÉTAPE 5 Cliquez sur **Appliquer** pour enregistrer les modifications dans la configuration d'exécution. Si la macro Port intelligent et/ou ses valeurs de paramètre associées au Type de port intelligent sont modifiées, le Port intelligent automatique réapplique automatiquement la macro aux interfaces qui sont actuellement attribuées avec le Type de port intelligent par le Port intelligent automatique. Le Port intelligent automatique n'applique pas les modifications aux interfaces auxquelles un Type de port intelligent a été attribué de façon statique.

REMARQUE Il n'existe aucune méthode permettant de valider les paramètres de macro, car ils n'ont aucune association de type. Toutefois, n'importe quelle entrée est valide à ce stade. Néanmoins, des valeurs de paramètre non valides peuvent entraîner des erreurs lorsque le Type de port intelligent est attribué à une interface appliquant la macro associée.

Paramètres d'interface de port intelligent

Utilisez la page *Paramètres d'interface* pour effectuer les tâches suivantes :

- Appliquez de manière statique un Type de port intelligent spécifique à une interface, avec des valeurs spécifiques à l'interface pour les paramètres de macro.
- Activez le Port intelligent automatique sur une interface.
- Diagnostiquez une macro Port intelligent dont l'application a échoué et a généré l'état Inconnu du Type de port intelligent.
- Réappliquez une macro Port intelligent après son échec pour l'un des types d'interface suivants : commutateur, routeur et point d'accès. Nous partons du principe que vous avez effectué les corrections nécessaires avant de cliquer sur **Réappliquer**. Pour obtenir des conseils de dépannage, reportez-vous à la zone de workflow dans **Tâches courantes de port intelligent**.
- Réappliquez une macro Port intelligent à une interface. Dans certaines circonstances, il se peut que vous souhaitiez réappliquer une macro Port intelligent pour mettre à jour la configuration sur une interface. Par exemple, en réappliquant une macro Port intelligent de commutateur sur une interface de commutateur, l'interface devient membre des VLAN qui ont été créés depuis la dernière application de la macro. Vous devez connaître les configurations actuelles du commutateur et la définition de la macro pour déterminer si une réapplication aura un impact sur l'interface.
- Réinitialisez les interfaces inconnues. Le mode des interfaces inconnues est ainsi défini sur Par défaut.

Pour appliquer une macro Port intelligent :

ÉTAPE 1 Cliquez sur **Port intelligent > Paramètres d'interface**. La page *Paramètres d'interface* s'ouvre.

Réappliquez la macro Port intelligent associée comme suit :

- Sélectionnez un groupe de Types de port intelligent (commutateurs, routeurs ou points d'accès) et cliquez sur **Réappliquer la macro de port intelligent.** Les macros sont appliquées à tous les types d'interface sélectionnés.
- Sélectionnez une interface UP et cliquez sur **Réappliquer** pour réappliquer la dernière macro qui a été appliquée à l'interface.

L'action **Réappliquer** ajoute aussi l'interface à tous les VLAN nouvellement créés.

ÉTAPE 2 Diagnostic de port intelligent.

Si une macro Port intelligent échoue, le Type de port intelligent de l'interface est Inconnu. Sélectionnez une interface dont le type est inconnu, puis cliquez sur **Afficher les diagnostics**. Le système affiche la commande où l'application de la macro a échoué. Pour obtenir des conseils de dépannage, reportez-vous à la zone de workflow dans **Tâches courantes de port intelligent**. Corrigez le problème et réappliquez la macro.

ÉTAPE 3 Réinitialisation de toutes les interfaces inconnues au type Par défaut.

- Activez la case à cocher *Type de port est égal à*.
- Sélectionnez *Inconnu* et cliquez sur **OK**.
- Cliquez sur **Réinitialiser tous les ports intelligents inconnus**. Réappliquez ensuite la macro comme indiqué ci-dessus. Cette opération réinitialise l'ensemble des interfaces de type Inconnu, ce qui signifie que le type Par défaut est réattribué à toutes les interfaces. Une fois que vous avez corrigé l'erreur dans la macro et/ou dans la configuration d'interface actuelle, vous pouvez appliquer une nouvelle macro.

REMARQUE La réinitialisation de l'interface de type inconnu ne réinitialise pas la configuration effectuée par la macro qui a échoué. Ce nettoyage doit être réalisé manuellement.

Pour attribuer un Type de port intelligent à une interface ou activer la fonction Port intelligent automatique sur l'interface :

ÉTAPE 1 Sélectionnez une interface et cliquez sur **Modifier**. La page *Modifier les paramètres d'interface* s'ouvre.

ÉTAPE 2 Renseignez les champs.

- **Interface :** sélectionnez le port ou LAG.
- **Type de port intelligent** : affiche le Type de port intelligent actuellement attribué au port/LAG.
- **Application de port intelligent** : sélectionnez le Type de port intelligent dans le menu déroulant Application de port intelligent.
- **Méthode d'application de port intelligent** : si le Port intelligent automatique est sélectionné, il attribue automatiquement le Type de port intelligent en fonction de l'annonce CDP et/ou LLDP reçue des appareils en cours de connexion, et applique la macro Port intelligent correspondante. Pour

attribuer un Type de port intelligent de manière statique et appliquer la macro Port intelligent correspondante à l'interface, sélectionnez le Type de port intelligent souhaité.

- **État persistant** : sélectionnez cette option pour activer l'État persistant. S'il est activé, l'association d'un Type de port intelligent à une interface est conservée même si l'interface est désactivée ou que le commutateur est redémarré. L'État persistant s'applique uniquement si l'Application de port intelligent de l'interface est Port intelligent automatique. L'activation de l'État persistant sur une interface élimine le retard de détection de l'appareil.
- **Paramètres de macro** : affiche les champs suivants pour un maximum de trois paramètres dans la macro :
  - *Nom du paramètre* : nom du paramètre dans la macro.
  - *Valeur du paramètre* : valeur actuelle du paramètre dans la macro. Vous pouvez la modifier ici.
  - *Description du paramètre* : description du paramètre.

ÉTAPE 3 Cliquez sur **Réinitialiser** pour définir une interface sur Par défaut si elle a l'état Inconnu (en raison d'un échec d'application de macro). La macro peut être réappliquée sur la page principale.

ÉTAPE 4 Cliquez sur **Appliquer** pour mettre à jour les modifications et attribuer le Type de port intelligent à l'interface.

Macros Port intelligent intégrées

Vous trouverez ci-dessous une description de la paire de macros intégrées pour chaque Type de port intelligent. Pour chaque Type de port intelligent, une macro permet de configurer l'interface et une anti-macro permet de supprimer la configuration.

Le code de macro des Types de port intelligent suivants est indiqué ci-après :

- **desktop**
- **printer**
- **guest**
- **server**
- **host**

- ip_camera
- ip_phone
- ip_phone_desktop
- switch
- router
- ap

desktop

```
[desktop]
#interface configuration, for increased network security and reliability when
connecting a desktop device, such as a PC, to a switch port.
#macro description Desktop
#macro keywords $native_vlan $max_hosts
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                       $max_hosts: Nombre maximal d'appareils autorisés sur
le port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_desktop

```
[no_desktop]
#macro description No Desktop
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
```

```
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

printer

```
[printer]
#macro description printer
#macro keywords $native_vlan
#
#macro key description: $native_vlan: VLAN sans balise qui sera configuré sur
le port
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_printer

```
[no_printer]
#macro description No printer
#
no switchport access vlan
no switchport mode
#
no port security
```

```
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

guest

```
[guest]
#macro description guest
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré
sur le port
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_guest

```
[no_guest]
#macro description No guest
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
```

```
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

server

```
[server]
#macro description server
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                        $max_hosts: Nombre maximal d'appareils autorisés sur
le port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_server

```
[no_server]
#macro description No server
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
```

```
#
spanning-tree portfast auto
#
@
```

host

```
[host]
#macro description host
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                        $max_hosts: Nombre maximal d'appareils autorisés sur
le port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_host

```
[no_host]
#macro description No host
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
```

```
#
spanning-tree portfast auto
#
@
```

ip_camera

```
[ip_camera]
#macro description ip_camera
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré
sur le port
#Default Values are
#$native_vlan = Default VLAN
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_camera

```
[no_ip_camera]
#macro description No ip_camera
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone

```
[ip_phone]
#macro description ip_phone
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                         $voice_vlan: ID du VLAN voix
#                        $max_hosts: Nombre maximal d'appareils autorisés sur
le port
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone

```
[no_ip_phone]
#macro description no ip_phone
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: ID du VLAN voix
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
```

```
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone_desktop

```
[ip_phone_desktop]
#macro description ip_phone_desktop
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                         $voice_vlan: ID du VLAN voix
#                        $max_hosts: Nombre maximal d'appareils autorisés sur
le port
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone_desktop

```
[no_ip_phone_desktop]
#macro description no ip_phone_desktop
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: ID du VLAN voix
#
#Default Values are
#$voice_vlan = 1
#
```

```
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

switch

```
[switch]
#macro description switch
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                        $voice_vlan: ID du VLAN voix
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
#
@
```

no_switch

```
[no_switch]
#macro description No switch
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: ID du VLAN voix
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

router

```
[router]
#macro description router
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                        $voice_vlan: ID du VLAN voix
#
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree link-type point-to-point
#
@
```

no_router

[no_router]

#macro description No router

#macro keywords $voice_vlan

#

#macro key description: $voice_vlan: ID du VLAN voix

#

no smartport switchport trunk native vlan

smartport switchport trunk allowed vlan remove all

#

no smartport storm-control broadcast enable

no smartport storm-control broadcast level

#

no spanning-tree link-type

```
#
@
```

ap

```
[ap]
#macro description ap
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                        $voice_vlan: ID du VLAN voix
#
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
#
@
```

no_ap

```
[no_ap]
#macro description No ap
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: ID du VLAN voix
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

11

Gestion des appareils PoE

La fonctionnalité PoE (Power over Ethernet) n'est disponible que sur les appareils basés sur PoE. Une liste de ces appareils vous est présentée à la section **Modèles de commutateurs**.

Cette section décrit comment utiliser la fonctionnalité PoE.

Elle couvre les rubriques suivantes :

- **PoE sur le commutateur**
- **Configuration des propriétés PoE**
- **Configurer la puissance, la priorité et la classe PoE**

PoE sur le commutateur

Un commutateur PoE est un appareil PSE (Power Sourcing Equipment) qui fournit une alimentation électrique à des appareils alimentés (PD, Powered Devices) sur des câbles en cuivre existants sans avoir à interférer avec le trafic réseau, à mettre à jour le réseau physique ni à modifier l'infrastructure réseau.

Consultez la section **Modèles de commutateurs** pour en savoir plus sur la prise en charge PoE sur les différents modèles.

Fonctionnalités PoE

PoE offre les fonctionnalités suivantes :

- Élimine le besoin de fournir une alimentation de 110/220 VCA à tous les appareils connectés à un LAN câblé.
- Supprime le besoin de placer tous les appareils réseau à proximité de sources d'alimentation.

- Élimine le besoin de déployer des systèmes à double câblage dans une entreprise et permet ainsi de réduire de façon significative les coûts d'installation.

PoE peut être utilisé dans tout réseau d'entreprise déployant des appareils de puissance relativement faible connectés auLAN Ethernet et notamment :

- les téléphones IP,
- les points d'accès sans fil,
- les passerelles IP,
- les appareils de surveillance audio et vidéo à distance.

Fonctionnement de PoE

La mise en œuvre de PoE comprend les étapes suivantes :

- Détection : envoie des impulsions spéciales sur le câble en cuivre. Lorsqu'un appareilPoE est situé à l'autre extrémité, cet appareil répond à ces impulsions.
- Classification : la négociation entre le PSE (Power Sourcing Equipment) et l'appareil alimenté (PD, Powered Device) débute après l'étape de détection. Au cours de la négociation, le PD spécifie sa classe, qui correspond à la puissance maximale qu'il consomme.
- Consommation électrique : une fois l'étape de classification terminée, le PSE fournit de la puissance au PD. Si ce dernier prend en charge PoE, il est considéré en l'absence d'une classification comme étant de classe 0 (le maximum). Si un PD essaie de consommer plus de puissance que ne l'autorise la norme, le PSE arrête d'alimenter le port.

PoE prend en charge deux modes :

- Limite du port : la puissance maximale que le commutateur accepte de fournir est limitée à la valeur configurée par l'administrateur système, ceci indépendamment du résultat de la classification.
- Limite de classe : la puissance maximale que le commutateur accepte de fournir est déterminée par les résultats de l'étape Classification. Cela signifie qu'elle est définie conformément à la demande du client.

Considérations relatives à la configuration de PoE

Deux facteurs sont à prendre en considération dans la fonctionnalité PoE :

- la quantité de puissance que le PSE peut fournir ;
- la quantité de puissance que le PD essaie véritablement de consommer.

Vous pouvez décider :

- de la puissance maximale qu'un PSE est autorisé à fournir à un PD ;
- alors que l'appareil fonctionne, de changer le mode de Limite de classe en Limite du port et vice versa. de conserver les valeurs de puissance par port ayant été configurées pour le mode Limite du port ;
- de la limite de port maximale autorisée en tant que limite numérique par port enmW (mode Limite du port) ;
- de générer un message « trap » lo'squ'un PD essaie de consommer trop de puissance et pour déterminer à quel pourcentage de la puissance maximale ce message est généré.

Le matériel PoE spécifique détecte automatiquement la classe du PD et sa limite de puissance en fonction de la classe de l'appareil connecté à chaque port spécifique (mode Limite de classe).

Si, à tout moment au cours de la connexion, un PD relié nécessite plus de puissance de la part du commutateur que ce que permet l'allocation configurée (que le commutateur soit en mode Limite de classe ou Limite du port), le commutateur :

- maintient l'état actif/inactif de la liaison du port PoE ;
- désactive la fourniture de puissance au port PoE ;
- journalise le motif de l'arrêt de l'alimentation ;
- génère un message « trap » pour un serveur de journalisation distant.

ATTENTION Tenez compte des éléments suivants lorsque vous connectez des commutateurs capables de fournir le PoE :

les modèles PoE des séries Sx200, Sx300 et Sx500 sont des appareils PSE (Power Sourcing Equipment) qui peuvent fournir une alimentation CC à des périphériques connectés (PD, Powered Devices). Ces derniers englobent notamment des téléphones VoIP, des caméras IP et des points d'accès sans fil. Les commutateurs PoE peuvent détecter et alimenter des périphériques connectés

PoE existants pré-standard. En raison de la prise en charge du PoE hérité, un commutateur PoE agissant en tant qu'appareil PSE peut détecter et alimenter à tort un appareil PSE connecté, y compris d'autres commutateurs PoE, en tant que PD hérité.

Même si les commutateurs PoE Sx200/300/500 sont des appareils PSE qui doivent bénéficier de courant alternatif, ils peuvent être alimentés en tant que PD hérité par un autre appareil PSE suite à une erreur de détection. Si vous êtes confronté à cette situation, le commutateur PoE risque de ne pas fonctionner correctement et peut également ne pas alimenter convenablement ses PD connectés.

Pour éviter toute erreur de détection, vous devez désactiver le PoE au niveau des ports des commutateurs PoE que vous utilisez pour vous connecter à des appareils PSE. Vous devez également d'abord alimenter un appareil PSE avant de le connecter à un commutateur PoE. Lorsqu'un périphérique est considéré à tort comme un PD, vous devez déconnecter le périphérique du port PoE, puis l'alimenter avec du courant alternatif avant de reconnecter ses ports PoE.

Configuration des propriétés PoE

La page *Propriétés PoE* permet de sélectionner le mode PoE Limite du port ou Limite de classe, et de spécifier les messages « trap » PoE à générer.

Ces paramètres sont saisis à l'avance. Lorsque le PD se connecte et consomme de la puissance, il peut consommer bien moins que la puissance maximale autorisée.

La puissance de sortie est désactivée lors du redémarrage, de l'initialisation et de la configuration système pour veiller à ne pas endommager les PD.

Pour configurer PoE sur le commutateur et surveiller la puissance consommée :

ÉTAPE 1 Cliquez sur **Gestion des ports > PoE > Propriétés**. La page *Propriétés PoE* s'ouvre.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **Mode d'alimentation :** sélectionnez l'une des options suivantes :
  - *Limite du port :* la limite maximale de puissance par port est configurée par l'utilisateur.

- *Limite de classe :* la limite maximale de puissance par port est déterminée par la classe de l'appareil, elle-même résultant de l'étape de Classification.

- **Interceptions** : permettent d'activer ou de désactiver une interception SYSLOG.

- **Seuil des interceptions d'alimentation :** saisissez le seuil d'utilisation sous la forme d'un pourcentage de la limite de puissance. Une alarme se déclenche si la puissance dépasse cette valeur.

Les compteurs suivants sont affichés pour chaque périphérique :

- **Puissance nominale :** la quantité totale de puissance que le commutateur peut fournir à l'ensemble des PD connectés.
- **Consommation :** puissance actuellement consommée par les ports PoE.
- **Puissance disponible :** puissance nominale moins la quantité de puissance consommée.

ÉTAPE 3 Cliquez sur **Appliquer** pour enregistrer les propriétés PoE.

Configurer la puissance, la priorité et la classe PoE

La page *Paramètres PoE* affiche les informationsPoE système pour l'activation de PoE sur les interfaces et la surveillance de la consommation actuelle ainsi que de la limite maximale de puissance par port.

Cliquez sur **Gestion des ports > PoE > Propriétés**. La page *Paramètres* s'ouvre.

Cette page permet de limiter la puissance par port de deux façons différentes, ceci en fonction du mode d'alimentation :

- **Limite du port :** la puissance est limitée à une consommation en watts spécifique. Pour que ces paramètres soient actifs, le système doit être en mode Limite du port PoE. Vous pouvez configurer ce mode sur la page *Propriétés PoE*.

  Lorsque la puissance consommée sur le port dépasse la limite du port, l'alimentation du port est désactivée.

- **Limite de classe :** la puissance est limitée en fonction de la classe du PD connecté. Pour que ces paramètres soient actifs, le système doit être en

mode Limite de classe PoE. Vous pouvez configurer ce mode sur la page *Propriétés PoE*.

Lorsque la puissance consommée sur le port dépasse la limite de classe, l'alimentation du port est désactivée.

Exemple de priorité PoE :

Supposition : un commutateur à 48 ports fournit un total de 375 watts.

L'administrateur configure tous les ports pour qu'ils allouent jusqu'à 30 watts. Au final, si les 48 ports allouent 30 watts chacun, on obtient 1 440 watts, ce qui est bien trop. Le commutateur ne peut pas fournir suffisamment de puissance à chaque port, il suit donc certaines priorités.

L'administrateur définit la priorité de chaque port, en lui allouant autant de puissance que possible.

Vous devez entrer ces priorités sur la page *Paramètres PoE*.

Reportez-vous à la section **Modèles de commutateurs** pour obtenir une description des modèles de commutateurs qui prennent en charge la fonctionnalité PoE et connaître la puissance maximale pouvant être allouée aux ports PoE.

Pour configurer les paramètres de port PoE :

ÉTAPE 1 Cliquez sur **Gestion des ports > PoE > Propriétés**. La page *Paramètres* s'ouvre. La liste des champs ci-dessous correspond au mode d'alimentation Limite du port. Les champs peuvent légèrement différer si le mode d'alimentation est Limite de classe.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier.** La page *Modifier les paramètres PoE* s'ouvre. La liste des champs ci-dessous correspond au mode d'alimentation Limite du port. Les champs peuvent légèrement différer si le mode d'alimentation est Limite de classe.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **Interface** : sélectionnez le port à configurer.
- **État administratif PoE** : permet d'activer ou de désactiver PoE sur le port.

- **Niveau de priorité d'alimentation :** sélectionnez la priorité du port (faible, élevée ou critique) qui sera utilisée en cas de manque de puissance. Par exemple, si 99 % de la puissance disponible est consommée, et que le port 1 a une priorité élevée et le port 3 une priorité faible, le port 1 sera alimenté, contrairement au port 3.
- **Affectation de puissance administrative** : ce champ ne s'affiche que si le mode d'alimentation Limite du port est défini sur la page *Propriétés PoE*. Si le mode d'alimentation Limite du port est sélectionné, saisissez la puissance affectée au port (en milliwatts).
- **Affectation de puissance maximale** : affiche la puissance maximale autorisée sur ce port.
- **Classe** : ce champ ne s'affiche que si le mode d'alimentation Limite de classe est défini sur la page *Propriétés PoE*. La classe détermine le niveau de puissance :

Classe	Puissance maximale fournie par le port du commutateur
0	15,4 W
1	4,0 W
2	7,0 W
3	15,4 W
4	30,0 W

- **Consommation électrique :** affiche la puissance (en milliwatts) affectée à l'appareil alimenté connecté à l'interface sélectionnée.
- **Nombre de surcharges :** affiche le nombre total d'occurrences de surcharges de courant.
- **Nombre de courts-circuits :** affiche le nombre total d'occurrences de courts-circuits électriques.
- **Nombre de refus :** affiche le nombre de fois où l'alimentation a été refusée pour l'appareil alimenté.
- **Nombre d'absences :** affiche le nombre de fois où l'alimentation de l'appareil alimenté a été arrêtée, l'appareil n'étant plus détecté.

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

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres PoE du port sont consignés dans le fichier de Configuration d'exécution.

12

Gestion des VLAN

Cette section couvre les rubriques suivantes :

- VLAN
- Configuration des paramètres VLAN par défaut
- Création d'un VLAN
- Configuration des paramètres d'interface VLAN
- Définition de l'appartenance VLAN
- VLAN voix

VLAN

Un VLAN est un groupe de ports logique qui permet aux périphériques qui lui sont associés de communiquer entre eux sur une couche MAC Ethernet, quel que soit le segment LAN physique du réseau raccordé auquel ils sont connectés.

Description des VLAN

Les VLAN sont configurés avec un VID unique (ID VLAN) dont la valeur est comprise entre 1 et 4094. Un port sur un périphérique d'un réseau raccordé est membre d'un VLAN s'il peut échanger (envoyer/recevoir) des données avec le VLAN. Un port est un membre non balisé d'un VLAN si aucun des paquets qui lui sont destinés ne dispose de balise. Un port est un membre balisé d'un VLAN si tous les paquets qui lui sont destinés disposent d'une balise VLAN. Un port peut être membre d'un seul VLAN non balisé et de plusieurs VLAN balisés.

Un port en mode Accès VLAN ne peut faire partie que d'un seul VLAN. S'il est en mode Général ou Liaison, le port peut faire partie d'un ou plusieurs VLAN.

Les VLAN traitent les problèmes de sécurité et d'extensibilité. Le trafic d'un VLAN reste à l'intérieur du VLAN et se termine à ses périphériques. Il facilite également la configuration réseau en connectant logiquement les périphériques sans les transférer physiquement.

Si une trame est balisée VLAN, une balise VLAN à 4 octets est ajoutée à chaque trame Ethernet. La balise contient un ID VLAN compris entre 1 et 4094 et une balise de priorité VLAN (VPT) comprise entre 0 et 7. Pour plus d'informations sur VPT, reportez-vous à **Configuration de la QoS (Qualité de service)**.

Lorsqu'une trame entre dans un périphérique tenant compte du VLAN, elle est classée comme appartenant à un VLAN spécifique en vertu de sa balise VLAN à 4 octets au sein de la trame.

S'il n'existe aucune balise VLAN dans la trame ou si la trame comporte une balise de priorité, elle est catégorisée dans le VLAN selon le PVID (identificateur de port VLAN) configuré au port de réception de la trame.

La trame est désactivée au port d'entrée si le filtrage d'entrée est activé et le port d'entrée n'est pas membre du VLAN auquel appartient le paquet. Une trame est considérée comme trame de priorité si le VID dans sa balise VLAN est 0.

Les trames appartenant à un VLAN restent dans le VLAN. Ceci s'applique en envoyant ou en transférant une trame uniquement à des ports de sortie membres du VLAN cible. Un port de sortie peut être un membre balisé ou non balisé d'un VLAN.

Le port de sortie :

- Ajoute une balise VLAN à la trame si le port de sortie est un membre balisé du VLAN cible et si la trame d'origine n'a pas de balise VLAN.
- Supprime la balise VLAN de la trame si le port de sortie est un membre non balisé du VLAN cible et si la trame d'origine a une balise VLAN.

Rôles du VLAN

Tout le trafic VLAN (monodiffusion/diffusion/multidiffusion) demeure au sein du VLAN. Les périphériques reliés à différents VLAN n'ont pas de connectivité directe entre eux sur la couche MAC Ethernet.

Les VLAN d'un périphérique peuvent uniquement être créés de manière statique.

Certains VLAN peuvent avoir des rôles supplémentaires, notamment :

- VLAN voix : pour plus d'informations, reportez-vous à la section *VLAN voix*.
- VLAN invité : défini sur la page *Modifier l'authentification VLAN.*

- VLAN par défaut : pour plus d'informations, reportez-vous à la section *Définition des paramètres VLAN par défaut*.
- VLAN de gestion : pour plus d'informations, reportez-vous à la section *Configuration des informations IP*.

QinQ

QinQ fournit l'isolation entre les réseaux de fournisseur de services et les réseaux de client. Le commutateur est un pont fournisseur qui prend en charge l'interface de service « c-tagged » basée sur les ports.

Avec QinQ, le commutateur ajoute une balise ID appelée Service Tag (S-tag) qui permet de transférer le trafic sur le réseau. La balise S-tag permet de répartir le trafic entre plusieurs clients, tout en conservant les balises VLAN du client.

Le trafic du client est encapsulé avec une balise S-tag avec TPID 0x8100, peut importe s'il a été balisé en « c-tagged » ou non balisé au départ. La balise S-tag permet à ce trafic d'être traité comme un agrégat au sein d'un réseau de pont fournisseur, dans lequel le pontage est uniquement basé sur le VID S-tag (S-VID).

La balise S-Tag est conservée lorsque le trafic est transféré par le biais de l'infrastructure du fournisseur de services réseau ; elle est ensuite supprimée par un périphérique de sortie.

Un autre avantage de QinQ est qu'il n'est pas nécessaire de configurer les dispositifs de bordure du client.

Vous pouvez activer QinQ sur la page Gestion des VLAN > *Paramètres d'interface*.

Charge de travail de la configuration VLAN

Pour configurer les VLAN :

1. Dans la mesure où cela est requis, modifiez le VLAN par défaut en utilisant la section **Configuration des paramètres VLAN par défaut**.
2. Créez les VLAN requis à l'aide de la section **Création d'un VLAN**.
3. Définissez la configuration VLAN souhaitée pour les ports et activez QinQ sur une interface en suivant les indications de la section **Configuration des paramètres d'interface VLAN** .
4. Assignez des interfaces aux VLAN à l'aide de la section **Configuration de ports vers un VLAN** ou de la section **Configuration d'une appartenance VLAN**.
5. Affichez l'appartenance actuelle du port VLAN pour toutes les interfaces en suivant les indications de la section **Configuration d'une appartenance VLAN**.

Configuration des paramètres VLAN par défaut

Si les paramètres d'usine par défaut sont utilisés, le commutateur crée automatiquement un VLAN 1 en tant que VLAN par défaut. L'état de l'interface par défaut de tous les ports est défini sur Liaison et tous les ports sont configurés en tant que membres non balisés du VLAN par défaut.

Le VLAN par défaut comporte les caractéristiques suivantes :

- Il est distinct, non statique/non dynamique et tous les ports sont des membres non balisés par défaut.
- Il peut être supprimé.
- Il ne peut recevoir d'étiquette.
- Il ne peut pas être utilisé pour un rôle spécial tel qu'un VLAN non authentifié ou un VLAN voix. Cette option ne concerne que les VLAN voix définis sur OUI activé.
- Si un port n'est plus membre d'un VLAN, le commutateur configure automatiquement le port en tant que membre non balisé du VLAN par défaut. Un port n'est plus membre d'un VLAN si le VLAN est supprimé ou s'il est supprimé du VLAN.

Lorsque le VID du VLAN par défaut est modifié, le commutateur exécute les opérations suivantes sur tous les ports du VLAN après avoir enregistré la configuration et redémarré le commutateur :

- Supprime l'appartenance VLAN des ports au VLAN par défaut d'origine (uniquement possible après le redémarrage).
- Remplace le PVID (identificateur de port VLAN) des ports par le VID du nouveau VLAN par défaut.
- L'ID VLAN par défaut d'origine est supprimé du commutateur. Il doit être recréé pour pouvoir être utilisé.
- Ajoute des ports en tant que membres VLAN non balisés du nouveau VLAN par défaut.

Pour changer le VLAN par défaut :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres VLAN par défaut**. La page *Paramètres VLAN par défaut* s'affiche.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **ID VLAN par défaut actuel** : affiche l'ID VLAN par défaut actuel.
- **ID VLAN par défaut après redémarrage** : saisissez un nouvel ID VLAN pour remplacer l'ID VLAN par défaut après le redémarrage.

ÉTAPE 3 Cliquez sur **Appliquer**.

ÉTAPE 4 Cliquez sur **Enregistrer** (dans le coin supérieur droit de la fenêtre) et enregistrez la Configuration d'exécution dans la Configuration de démarrage.

L'**ID VLAN par défaut après réinitialisation** devient l'**ID VLAN par défaut actuel** après le redémarrage du commutateur.

Création d'un VLAN

Vous pouvez créer un VLAN mais cela n'a aucun effet tant que le VLAN n'est pas manuellement ou dynamiquement lié à au moins un port. Les ports doivent toujours appartenir à un ou plusieurs VLAN.

Le commutateur de la série 200 prend en charge jusqu'à 256 VLAN, y compris le VLAN par défaut.

Chaque VLAN doit être configuré avec un VID unique (ID VLAN) dont la valeur est comprise entre 1 et 4 094. Le commutateur conserve le VID 4095 comme VLAN d'abandon. Tous les paquets classés comme VLAN d'abandon sont abandonnés à l'entrée et ne sont pas transférés vers un port.

Pour créer un VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Créer un VLAN**. La page *Créer un VLAN* s'affiche.

La page Créer un VLAN affiche les champs suivants pour tous les VLAN :

- **ID VLAN** : ID VLAN défini par l'utilisateur.
- **Nom du VLAN** : nom du VLAN défini par l'utilisateur.
- **Type** : type du VLAN :
  - *Statique* : le VLAN a été défini par l'utilisateur.
  - *Défaut* : c'est le VLAN par défaut.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un nouveau VLAN ou sélectionnez un VLAN existant, puis cliquez sur **Modifier** pour modifier les paramètres du VLAN. La page *Ajouter/modifier un VLAN* apparaît.

La page permet la création d'un VLAN unique ou d'une plage de VLAN.

ÉTAPE 3 Pour créer un VLAN unique, sélectionnez le bouton **VLAN**, saisissez l'ID VLAN (VID) et le nom du VLAN (facultatif).

Pour créer une plage de VLAN, sélectionnez le bouton **Plage** et spécifiez la plage de VLAN à créer en saisissant le VID de départ et le VID de fin (ces valeurs sont comprises). Si vous utilisez la fonction **Plage**, le nombre maximal de VLAN que vous pouvez créer en une seule fois est 100.

ÉTAPE 4 Cliquez sur **Appliquer** pour créer le ou les VLAN.

Configuration des paramètres d'interface VLAN

La page *Paramètres d'interface* affiche et active la configuration des paramètres VLAN pour toutes les interfaces.

Pour configurer les paramètres VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres d'interface**. La page *Paramètres d'interface* s'affiche.

ÉTAPE 2 Sélectionnez un type d'interface (Port ou LAG) et cliquez sur **OK**. Les ports ou LAG et leurs paramètres VLAN s'affichent.

ÉTAPE 3 Pour configurer un port ou LAG, sélectionnez-le puis cliquez sur **Modifier**. La page *Modifier les paramètres d'interface* s'affiche.

ÉTAPE 4 Saisissez les valeurs pour les champs suivants :

- **Interface** : sélectionnez un port/LAG.
- **Mode d'interface VLAN** : sélectionnez le mode d'interface du VLAN. Les options sont les suivantes :

- *Général* : l'interface peut prendre en charge toutes les fonctions telle qu'elles sont définies dans les caractéristiques techniques IEEE 802.1q. Elle peut être un membre balisé ou non balisé d'un ou plusieurs VLAN.
- *Accès* : l'interface est un membre non balisé d'un VLAN unique. Un port configuré dans ce mode est connu comme port d'accès.
- *Liaison* : l'interface est un membre non balisé d'au moins un VLAN ainsi qu'un membre balisé de zéro ou plusieurs VLAN. Un port configuré dans ce mode est connu comme port de liaison.
- *Client* : sélectionnez cette option pour mettre l'interface en mode QinQ. Vous pouvez ainsi appliquer votre propre agencement VLAN (PVID) sur le réseau du fournisseur. Le commutateur est en mode Q-in-Q lorsqu'il comporte un ou plusieurs ports client. Reportez-vous à la section **QinQ**.

▪ **PVID administratif** : saisissez l'ID VLAN du port (PVID) du VLAN dans lequel les trames non balisées entrantes et les trames balisées de priorité sont classées. Les valeurs possibles sont comprises entre 1 et 4094.

▪ **Type de trame** : sélectionnez le type de trame que l'interface peut recevoir. Les trames qui n'ont pas le type configuré sont abandonnées à l'entrée. Ces types de trames sont uniquement disponibles en mode Général. Ce champ peut prendre les valeurs suivantes :

- *Tout admettre* : l'interface accepte tous les types de trames : trames non balisées, trames balisées et trames balisées de priorité.
- *Admettre balisées uniquement* : l'interface accepte uniquement les trames balisées.
- *Admettre non balisées uniquement* : l'interface accepte uniquement les trames de priorité et non balisées.

▪ **Filtrage d'entrée** (uniquement disponible en mode Général) : sélectionnez cette option pour activer le Filtrage d'entrée. Lorsqu'une interface est en mode Filtrage d'entrée, elle abandonne toutes les trames entrantes qui sont classées comme appartenant aux VLAN dont elle n'est pas membre. Le filtrage d'entrée peut être désactivé ou activé sur les ports généraux. Il est toujours activé sur les ports d'accès et les ports de liaison.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres sont écrits dans le fichier de Configuration d'exécution.

Définition de l'appartenance VLAN

Les pages *Port vers VLAN* et *Appartenance VLAN des ports* affichent les appartenances VLAN des ports dans diverses présentations. Vous pouvez les utiliser pour ajouter des appartenances aux VLAN ou en supprimer de ces derniers.

Lorsqu'un port est interdit d'appartenance au VLAN par défaut, il ne disposera d'aucune autorisation d'appartenance à aucun autre VLAN. Le VID interne 4095 est assigné au port.

Pour transférer correctement les paquets, les périphériques intermédiaires tenant compte du VLAN qui acheminent le trafic VLAN entre les nœuds d'extrémité doivent être configurés manuellement.

Les ports non balisés de deux périphériques prenant en compte le VLAN sans aucune intervention des périphériques doivent disposer de la même appartenance VLAN. En d'autres termes, le PVID sur les ports entre les deux périphériques doit être le même si les ports doivent échanger (envoyer/recevoir) des paquets non balisés avec le VLAN. Dans le cas contraire, le trafic peut fuir d'un VLAN vers un autre.

Les trames balisées VLAN peuvent traverser d'autres périphériques réseau prenant ou non en compte les VLAN. Si un nœud d'extrémité de destination ne prend pas en compte le VLAN, mais doit recevoir du trafic depuis un VLAN, alors le dernier périphérique prenant en compte le VLAN (s'il existe) doit envoyer les trames du VLAN de destination au nœud d'extrémité non balisé.

Configuration de ports vers un VLAN

Utilisez la page *Port vers VLAN* pour afficher et configurer les ports dans un VLAN spécifique.

Pour mapper les ports ou les LAG à un VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Port vers VLAN**. La page *Port vers VLAN* s'affiche.

ÉTAPE 2 Sélectionnez un VLAN et le type d'interface (Port ou LAG), puis cliquez sur **OK** afin d'afficher ou de modifier la caractéristique du port relative au VLAN.

Le mode de chaque port ou LAG s'affiche dans son état actuel (Accès, Liaison ou Général). Vous pouvez le définir sur la page *Paramètres d'interface*.

Chaque port ou LAG s'affiche avec son enregistrement actuel au VLAN.

ÉTAPE 3 Modifiez l'enregistrement d'une interface au VLAN en sélectionnant l'option souhaitée dans la liste suivante :

- **Interdit** : l'interface n'est pas autorisée à rejoindre le VLAN. Lorsqu'un port n'est pas membre d'un autre VLAN, l'activation de cette option sur le port l'intègre au VLAN interne 4095 (VID réservé).
- **Exclu** : l'interface n'est actuellement pas membre du VLAN. Ceci est le paramètre par défaut pour tous les ports et LAG lorsqu'un nouveau VLAN vient d'être créé.
- **Balisé** : l'interface est un membre balisé du VLAN.
- **Non balisé** : l'interface est un membre non balisé du VLAN. Les trames du VLAN sont envoyées non balisées à l'interface VLAN.
- **PVID** : sélectionnez cette option pour définir le PVID de l'interface sur le VID du VLAN. Le PVID est un paramètre par port.

ÉTAPE 4 Cliquez sur **Appliquer**. Les interfaces sont attribuées au VLAN et écrites dans le fichier de Configuration d'exécution.

Vous pouvez continuer d'afficher et/ou de configurer l'appartenance de port à un autre VLAN en sélectionnant l'ID d'un autre VLAN.

Configuration d'une appartenance VLAN

La page *Appartenance VLAN des ports* affiche tous les ports du périphérique, ainsi qu'une liste des VLAN auxquels chaque port appartient.

Si la méthode d'authentification basée sur les ports pour une interface est 802.1x et que le Contrôle de port administratif est Auto, alors :

- Tant que le port n'est pas authentifié, il est exclu de tous les VLAN, à l'exception des VLAN invités et non authentifiés. Sur la page VLAN vers port, le port est marqué d'un « P ».
- Lorsque le port est authentifié, il reçoit l'appartenance dans le VLAN où il a été configuré.

Pour attribuer un port à un ou plusieurs VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Appartenance VLAN du port**. La page *Appartenance VLAN des ports* s'affiche.

ÉTAPE 2 Sélectionnez un type d'interface (Port ou LAG), puis cliquez sur **OK**. Les champs suivants s'affichent pour toutes les interfaces du type sélectionné :

- **Interface** : ID du port/LAG.
- **Mode** : mode VLAN d'interface qui a été sélectionné sur la page *Paramètres d'interface*.
- **VLAN administratifs** : liste déroulante qui affiche tous les VLAN dont l'interface peut être membre.
- **VLAN opérationnels** : liste déroulante qui affiche tous les VLAN dont l'interface est actuellement membre.
- **LAG** : si l'interface sélectionnée est Port, affiche le LAG dont elle est membre.

ÉTAPE 3 Sélectionnez un port et cliquez sur le bouton **Connecter le VLAN**. La page *Rejoindre le VLAN* s'affiche.

ÉTAPE 4 Saisissez les valeurs pour les champs suivants :

- **Interface** : sélectionnez un port/LAG.
- **Mode** : affiche le mode VLAN du port qui a été sélectionné sur la page *Paramètres d'interface*.
- **Sélectionner le VLAN** : pour associer un port à un ou plusieurs VLAN, déplacez le ou les ID VLAN de la liste de gauche vers la liste de droite à l'aide des flèches. Le VLAN par défaut peut apparaître dans la liste de droite s'il est balisé. Il ne peut cependant être sélectionné.
- **Balisage** : sélectionnez une des options de PVID/balisage suivantes :
  - **Interdit** : l'interface n'est pas autorisée à rejoindre le VLAN. Lorsqu'un port n'est pas membre d'un autre VLAN, l'activation de cette option sur le port l'intègre au VLAN interne 4095 (VID réservé).
  - **Exclu** : l'interface n'est actuellement pas membre du VLAN. Ceci est le paramètre par défaut pour tous les ports et LAG lorsqu'un nouveau VLAN vient d'être créé.
  - **Balisé** : sélectionnez cette option pour baliser le port. Cette option ne concerne pas les ports d'accès.

- **Non balisé** : sélectionnez cette option pour que le port soit non balisé. Cette option ne concerne pas les ports d'accès.
- **PVID** : le PVID du port est défini sur ce VLAN. Si l'interface est en mode Accès ou Liaison, le commutateur fait automatiquement de l'interface un membre non balisé du VLAN. Si l'interface est en mode général, vous devez configurer manuellement l'appartenance VLAN.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres sont modifiés et écrits dans le fichier de Configuration d'exécution.

ÉTAPE 6 Pour afficher les VLAN administratifs et opérationnels sur une interface, cliquez sur **Détails**.

VLAN voix

Dans un LAN, les périphériques vocaux tels que les téléphones IP, les points d'extrémité VoIP et les systèmes vocaux sont placés dans le même VLAN. On appelle ce VLAN un VLAN voix. Si les périphériques vocaux se trouvent dans d'autres VLAN voix, des routeurs IP (Layer 3) sont requis pour établir la communication.

Cette rubrique aborde les points suivants :

- **Présentation du VLAN voix**
- **Configuration du VLAN voix**

Présentation du VLAN voix

Cette rubrique aborde les points suivants :

- **Modes VLAN voix dynamiques**
- **VLAN voix automatique, Port intelligent automatique, CDP et LLDP**
- **QoS VLAN voix**
- **Contraintes du VLAN voix**
- **Workflows de VLAN voix**

Vous trouverez ci-après des exemples de déploiement vocal classiques, accompagnés des configurations appropriées :

- **UC3xx/UC5xx hébergé :** tous les téléphones et points d'extrémité VoIP Cisco prennent en charge ce modèle de déploiement. Pour ce modèle (UC3xx/UC5xx), les téléphones et points d'extrémité VoIP Cisco résident sur le même VLAN voix. Par défaut, le VLAN voix de UC3xx/UC5xx est le VLAN 100.
- **PBX IP tiers hébergé :** les téléphones SBTG CP-79xx et SPA5xx ainsi que les points d'extrémité SPA8800 Cisco prennent en charge ce modèle de déploiement. Dans ce modèle, le VLAN utilisé par les téléphones est déterminé par la configuration réseau. Il peut éventuellement y avoir des VLAN voix et données séparés. Les téléphones et points d'extrémité VoIP s'inscrivent sur un PBX IP sur site.
- **Centrex/ITSP IP hébergé :** les téléphones CP-79xx et SPA5xx ainsi que les points d'extrémité SPA8800 Cisco prennent en charge ce modèle de

déploiement. Dans ce modèle, le VLAN utilisé par les téléphones est déterminé par la configuration réseau. Il peut éventuellement y avoir des VLAN voix et données séparés. Les téléphones et points d'extrémité VoIP s'inscrivent sur un proxy SIP hors site dans « le nuage ».

En ce qui concerne le VLAN, les modèles ci-dessus fonctionnent dans des environnements tenant compte du VLAN et ne tenant pas compte du VLAN. Dans l'environnement tenant compte du VLAN, le VLAN voix fait partie des nombreux VLAN configurés dans une installation. L'exemple ne tenant pas compte du VLAN est équivalent à un environnement tenant compte du VLAN avec un seul VLAN.

Le commutateur fonctionne toujours en tant que commutateur tenant compte du VLAN.

Le commutateur prend en charge un seul VLAN voix. Par défaut, le VLAN voix est le VLAN 1. Vous avez la possibilité de configurer manuellement un autre VLAN voix. Il peut aussi être appris dynamiquement lorsque la fonction VLAN voix automatique est activée.

Vous pouvez ajouter des ports manuellement au VLAN voix à l'aide de la configuration VLAN de base décrite à la section *Configuration des paramètres d'interface VLAN* ou en appliquant manuellement aux ports la macro Port intelligent relative à la voix. Vous avez aussi la possibilité de les ajouter dynamiquement si le commutateur est en mode OUI de téléphonie ou que la fonction Port intelligent automatique est activée pour celui-ci.

Modes VLAN voix dynamiques

Le commutateur prend en charge deux modes VLAN voix dynamiques : OUI de téléphonie (Organization Unique Identifier) et VLAN voix automatique. Les deux modes ont des répercussions sur la façon dont le VLAN voix et/ou les appartenances VLAN des ports sont configurés. Les deux modes s'excluent mutuellement.

- **OUI de téléphonie**

  En mode OUI de téléphonie, le VLAN voix doit être un VLAN configuré manuellement et ne peut pas être le VLAN par défaut.

  Lorsque le commutateur est en mode OUI de téléphonie et qu'un port est configuré manuellement comme candidat au VLAN voix, le commutateur ajoute dynamiquement le port au VLAN voix s'il reçoit un paquet dont l'adresse MAC source correspond à celle des OUI de téléphonie

configurés. Un OUI correspond aux trois premiers octets d'une adresse MAC Ethernet. Pour plus d'informations sur le mode OUI de téléphonie, reportez-vous à la section **Configuration de l'OUI de téléphonie**.

- **VLAN voix automatique**

  En mode VLAN voix automatique, le VLAN voix peut être le VLAN voix par défaut manuellement configuré ou peut être appris à partir de périphériques externes comme UC3xx/5xx et de commutateurs qui annoncent le VLAN voix dans CDP ou VSDP. VSDP est un protocole défini par Cisco pour la détection des services vocaux.

  À la différence du mode OUI de téléphonie qui détecte les périphériques vocaux basés sur le mode OUI de téléphonie, le mode VLAN voix automatique dépend de la fonction Port intelligent automatique pour ajouter dynamiquement les ports au VLAN voix. Si elle est activée, la fonction Port intelligent automatique ajoute un port au VLAN voix lorsqu'elle détecte sur le port un périphérique en cours d'association qui s'annonce en tant que téléphone ou points d'extrémité de média, par l'intermédiaire de CDP et/ou LLDP-MED.

Points d'extrémité vocaux

Pour qu'un VLAN voix fonctionne correctement, les périphériques vocaux tels que les téléphones et points d'extrémité VoIP Cisco doivent être attribués au VLAN pouvant envoyer et recevoir leur trafic vocal. Voici quelques exemples possibles :

- Un téléphone/point d'extrémité peut être configuré de manière statique avec le VLAN voix.
- Un téléphone/point d'extrémité peut obtenir le VLAN voix dans le fichier de démarrage qu'il télécharge à partir d'un serveur TFTP. Un serveur DHCP peut spécifier le fichier de démarrage et le serveur TFTP lorsqu'il attribue une adresse IP au téléphone.
- Un téléphone/point d'extrémité peut obtenir les informations VLAN voix à partir des annonces CDP et LLDP-MED qu'il reçoit de ses systèmes vocaux et commutateurs voisins.

Le commutateur attend des périphériques vocaux en cours de raccordement qu'ils envoient des paquets VLAN balisés. Sur les ports où le VLAN voix est également le VLAN natif, les paquets VLAN voix non balisés sont possibles.

VLAN voix automatique, Port intelligent automatique, CDP et LLDP

Valeurs par défaut

Par défaut (paramètres d'usine), CDP, LLDP et LLDP-MED sont activés sur le commutateur, le mode Port intelligent automatique est activé, le mode de base de QoS avec DSCP de confiance est activé, et tous les ports sont membres du VLAN 1 par défaut, qui est aussi le VLAN voix par défaut.

En outre, le mode VLAN voix dynamique est la valeur par défaut du VLAN voix automatique avec activation basée sur le déclenchement, et la fonction Port intelligent automatique est la valeur par défaut à activer en fonction du VLAN voix automatique.

Déclenchements de VLAN voix

Lorsque le mode VLAN voix dynamique est activé sur VLAN voix automatique, cela signifie que le VLAN voix automatique ne devient opérationnel que si un ou plusieurs déclenchements se produisent. Les déclenchements possibles sont la configuration de VLAN voix statique, la réception d'informations VLAN voix dans une annonce de voisinage CDP et la réception d'informations VLAN voix dans le protocole VSDP (Voice VLAN Discovery Protocol). Si vous le souhaitez, vous pouvez rendre le mode VLAN voix automatique immédiatement opérationnel sans attendre de déclenchement.

Si la fonction Port intelligent automatique est activée en fonction du mode VLAN voix automatique, la fonction Port intelligent automatique est activée lorsque le mode VLAN voix automatique devient opérationnel. Si vous le souhaitez, vous pouvez activer la fonction Port intelligent automatique indépendamment du mode VLAN voix automatique.

REMARQUE La liste de configuration par défaut s'applique ici aux commutateurs dont la version du micrologiciel prend directement en charge le mode VLAN voix automatique. Elle s'applique également aux commutateurs non configurés qui ont été mis à niveau vers la version du micrologiciel prenant en charge le mode VLAN voix automatique.

REMARQUE Les déclenchements par défaut et de VLAN voix sont conçus pour n'avoir aucun effet sur les installations ne comportant pas de VLAN voix, ainsi que sur les commutateurs qui ont déjà été configurés. Vous pouvez désactiver et activer manuellement le mode VLAN voix automatique et/ou Port intelligent automatique en fonction de votre déploiement.

VLAN voix automatique

Le mode VLAN voix automatique permet de gérer le VLAN voix, mais dépend de la fonction Port intelligent automatique pour gérer l'appartenance des ports VLAN voix. Le mode VLAN voix automatique offre les fonctions suivantes lorsqu'il est opérationnel :

- Il détecte les informations VLAN voix dans les annonces CDP provenant des périphériques voisins à connexion directe.
- Si plusieurs commutateurs et/ou routeurs voisins, tels que des périphériques Cisco Unified Communication (UC), annoncent leur VLAN voix, le VLAN voix du périphérique ayant l'adresse MAC la plus basse est utilisé.

  REMARQUE En cas de connexion du commutateur à un périphérique UC Cisco, vous devrez peut-être configurer le port sur le périphérique UC à l'aide de la commande *`switchport voice vlan`*, afin de vous assurer que le périphérique UC annonce son VLAN voix dans CDP sur le port.
- Il synchronise les paramètres VLAN voix avec les autres commutateurs activés pour le mode VLAN voix automatique, par l'intermédiaire du protocole VSDP (Voice Service Discovery Protocol). Le commutateur se configure toujours lui-même avec le VLAN voix provenant de la source de priorité la plus élevée qu'il détecte. La priorité est basée sur le type de source et l'adresse MAC de la source qui fournit les informations de VLAN voix. Les priorités de type de source, de la plus haute à la plus basse, sont la configuration VLAN statique, l'annonce CDP et la configuration par défaut basée sur le VLAN par défaut modifié, ainsi que le VLAN voix par défaut. Une adresse MAC numériquement basse a une priorité plus élevée qu'une adresse MAC numériquement haute.
- Il conserve le VLAN voix jusqu'à ce qu'un nouveau VLAN voix provenant d'une source de priorité plus élevée soit détecté ou jusqu'à ce que le mode VLAN voix automatique soit redémarré par l'utilisateur. Après le redémarrage, le commutateur rétablit le VLAN voix par défaut et relance la détection VLAN voix automatique.
- Lorsqu'un nouveau VLAN voix est configuré/détecté, le commutateur le crée automatiquement et remplace toutes les appartenances de port du VLAN voix existant par celles du nouveau VLAN voix. Cette opération est susceptible d'interrompre ou de terminer des sessions vocales existantes, notamment lorsque la topologie réseau a été modifiée.

REMARQUE Si le commutateur est en mode système Layer 2, il peut uniquement se synchroniser avec les commutateurs compatibles VSDP qui sont situés dans le même VLAN de gestion. Si le commutateur est en mode système Layer 3, il peut se synchroniser avec les commutateurs compatibles VSDP se trouvant sur les sous-réseaux IP à connexion directe qui sont configurés sur le commutateur.

Port intelligent automatique fonctionne avec CDP/LLDP pour gérer les appartenances de port du VLAN voix lorsque des points d'extrémité vocaux sont détectés à partir des ports :

- Lorsque CDP et LLDP sont activés, le commutateur envoie périodiquement des paquets CDP et LLDP pour annoncer au VLAN voix les points d'extrémité vocaux à utiliser.
- Lorsqu'un périphérique en cours d'association à un port s'annonce lui-même en tant que point d'extrémité vocal, par l'intermédiaire de CDP et/ou LLDP, la fonction Port intelligent automatique ajoute automatiquement le port au VLAN voix en appliquant au port la macro Port intelligent correspondante (si aucun autre périphérique provenant du port n'annonce une fonctionnalité conflictuelle ou supérieure). Si un périphérique s'annonce lui-même en tant que téléphone, la macro Port intelligent par défaut est le téléphone. Si un périphérique s'annonce lui-même en tant que téléphone et hôte, ou téléphone et pont, la macro Port intelligent par défaut est le téléphone + bureau.

QoS VLAN voix

Le VLAN voix peut propager les paramètres CoS/802.1p et DSCP à l'aide des stratégies réseau LLDP-MED. Par défaut, le protocole LLDP-MED est défini pour répondre avec le paramètre QoS voix lorsqu'un dispositif envoie des paquets LLDP-MED. Les périphériques prenant en charge MED doivent envoyer leur trafic vocal avec les mêmes valeurs CoS/802.1p et DSCP que celles reçues avec la réponse LLDP-MED.

Vous pouvez désactiver la mise à jour automatique entre le VLAN voix et LLDP-MED, et utiliser vos propres stratégies réseau.

S'il utilise le mode OUI, le commutateur peut en outre configurer le mappage et le re-marquage (CoS/802.1p) du trafic vocal basé sur le OUI.

Par défaut, toutes les interfaces sont approuvées pour CoS/802.1p. Le commutateur applique la qualité de service basée sur la valeur CoS/802.1p qui a été trouvée dans le flux vocal. Pour les flux vocaux OUI de téléphonie, vous pouvez remplacer la qualité de service et éventuellement re-marquer la valeur 802.1p des flux vocaux en spécifiant les valeurs CoS/802.1p souhaitées et en utilisant l'option de re-marquage sous OUI de téléphonie.

Contraintes du VLAN voix

Les contraintes suivantes doivent être prises en compte :

- Seul un VLAN voix est pris en charge.
- Un VLAN défini en tant que VLAN voix ne peut pas être supprimé.

En outre, les contraintes suivantes s'appliquent au OUI de téléphonie :

- Le VLAN voix ne peut pas être le VLAN 1 (VLAN par défaut).
- Le VLAN voix ne peut pas être activé pour le mode Port intelligent.
- À l'exception de la décision QoS relative à la stratégie, la décision QoS du VLAN voix est prioritaire sur toute autre décision QoS.
- Un nouvel ID VLAN peut être configuré pour le VLAN voix uniquement si le VLAN voix actuel n'a pas de ports candidats.
- L'interface VLAN d'un port candidat doit être en mode Général ou Liaison.
- La QoS du VLAN voix est appliquée aux ports statiques ainsi qu'aux ports candidats qui ont rejoint le VLAN voix.
- Le flux de voix est accepté si l'adresse MAC peut être apprise par la FDB (Forwarding Database). (s'il n'existe aucun espace disponible dans la FDB, aucune action ne se produit).

Workflows de VLAN voix

La configuration par défaut du commutateur sur VLAN voix automatique, Port intelligent automatique, CDP et LLDP couvre la plupart des cas de déploiement vocal courants. Cette section décrit la façon de déployer un VLAN voix lorsque la configuration par défaut ne peut pas être utilisée.

Workflow 1 : *pour configurer le VLAN voix automatique :*

ÉTAPE 1 Ouvrez la page *Gestion des VLAN > VLAN voix > Propriétés*.

ÉTAPE 2 Sélectionnez l'ID du VLAN voix. Il ne peut pas être défini sur l'ID de VLAN 1 (cette étape n'est pas obligatoire pour le VLAN voix dynamique).

ÉTAPE 3 Sélectionnez **VLAN voix dynamique** pour activer le mode VLAN voix automatique.

ÉTAPE 4 Sélectionnez la méthode **Activation du VLAN voix automatique**.

REMARQUE Si le périphérique est actuellement en mode OUI de téléphonie, vous devez le désactiver pour pouvoir configurer le mode VLAN voix automatique.

ÉTAPE 5 Cliquez sur **Appliquer**.

ÉTAPE 6 Configurez les ports intelligents comme indiqué dans la section **Tâches courantes de port intelligent**.

ÉTAPE 7 Configurez LLDP/CDP comme décrit respectivement dans les sections **Configuration de LLDP** et **Configuration de CDP**.

ÉTAPE 8 Activez la fonction Port intelligent sur les ports appropriés par l'intermédiaire de la page *Port intelligent > Paramètres d'interface*.

REMARQUE Les étapes 7 et 8 sont facultatives, car elles sont activées par défaut.

Workflow 2 : *pour configurer la méthode OUI de téléphonie :*

ÉTAPE 1 Ouvrez la page *Gestion des VLAN > VLAN voix > Propriétés*. Sélectionnez **VLAN voix dynamique** pour activer le mode OUI de téléphonie.

REMARQUE Si le périphérique est actuellement en mode VLAN voix automatique, vous devez le désactiver pour pouvoir activer le mode OUI de téléphonie.

ÉTAPE 2 Configurez OUI de téléphonie sur la page *OUI de téléphonie*.

ÉTAPE 3 Configurez l'appartenance VLAN OUI de téléphonie pour les ports sur la page *Interface des OUI de téléphonie*.

Configuration du VLAN voix

Cette section explique comment configurer le VLAN voix. Elle couvre les rubriques suivantes :

- **Configuration des propriétés du VLAN voix**
- **Affichage des Paramètres du VLAN voix automatique**
- **Configuration de l'OUI de téléphonie**

Configuration des propriétés du VLAN voix

Utilisez la page *Propriétés du VLAN voix* pour effectuer les tâches suivantes :

- Affichez les paramètres de configuration actuels du VLAN voix.
- Configurez l'ID de VLAN du VLAN voix.
- Configurez les paramètres QoS du VLAN voix.
- Configurez le mode VLAN voix (OUI de téléphonie ou VLAN voix automatique).
- Configurez la façon dont le VLAN voix automatique se déclenche.

Pour afficher et configurer les propriétés du VLAN voix :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **Propriétés**. La page *Propriétés* apparaît.

- Les paramètres VLAN voix configurés sur le commutateur s'affichent dans le bloc **Paramètres du VLAN voix (État administratif)**.
- Les paramètres VLAN voix actuellement appliqués au déploiement VLAN voix s'affichent dans le bloc **Paramètres du VLAN voix (État opérationnel)**.

ÉTAPE 2 Saisissez les valeurs appropriées dans les champs suivants :

- **ID VLAN voix** : entrez le VLAN qui sera le VLAN voix.

REMARQUE Les modifications apportées à l'ID du VLAN voix, CoS/802.1p et/ou DSCP obligent le commutateur à annoncer le VLAN voix administratif en tant que VLAN voix statique. Si l'option *Activation du VLAN voix automatique* déclenchée par le VLAN voix externe est sélectionnée, les valeurs par défaut doivent être conservées.

- **CoS/802.1p** : sélectionnez une valeur CoS/802.1p utilisée par LLDP-MED en tant que stratégie réseau de voix. Pour plus d'informations, reportez-vous à *Administration > Détection > LLDP > Stratégie réseau LLDP MED*.
- **DSCP** : sélection de valeurs DSCP utilisées par LLDP-MED en tant que stratégie réseau de voix. Pour plus d'informations, reportez-vous à *Administration > Détection > LLDP > Stratégie réseau LLDP MED*.
- **VLAN voix dynamique** : sélectionnez ce champ pour désactiver ou activer la fonction VLAN voix de l'une des manières suivantes :
  - *Activer le VLAN voix automatique* : active le VLAN voix dynamique en mode VLAN voix automatique.
  - *Activer OUI de téléphonie* : active le VLAN voix dynamique en mode OUI de téléphonie.
  - *Désactiver* : désactive le VLAN voix automatique ou le OUI de téléphonie.
- **Activation du VLAN voix automatique** : sélectionnez l'une des options suivantes pour activer le VLAN voix automatique :
  - *Immédiat* : le VLAN voix automatique sur le commutateur est activé et immédiatement opérationnel.
  - *Par déclenchement du VLAN voix externe* : le VLAN voix automatique sur le commutateur est activé et opérationnel uniquement si le commutateur détecte un périphérique qui annonce le VLAN voix.

REMARQUE La reconfiguration manuelle de l'ID de VLAN voix, CoS/802.1p et/ou DSCP à partir de leurs valeurs par défaut génère un VLAN voix statique ayant une priorité plus élevée que le VLAN voix automatique qui a été appris des sources externes.

ÉTAPE 3 Cliquez sur **Appliquer**. Les propriétés du VLAN sont écrites dans le fichier de Configuration d'exécution.

Affichage des Paramètres du VLAN voix automatique

Si le mode VLAN voix automatique est activé, utilisez la page VLAN voix automatique pour afficher les paramètres globaux et d'interface appropriés.

Vous pouvez aussi utiliser cette page pour redémarrer manuellement le VLAN voix automatique, en cliquant sur **Redémarrer VLAN voix automatique**. Au bout de quelques instants, le système rétablit le VLAN voix par défaut, et relance la détection VLAN voix automatique et le processus de synchronisation sur tous les commutateurs du LAN pour lesquels le mode VLAN voix automatique est activé.

REMARQUE Cette opération rétablit uniquement le VLAN voix par défaut si le Type de source a l'état *Inactif*.

Pour afficher les paramètres VLAN voix automatique :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **VLAN voix automatique**. La page *VLAN voix automatique* s'affiche.

Le bloc d'état opérationnel figurant sur cette page affiche des informations sur le VLAN voix actuel et sa source :

- **État de VLAN voix automatique** : indique si le VLAN voix automatique est activé.
- **ID du VLAN voix** : identificateur du VLAN voix actuel.
- **Type de source** : indique le type de source où le VLAN voix a été détecté par le commutateur racine.
- **CoS/802.1p** : affiche les valeurs CoS/802.1p utilisées par le LLDP-MED en tant que stratégie réseau de voix.
- **DSCP** : affiche les valeurs DSCP utilisées par le LLDP-MED en tant que stratégie réseau de voix.
- **Adresse MAC commutateur racine** : adresse MAC du périphérique racine VLAN voix automatique qui détecte ou est configuré avec le VLAN voix à partir duquel le VLAN voix est appris.
- **Adresse MAC du commutateur** : adresse MAC de base du commutateur. Si l'adresse MAC de commutateur du périphérique est l'adresse MAC commutateur racine, le périphérique est le périphérique racine VLAN voix automatique.
- **Heure de changement de l'ID VLAN voix** : dernière fois que le VLAN voix a été mis à jour.

ÉTAPE 2 Cliquez sur **Redémarrer VLAN voix automatique** pour rétablir le VLAN voix par défaut et relancer la détection VLAN voix automatique sur tous les commutateurs du LAN pour lesquels la fonction VLAN voix automatique est activée.

La Table locale VLAN voix affiche le VLAN voix configuré sur le commutateur ainsi que toute configuration VLAN voix annoncée par des périphériques voisins à connexion directe. Elle contient les champs suivants :

- **Interface** : affiche l'interface sur laquelle la configuration VLAN voix a été reçue ou configurée. Si *S/O* est affiché, cela signifie que la configuration a été effectuée sur le commutateur lui-même. Si une interface est affichée, cela signifie qu'une configuration de voix a été reçue d'un voisin.
- **Adresse MAC source** : adresse MAC d'un UC à partir duquel la configuration de voix a été reçue.
- **Type de source** : type d'UC à partir duquel la configuration de voix a été reçue. Les options suivantes sont disponibles :
  - *Défaut* : configuration VLAN voix par défaut sur le commutateur
  - *Statique* : configuration VLAN voix définie par l'utilisateur qui est définie sur le commutateur
  - *CDP* : indique que l'UC qui a annoncé la configuration VLAN voix exécute CDP.
  - *LLDP* : indique que l'UC qui a annoncé la configuration VLAN voix exécute LLDP.
  - *ID du VLAN voix* : identificateur du VLAN voix annoncé ou configuré
- **ID du VLAN voix** : identificateur du VLAN voix actuel
- **CoS/802.1p** : valeurs CoS/802.1p annoncées ou configurées qui sont utilisées par le LLDP-MED en tant que stratégie réseau de voix
- **DSCP** : valeurs DSCP annoncées ou configurées qui sont utilisées par le LLDP-MED en tant que stratégie réseau de voix
- **Meilleure source locale** : indique si ce VLAN voix a été utilisé par le commutateur. Les options suivantes sont disponibles :
  - *Oui* : le commutateur utilise ce VLAN voix pour se synchroniser avec les autres commutateurs activés pour le mode VLAN voix automatique. Ce VLAN voix est celui utilisé pour le réseau, sauf si un VLAN voix provenant d'une source de priorité plus élevée est détecté. Une seule source locale peut être la meilleure source locale.

- *Non* : il ne s'agit pas de la meilleure source locale.

ÉTAPE 3 Cliquez sur **Actualiser** pour actualiser les informations figurant sur la page.

Configuration de l'OUI de téléphonie

Les OUI (Organizationally Unique Identifiers) sont attribués par l'autorité d'enregistrement intégrée IEEE (Institute of Electrical and Electronics Engineers). Étant donné que le numéro des fabricants de téléphone IP est limité et connu, les valeurs d'OUI connues entraînent l'affectation automatique au VLAN voix des trames appropriées et du port sur lequel elles sont détectées.

La table globale OUI peut contenir jusqu'à 128 entrées.

Cette rubrique aborde les points suivants :

- **Ajout de OUI à la Table des OUI de téléphonie**
- **Ajout d'interfaces au VLAN voix sur la base des OUI**

Ajout de OUI à la Table des OUI de téléphonie

Utilisez la page *OUI de téléphonie* pour configurer les propriétés QoS des OUI de téléphonie. Vous pouvez également configurer le Délai d'expiration d'appartenance automatique. Si la période expire sans aucune activité téléphonique, le port est supprimé du VLAN voix.

Utilisez la page *OUI de téléphonie* pour afficher les OUI existants et en ajouter de nouveaux.

Pour configurer les OUI de téléphonie et/ou ajouter un nouveau OUI de VLAN voix :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **OUI de téléphonie**. La page *OUI de téléphonie* s'affiche.

La page *OUI de téléphonie* contient les champs suivants :

- **État opérationnel OUI de téléphonie** : indique si les OUI sont utilisés pour identifier le trafic vocal.
- **CoS/802.1p** : sélectionnez la file d'attente CoS à attribuer au trafic vocal.
- **Remark CoS/802.1p** : sélectionnez cette option pour re-marquer le trafic sortant.
- **Délai d'expiration d'appartenance automatique** : entrez le délai à l'issue duquel un port doit être supprimé du VLAN vocal une fois que toutes les adresses MAC des téléphones détectés sur les ports ont expiré.

ÉTAPE 2 Cliquez sur **Appliquer** pour mettre à jour la Configuration d'exécution du commutateur avec ces valeurs.

La Table des OUI de téléphonie s'affiche :

- **Téléphonie OUI** : six premiers chiffres de l'adresse MAC réservés pour les OUI.
- **Description** : description de l'OUI assigné à l'utilisateur.

ÉTAPE 3 Cliquez sur **Restaurer les OUI par défaut** pour supprimer tous les OUI créés par l'utilisateur et conserver uniquement les OUI par défaut dans la table.

Pour supprimer tous les OUI, cochez la case du haut. Tous les OUI sont sélectionnés et peuvent être supprimés en cliquant sur **Supprimer**. Si vous cliquez ensuite sur **Restaurer les OUI par défaut**, le système récupère les OUI connus.

ÉTAPE 4 Pour ajouter un nouveau OUI, cliquez sur **Ajouter**. La page *Ajouter un OUI de téléphonie* s'affiche.

ÉTAPE 5 Saisissez les valeurs pour les champs suivants :

- **OUI de téléphonie** : saisissez un nouvel OUI.
- **Description** : saisissez un nom d'OUI.

ÉTAPE 6 Cliquez sur **Appliquer**. Le OUI est ajouté à la Table des OUI de téléphonie.

Ajout d'interfaces au VLAN voix sur la base des OUI

Les attributs de la QoS peuvent être attribués pour chaque port aux paquets voix dans l'un des deux modes suivants :

- **Tout** : les valeurs de qualité de service (QoS) configurées sur le VLAN voix sont appliquées à toutes les trames entrantes reçues sur l'interface et catégorisées comme VLAN voix.
- **Adresse MAC source de téléphonie** : les valeurs de QoS configurées pour le VLAN voix sont appliquées à toute trame entrante catégorisée comme VLAN voix et contenant un OUI dans l'adresse MAC source qui correspond à un OUI de téléphonie configuré.

Utilisez la page *Interface des OUI de téléphonie* pour ajouter une interface au VLAN voix sur la base de l'identificateur OUI et pour configurer le mode QoS OUI du VLAN voix.

Pour configurer l'OUI de téléphonie sur une interface :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **Interface des OUI de téléphonie**. La page *Interface des OUI de téléphonie* s'affiche.

La page *Interface des OUI de téléphonie* affiche les paramètres OUI du VLAN voix pour toutes les interfaces.

ÉTAPE 2 Pour configurer une interface en tant que port candidat du VLAN voix basé sur les OUI de téléphonie, cliquez sur **Modifier**. La page *Modifier les paramètres d'interface* s'affiche.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **Interface** : sélectionnez une interface.
- **Adhésion VLAN OUI de téléphonie** : si cette option est activée, l'interface est un port candidat du VLAN voix basé sur les OUI de téléphonie. Lorsque des paquets correspondant à l'un des OUI de téléphonie configurés sont reçus, le port est ajouté au VLAN voix.
- **Mode de QoS VLAN voix** : sélectionnez l'une des options suivantes :
  - *Tous* : les attributs QoS sont appliqués à tous les paquets catégorisés comme VLAN voix.
  - *Adresse MAC source de téléphonie* : les attributs QoS sont uniquement appliqués aux paquets provenant de téléphones IP.

ÉTAPE 4 Cliquez sur **Appliquer**. L'OUI est ajouté.

13

Configuration du protocole STP

Cette section décrit le protocole STP (Spanning Tree Protocol) (IEEE802.1D et IEEE802.1Q) et couvre les rubriques suivantes :

- **Types de STP**
- **Configuration de l'état STP et des paramètres globaux**
- **Définition des paramètres d'interface du Spanning Tree**
- **Configuration des paramètres Rapid Spanning Tree**

Types de STP

Le protocole STP protège un domaine de diffusion de couche 2 (Layer 2) contre les tempêtes de diffusion en paramétrant sélectivement des liens sur le mode de réserve pour empêcher les boucles. En mode de réserve, ces liens arrêtent de transférer des données d'utilisateur pendant un moment. Les liens sont automatiquement réactivés lorsque la topologie permet à nouveau le transfert de données.

Des boucles se produisent lorsque des routes alternatives existent entre les hôtes. Les boucles d'un réseau étendu peuvent utiliser des commutateurs pour acheminer indéfiniment le trafic, ce qui augmente la charge de ce dernier et diminue l'efficacité du réseau.

Le protocole STP fournit une topologie en arborescence pour l'agencement de commutateurs et de liens d'interconnexion afin de créer un chemin d'accès unique entre des stations d'arrivée sur un réseau et d'éliminer les boucles.

Le commutateur prend en charge les versions de protocole STP suivantes :

- Le STP classique fournit un chemin d'accès unique entre deux stations d'arrivée afin d'empêcher et d'éliminer les boucles.
- Le STP rapide (RSTP) détecte les topologies de réseau afin de fournir une convergence du Spanning Tree plus rapide. Ce protocole est plus efficace

lorsque la topologie du réseau est naturellement structurée en arborescence et permet une convergence plus rapide. RSTP est activé par défaut.

REMARQUE Les commutateurs de la série 200 ne prennent pas en charge le STP multiple (MSTP).

Configuration de l'état STP et des paramètres globaux

La page *État et paramètres globaux STP* contient les paramètres permettant d'activer STP ou RSTP.

Utilisez les pages *Paramètres d'interface STP* et *Paramètres d'interface RSTP*, *respectivement, pour configurer ces modes sur les ports.*

Pour définir l'état et les paramètres globaux STP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **État STP et paramètres globaux**. La page *État et paramètres globaux STP* s'affiche.

ÉTAPE 2 Saisissez les paramètres.

Paramètres globaux :

- **État du Spanning Tree :** activez ou désactivez STP sur le commutateur.
- **Mode de fonctionnement STP :** sélectionnez un mode STP.
- **Gestion BPDU** : sélectionnez la manière dont les paquets BPDU sont gérés lorsque STP est désactivé sur le port ou le commutateur. Les BPDU sont utilisés pour transmettre des informations du Spanning Tree.
  - *Filtrage* : filtre les paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
  - *Inondation* : inonde les paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
- **Valeurs par défaut du coût de chemin :** sélectionne la méthode utilisée pour assigner des coûts de chemin par défaut aux ports STP. Le coût de chemin par défaut assigné à une interface varie selon la méthode sélectionnée.
  - *Court* : spécifie la plage de 1 à 65 535 pour les coûts de chemin des ports.

- *Long* : spécifie la plage de 1 à 200 000 000 pour les coûts de chemin des ports.

Paramètres des ponts :

- **Priorité** : définit la valeur de priorité du pont. Après l'échange de BPDU, le périphérique de priorité inférieure devient le pont racine. Si tous les ponts utilisent la même priorité, leurs adresses MAC sont alors utilisées pour déterminer le pont racine. La valeur de priorité du pont est fournie par paliers de4096. Par exemple 4096,8192,12288, etc.
- **Délai Hello :** définissez le temps d'attente en secondes d'un pont racine entre deux messages de configuration. Ce délai peut être de 1 à 10 secondes.
- **Délai maximum :** définissez la durée en secondes durant laquelle le commutateur attend avant de tenter de redéfinir sa propre configuration lorsqu'il ne reçoit pas de message de configuration.
- **Délai de transfert :** définissez la durée en secondes durant laquelle le pont reste en mode d'apprentissage avant de transférer des paquets. Pour plus d'informations, reportez-vous à la section **Définition des paramètres d'interface du Spanning Tree**.

Racine désignée :

- **ID du pont :** la priorité du pont est concaténée avec l'adresse MAC du commutateur.
- **ID du pont racine :** la priorité du pont racine est concaténée avec l'adresse MAC du pont racine.
- **Port racine :** port proposant un chemin de coût inférieur entre ce pont et le pont racine. (Cette information est importante lorsque le pont n'est pas le pont racine.)
- **Coût d'acheminement vers la racine :** affiche le coût d'acheminement entre ce pont et le pont racine.
- **Nombre de changements de topologie :** nombre total des changements de topologie STP effectués.
- **Dernier changement de topologie :** intervalle de temps écoulé depuis le dernier changement de topologie. Cette durée s'affiche au format jours/heures/minutes/secondes.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres globaux STP sont écrits dans le fichier de Configuration d'exécution.

Définition des paramètres d'interface du Spanning Tree

La page *Paramètres d'interface STP* vous permet de configurer STP port par port et d'afficher les informations apprises par le protocole, tel que le pont désigné.

La configuration définie est valide pour toutes les variantes du protocole STP.

Pour configurer STP sur une interface :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **Paramètres d'interface STP**. La page *Paramètres d'interface STP* s'affiche.

ÉTAPE 2 Sélectionnez une interface et cliquez sur **Modifier**. La page *Modifier les paramètres d'interface* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Interface :** sélectionnez le port ou le LAG sur lequel Spanning Tree est configuré.
- **STP :** active ou désactive STP sur le port.
- **Port de bordure :** active ou désactive Fast Link sur le port. Si le mode Fast Link est activé pour un port, le port est automatiquement placé en mode Transfert lorsque le lien du port est actif. Fast Link optimise la convergence du protocole STP. Les options sont les suivantes :
  - *Activer* : active immédiatement Fast Link.
  - *Auto* : active Fast Link quelques secondes après l'activation de l'interface. Ceci permet à STP de résoudre les problèmes de boucles avant d'activer Fast Link.
  - *Désactiver* : désactive Fast Link.

    REMARQUE Il est recommandé de définir la valeur à Auto afin que le commutateur place le port en mode Fast Link lorsqu'un hôte y est connecté, ou qu'il le définisse comme étant un port STP normal lorsqu'il est connecté à un autre commutateur. Cela permet d'éviter les boucles.

- **Gestion BPDU** : sélectionnez la manière dont les paquets BPDU sont gérés lorsque STP est désactivé sur le port ou le commutateur. Les BPDU sont utilisés pour transmettre des informations du Spanning Tree.
  - *Utiliser les paramètres globaux* : sélectionnez cette option pour utiliser les paramètres définis sur la page *État et paramètres globaux STP*.
  - *Filtrage* : filtre les paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
  - *Inondation* : inonde les paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
- **Coût de chemin :** définissez la contribution du port au coût du chemin racine ou utilisez le coût par défaut généré par le système.
- **Priorité** : définissez la valeur de priorité du port. La valeur de priorité influence le choix du port lorsqu'un pont dispose de deux ports connectés au sein d'une boucle. La priorité est une valeur comprise entre 0 et 240, et fonctionne par multiples de 16.
- **État du port :** affiche l'état STP actuel d'un port.
  - *Désactivé* : le protocole STP est actuellement désactivé sur le port. Le port transfère le trafic tout en apprenant les adresses MAC.
  - *Blocage* : le port est actuellement bloqué et ne peut ni transférer le trafic (à l'exception des données BPDU) ni connaître les adresses MAC.
  - *Écoute* : le port est en mode Écoute. Il ne peut ni transférer le trafic ni connaître les adresses MAC.
  - *Apprentissage* : le port est en mode Apprentissage. Il ne peut pas transférer le trafic mais il peut prendre connaissance de nouvelles adresses MAC.
  - *Transfert* : le port est en mode Transfert. Il peut réacheminer du trafic et apprendre de nouvelles adressesMAC.
- **ID du pont désigné** : affiche la priorité du pont et les adresses MAC du pont désigné.
- **ID du port désigné** : affiche la priorité et l'interface du port sélectionné.
- **Coût désigné** : affiche le coût du port participant à la topologie STP. Les ports de coûts inférieurs sont peu susceptibles d'être bloqués si STP détecte des boucles.

- **Transitions de transfert :** affiche le nombre de fois où le port est passé de l'état **Blocage** à l'état **Transfert**.
- **Vitesse :** affiche la vitesse du port.
- **LAG :** affiche le LAG auquel appartient le port. Si un port est membre d'un LAG, les paramètres du LAG remplacent ceux du port.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres d'interface sont écrits dans le fichier de Configuration d'exécution.

Configuration des paramètres Rapid Spanning Tree

Le protocole RSTP (Rapid Spanning Tree Protocol) permet une convergence STP plus rapide sans création de boucles de transfert.

La page *Paramètres d'interface RSTP* vous permet de configurer RSTP par port. Toute configuration effectuée sur cette page est active lorsque le mode STP global est défini sur RSTP .

Pour entrer les paramètres RSTP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **État STP et paramètres globaux**. La page *État et paramètres globaux STP* s'affiche. Activez **RSTP**.

ÉTAPE 2 Cliquez sur **Spanning Tree** > **Paramètres d'interfaceRSTP**. La page *Paramètres d'interface RSTP* s'ouvre :

ÉTAPE 3 Sélectionnez un port.

REMARQUE Activer la migration des protocoles est uniquement disponible après avoir sélectionné le port connecté au pont associé en cours de test.

ÉTAPE 4 Si un partenaire de lien est détecté via STP, cliquez sur **Activer la migration des protocoles** pour effectuer un test de migration des protocoles. Cette opération détecte si le lien associé utilisant STP existe toujours et, si c'est le cas, s'il a migré vers RSTP. S'il existe toujours en tant que lien STP, le périphérique continue de communiquer avec lui via STP. Sinon, s'il a migré vers RSTP, le périphérique communique avec lui respectivement via RSTP.

ÉTAPE 5 Sélectionnez une interface et cliquez sur **Modifier**. La page *Modifier le paramètre d'interface RSTP* s'affiche.

ÉTAPE 6 Saisissez les paramètres.

- **Interface :** définissez l'interface et précisez le port ou LAG où RSTP doit être configuré.
- **État administratif point à point** : définissez l'état du lien point à point. Les ports définis en tant que Full Duplex sont considérés comme liens de port point à point.
  - *Activer :* ce port devient un port de bordure RSTP lorsque cette option est activée et il est placé rapidement en mode Transfert (généralement en 2secondes).
  - *Désactiver :* le port n'est pas considéré comme port point à point pour le RSTP; par conséquent, STP fonctionne sur ce port à une vitesse normale et non à haute vitesse.
  - *Auto :* détermine automatiquement l'état du commutateur en utilisant les BPDU RSTP.
- **État opérationnel point à point** : affiche l'état opérationnel point à point si l'**État administratif point à point** est défini sur Auto.
- **Rôle :** affiche le rôle du port qui a été assigné par STP afin de fournir des chemins STP. Les rôles possibles sont :
  - *Racine :* chemin de coût inférieur pour transférer des paquets au pont racine.
  - *Désigné :* interface par laquelle le pont est relié au LAN et qui fournit le chemin de coût inférieur depuis le LAN vers le pont racine.
  - *Secondaire :* fournit un chemin alternatif de l'interface racine au pont racine.
  - *Sauvegarde :* fournit un chemin de sauvegarde pour le chemin de port désigné vers les nœuds terminaux STP. Cela fournit une configuration dans laquelle deux ports sont reliés dans une boucle par un lien point à point. Des ports de secours sont également utilisés lorsqu'un LAN possède deux ou plusieurs connexions établies à un segment partagé.
  - *Désactivé* : le port ne participe pas au Spanning Tree.
- **Mode :** affiche le mode Spanning Tree actuel : RSTP ou STP classique.
- **État opérationnel Fast Link** : indique si Fast Link (port de bordure) est activé, désactivé ou automatique pour l'interface. Les valeurs disponibles sont les suivantes :

- *Activé* : Fast Link est activé.
- *Désactivé* : Fast Link est désactivé.
- *Auto :* le mode Fast Link s'active quelques secondes après l'activation de l'interface.

▪ **État des ports :** affiche l'état RSTP sur le port spécifique.

- *Désactivé :* le protocole STP est actuellement désactivé sur le port.
- *Blocage :* le port est actuellement bloqué et ne peut ni transférer le trafic ni connaître les adresses MAC.
- *Écoute :* le port est en mode Écoute. Il ne peut ni transférer le trafic ni connaître les adresses MAC.
- *Apprentissage :* le port est en mode Apprentissage. Il ne peut pas transférer le trafic mais il peut prendre connaissance des nouvelles adresses MAC.
- *Transfert :* le port est en mode Transfert. Il peut réacheminer du trafic et apprendre de nouvelles adressesMAC.

ÉTAPE 7 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

14

Gestion des tables d'adresses MAC

Cette section vous explique comment ajouter des adresses MAC au système. Elle couvre les rubriques suivantes :

- **Configuration d'adresses MAC statiques**
- **Gestion des adresses MAC dynamiques**

Types d'adresses MAC

Il existe deux types d'adresses MAC : statiques et dynamiques. En fonction de leur type, les adresses MAC sont stockées avec les informations relatives aux VLAN et aux ports soit dans la table des *adresses statiques*, soit dans la table des *adresses dynamiques*.

Les adresses statiques sont configurées par l'utilisateur et n'expirent donc jamais.

Une nouvelle adresse MAC source qui apparaît dans une trame reçue par le commutateur est ajoutée à la table des adresses dynamiques. Cette adresse MAC est conservée pendant une période que vous pouvez configurer. Si aucune autre trame disposant de la même adresse MAC source n'apparaît sur le commutateur avant l'expiration de ce délai, l'entrée MAC est supprimée (expirée) de la table.

Lorsqu'une trame arrive au niveau du commutateur, celui-ci recherche une adresse MAC de destination correspondant à une entrée de la table des adresses statiques ou dynamiques. En cas de correspondance, la trame est marquée en sortie sur un port spécifique de la table. Les trames adressées à une adresse MAC n'ayant pas été trouvée dans les tables sont diffusées/transmises à tous les ports du VLAN approprié. On les appelle des trames de monodiffusion inconnue.

Le commutateur prend en charge un maximum de 8 000 adresses MAC statiques et dynamiques.

Configuration d'adresses MAC statiques

Les adresses MAC statiques sont affectées à une interface physique et à un VLAN spécifiques sur le commutateur. Si cette adresse est détectée sur une autre interface, elle est ignorée et n'est pas consignée dans la table des adresses.

Pour définir une adresse statique :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC > Adresses statiques**. La page *Adresses statiques* s'ouvre.

La page *Adresses statiques* affiche les adresses statiques définies.

ÉTAPE 2 Cliquez sur **Ajouter**. La page *Ajouter une adresse statique* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **ID de VLAN :** sélectionnez l'ID de VLAN du port.
- **AdresseMAC** : saisissez l'adresse MAC de l'interface.
- **Interface** : sélectionnez une interface (port ou LAG) pour l'entrée.
- **État :** sélectionnez le mode de traitement de l'entrée. Les options sont les suivantes :
  - *Permanent* : le système ne supprime jamais cette adresse MAC. Si l'adresse MAC statique est enregistrée dans la Configuration de démarrage, elle est conservée après redémarrage.
  - *Suppr. à la réinitialisation* : l'adresse MAC statique est supprimée lorsque le périphérique est réinitialisé.
  - *Supprimer à l'expiration :* l'adresse MAC est supprimée à expiration du délai.
  - *Sécurisé*: l'adresse MAC est sécurisée lorsque l'interface est en mode verrouillé classique (voir **Configuration de la sécurité des ports**).

ÉTAPE 4 Cliquez sur **Appliquer**. Une nouvelle entrée apparaît dans la table.

Gestion des adresses MAC dynamiques

La table des adresses dynamiques (table de pontage) contient les adresses MAC obtenues en surveillant les adresses source des trames entrant dans le commutateur.

Pour éviter de surcharger cette table et pour garder de l'espace pour de nouvelles adresses MAC, une adresse est supprimée si elle n'enregistre aucun trafic pendant une période donnée. Ce délai correspond au délai d'expiration.

Configuration du délai d'expiration d'adresses MAC dynamiques

Pour configurer le délai d'expiration des adresses dynamiques :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC > Paramètres des adresses dynamiques**. La page *Paramètres des adresses dynamiques* s'ouvre.

ÉTAPE 2 Saisissez le **Délai d'expiration**. Le délai d'expiration est une valeur comprise entre la valeur configurée par l'utilisateur et deux fois cette valeur moins 1. Par exemple, si vous avez entré 300 secondes, le délai d'expiration sera compris entre 300 et 599 secondes.

ÉTAPE 3 Cliquez sur **Appliquer**. Le délai d'expiration est mis à jour.

Interrogation d'adresses dynamiques

Pour interroger la table des adresses dynamiques :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC > Adresses dynamiques**. La page *Adresses dynamiques* s'ouvre.

ÉTAPE 2 Dans le bloc *Filtre*, vous pouvez saisir les critères d'interrogation suivants :

- **ID de VLAN** : saisissez l'ID de VLAN pour lequel la table est interrogée.
- **AdresseMAC** : saisissez l'adresse MAC pour laquelle la table est interrogée.
- **Interface** : sélectionnez l'interface au sujet de laquelle la table est interrogée. L'interrogation peut également rechercher des unités/logements, ports ou LAG spécifiques.

ÉTAPE 3 Renseignez le champ **Clé de tri de la table des adresses dynamiques** en fonction duquel la table est triée. La table des adresses peut être triée en fonction de l'ID de VLAN, de l'adresse MAC ou de l'interface.

ÉTAPE 4 Cliquez sur **OK**. La Table des adresses MAC dynamiques est interrogée et les résultats s'affichent.

Cliquez sur **Effacer la table** pour supprimer toutes les adresses MAC dynamiques.

15

Configuration du transfert de multidiffusion

Cette section décrit la fonction de transfert de multidiffusion et couvre les rubriques suivantes :

- **Transfert de multidiffusion**
- **Définition des propriétés de multidiffusion**
- **Ajout d'une adresse MAC de groupe**
- **Ajout d'adresses IP de groupe de multidiffusion**
- **Configuration de la surveillance de trafic IGMP**
- **Surveillance MLD**
- **Interrogation du groupe de multidiffusion IP IGMP/MLD**
- **Définition des ports de routeur de multidiffusion**
- **Définition de la multidiffusion Tout transférer**
- **Définition des paramètres de multidiffusion non enregistrée**

Transfert de multidiffusion

Le transfert de multidiffusion permet la transmission d'informations en mode 1-à-n. Les applications de multidiffusion sont particulièrement utiles pour transmettre des informations à plusieurs clients lorsque ces clients n'ont pas besoin de l'intégralité du service disponible. Ceci est par exemple le cas dans le cadre d'une application de TV par câble où les clients peuvent contacter une chaîne au milieu d'une transmission et interrompre la connexion avant la fin.

Les données ne sont envoyées qu'aux ports pertinents. Le fait de ne transférer les données qu'aux ports concernés permet d'économiser de la bande passante et des ressources d'hôte sur la liaison.

Pour que le transfert de multidiffusion fonctionne sur des sous-réseaux IP, les nœuds et les routeurs doivent être compatibles avec la multidiffusion. Un nœud compatible avec la multidiffusion doit pouvoir :

- Envoyer et recevoir des paquets de multidiffusion
- Enregistrer les adresses de multidiffusion que le nœud écoute auprès des routeurs locaux afin que les routeurs locaux et distants puissent router le paquet de multidiffusion vers les nœuds.

Configuration de multidiffusion typique

Alors que les routeurs de multidiffusion routent les paquets de multidiffusion d'un sous-réseau IP à un autre, les commutateurs Layer 2 compatibles avec la multidiffusion transfèrent les paquets de multidiffusion vers les nœuds enregistrés d'un LAN ou d'un VLAN.

La configuration typique inclut un routeur qui transfère les flux de multidiffusion d'un réseau IP privé et/ou public à l'autre, un commutateur doté de fonctions de traçage (Snooping) IGMP (Internet Group Membership Protocol, protocoles d'appartenance aux groupes Internet) ou MLD (Multicast Listener Discovery, détection des services d'écoute de multidiffusion) et un client de multidiffusion qui souhaite recevoir un flux de multidiffusion. Dans cette configuration, le routeur envoie des requêtes IGMP à intervalle régulier.

REMARQUE MLD pour IPv6 provient d'IGMPv2 pour IPv4. Même si la description de cette section concerne principalement IGMP, elle décrit également l'utilisation de MLD lorsque cela s'applique.

Ces requêtes atteignent le commutateur, qui répond en transmettant les requêtes au VLAN et en reconnaissant le port où réside un routeur de multidiffusion (Mrouter). Lorsqu'un hôte reçoit le message de requête IGMP, il répond en envoyant un message d'adhésion IGMP indiquant que l'hôte souhaite recevoir un flux de multidiffusion spécifique en provenance (facultatif) d'une source spécifique. Le commutateur avec fonction de traçage IGMP Snooping analyse les messages d'adhésion et apprend que le flux de multidiffusion demandé par l'hôte doit être transféré à ce port spécifique. Il transfère ensuite l'adhésion IGMP, uniquement vers le routeur Mrouter. De même, lorsque le routeur Mrouter reçoit un message d'adhésion IGMP, il apprend que l'interface à partir de laquelle il a reçu ce message souhaite recevoir un flux de multidiffusion spécifique. Le routeur Mrouter transfère le flux de multidiffusion demandé vers l'interface.

Fonctionnement de la multidiffusion

Dans un service de multidiffusion Layer2, un commutateur Layer 2 reçoit une seule trame, adressée à une adresse de multidiffusion spécifique. Il crée des copies de la trame pour les transmettre à chacun des ports concernés.

Lorsque le commutateur possède une fonction de traçage IGMP/MLD Snooping et qu'il reçoit une trame de flux de multidiffusion, il la transfère à tous les ports enregistrés pour recevoir le flux de multidiffusion en question à l'aide de messages d'adhésion IGMP.

Le commutateur peut transférer des flux de multidiffusion sur la base de l'une des options suivantes :

- Adresse MAC de groupe de multidiffusion
- Adresse IP de multidiffusion de groupe (G)
- Combinaison de l'adresse IP source (S) et de l'adresse IP de multidiffusion de groupe (G) du paquet de multidiffusion

Vous ne pouvez configurer qu'une seule de ces options pour chaque VLAN.

Le système gère des listes de groupes de multidiffusion pour chaque VLAN. Ceci permet de gérer les informations de multidiffusion que chaque port doit recevoir. Les groupes de multidiffusion et les ports destinataires associés peuvent être configurés de manière statique ou appris de manière dynamique via le traçage de protocole IGMP Snooping ou MLD (Multicast Listener Discovery) Snooping.

Enregistrement de multidiffusion

L'enregistrement de multidiffusion est le processus qui consiste à écouter les protocoles d'enregistrement de multidiffusion et à y répondre. Les protocoles disponibles sont IGMP pour IPv4 et MLD pour IPv6.

Lorsque le traçage IGMP/MLD Snooping est activé sur un commutateur d'un VLAN, il analyse les paquets IGMP/MLD qu'il reçoit à partir du VLAN connecté au commutateur et à tous les routeurs de multidiffusion du réseau.

Lorsqu'un commutateur apprend qu'un hôte utilise des messages IGMP/MLD pour enregistrer un flux de multidiffusion, éventuellement à partir d'une source spécifique, ce commutateur ajoute l'enregistrement à sa base MFDB (Multicast Forwarding Data Base, base de données de transfert de multidiffusion).

Le traçage IGMP/MLD Snooping peut réduire le trafic de multidiffusion en provenance d'applications IP grosses consommatrices de bande passante de flux. Un commutateur qui utilise le traçage IGMP/MLD Snooping ne transfère le trafic de multidiffusion que vers les hôtes intéressés par ce trafic. Cette réduction du trafic de multidiffusion diminue la charge de traitement des paquets sur le commutateur et réduit la charge de travail des hôtes puisqu'ils n'ont pas besoin de recevoir tout le trafic de multidiffusion généré sur le réseau et de le filtrer.

Les versions suivantes sont prises en charge :

- IGMP v1/v2/ v3
- MLD v1/v2

Propriétés d'adresse de multidiffusion

Les adresses de multidiffusion possèdent les propriétés suivantes :

- Chaque adresse de multidiffusion IPv4 se trouve dans la plage d'adresses situées entre 224.0.0.0 et 239.255.255.255.
- L'adresse de multidiffusion IPv6 est FF00:/8.
- Pour mapper une adresse IP de multidiffusion de groupe sur une adresse de multidiffusion Layer 2 :
  - Pour IPv4, le mappage s'effectue en prenant les 23 bits de poids faible (de droite) de l'adresse IPv4 et en les ajoutant au préfixe 01:00:5e. Normalement, les neuf bits supérieurs de l'adresse IP sont ignorés et toutes les adresses IP qui diffèrent uniquement par ces bits supérieurs sont mappées sur la même adresse Layer 2 puisque les 23 bits inférieurs utilisés sont identiques. Par exemple, l'adresse 234.129.2.3 est mappée sur l'adresse MAC de groupe de multidiffusion 01:00:5e :01:02:03. Il est possible de mapper jusqu'à 32 adresses IP de multidiffusion de groupe sur une même adresse Layer 2.
  - Pour IPv6, le processus de mappage utilise les 32 bits de poids faible (de droite) de l'adresse de multidiffusion et ajoute le préfixe 33:33. Par exemple, l'adresse de multidiffusion IPv6 FF00:1122:3344 est mappée sur l'adresse de multidiffusion Layer 2 33:33:11:22:33:44.

Définition des propriétés de multidiffusion

La page *Propriétés* permet de configurer l'état de filtrage multidiffusion par ponts.

Par défaut, toutes les trames de multidiffusion sont envoyées sur tous les ports du VLAN. Pour ne transférer les données, de façon sélective, que vers les ports concernés et filtrer (éliminer) le flux de multidiffusion sur les autres ports, activez le filtrage multidiffusion par ponts sur la page *Propriétés.*

Si le filtrage est activé, les trames de multidiffusion sont transférées vers un sous-ensemble des ports sur le VLAN concerné, comme il aura été défini dans la base MFDB (Multicast Forwarding Data Base, base de données de transfert de multidiffusion). Le filtrage multidiffusion s'exerce sur l'ensemble du trafic. Par défaut, ce type de trafic est envoyé à tous les ports concernés mais vous pouvez limiter le transfert à un sous-ensemble plus réduit.

L'une des méthodes couramment utilisées de représentation des membres de multidiffusion est la notation (S,G), où « S » représente la source (unique) qui envoie un flux de données de multidiffusion et « G » représente l'adresse IPv4 ou IPv6 de groupe. Si un client Multicast peut recevoir du trafic de multidiffusion à partir de n'importe quelle source d'un groupe de multidiffusion donné, cette notation devient (*,G).

Voici différentes méthodes de transfert des trames de multidiffusion :

- **Adresse MAC de groupe** : basée sur l'adresse MAC de destination dans la trame Ethernet.

  REMARQUE Comme indiqué précédemment, il est possible de mapper une ou plusieurs adresses IP de multidiffusion de groupe sur une seule adresse MAC de groupe. Le transfert basé sur une adresse MAC de groupe peut provoquer le transfert d'un flux de multidiffusion IP vers des ports qui ne possèdent aucun récepteur pour ce flux.

- **Adresse IP de groupe** : basée sur l'adresse IP de destination du paquet IP (*,G).

- **Adresse IP source de groupe** : basée à la fois sur l'adresse IP de destination et l'adresse IP source du paquet IP (S,G).

En sélectionnant le mode de transfert, vous pouvez définir la méthode utilisée par le matériel pour identifier le flux de multidiffusion à l'aide de l'une des options suivantes : Adresse MAC de groupe, Adresse IP de groupe ou Adresse IP source de groupe.

(S,G) est pris en charge par IGMPv3 et MLDv2 alors qu'IGMPv1/2 et MLDv1 ne prennent en charge que (*.G), qui inclut uniquement l'ID de groupe.

Le commutateur peut prendre en charge jusqu'à 256 adresses de groupe de multidiffusion statiques et dynamiques.

Pour activer le filtrage multidiffusion et sélectionner la méthode de transfert :

ÉTAPE 1 Cliquez sur **Multidiffusion> Propriétés**. La page *Propriétés* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **État du filtrage multidiffusion par ponts** : sélectionnez cette option pour activer le filtrage.
- **ID VLAN** : sélectionnez l'ID du VLAN voulu pour définir sa méthode de transfert.
- **Méthode de transfert pourIPv6** : choisissez l'une des méthodes de transfert suivantes pour les adresses IPv6 : Adresse MAC de groupe, Adresse IP de groupe ou Adresse IP source de groupe.
- **Méthode de transfert pour IPv4** : choisissez l'une des méthodes de transfert suivantes pour les adresses IPv4 : Adresse MAC de groupe, Adresse IP de groupe ou Adresse IP source de groupe.

ÉTAPE 3 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Ajout d'une adresse MAC de groupe

Le commutateur prend en charge le transfert du trafic de multidiffusion entrant sur la base des informations de groupe de multidiffusion. Ces informations sont tirées des paquets IGMP/MLD reçus ou résultent d'une configuration manuelle. Elles sont stockées dans la base MFDB (Multicast Forwarding Database, base de données de transfert de multidiffusion).

Lorsque le système reçoit une trame d'un VLAN configuré pour transférer les flux de multidiffusion sur la base des adresses MAC de groupe et que l'adresse de destination est une adresse de multidiffusion Layer 2, la trame est transférée vers tous les ports membres de l'adresse MAC de groupe.

La page *Adresse de groupe MAC* offre les fonctions suivantes :

- Interrogation et affichage d'informations tirées de la base de données de filtrage multidiffusion concernant un ID de VLAN spécifique ou un groupe particulier d'adresses MAC. Ces données sont acquises de manière dynamique par traçage IGMP/MLD Snooping ou de manière statique par saisie manuelle.
- Ajout ou suppression d'entrées statiques dans la base MFDB, qui fournit des informations de transfert statiques basées sur les adresses MAC de destination.
- Affichage de la liste de tous les ports/LAG membres de chaque ID de VLAN ou adresse MAC de groupe, et indication précisant si le trafic doit ou non être transféré vers cette destination.

Pour afficher les informations de transfert, une fois en mode *Adresse IP de groupe* ou en mode *Groupe IP et source*, utilisez la page *Adresse IP de groupe de multidiffusion*.

Pour définir et afficher des groupes de multidiffusion MAC :

ÉTAPE 1 Cliquez sur **Multidiffusion > Adresse MAC de groupe**. La page *Adresse de groupe MAC* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **ID VLAN est égal à** : saisissez l'ID de VLAN du groupe à afficher.
- **Adresse MAC de groupe égale à** : définissez l'adresse MAC du groupe de multidiffusion à afficher. Si aucune adresse MAC de groupe n'est indiquée, la page affiche toutes les adresses MAC de groupe du VLAN sélectionné.

ÉTAPE 3 Cliquez sur **OK**. Les adresses MAC de groupe de multidiffusion sont affichées dans le bloc inférieur.

Le système affiche les entrées qui ont été créées sur cette page et sur la page *Adresse IP de groupe de multidiffusion*. Pour celles qui ont été créées sur la page *Adresse IP de groupe de multidiffusion*, les adresses IP sont converties en adresses MAC.

ÉTAPE 4 Cliquez sur **Ajouter** pour ajouter une adresse MAC de groupe statique. La page *Ajouter une adresse de groupe MAC* s'ouvre.

ÉTAPE 5 Saisissez les paramètres.

- **ID VLAN** : définit l'ID de VLAN du nouveau groupe de multidiffusion.

- **Adresse de groupe MAC** : définit l'adresse MAC du nouveau groupe de multidiffusion.

ÉTAPE 6 Cliquez sur **Appliquer** et l'adresse MAC du groupe de multidiffusion est écrite dans le fichier de Configuration d'exécution.

Pour configurer et afficher l'enregistrement des interfaces au sein du groupe, sélectionnez une adresse et cliquez sur **Détails**. La page *Paramètres d'adresse de groupe MAC* s'ouvre.

La page affiche les éléments suivants :

- **ID VLAN** : ID de VLAN du groupe de multidiffusion.
- **Adresse de groupe MAC** : adresse MAC du groupe.

ÉTAPE 7 Sélectionnez dans le menu **Filtre : Type d'interface** le port ou le LAG à afficher.

ÉTAPE 8 Cliquez sur **OK** pour afficher les membres (ports ou LAG).

ÉTAPE 9 Sélectionnez la façon dont chaque interface est associée au groupe de multidiffusion :

- **Statique** : rattache l'interface au groupe de multidiffusion en tant que membre statique.
- **Dynamique** : indique que l'interface a été ajoutée au groupe de multidiffusion via le traçage IGMP/MLD Snooping.
- **Interdit** : spécifie que ce port n'est pas autorisé à rejoindre ce groupe sur ce VLAN.
- **Aucun** : spécifie que le port n'est actuellement pas membre de ce groupe de multidiffusion sur ce VLAN.

ÉTAPE 10 Cliquez sur **Appliquer** ; le fichier de Configuration d'exécution est mis à jour.

REMARQUE Les entrées qui ont été créées sur la page *Adresse IP de groupe de multidiffusion* ne peuvent pas être supprimées sur cette page (même si elles sont sélectionnées).

Ajout d'adresses IP de groupe de multidiffusion

La page *Adresse IP de groupe de multidiffusion* est identique à la page *Adresse de groupe MAC*, à la seule différence que les groupes de multidiffusion y sont identifiés par leurs adresses IP.

La page *Adresse IP de groupe de multidiffusion* vous permet d'interroger et d'ajouter des IP de groupes de multidiffusion.

Pour définir et afficher des IP de multidiffusion de groupes :

ÉTAPE 1 Cliquez sur **Multidiffusion > Adresse IP de multidiffusion de groupe**. La page *Adresse IP de groupe de multidiffusion* s'ouvre.

La page affiche toutes les adresses IP de multidiffusion de groupe apprises via le traçage (Snooping).

ÉTAPE 2 Saisissez les paramètres nécessaires pour le filtrage.

- **ID VLAN est égal à** : définissez l'ID de VLAN du groupe à afficher.
- **VersionIP est égale à** : sélectionnez IPv6 ou IPv4.
- **AdresseIP de multidiffusion de groupe égale à** : définissez l'adresse IP de multidiffusion du groupe à afficher. Cela s'applique uniquement lorsque le mode de transfert est (S,G).
- **AdresseIP source est égale à** : définissez l'adresse IP source du périphérique émetteur. Si le mode est (S,G), saisissez la valeur S (indiquant l'expéditeur). Combinée à l'adresse IP de groupe, cette valeur définit l'ID de multidiffusion du groupe (S,G) à afficher. Si le mode est (*.G), saisissez un astérisque (*) pour indiquer que le groupe de multidiffusion n'est défini que par sa destination.

ÉTAPE 3 Cliquez sur **OK**. Les résultats s'affichent dans le bloc inférieur. Lorsque vous activez à la fois Bonjour et IGMP sur un commutateur en mode système Layer 2, l'adresse IP de multidiffusion de Bonjour est affichée.

ÉTAPE 4 Cliquez sur **Ajouter** pour ajouter une adresse IP de multidiffusion statique de groupe. La page *Adresse IP de groupe de multidiffusion* s'ouvre.

ÉTAPE 5 Saisissez les paramètres.

- **ID VLAN** : définit l'ID de VLAN du groupe à ajouter.
- **Version IP** : sélectionnez le type d'adresse IP approprié.

- **Adresse IP de multidiffusion de groupe** : définit l'adresse IP de multidiffusion du nouveau groupe.
- **Propre à la source** : indique que l'entrée contient une source spécifique et ajoute l'adresse correspondante dans le champ Adresse IP source. Dans le cas contraire, l'entrée est ajoutée sous la forme (*,G), c'est-à-dire une adresse IP de groupe associée à toutes les sourcesIP.
- **Adresse IP source** : définit l'adresse source à inclure.

ÉTAPE 6 Cliquez sur **Appliquer**. L'IP de multidiffusion du groupe est ajouté et le périphérique est mis à jour.

ÉTAPE 7 Pour configurer et afficher l'enregistrement d'une adresse IP de groupe, sélectionnez une adresse puis cliquez sur **Détails**. La page *Paramètres d'interface de multidiffusion IP* s'ouvre.

Les ID de VLAN, Version IP, Adresse IP de groupe de multidiffusion et Adresse IP source sélectionnés s'affichent en lecture seule en haut de la fenêtre. Vous pouvez sélectionner le type de filtre :

- **Type d'interface est égal à** : choisissez d'afficher les ports ou les LAG.

ÉTAPE 8 Sélectionnez le type d'association de chaque interface. Les options disponibles sont les suivantes :

- **Statique** : rattache l'interface au groupe de multidiffusion en tant que membre statique.
- **Interdit** : spécifie que ce port n'est pas autorisé à rejoindre ce groupe sur ce VLAN.
- **Aucun** : indique que le port n'est actuellement pas membre de ce groupe de multidiffusion sur ce VLAN. Cette option est définie par défaut tant que l'option Statique ou Interdit n'est pas sélectionnée.

ÉTAPE 9 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Configuration de la surveillance de trafic IGMP

Pour prendre en charge le transfert de multidiffusion sélectif (IPv4), vous devez activer le filtrage multidiffusion par ponts (sur la page *Propriétés*). Vous devez aussi activer le traçage IGMP Snooping globalement ainsi que pour chacun des VLAN concernés (sur la page *Traçage IGMP Snooping*).

Par défaut, un commutateur Layer 2 transfère les trames de multidiffusion vers tous les ports du VLAN concerné, traitant en fait les trames comme s'il s'agissait de diffusions. Avec le traçage IGMP Snooping, le commutateur transfère les trames de multidiffusion vers les ports comportant des clients de multidiffusion enregistrés.

REMARQUE Le commutateur n'effectue le traçage IGMP Snooping que sur les VLAN statiques. Le traçage IGMP Snooping n'est pas pris en charge pour les VLAN dynamiques.

Lorsque vous activez le traçage IGMP Snooping, globalement ou sur un VLAN, tous les paquets IGMP sont transférés vers le CPU (l'unité centrale, l'UC). Le CPU analyse les paquets entrants et détermine les éléments suivants :

- Ports qui demandent à rejoindre tel ou tel groupe de multidiffusion sur un VLAN spécifique.
- Ports connectés aux routeurs de multidiffusion (Mrouters) qui génèrent des requêtes IGMP.
- Ports qui reçoivent les protocoles de requête PIM, DVMRP ou IGMP.

Ces informations sont affichées sur la page *Traçage IGMP Snooping*.

Les ports demandant à rejoindre un groupe de multidiffusion spécifique envoient un rapport IGMP qui spécifie le ou les groupes que l'hôte concerné souhaite rejoindre. Cela provoque la création d'une entrée de transfert dans la base de données de transfert de multidiffusion.

Pour activer le traçage IGMP Snooping et identifier le commutateur en tant qu'émetteur de requêtes de traçage IGMP Snooping sur un VLAN :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **IGMP Snooping**. La page *Traçage IGMP Snooping* s'ouvre.

ÉTAPE 2 Activez ou désactivez l'état IGMP Snooping.

Lorsque le traçage IGMP Snooping est activé au niveau global, le périphérique qui surveille le trafic réseau peut détecter les hôtes qui ont demandé à recevoir le trafic de multidiffusion.

Le commutateur exécute uniquement le traçage IGMP Snooping si vous avez activé à la fois IGMP Snooping et le filtrage multidiffusion par ponts.

ÉTAPE 3 Sélectionnez un VLAN et cliquez sur **Modifier**. La page *Modifier IGMP Snooping* s'ouvre.

ÉTAPE 4 Saisissez les paramètres.

- **ID VLAN** : sélectionnez l'ID du VLAN sur lequel le traçage IGMP Snooping est défini.
- **État IGMP Snooping** : active ou désactive la surveillance du trafic réseau pour le VLAN sélectionné.
- **État IGMP Snooping opérationnel** : affiche l'état actuel du traçage IGMP Snooping pour le VLAN sélectionné.
- **Apprentissage automatique des ports MRouter** : permet d'activer ou de désactiver l'apprentissage automatique des ports sur lesquels le routeur de multidiffusion (Mrouter) est connecté.
- **Robustesse des requêtes** : saisissez la valeur de la variable de robustesse à utiliser si ce commutateur est choisi comme émetteur de requêtes.
- **Robustesse des requêtes opérationnelles** : affiche la variable de robustesse envoyée par l'émetteur de requêtes choisi.
- **Intervalle de requête** : saisissez l'intervalle à appliquer entre deux requêtes générales si ce commutateur est choisi comme émetteur de requêtes.
- **Intervalle de requête opérationnelle** : intervalle en secondes qui sépare deux requêtes générales envoyées par l'émetteur de requêtes choisi.
- **Intervalle de réponse max aux requêtes** : saisissez la durée utilisée pour calculer le code de réponse maximal inséré dans les requêtes générales périodiques.

- **Intervalle de réponse max aux requêtes opérationnelles** : indique l'intervalle maximal de réponse aux requêtes inclus dans les requêtes générales envoyées par l'émetteur de requêtes choisi.
- **Nombre de requêtes du dernier membre** : indiquez le nombre de requêtes propres au groupe IGMP envoyées avant que le commutateur considère qu'il n'existe aucun autre membre pour le groupe, dans la mesure où ce commutateur a été choisi comme émetteur de requêtes.
- **Nombre de requêtes du dernier membre opérationnel** : affiche la valeur opérationnelle du compteur de requêtes du dernier membre.
- **Intervalle de requête du dernier membre** : saisissez le délai maximal de réponse aux requêtes à utiliser si le commutateur ne peut pas lire cette valeur dans les requêtes propres au groupe envoyées par l'émetteur de requêtes choisi.
- **Intervalle de requête du dernier membre opérationnel** : affiche l'intervalle de requête du dernier membre, envoyé par l'émetteur de requêtes choisi.
- **Sortie immédiate** : activez Sortie immédiate pour réduire la durée nécessaire au blocage d'un flux de multidiffusion envoyé à un port membre lorsque ce dernier reçoit un message de sortie de groupe IGMP.

ÉTAPE 5 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Surveillance MLD

Les hôtes emploient le protocole MLD pour signaler leur participation aux sessions de multidiffusion tandis que le commutateur utilise la surveillance MLD pour générer des listes de membres de multidiffusion. Ces listes servent à transmettre les paquets de multidiffusion uniquement aux ports du commutateur où existent des nœuds hôtes membres des groupes de multidiffusion. Le commutateur ne prend pas en charge l'émetteur de requêtes MLD.

Les hôtes emploient le protocole MLD pour signaler leur participation aux sessions de multidiffusion.

Le commutateur prend en charge deux versions du traçage MLD Snooping :

- Le traçage MLDv1 Snooping détecte les paquets de contrôle MLDv1 puis établit un pont pour le trafic sur la base d'adresses de multidiffusion de destinationIPv6.
- Le traçage MLDv2 Snooping utilise des paquets de contrôle MLDv2 pour transférer le trafic sur la base de l'adresse IPv6 source et de l'adresse de multidiffusion de destination IPv6.

La version MLD réelle est sélectionnée par le routeur de multidiffusion sur le réseau.

Dans une approche semblable au traçage IGMP Snooping, le trames MLD font l'objet d'un traçage lorsqu'elles sont transférées par le commutateur des stations de travail vers un routeur de multidiffusion en amont et inversement. Cette fonction permet à un commutateur de déterminer :

- les ports sur lesquels il existe des stations de travail intéressées par l'adhésion à un groupe de multidiffusion particulier ;
- les ports sur lesquels résident les routeurs de multidiffusion qui envoient des trames de multidiffusion.

Ces connaissances servent à exclure des ports dénués d'intérêt (ceux sur lesquels aucune station de travail n'est enregistrée pour recevoir un groupe de multidiffusion spécifique) de l'ensemble de transfert d'une trame de multidiffusion entrante.

Si vous activez le traçage MLD Snooping en plus des groupes de multidiffusion configurés manuellement, cela crée une union entre les membres de groupes et de ports multidiffusions dérivés de la configuration manuelle et la détection dynamique par traçage MLD Snooping. Seules les définitions statiques sont conservées au redémarrage du système.

Pour activer le traçage MLD Snooping :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **MLD Snooping**. La page *Traçage MLD Snooping* s'ouvre.

ÉTAPE 2 Activez ou désactivez l'option **État MLD Snooping**. Lorsque le traçage MLD Snooping est activé au niveau global, le périphérique qui surveille le trafic réseau peut détecter les hôtes qui ont demandé à recevoir le trafic de multidiffusion. Le

commutateur exécute uniquement le traçage MLD Snooping si vous avez activé à la fois MLD Snooping et le filtrage multidiffusion par ponts.

ÉTAPE 3 Sélectionnez un VLAN et cliquez sur **Modifier**. La page *Modifier MLD Snooping* s'ouvre.

ÉTAPE 4 Saisissez les paramètres.

- **ID VLAN** : sélectionnez l'ID du VLAN.
- **État MLD Snooping** : activez ou désactivez le traçage MLD Snooping sur le VLAN. Le commutateur surveille le trafic réseau pour déterminer les hôtes qui ont demandé à recevoir du trafic de multidiffusion. Le commutateur exécute uniquement le traçage MLD Snooping si vous avez activé à la fois MLD Snooping et le filtrage multidiffusion par ponts.
- **État MLD Snooping opérationnel** : affiche l'état actuel du traçage MLD Snooping pour le VLAN sélectionné.
- **Apprentissage automatique des ports MRouter** : permet d'activer ou de désactiver l'apprentissage automatique pour le routeur de multidiffusion.
- **Robustesse des requêtes** : saisissez la valeur de la variable de robustesse à utiliser si le commutateur ne peut pas lire cette valeur dans les messages envoyés par l'émetteur de requêtes choisi.
- **Robustesse des requêtes opérationnelles** : affiche la variable de robustesse envoyée par l'émetteur de requêtes choisi.
- **Intervalle de requête** : saisissez la valeur d'intervalle de requête que le commutateur doit appliquer s'il ne peut pas extraire la valeur des messages envoyés par l'émetteur de requêtes choisi.
- **Intervalle de requête opérationnelle** : intervalle en secondes entre deux requêtes générales reçues de l'émetteur de requêtes choisi.
- **Intervalle de réponse max aux requêtes** : saisissez le délai maximal de réponse aux requêtes à utiliser si le commutateur ne peut pas lire cette valeur dans les requêtes générales envoyées par l'émetteur de requêtes choisi.
- **Intervalle de réponse max aux requêtes opérationnelles** : saisissez la durée utilisée pour calculer le code de réponse maximal inséré dans les requêtes générales.
- **Nombre de requêtes du dernier membre** : saisissez le nombre de requêtes du dernier membre à utiliser si le commutateur ne peut pas dériver cette valeur des messages envoyés par l'émetteur de requêtes choisi.

- **Nombre de requêtes du dernier membre opérationnel** : affiche la valeur opérationnelle du compteur de requêtes du dernier membre.
- **Intervalle de requête du dernier membre** : saisissez le délai maximal de réponse aux requêtes à utiliser si le commutateur ne peut pas lire cette valeur dans les requêtes propres au groupe envoyées par l'émetteur de requêtes choisi.
- **Intervalle de requête du dernier membre opérationnel** : intervalle de requête du dernier membre, envoyé par l'émetteur de requêtes choisi.
- **Sortie immédiate** : activez cette option pour réduire la durée nécessaire au blocage du trafic MLD inutile envoyé à un port du commutateur.

ÉTAPE 5 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Interrogation du groupe de multidiffusion IP IGMP/MLD

La page *Groupe de multidiffusion IP IGMP/MLD* affiche l'adresse IPv4 et IPv6 des groupes appris à partir des messages IGMP/MLD.

Il peut y avoir une différence entre les informations affichées sur cette page et, par exemple, les informations affichées sur la page *Adresse de groupe MAC.* Supposez que le système comporte des groupes basés sur l'adresse MAC et qu'un port ait demandé à rejoindre les groupes de multidiffusion 224.1.1.1 et 225.1.1.1, tous deux mappés sur la même adresse de multidiffusion MAC 01:00:5e:01:01:01. Dans ce cas, la page de *multidiffusion MAC* comporte une seule entrée mais la page décrite ici en comporte deux.

Pour émettre une requête de recherche d'un groupe de multidiffusion IP :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **IP de multidiffusion de groupes IGMP/MLD**. La page *Groupe de multidiffusion IP IGMP/MLD* s'ouvre.

ÉTAPE 2 Définissez le type de groupe de traçage (Snooping) à rechercher : IGMP ou MLD.

ÉTAPE 3 Saisissez tout ou partie des critères de filtrage des requêtes suivants :

- **Adresse de groupe est égale à** : définit l'adresse MAC ou IP du groupe de multidiffusion à interroger.
- **Adresse source est égale à** : définit l'adresse d'expéditeur à interroger.

- **ID VLAN est égal à** : définit l'ID de VLAN à interroger.

ÉTAPE 4 Cliquez sur **OK**. Les champs suivants sont affichés pour chaque groupe de multidiffusion :

- **VLAN** : ID du VLAN.
- **Adresse de groupe** : adresse MAC ou IP du groupe de multidiffusion.
- **Adresse source** : adresse d'expéditeur pour tous les ports du groupe spécifié.
- **Ports inclus** : liste des ports de destination pour le flux de multidiffusion.
- **Ports exclus** : liste des ports qui ne sont pas inclus dans le groupe.
- **Mode de compatibilité** : version d'enregistrement IGMP/MLD la plus ancienne que le commutateur reçoit des hôtes à l'adresse IP du groupe.

Définition des ports de routeur de multidiffusion

Un port de routeur de multidiffusion (Mrouter) est un port qui se connecte à un routeur de multidiffusion. Le commutateur inclut le ou les numéros de ports de routeur de multidiffusion lorsqu'il transfère les flux de multidiffusion et les messages d'enregistrement IGMP/MLD. Cela est indispensable pour que les routeurs de multidiffusion puissent, à leur tour, transférer les flux de multidiffusion et propager les messages d'enregistrement vers d'autres sous-réseaux.

Pour configurer de manière statique ou afficher les ports dynamiquement détectés qui sont connectés au routeur de multidiffusion :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Port de routeur de multidiffusion**. La page *Port de routeur de multidiffusion* s'ouvre.

ÉTAPE 2 Saisissez tout ou partie des critères de filtrage des requêtes suivants :

- **ID VLAN est égal à** : sélectionnez l'ID de VLAN des ports de routeur qui sont décrits.
- **Version IP est égale à** : sélectionnez la version IP prise en charge par le routeur de multidiffusion.
- **Type d'interface est égal à** : choisissez d'afficher les ports ou les LAG.

ÉTAPE 3 Cliquez sur **OK**. Les interfaces répondant aux critères de requête sont affichées.

ÉTAPE 4 Sélectionnez le type d'association de chaque port ou LAG. Les options disponibles sont les suivantes :

- **Statique** : le port est configuré de manière statique en tant que port de routeur de multidiffusion.
- **Dynamique** : (affichage uniquement) le port est configuré de manière dynamique en tant que port de routeur de multidiffusion à l'aide d'une requête MLD/IGMP. Pour activer l'apprentissage dynamique des ports de routeurs de multidiffusion, accédez à la page **Multidiffusion** > **IGMP Snooping** et à la page **Multidiffusion** > **MLD Snooping**.
- **Interdit** : ce port ne doit pas être configuré en tant que port de routeurs de multidiffusion, même s'il reçoit des requêtes IGMP ou MLD. Si l'option Interdit est activée sur un port, l'apprentissage des ports MRouter n'a pas lieu sur ce port (ce qui signifie que l'option Apprentissage automatique des ports MRouter n'est pas activée sur ce port).
- **Aucun** : le port n'est actuellement pas un port de routeur de multidiffusion.

ÉTAPE 5 Cliquez sur **Appliquer** pour mettre le commutateur à jour.

Définition de la multidiffusion Tout transférer

La page *Tout transférer* active et affiche la configuration des ports et/ou LAG qui doivent recevoir des flux de multidiffusion en provenance d'un VLAN spécifique. Cette fonction exige que vous activiez le filtrage multidiffusion par ponts sur la page *Propriétés*. Si cette fonction est désactivée, tout le trafic de multidiffusion est envoyé aux ports du commutateur.

Vous pouvez configurer (manuellement) un port en mode Tout transférer de manière statique si les périphériques qui se connectent à ce port ne prennent pas en charge IGMP et/ou MLD.

Les messages IGMP ou MLD ne sont pas transférés aux ports définis en mode *Tout transférer*.

REMARQUE Cette configuration affecte uniquement les ports membres du VLAN sélectionné.

Pour définir la multidiffusion Tout transférer :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Tout transférer**. La page *Tout transférer* s'ouvre.

ÉTAPE 2 Définissez les éléments suivants :

- **ID VLAN est égal à** : ID du VLAN où les ports/LAG doivent être affichés.
- **Type d'interface est égal à** : choisissez d'afficher les ports ou les LAG.

ÉTAPE 3 Cliquez sur **OK**. L'état de tous les ports/LAG est affiché.

ÉTAPE 4 Sélectionnez le port/LAG à définir en mode Tout transférer à l'aide des méthodes suivantes :

- **Statique** : le port reçoit tous les flux de multidiffusion.
- **Interdit** : les ports ne peuvent pas recevoir de flux de multidiffusion, même si le traçage IGMP/MLD Snooping a désigné le port concerné comme devant rejoindre un groupe de multidiffusion.
- **Aucun** : le port n'est actuellement pas un port Tout transférer.

ÉTAPE 5 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Définition des paramètres de multidiffusion non enregistrée

En général, les trames de multidiffusion sont transférées vers tous les ports du VLAN. Lorsque vous activez le traçage IGMP/MLD Snooping, le commutateur apprend l'existence des groupes de multidiffusion et surveille les ports membres de tel ou tel groupe. Les groupes de multidiffusion peuvent aussi être configurés de façon statique. Qu'ils aient été appris dynamiquement ou configurés de façon statique, ces groupes de multidiffusion sont considérés comme enregistrés.

Le commutateur transfère les trames de multidiffusion (depuis un groupe de multidiffusion enregistré) uniquement vers les ports enregistrés dans ce groupe de multidiffusion.

La page *Multidiffusion non enregistrée* permet de gérer les trames de multidiffusion appartenant à des groupes inconnus du commutateur (groupes de multidiffusion non enregistrés). En général, les trames de multidiffusion non enregistrées sont transférées vers tous les ports du VLAN.

Vous pouvez sélectionner un port pour qu'il reçoive les flux de multidiffusion non enregistrée ou pour qu'il les filtre. Cette configuration est valide pour tous les VLAN dont il est (ou sera) membre.

Cette fonction garantit que le client reçoit uniquement les groupes de multidiffusion demandés et non les autres groupes éventuellement transmis sur le réseau.

Pour définir des paramètres de multidiffusion non enregistrée :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Multidiffusion non enregistrée**. La page *Multidiffusion non enregistrée* s'ouvre.

ÉTAPE 2 Définissez les éléments suivants :

- **Type d'interface est égal à** : choisissez d'afficher tous les ports ou tous les LAG.
- **Port/LAG** : affiche l'ID de port ou de LAG.
- **Multidiffusion non enregistrée** : affiche l'état de transfert de l'interface sélectionnée. Ce champ peut prendre les valeurs suivantes :
  - *Transfert* : active le transfert des trames de multidiffusion non enregistrée vers l'interface sélectionnée.
  - *Filtrage* : active le filtrage (rejet) des trames de multidiffusion non enregistrée sur l'interface sélectionnée.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres sont enregistrés et le fichier de Configuration d'exécution est mis à jour.

16

Configuration des informations IP

Les adresses d'interface IP peuvent être configurées manuellement par l'utilisateur ou automatiquement via un serveur DHCP. Cette section fournit des informations sur la définition des adressesIP du commutateur, soit manuellement soit en faisant du commutateur un client DHCP.

Cette rubrique aborde les points suivants :

- **Interfaces de gestion et IP**
- **Configuration d'ARP**
- **DNS (Domain Name System, système de noms de domaine)**

Interfaces de gestion et IP

Adressage IP Layer 2

Le commutateur possède une adresse IP unique sur le VLAN de gestion. Cette adresse IP et la passerelle par défaut peuvent être configurées manuellement ou par DHCP. Vous pouvez configurer l'adresseIP statique et la passerelle par défaut dans la page *Interface IPv4*. Le commutateur utilise la passerelle par défaut (si elle existe) pour communiquer avec les périphériques qui ne se trouvent pas sur le même sous-réseau IP. Par défaut, VLAN1 est le VLAN de gestion mais vous pouvez modifier ce paramètre. Le commutateur n'est accessible à l'adresse IP configurée que via son VLAN de gestion.

Le paramètre d'usine par défaut de la configuration de l'adresse IP est *DHCP*. Cela signifie que le commutateur joue le rôle de client DHCP et envoie une demande DHCP lors de l'amorçage.

Si le commutateur reçoit une réponse DHCP du serveur DHCP (contenant une adresse IP), il envoie des paquets ARP (Address Resolution Protocol, protocole de résolution d'adresse) pour vérifier que cette adresse IP est unique. Si la réponse ARP indique que l'adresse IP est déjà utilisée, le commutateur envoie le message DHCP DECLINE (Refus DHCP) au serveur DHCP répondu. Il envoie ensuite un nouveau paquet DHCPDISCOVER (Détection DHCP) pour relancer le processus.

Si le commutateur n'a reçu aucune réponse DHCP au bout de 60 secondes, il continue à lancer des requêtes DHCPDISCOVER et utilise l'adresse IP 192.168.1.254/24.

Des collisions d'adresse IP se produisent lorsqu'une même adresse IP est utilisée par plusieurs périphériques sur un même sous-réseau IP. Les collisions d'adresse nécessitent une action de la part de l'administrateur sur le serveur DHCP et/ou sur le périphérique en conflit avec le commutateur.

Lorsqu'un VLAN est configuré pour utiliser des adresses IP dynamiques, le commutateur envoie des demandes DHCP jusqu'à ce qu'un serveur DHCP lui attribue une adresse IP. Vous pouvez configurer le VLAN de gestion avec une adresseIP statique ou dynamique.

Les règles d'affectation d'adresse IP au commutateur sont les suivantes :

- Si le commutateur n'est pas configuré avec une adresse IP statique, il émet des requêtes DHCP jusqu'à ce qu'il reçoive une réponse d'un serveur DHCP.
- Si l'adresse IP du commutateur change, ce dernier envoie des paquets ARP gratuits au VLAN correspondant pour rechercher les éventuelles collisions d'adresse IP. Cette règle s'applique également lorsque le commutateur revient à l'adresse IP par défaut.
- La DEL d'état du système s'allume en vert lorsque le serveur DHCP envoie une nouvelle adresse IP unique. Si une adresse IP statique a été définie, la DEL d'état du système s'allume également en vert. Cette DEL clignote pendant que le commutateur acquiert son adresse IP et qu'il utilise l'adresse IP par défaut définie en usine (192.168.1.254).
- Les mêmes règles s'appliquent lorsqu'un client doit renouveler son bail avant la date d'expiration, via un message DHCP REQUEST (Demande DHCP).
- Avec les paramètres d'usine, si aucune adresse IP n'est disponible (qu'elle soit définie de manière statique ou acquise via DHCP), le système utilise l'adresse IP par défaut. Lorsque d'autres adresses IP deviennent disponibles, elles sont automatiquement utilisées. L'adresse IP par défaut se trouve toujours sur le VLAN de gestion.

Définition d'une interface IPv4

Pour que vous puissiez gérer le commutateur à l'aide de l'utilitaire Web de configuration du commutateur, vous devez définir et connaître l'adresse de gestion IPv4 du commutateur. L'adresse IP du commutateur peut être configurée manuellement ou obtenue automatiquement depuis un serveur DHCP.

Pour configurer une adresse IPv4 pour le commutateur :

ÉTAPE 1 Cliquez sur **Administration > Interface de gestion > Interface IPv4**. La page *Interface IPv4* s'ouvre.

ÉTAPE 2 Saisissez les valeurs appropriées dans les champs suivants :

- **VLAN de gestion :** sélectionnez le VLAN de gestion utilisé pour accéder au commutateur via telnet ou l'interface utilisateur graphique (GUI) Web. VLAN1 est le VLAN de gestion par défaut.
- **Type d'adresse IP** : sélectionnez l'une des options suivantes :
  - *Dynamique :* détectez l'adresseIP via DHCP sur le VLAN de gestion.
  - *Statique* : définissez manuellement une adresse IP statique.

  REMARQUE L'option 12 DHCP (option Nom d'hôte) est prise en charge lorsque le périphérique est un client DHCP. Si l'option 12 DHCP est reçue d'un serveur DHCP, elle est enregistrée en tant que nom d'hôte du serveur. L'option 12 DHCP ne sera pas demandée par le commutateur. Le serveur DHCP doit être configuré pour envoyer l'option 12 indépendamment de ce qui est demandé afin de pouvoir utiliser cette fonctionnalité.

Si vous utilisez une adresse IP statique, configurez les champs suivants.

- **Adresse IP :** saisissez l'adresse IP et configurez l'un des champs suivants :
  - **Masque réseau** : sélectionnez et saisissez le masque d'adresse IP.
  - **Longueur du préfixe :** sélectionnez et saisissez la longueur du préfixe d'adresse IPv4.
- **Passerelle par défaut administrative** : sélectionnez **Défini par l'utilisateur** et saisissez l'adresse IP de la passerelle par défaut. Vous pouvez aussi sélectionner **Aucun** pour supprimer de l'interface l'adresse IP de passerelle par défaut sélectionnée.
- **Passerelle opérationnelle par défaut :** indique l'état de la passerelle par défaut actuelle.

REMARQUE Si aucune passerelle par défaut n'est configurée pour le commutateur, ce dernier ne peut pas communiquer avec les périphériques qui ne font pas partie du même sous-réseau IP.

Si le système récupère une adresse IP dynamique auprès du serveur DHCP, parmi les champs suivants, sélectionnez ceux que vous souhaitez activer :

- **Renouveler l'adresse IP maintenant :** l'adresse IP dynamique du commutateur peut être renouvelée à tout moment après son affectation par un serveur DHCP. Notez que, selon la configuration de votre serveur DHCP, le commutateur peut recevoir une nouvelle adresse IP après le renouvellement, ce qui nécessite le paramétrage de l'utilitaire Web de configuration du commutateur à la nouvelle adresseIP.
- **Configuration automatique via DHCP :** affiche l'état de la fonction Configuration automatique. Vous pouvez configurer cette fonction à l'aide de l'option *Administration > Gestion de fichiers > Configuration automatique DHCP*.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres d'interface IPv4 sont modifiés et écrits dans le fichier de Configuration d'exécution.

Gestion d'IPv6

Internet Protocol version6 (IPv6) est un protocole de couche réseau utilisé dans les communications entre réseaux à commutation de paquets. IPv6 a été conçu pour remplacer IPv4, le protocole Internet le plus souvent déployé.

IPv6 apporte davantage de souplesse dans l'affectation des adresses IP car la taille des adresses passe de 32 à 128 bits. Les adresses IPv6 sont constituées de huit groupes de quatre chiffres hexadécimaux, par exemple FE80:0000:0000:0000:0000:9C00:876A:130B. La forme abrégée, dans laquelle un groupe de zéros peut être ignoré et remplacé par « :: », est également admise. Exemple : ::-FE80::9C00:876A:130B.

Les nœuds IPv6 nécessitent un mécanisme de mappage intermédiaire pour communiquer avec d'autres nœuds IPv6 sur un réseau uniquement IPv4. Ce mécanisme, appelé tunnel, permet à des hôtes uniquement IPv6 de contacter des services IPv4, ainsi qu'à des hôtes et réseaux IPv6 isolés de contacter un nœud IPv6 sur une infrastructure IPv4.

La fonction de Tunneling utilise le mécanisme ISATAP. Ce protocole considère le réseau IPv4 comme une liaison locale IPv6 virtuelle, avec des mappages entre chaque adresse IPv4 et une adresse IPv6 de liaison locale.

Le commutateur détecte les trames IPv6 d'après le type IPv6Ethertype.

Définition de la configuration globale IPv6

La page *Configuration globale IPv6* définit la fréquence des messages d'erreur ICMPIPv6 générés par le commutateur.

Pour définir des paramètres IPv6 globaux :

ÉTAPE 1 Cliquez sur **Administration > Interface de gestion > Configuration globale IPv6.**

La page *Configuration globale IPv6* s'ouvre.

ÉTAPE 2 Saisissez les valeurs appropriées dans les champs suivants :

- **Intervalle de limites de débit ICMPv6** : saisissez la fréquence à laquelle les messages d'erreur ICMP sont générés.
- **Taille des cases de limite de débit ICMPv6** : saisissez le nombre maximal de messages d'erreur ICMP que le commutateur peut envoyer dans chaque intervalle.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres globaux IPv6 sont écrits dans le fichier de Configuration d'exécution.

Définition d'une interface IPv6

Vous pouvez configurer l'interface IPv6 sur une interface de port, de LAG, de VLAN ou de tunnel ISATAP. Le commutateur prend en charge une seule interface IPv6 en tant que périphérique d'extrémitéIPv6.

Une interface de tunnel est configurée avec une adresse IPv6 sur la base des paramètres définis sur la page *Tunnel IPv6*.

Pour définir une interface IPv6 :

ÉTAPE 1 Cliquez sur **Administration** > **Interface de gestion** > **Interface IPv6.**

La page *Interface IPv6* s'ouvre.

Cette page affiche les interfaces IPv6 déjà configurées.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter une nouvelle interface sur laquelle IPv6 est activé.

ÉTAPE 3 La page *Ajouter une interface IPv6* s'ouvre.

ÉTAPE 4 Saisissez les valeurs appropriées.

- **Interface IPv6** : sélectionnez un port, un LAG, un VLAN ou un tunnel ISATAP spécifique.
- **Nombre de tentatives DAD** : saisissez le nombre de messages de sollicitation des voisins consécutifs à envoyer lors du processus DAD (Duplicate Address Detection, détection des adresses en double) sur les adresses IPv6 Unicast de l'interface. DAD vérifie l'unicité d'une nouvelle adresse IPv6 Unicast avant de l'attribuer. Les nouvelles adresses restent à l'état provisoire pendant la vérification DAD. Saisissez **0** dans ce champ pour désactiver le traitement de détection des adresses en double sur l'interface indiquée. Saisissez **1** dans ce champ pour indiquer une transmission unique, sans transmission de suivi.
- **Configuration automatique d'adresses IPv6** : active la configuration automatique des adresses. Si vous activez cette option, le commutateur prend en charge la configuration automatique des adresses IPv6 sans conservation d'état pour les adresses IP locales et globales de site, à partir de l'annonce de routeur IPv6 reçue sur l'interface. Le commutateur ne prend pas en charge la configuration automatique des adresses avec conservation d'état. Si la configuration automatique n'est pas activée, définissez une adresse IPv6 à la page *Adresses IPv6*.
- **Envoyer des messages ICMPv6** : active la génération de messages concernant les destinations injoignables.

ÉTAPE 5 Cliquez sur **Appliquer** pour activer le traitement IPv6 sur l'interface sélectionnée. Pour les interfaces IPv6 standard, les adresses suivantes sont configurées automatiquement :

- Adresse de liaison locale, à l'aide de l'ID d'interface au format EUI-64, sur la base de l'adresse MAC d'un périphérique
- Toutes les adresses de multidiffusion de liaison locale des nœuds (FF02::1)
- Adresse de multidiffusion de nœud sollicité (au format FF02::1:FFXX:XXXX)

ÉTAPE 6 Cliquez sur **Table des adresses IPv6** pour affecter manuellement des adresses IPv6 à l'interface, si nécessaire. Cette page est décrite à la section **Définition d'adresses IPv6**.

Définition d'adresses IPv6

Pour affecter une adresse IPv6 à une interface IPv6 :

ÉTAPE 1 Cliquez sur **Administration** > **Interface de gestion** > **Adresses IPv6.**

La page *Adresses IPv6* s'ouvre.

ÉTAPE 2 Pour filtrer la table, sélectionnez un nom d'interface et cliquez sur **OK**. L'interface s'affiche dans la table des adresses IPv6.

ÉTAPE 3 Cliquez sur **Ajouter**. La page *Ajouter une adresse IPv6* s'ouvre.

ÉTAPE 4 Saisissez les valeurs des champs.

- **Interface IPv6 :** affiche l'interface sur laquelle l'adresse IPv6 doit être définie.
- **Type d'adresse IPv6** : sélectionnez Liaison locale ou Global comme type d'adresse IPv6 à ajouter.
  - *Liaison locale :* l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPV6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Adresse IPv6** : le commutateur prend en charge une seule interface IPv6. Outre les adresses de liaison locale et de multidiffusion par défaut, le périphérique ajoute aussi automatiquement des adresses globales à l'interface sur la base des annonces de routeur qu'il reçoit. Le périphérique prend en charge un maximum de 128 adresses sur l'interface. Chaque adresse doit correspondre à une adresse IPv6 valide, spécifiée au format hexadécimal en utilisant des valeurs de 16 bits séparées par le caractère deux-points.

  REMARQUE Il est impossible de configurer des adresses IPv6 directement sur une interface de tunnel ISATAP.
- **Longueur du préfixe** : la longueur du préfixe IPv6 global est une valeur comprise entre 0 et 128 qui indique le nombre de bits contigus les plus significatifs de l'adresse dont se compose le préfixe (la partie réseau de l'adresse).

- **EUI-64** : sélectionnez cette option pour employer le paramètre EUI-64 afin d'identifier la portion de l'adresse IPv6 globale correspondant à l'ID d'interface en utilisant le format EUI-64 sur la base de l'adresse MAC d'un périphérique.

ÉTAPE 5 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Définition d'une liste de routeurs IPv6 par défaut

La page *Liste des routeurs par défaut IPv6* vous permet de configurer et d'afficher les adresses de routeur IPv6 par défaut. Cette liste contient les routeurs susceptibles de devenir le routeur par défaut du commutateur pour le trafic non local (elle peut être vide). Le commutateur sélectionne un routeur au hasard dans la liste. Le commutateur prend en charge un seul routeur IPv6 statique par défaut. Les routeurs dynamiques par défaut sont des routeurs qui ont envoyé des annonces de routeur à l'interface IPv6 du commutateur.

Lorsque vous ajoutez ou supprimez des adresses IP, les événements suivants se produisent :

- Lorsque vous supprimez une interfaceIP, toutes les adresses IP de routeur par défaut sont supprimées.
- Il est impossible de supprimer des adresses IP dynamiques.
- Un message d'alerte s'affiche lorsque vous tentez d'insérer plus d'une adresse définie par l'utilisateur.
- Un message d'alerte s'affiche lorsque vous tentez d'insérer une adresse d'un type autre qu'une liaison locale « fe80: ».

Pour définir un routeur par défaut :

ÉTAPE 1 Cliquez sur **Administration** > **Interface de gestion** > **Liste des routeurs par défaut IPv6**.

La page *Liste des routeurs par défaut IPv6* s'ouvre.

Cette page affiche les champs suivants pour chaque routeur par défaut :

- **Adresse IPv6 du routeur par défaut** : adresse IP de liaison locale du routeur par défaut.
- **Interface** : interface IPv6 sortante où réside le routeur par défaut.

- **Type** : configuration du routeur par défaut qui inclut les options suivantes :
  - *Statique* : le routeur par défaut a été ajouté manuellement à cette table à l'aide du bouton **Ajouter**.
  - *Dynamique* : le routeur par défaut a été configuré de manière dynamique.

  État : les options d'état du routeur par défaut sont les suivantes :
  - *Incomplet* : résolution d'adresse en cours. Le routeur par défaut n'a pas encore répondu.
  - *Accessible* : une confirmation positive a été reçue dans le *Délai d'accessibilité*.
  - *Périmé* : un voisin réseau précédemment connu n'est plus accessible et aucune action ne va être entreprise pour vérifier son accessibilité tant qu'il n'est pas nécessaire de lui envoyer du trafic.
  - *Retard* : un voisin réseau précédemment connu est inaccessible. L'appareil reste à l'état Retard pour un *Délai de retard* prédéfini. Si aucune confirmation n'est reçue, l'état passe à Sonde.
  - *Sonde* : le voisin réseau est inaccessible et des sondes UNS (Unicast Neighbor Solicitation, sollicitation de voisinage Unicast) sont envoyées pour vérifier son état.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un routeur par défaut statique. La page *Ajouter un routeur par défaut* s'ouvre.

La fenêtre affiche l'interface de liaison locale. Il peut s'agir d'un port, d'un LAG, d'un VLAN ou d'un tunnel.

ÉTAPE 3 Saisissez l'adresseIP du routeur par défaut statique dans le champ **Adresse IPv6 du routeur par défaut**.

ÉTAPE 4 Cliquez sur **Appliquer**. Le routeur par défaut est écrit dans le fichier de Configuration d'exécution.

Configuration de tunnelsIPv6

Le protocole ISATAP (Intra-Site Automatic Tunnel Addressing Protocol, protocole d'adressage automatique de tunnel intrasite) permet d'encapsuler des paquets IPv6 dans des paquets IPv4 pour les transmettre sur des réseaux IPv4. Pour configurer un tunnel, procédez comme suit :

- Activez et configurez manuellement un tunnel ISATAP.
- Définissez manuellement une interface IPv6 pour le tunnel ISATAP.

Une fois ces opérations effectuées, le commutateur configure automatiquement l'adresse IPv6 de liaison locale sur l'interface IPv6.

Notez les éléments suivants pour la définition de tunnels ISATAP :

- Une adresse IPv6 de liaison locale est affectée à l'interface ISATAP. L'adresse IP initiale est affectée à l'interface, qui est alors activée.
- Si une interface ISATAP est active, l'adresse IPv4 du routeur ISATAP est résolue via DNS à l'aide d'un mappage ISATAP-à-IPv4. Si l'enregistrement DNS ISATAP n'est pas résolu, le mappage nom d'hôte-à-adresse ISATAP est recherché dans la table de mappage des hôtes.
- S'il est impossible de résoudre l'adresse IPv4 du routeur ISATAP à l'aide du processus DNS, l'interface IP ISATAP reste active. Le système ne comportera un routeur par défaut pour le trafic ISATAP qu'après résolution du processusDNS.

Pour configurer un tunnel IPv6 :

ÉTAPE 1 Cliquez sur **Administration > Interface de gestion > Tunnel IPv6**.

La page *Tunnel IPv6* s'ouvre.

ÉTAPE 2 Saisissez les valeurs appropriées dans les champs suivants :

- **Numéro du tunnel** : affiche le numéro de domaine du routeur de tunnel automatique.
- **Type du tunnel** : toujours affiché comme ISATAP.
- **Adresse IPv4 source** : désactivez le tunnel ISATAP ou activez-le sur une interface IPv4. L'adresse IPv4 de l'interface IPv4 sélectionnée sera utilisée pour constituer une partie de l'adresse IPv6 sur l'interface de tunnel ISATAP. L'adresse IPv6 comporte un préfixe réseau de 64 bits, constitué de fe80::, suivi de la concaténation de 0000:5EFE et de l'adresse IPv4.

- *Auto* : sélectionne automatiquement l'adresse IPv4 la plus basse parmi toutes les interfaces IPv4 configurées.
- *Aucun* : désactivez le tunnel ISATAP.
- *Manuel* : configurez manuellement une adresse IPv4. L'adresse IPv4 configurée doit être l'une des adresses IPv4 des interfaces IPv4 du commutateur.

- **Nom de domaine du routeur de tunnel** : chaîne globale qui représente un nom de domaine de routeur de tunnel automatique spécifique. Il peut s'agir du nom par défaut (ISATAP) ou d'un nom défini par l'utilisateur.
- **Intervalle de requête** : nombre de secondes (de 10 à 3 600) entre deux requêtes DNS pour ce tunnel (avant que l'adresse IP du routeur ISATAP soit connue). Il peut s'agir de l'intervalle par défaut (10 secondes) ou d'une valeur d'intervalle définie par l'utilisateur.
- **Intervalle de sollicitation ISATAP** : nombre de secondes (de 10 à 3 600) entre deux messages de sollicitation de routeur ISATAP, si aucun routeur ISATAP n'est actif. Il peut s'agir de l'intervalle par défaut (10 secondes) ou d'une valeur d'intervalle définie par l'utilisateur.
- **Robustesse ISATAP** : permet de calculer l'intervalle des requêtes DNS ou de sollicitation de routeur. Plus la valeur est élevée, plus les requêtes sont fréquentes. La valeur par défaut est 3. La plage valide se situe entre 1 et 20.

  REMARQUE Le tunnel ISATAP ne sera pas opérationnel si l'interface IPv4 sous-jacente n'est pas active.

ÉTAPE 3 Cliquez sur **Appliquer**. Le tunnel est écrit dans le fichier de Configuration d'exécution.

Définition des informations sur les voisins IPv6

La page *Voisins IPv6* vous permet de configurer et d'afficher la liste des voisins IPv6 sur l'interface IPv6. La table Voisins IPv6, également appelée Cache de détection du voisinage IPv6, affiche les adresses MAC des voisins IPv6 qui font partie du même sous-réseau IPv6 que le commutateur. Cela vous permet de

vérifier l'accessibilité du voisin concerné. C'est l'équivalent IPv6 de la table ARPIPv4. Lorsque le commutateur a besoin de communiquer avec ses voisins, il utilise la table de voisinage IPv6 pour déterminer les adresses MAC à partir de leurs adresses IPv6.

Cette page affiche les voisins détectés automatiquement ou configurés manuellement. Chaque entrée indique l'interface à laquelle le voisin est connecté, les adresses IPv6 et MAC de ce voisin, son type de configuration (statique ou dynamique) et l'état du voisin.

Pour définir des voisins IPv6 :

ÉTAPE 1 Cliquez sur **Administration > Interface de gestion > Voisins IPv6.**

La page *Voisins IPv6* s'ouvre.

ÉTAPE 2 Vous pouvez sélectionner une option **Effacer la table** afin d'effacer certaines adresses IPv6 (ou toutes) de la table de voisinage IPv6.

- **Statique uniquement** : supprime les entrées d'adresse IPv6 statiques.
- **Dynamique uniquement** : supprime les entrées d'adresse IPv6 dynamiques.
- **Dynamique et statique** : supprime les entrées d'adresse IPv6 statiques et dynamiques.

Les champs suivants sont affichés pour les interfaces de voisinage :

- **Interface** : type d'interface de voisinage IPv6.
- **Adresse IPv6** : adresse IPv6 d'un voisin.
- **Adresse MAC** : adresse MAC mappée sur l'adresse IPv6 spécifiée.
- **Type :** type de saisie des informations de cache de découverte des voisins (statique ou dynamique).
- **État** : indique l'état du voisin IPv6. Les valeurs disponibles sont les suivantes :
  - *Incomplet* : résolution d'adresse en cours. Le voisin n'a pas encore répondu.
  - *Atteignable* : le voisin est reconnu comme étant accessible.
  - *Périmé* : un voisin précédemment connu est inaccessible. Aucune action n'est entreprise pour vérifier son accessibilité tant qu'il n'est pas nécessaire de lui envoyer du trafic.

- *Retard* : un voisin précédemment connu est inaccessible. L'interface reste à l'état Retard pour la durée prédéfinie indiquée par Délai de retard. Si aucune confirmation d'accessibilité n'est reçue, l'état passe à Sonde.
- *Sonde* : le voisin n'est plus reconnu comme inaccessible et des sondes UNS (Unicast Neighbor Solicitation, sollicitation de voisinage Unicast) sont envoyées pour vérifier son accessibilité.

ÉTAPE 3 Pour ajouter un voisin à la table, cliquez sur **Ajouter**. La page *Ajouter des voisins IPv6* s'ouvre.

ÉTAPE 4 Saisissez les valeurs appropriées dans les champs suivants :

- **Interface** : interface de voisinage IPv6 à ajouter.
- **Adresse IPv6** : saisissez l'adresse réseau IPv6 affectée à l'interface. Cette adresse doit être une adresse IPv6 valide.
- **Adresse MAC** : saisissez l'adresse MAC mappée sur l'adresse IPv6 spécifiée.

ÉTAPE 5 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

ÉTAPE 6 Pour changer le type d'une adresse IP de Dynamique en Statique, utilisez la page *Modifier les voisins IPv6*.

Affichage des tables de routage IPv6

La page *Routes IPv6* affiche la *Table de routage IPv6*. La table contient une seule route par défaut (adresseIPv6:0), qui utilise le routeur par défaut sélectionné dans la liste des routeurs par défaut IPv6 afin d'envoyer des paquets aux périphériques de destination qui ne font pas partie du même sous-réseau IPv6 que le commutateur. Outre la route par défaut, la table contient aussi des routes dynamiques, qui sont des routes de redirection ICMP reçues des routeurs IPv6 via des messages de redirection ICMP. Cela peut se produire lorsque le routeur par défaut que le commutateur utilise n'est pas celui défini pour le trafic des sous-réseaux IPv6 avec lesquels le commutateur veut communiquer.

Pour visualiser les entrées de routage IPv6 :

ÉTAPE 1 Cliquez sur **Administration > Interface de gestion > Routes IPv6**.

La page *Routes IPv6* s'ouvre.

Cette page affiche les champs suivants :

- **Adresse IPv6** : adresse du sous-réseau IPv6.
- **Longueur du préfixe** : longueur du préfixe de routage IP pour l'adresse de sous-réseau IPv6 de destination. Il est précédé d'une barre oblique.
- **Interface** : interface utilisée pour transférer le paquet.
- **Saut suivant** : adresse vers laquelle le paquet est transféré. En général, il s'agit de l'adresse d'un routeur du voisinage. Ce doit être une adresse de liaison locale.
- **Métrique** : valeur utilisée pour comparer cette route à d'autres routes vers la même destination dans la table des routeurs IPv6. Toutes les routes par défaut ont la même valeur.
- **Durée de vie** : laps de temps durant lequel le paquet peut être envoyé et renvoyé, avant sa suppression.
- **Type de route** : mode de rattachement de la destination et méthode utilisée pour obtenir l'entrée. Les valeurs sont les suivantes :
  - *Local :* un réseau connecté directement dont le préfixe est dérivé de l'adresse IPv6 d'un commutateur configuré manuellement.
  - *Dynamique* : la destination est une adresse de sous-réseau IPv6 attachée de façon indirecte (à distance). L'entrée a été obtenue de manière dynamique via le protocoleND ou ICMP.
  - *Statique :* l'entrée a été configurée manuellement par un utilisateur.

Configuration d'ARP

Le commutateur gère une tableARP (Address Resolution Protocol, protocole de résolution d'adresse) pour tous les périphériques connus résidant sur ses sous-réseaux IP à connexion directe. Un sous-réseau IP à connexion directe désigne un sous-réseau auquel une interface IPv4 du commutateur est connectée. Lorsque le

commutateur doit envoyer/router un paquet vers un périphérique local, il effectue une recherche dans la table ARP pour obtenir l'adresse MAC du périphérique en question. La table ARP contient à la fois des adresses statiques et des adresses dynamiques. Les adresses statiques sont configurées manuellement et n'ont pas de limite de validité. Le commutateur crée des adresses dynamiques à partir des paquets ARP qu'il reçoit. Les adresses dynamiques ont une durée de vie limitée, que vous configurez.

REMARQUE Les informations de mappage d'adresse IP/MAC de la table ARP servent à transférer le trafic en provenance du commutateur.

Pour définir les tables ARP :

ÉTAPE 1 Cliquez sur **Configuration IP > ARP.** La page *Table ARP* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **Délai d'expiration des entrées ARP** : saisissez la durée en secondes pendant laquelle les adresses dynamiques peuvent rester dans la table ARP. Les adresses dynamiques ne sont valides dans la table que pour la durée définie par Délai d'expiration des entrées ARP. Lorsqu'une adresse dynamique arrive à expiration, elle est supprimée de la table et doit être réapprise pour figurer à nouveau dans cette table.
- **Effacer les entrées de la table ARP** : sélectionnez le type des entrées ARP à effacer du système.
  - *Tout* : supprime immédiatement toutes les adresses statiques et dynamiques.
  - *Dynamique* : supprime immédiatement toutes les adresses dynamiques.
  - *Statique* : supprime immédiatement toutes les adresses statiques.
  - *Délai d'expiration normal* : supprime les adresses dynamiques en fonction de la durée de vie configurée pour les entrées ARP.

ÉTAPE 3 Cliquez sur **Appliquer.** Les paramètres globaux ARP sont écrits dans le fichier de Configuration d'exécution.

La table ARP contient les champs suivants :

- **Interface** : interface IPv4 du sous-réseau IP à connexion directe où réside le périphérique IP.
- **Adresse IP** : adresse IP du périphérique IP.
- **Adresse MAC** : adresse MAC du périphérique IP.

- **État** : indique si l'entrée a été saisie manuellement ou apprise de manière dynamique.

ÉTAPE 4 Cliquez sur **Ajouter**. La page *Ajouter une entrée ARP* s'ouvre.

ÉTAPE 5 Configurez les paramètres suivants :

- **Version IP** : format d'adresse IP pris en charge par l'hôte. Seul IPv4 est pris en charge.
- **Interface** : interface IPv4 du commutateur.

Il n'existe qu'un seul sous-réseau IP à connexion directe, toujours situé sur le VLAN de gestion. Toutes les adresses statiques et dynamiques de la table ARP résident sur le VLAN de gestion.

- **Adresse IP** : saisissez l'adresse IP du périphérique local.
- **Adresse MAC** : saisissez l'adresse MAC du périphérique local.

ÉTAPE 6 Cliquez sur **Appliquer**. L'entrée ARP est écrite dans le fichier de Configuration d'exécution.

DNS (Domain Name System, système de noms de domaine)

Le DNS (Domain Name System, système de noms de domaine) convertit les noms de domaine définis par l'utilisateur en adresses IP en vue de localiser et de gérer ces objets.

En tant que client DNS, le commutateur résout les noms de domaine en adresses IP via un ou plusieurs serveurs DNS configurés.

Définition de serveurs DNS

Utilisez la page *Serveurs DNS* pour activer la fonction DNS, configurer les serveurs DNS et définir le domaine par défaut utilisé par le commutateur.

ÉTAPE 1 Cliquez sur **Configuration IP** > **Système de noms de domaine** > **Serveurs DNS**. La page *Serveurs DNS* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **DNS** : sélectionnez cette option pour désigner le commutateur comme client DNS et lui permettre de résoudre les noms DNS en adresses IP via un ou plusieurs serveurs DNS configurés.
- **Nom de domaine par défaut** : saisissez le nom de domaine DNS par défaut (de 1 à 158 caractères). Le commutateur ajoute ces informations à tous les noms de domaine incomplets, afin de les convertir en noms de domaine complets (FQDN).
- **Type** : affiche les options de type de domaine par défaut :
  - *DHCP* : le nom de domaine par défaut est attribué dynamiquement par le serveur DHCP.
  - *Statique* : le nom de domaine par défaut est défini par l'utilisateur.
  - S/O : aucun nom de domaine par défaut n'est utilisé.

Table des serveurs DNS :

- **Serveur DNS** : adresses IP des serveurs DNS. Vous pouvez définir jusqu'à huit serveurs DNS.
- **État du serveur** : le serveur DNS peut être actif ou inactif. Il ne peut exister qu'un seul serveur actif. Chaque serveur statique porte un ordre de priorité, la valeur la plus faible indiquant la priorité la plus élevée. Lors du premier envoi de la demande, le serveur statique avec le numéro de priorité le plus faible est utilisé. Après deux tentatives, si ce serveur ne répond pas, le système sélectionne le serveur qui vient ensuite dans l'ordre de priorité. Si aucun des serveurs statiques ne répond, le système sélectionne le premier serveur dynamique de la table (qui est triée dans l'ordre des adresses, de la plus basse à la plus élevée).

ÉTAPE 3 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

ÉTAPE 4 Pour ajouter un serveur DNS, cliquez sur **Ajouter**. La page *Ajouter un serveur DNS* s'ouvre.

ÉTAPE 5 Saisissez les paramètres.

- **Version IP** : sélectionnez Version 6 pour IPv6 ou Version 4 pour IPv4.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale :* l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPV6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, spécifiez si la réception s'effectue via VLAN2 ou ISATAP.
- **Adresse IP du serveur DNS** : saisissez l'adresse IP du serveur DNS.
- **Activer le serveur DNS** : sélectionnez cette option pour activer le nouveau serveur DNS.

ÉTAPE 6 Cliquez sur **Appliquer**. Le serveur DNS est écrit dans le fichier de Configuration d'exécution.

Mappage d'hôtes DNS

Le commutateur enregistre dans un cache DNS local les noms de domaine (acquis depuis les serveurs DNS) qui apparaissent fréquemment dans les requêtes. Le cache peut stocker jusqu'à 64 entrées statiques, 64 entrées dynamiques et une entrée pour chaque adresse IP configurée sur le commutateur par DHCP. La résolution des noms commence toujours par la vérification des entrées statiques, se poursuit par la vérification des entrées dynamiques et se termine par l'envoi de demandes au serveur DNS externe.

Vous pouvez associer plusieurs adresses IP à chaque DNS pour chaque nom d'hôte.

Pour ajouter un nom de domaine et son adresse IP :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Système de noms de domaine** > **Mappage d'hôtes**. La page *Mappage d'hôtes* s'ouvre.

Cette page affiche les champs suivants :

- **Nom d'hôte** : nom de domaine défini par l'utilisateur, comportant 158 caractères maximum.
- **Adresse IP** : adresse IP correspondant au nom d'hôte.

ÉTAPE 2 Pour ajouter un mappage d'hôtes, cliquez sur **Ajouter**. La page *Ajouter un mappage d'hôtes* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **Version IP** : sélectionnez Version 6 pour IPv6 ou Version 4 pour IPv4.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale :* l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPV6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, spécifiez si la réception s'effectue via VLAN2 ou ISATAP.
- **Nom d'hôte** : saisissez un nom de domaine, comportant 158 caractères maximum.
- **Adresse IP** : saisissez une adresse IPv4 ou jusqu'à quatre adresses d'hôte IPv6. Les adresses 2 à 4 sont des adresses de secours.

ÉTAPE 4 Cliquez sur **Appliquer**. L'hôte DNS est écrit dans le fichier de Configuration d'exécution.

17

Configuration de la sécurité

Cette section décrit le contrôle d'accès et la sécurité du commutateur. Le système gère différents types de sécurité.

La liste de rubriques suivante décrit les différents types de fonctions de sécurité présentées dans cette section. Certaines fonctionnalités sont utilisées pour plusieurs types de sécurité ou de contrôle et s'affichent donc à plusieurs reprises dans la liste des rubriques présentée ci-dessous.

L'autorisation d'administrer le commutateur est décrite dans les sections suivantes :

- **Définition d'utilisateurs**
- **Configuration de RADIUS**
- **Configuration de l'Authentification de l'accès de gestion**
- **Définition d'une méthode d'accès de gestion**
- **Configuration des services TCP/UDP**

La protection contre les attaques visant le CPU du commutateur est décrite dans les sections suivantes :

- **Configuration des services TCP/UDP**
- **Définition du contrôle des tempêtes**

Le contrôle d'accès au réseau des utilisateurs finaux par l'intermédiaire du commutateur est décrit dans les sections suivantes :

- **Configuration de l'Authentification de l'accès de gestion**
- **Définition d'une méthode d'accès de gestion**
- **Configuration de RADIUS**
- **Configuration de la sécurité des ports**
- **Configuration de 802.1X**

La protection contre les autres utilisateurs du réseau est décrite dans les sections suivantes. Il s'agit d'attaques qui transitent par le commutateur, mais qui ne sont pas dirigées vers ce dernier.

- **Configuration des services TCP/UDP**
- **Définition du contrôle des tempêtes**
- **Configuration de la sécurité des ports**

Définition d'utilisateurs

Le nom d'utilisateur/mot de passe par défaut est **cisco/cisco**. Lors de votre première ouverture de session avec le nom d'utilisateur et le mot de passe par défaut, vous devez saisir un nouveau mot de passe. La complexité des mots de passe est activée par défaut. Si le mot de passe que vous choisissez n'est pas suffisamment complexe (les **Paramètres de complexité du mot de passe** peuvent être activés sur la page *Sécurité du mot de passe*), le système vous invite à créer un autre mot de passe.

Définition de comptes d'utilisateurs

La page *Comptes d'utilisateur* vous permet de saisir des utilisateurs supplémentaires autorisés à accéder au commutateur (en lecture seule ou en lecture/écriture) ou de modifier les mots de passe d'utilisateurs existants.

Après l'ajout d'un utilisateur (comme décrit ci-dessous), l'utilisateur par défaut est supprimé du système.

REMARQUE Il est impossible de supprimer tous les utilisateurs. Si tous les utilisateurs sont sélectionnés, le bouton **Supprimer** est désactivé.

Pour ajouter un nouvel utilisateur :

ÉTAPE 1 Cliquez sur **Administration** > **Comptes d'utilisateurs**. La page *Comptes d'utilisateur* s'affiche.

Cette page affiche les utilisateurs définis dans le système ainsi que leur niveau de privilèges.

ÉTAPE 2 Sélectionnez **Service de récupération du mot de passe** pour activer cette fonction. Lorsque cette fonction est activée, un utilisateur final disposant d'un accès physique au port de console du périphérique peut accéder au menu de

démarrage et déclencher le processus de récupération du mot de passe. Lorsque le processus de démarrage du système est terminé, vous êtes autorisé à vous connecter au périphérique sans authentification de mot de passe. L'accès au périphérique est autorisé uniquement par le biais de la console et exclusivement lorsque la console est connectée au périphérique avec accès physique.

Lorsque le mécanisme de récupération du mot de passe est désactivé, l'accès au menu de démarrage est toujours autorisé et vous pouvez déclencher le processus de récupération du mot de passe. La différence est que dans ce cas, tous les fichiers de configuration et les fichiers des utilisateurs sont supprimés durant le processus de démarrage du système et un message de journal approprié est généré sur le terminal.

ÉTAPE 3 Cliquez sur **Ajouter** pour ajouter un nouvel utilisateur ou sur **Modifier** pour en modifier un. La page *Ajouter (ou modifier) un compte d'utilisateur* s'affiche.

ÉTAPE 4 Saisissez les paramètres.

- **Nom d'utilisateur** : saisissez un nouveau nom d'utilisateur comportant 20 caractères maximum. Les caractères UTF-8 sont interdits.
- **Mot de passe** : saisissez un mot de passe (les caractères UTF-8 sont interdits). Si vous définissez la sécurité et la complexité du mot de passe, le mot de passe de l'utilisateur doit être conforme à la stratégie configurée à la section **Définition des règles de complexité du mot de passe**.
- **Confirmer le mot de passe** : saisissez à nouveau le mot de passe.
- **Mesure de la robustesse du mot de passe** : affiche le niveau de robustesse du mot de passe. Vous pouvez définir la stratégie de sécurité et de complexité du mot de passe sur la page *Sécurité du mot de passe*.

ÉTAPE 5 Cliquez sur **Appliquer**. L'utilisateur est ajouté au fichier de Configuration d'exécution du commutateur.

Définition de règles de complexité des mots de passe

Les mots de passe permettent d'authentifier les utilisateurs qui accèdent au commutateur. Les mots de passe simples constituent des risques de sécurité potentiels. Par conséquent, les exigences de complexité du mot de passe sont appliquées par défaut et peuvent être configurées si nécessaire. Vous pouvez configurer les exigences de complexité du mot de passe sur la page **Sécurité du mot de passe** accessible via le menu déroulant Sécurité. En outre, le délai d'expiration du mot de passe peut être configuré sur cette page.

Pour définir les règles de complexité des mots de passe :

ÉTAPE 1 Cliquez sur **Sécurité** > **Fiabilité du mot de passe**. La page *Fiabilité du mot de passe* s'affiche.

ÉTAPE 2 Saisissez les paramètres d'expiration suivants pour les mots de passe :

- **Expiration du mot de passe** : si cette option est sélectionnée, l'utilisateur sera invité à modifier le mot de passe une fois le **Délai d'expiration du mot de passe** atteint.
- **Délai d'expiration du mot de passe** : saisissez la durée en jours à l'issue de laquelle le système invite l'utilisateur à changer de mot de passe.

  REMARQUE L'expiration du mot de passe s'applique aussi aux mots de passe de longueur nulle (pas de mot de passe).

ÉTAPE 3 Sélectionnez **Paramètres de complexité du mot de passe** afin d'activer les règles de complexité pour les mots de passe.

Si la complexité du mot de passe est activée, les nouveaux mots de passe doivent être conformes aux paramètres par défaut suivants :

- Avoir une longueur minimale de huit caractères.
- Contenir des caractères appartenant à au moins trois classes de caractères (caractères majuscules, minuscules, numériques et spéciaux disponibles sur un clavier standard).
- Être différents du mot de passe actuel.
- Ne pas contenir de caractère répété plus de trois fois consécutivement.
- Ne pas répéter ou inverser le nom d'utilisateur ou toute variante obtenue en changeant la casse des caractères.
- Ne pas répéter ou inverser le nom de fabricant ou toute variante obtenue en changeant la casse des caractères.

ÉTAPE 4 Si les **Paramètres de complexité du mot de passe** sont activés, les paramètres suivants peuvent être configurés :

- **Longueur minimale du mot de passe** : saisissez le nombre minimum de caractères requis pour les mots de passe.

  REMARQUE Un mot de passe de longueur nulle (pas de mot de passe) est autorisé, et un délai d'expiration du mot de passe peut lui être attribué.

- **Répétition de caractères autorisée** : saisissez le nombre de fois qu'un caractère peut être répété.
- **Nombre minimum de classes de caractères** : saisissez le nombre de classes de caractères qui doivent être présentes dans un mot de passe. Les classes de caractères sont minuscules (1), majuscules (2), chiffres (3) et symboles ou caractères spéciaux (4).
- **Le nouveau mot de passe doit être différent de l'actuel** : si cette option est sélectionnée, lors de la modification du mot de passe, le nouveau mot de passe ne peut pas être identique au mot de passe actuel.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres de mot de passe sont écrits dans le fichier de Configuration d'exécution.

Configuration de RADIUS

Les serveurs RADIUS (Remote Authorization Dial-In User Service) offrent un contrôle d'accès réseau basé sur MAC ou 802.1X centralisé. Le commutateur est un client RADIUS pouvant utiliser un serveur RADIUS pour fournir une sécurité centralisée.

Pour définir les paramètres du serveur RADIUS :

ÉTAPE 1 Cliquez sur **Sécurité** > **RADIUS**. La page *RADIUS* apparaît.

ÉTAPE 2 Saisissez les paramètres RADIUS par défaut, si nécessaire. Les valeurs entrées dans les *Paramètres par défaut* sont appliquées à tous les serveurs. Si une valeur n'est pas entrée pour un serveur spécifique (sur la page *Ajouter un serveur RADIUS*), le commutateur utilise les valeurs contenues dans ces champs.

- **Version IP** : affiche les versions IP prises en charge : sous-réseau IPv6 et/ou IPv4.
- **Tentatives** : saisissez le nombre de demandes transmises qui sont envoyées au serveur RADIUS avant que le système considère qu'une défaillance s'est produite.
- **Délai de réponse** : saisissez le nombre de secondes pendant lesquelles le commutateur attend une réponse du serveur RADIUS avant de relancer la demande ou de passer au serveur suivant.
- **Délai d'inactivité** : saisissez le nombre de minutes qui s'écoulent avant qu'un serveur RADIUS non réactif soit contourné pour les demandes de services. Si la valeur est égale à 0, le serveur n'est pas contourné.
- **Chaîne de clé** : saisissez la chaîne de clé par défaut utilisée pour l'authentification et le cryptage entre le commutateur et le serveur RADIUS. Cette clé doit correspondre à la clé configurée sur le serveur RADIUS. Une chaîne de clé est utilisée pour crypter les communications à l'aide de MD5. Vous pouvez saisir la clé en mode **Chiffré** ou **Texte en clair**. Si vous ne possédez pas de chaîne de clé chiffrée (à partir d'un autre périphérique), saisissez la chaîne de clé en mode Texte en clair et cliquez sur **Appliquer**. La chaîne de clé chiffrée est générée et affichée.

  Cette clé remplace la chaîne de clé par défaut, si une telle clé a été définie.
- **Adresse IPv4 source** : saisissez l'adresse IPv4 source à utiliser.
- **Adresse IPv6 source** : saisissez l'adresse IPv6 source à utiliser.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres RADIUS par défaut du commutateur sont mis à jour dans le fichier de Configuration d'exécution.

Pour ajouter un serveur RADIUS, cliquez sur **Ajouter**. La page *Ajouter un serveur RADIUS* s'affiche.

ÉTAPE 4 Entrez les valeurs dans les champs pour chaque serveur RADIUS. Pour utiliser les valeurs par défaut entrées sur la page *RADIUS*, sélectionnez **Valeurs par défaut**.

- **Version IP** : si le serveur RADIUS doit être identifié par son adresse IP, sélectionnez IPv4 ou IPv6 pour indiquer qu'il est entré au format sélectionné.
- **Type d'adresse IPv6** : indique que le type d'adresse IPv6 est Global.
- **Adresse IP du serveur/Nom** : indiquez si vous souhaitez spécifier le serveur RADIUS par son adresse IP ou son nom.

- **Priorité** : saisissez la priorité du serveur. La priorité détermine l'ordre dans lequel le commutateur essaie de contacter les serveurs pour authentifier un utilisateur. Le commutateur commence par le serveur RADIUS ayant la priorité la plus élevée (priorité zéro).

  Chaîne de clé : saisissez la chaîne de clé utilisée pour l'authentification et le cryptage des communications entre le commutateur et le serveur RADIUS. Cette clé doit correspondre à la clé configurée sur le serveur RADIUS. Si l'option **Valeurs par défaut** est sélectionnée, le commutateur essaie de s'authentifier sur le serveur RADIUS en utilisant la chaîne de clé par défaut.

- **Délai de réponse** : saisissez le nombre de secondes pendant lesquelles le commutateur attend une réponse du serveur RADIUS avant de relancer la demande ou de passer au serveur suivant si le nombre maximal de tentatives ont été effectuées. Si l'option **Valeurs par défaut** est sélectionnée, le commutateur utilise la valeur de délai par défaut.

- **Port d'authentification** : saisissez le numéro de port UDP du port du serveur RADIUS pour les demandes d'authentification.

- **Tentatives** : entrez le nombre de demandes envoyées au serveur RADIUS avant qu'un échec soit avéré. Si l'option **Valeurs par défaut** est sélectionnée, le commutateur utilise la valeur par défaut du nombre de tentatives.

- **Délai d'inactivité** : saisissez le nombre de minutes qui doivent s'écouler avant qu'un serveur RADIUS non réactif soit contourné pour les demandes de services. Si l'option **Valeurs par défaut** est sélectionnée, le commutateur utilise la valeur par défaut du délai d'inactivité. Si vous saisissez 0 minute, aucun délai d'inactivité ne sera appliqué.

- **Type d'utilisation** : saisissez le type d'authentification du serveur RADIUS. Les options sont les suivantes :

  - *Connexion* : le serveur RADIUS est utilisé pour l'authentification des utilisateurs qui demandent à administrer le commutateur.

  - *802.1X* : le serveur RADIUS est utilisé pour l'authentification 802.1x.

  - *Tous* : le serveur RADIUS est utilisé pour l'authentification des utilisateurs qui demandent à administrer le commutateur et pour l'authentification 802.1X.

ÉTAPE 5 Pour afficher les données sensibles sous la forme de texte en clair dans le fichier de configuration, cliquez sur **Afficher les données sensibles en texte clair**.

ÉTAPE 6 Cliquez sur **Appliquer**. La définition du serveur RADIUS est ajoutée au fichier de Configuration d'exécution du commutateur.

Configuration de l'Authentification de l'accès de gestion

Vous pouvez affecter des méthodes d'authentification à des sessions HTTP/HTTPS. L'authentification peut être effectuée localement ou sur un serveur RADIUS.

Pour que le serveur RADIUS accorde l'accès à l'utilitaire Web de configuration du commutateur, ce serveur doit renvoyer cisco-avpair = shell:priv-lvl=15.

L'authentification de l'utilisateur s'effectue en fonction de l'ordre de sélection des méthodes d'authentification. Si la première méthode d'authentification n'est pas disponible, la méthode suivante sera utilisée. Par exemple, si les méthodes d'authentification sélectionnées sont RADIUS et Local, et que tous les serveurs RADIUS configurés sont interrogés en vertu de leur ordre de priorité et qu'ils ne répondent pas, l'utilisateur sera authentifié au niveau local.

Si une méthode d'authentification échoue ou si le niveau de privilège d'un utilisateur est insuffisant, ce dernier se voit refuser l'accès au commutateur. En d'autres termes, si l'authentification échoue au niveau d'une méthode d'authentification, le commutateur n'essaie pas d'utiliser la méthode d'authentification suivante et s'arrête.

Pour définir les méthodes d'authentification d'une méthode d'accès :

ÉTAPE 1 Cliquez sur **Sécurité** > **Authentification de l'accès de gestion**. La page *Authentification de l'accès de gestion* s'affiche.

ÉTAPE 2 Sélectionnez une méthode d'accès dans la liste **Application**.

ÉTAPE 3 Utilisez les flèches pour déplacer la méthode d'authentification entre les colonnes Méthodes facultatives et Méthodes sélectionnées. La première méthode sélectionnée correspond à celle qui sera utilisée en premier.

- *RADIUS* : l'utilisateur est authentifié sur un serveur RADIUS. Vous devez avoir configuré un ou plusieurs serveurs RADIUS.
- *Aucun* : l'utilisateur est autorisé à accéder au commutateur sans avoir été authentifié.
- *Locale* : le nom d'utilisateur et le mot de passe sont comparés aux données stockées sur le commutateur local. Ces paires de nom d'utilisateur et mot de passe sont définies sur la page *Comptes d'utilisateur*.

  REMARQUE La méthode d'authentification **Local** ou **Aucun** doit toujours être sélectionnée en dernier. Toutes les méthodes d'authentification sélectionnées après **Local** ou **Aucun** sont ignorées.

ÉTAPE 4 Cliquez sur **Appliquer**. Les méthodes d'authentification sélectionnées sont associées à la méthode d'accès.

Définition d'une méthode d'accès de gestion

Les profils d'accès déterminent la façon d'authentifier les utilisateurs et de les autoriser à accéder au commutateur via différentes méthodes d'accès. Les profils d'accès peuvent limiter l'accès de gestion à partir de sources spécifiques.

Seuls les utilisateurs qui passent le profil d'accès actif et les méthodes d'authentification de l'accès de gestion peuvent accéder au commutateur.

Un seul profil d'accès à la fois peut être actif sur le commutateur.

Les profils d'accès contiennent une ou plusieurs règles. Les règles sont exécutées dans l'ordre c'est-à-dire en fonction de leur priorité dans le profil d'accès (de haut en bas).

Les règles sont composées de filtres qui incluent les éléments suivants :

- **Méthodes d'accès** : méthodes permettant l'accès au commutateur et sa gestion :
  - Hypertext Transfer Protocol (HTTP)
  - HTTPS (Secure HTTP)
  - Tous les éléments ci-dessus

- **Action** : permet d'autoriser ou de refuser l'accès à une interface ou à une adresse source.
- **Interface** : ports, LAG ou VLAN autorisés à accéder à l'utilitaire Web de configuration du commutateur ou interdits d'accès à celui-ci.
- **Adresse IP source** : adresses ou sous-réseaux IP auxquels l'accès est autorisé.

Profil d'accès actif

La page *Profils d'accès* affiche les profils d'accès définis et permet de sélectionner un profil d'accès en tant que profil actif.

Lorsqu'un utilisateur tente d'accéder au commutateur par le biais d'une méthode d'accès, le commutateur vérifie si le profil d'accès actif autorise explicitement l'accès de gestion au commutateur via cette méthode. Si aucune correspondance n'est trouvée, l'accès est refusé.

Lorsqu'une tentative d'accès au commutateur s'effectue en violation du profil d'accès actif, le commutateur génère un message SYSLOG pour en avertir l'administrateur système.

Pour plus d'informations, reportez-vous à la section **Définition de règles de profils**.

Utilisez la page *Profils d'accès* pour créer un profil d'accès et ajouter sa première règle. Si le profil d'accès ne contient qu'une seule règle, vous avez terminé. Pour ajouter des règles supplémentaires au profil, utilisez la page Règles de profils.

ÉTAPE 1 Cliquez sur **Sécurité** > **Méthode d'accès de gestion** > **Profils d'accès**. La page *Profils d'accès* s'affiche.

Cette page affiche tous les profils d'accès, qu'ils soient actifs ou non.

ÉTAPE 2 Pour modifier le profil d'accès actif, sélectionnez un profil dans le menu déroulant **Profil d'accès actif** et cliquez sur **Appliquer**. Le profil choisi devient alors le profil d'accès actif.

Si vous sélectionnez un autre profil d'accès, un message s'affiche pour vous avertir que, selon le profil d'accès sélectionné, vous pourriez être déconnecté de l'utilitaire Web de configuration du commutateur.

ÉTAPE 3 Cliquez sur **OK** pour sélectionner le profil d'accès actif ou sur **Annuler** pour abandonner cette action.

ÉTAPE 4 Cliquez sur **Ajouter** pour ouvrir la page *Ajouter un profil d'accès*. Cette page vous permet de configurer un nouveau profil ainsi qu'une règle.

ÉTAPE 5 Saisissez le **Nom du profil d'accès**. Ce nom peut comporter jusqu'à 32 caractères.

ÉTAPE 6 Saisissez les paramètres.

- **Priorité des règles** : saisissez la priorité des règles. Lorsque le paquet est mis en correspondance avec une règle, les groupes d'utilisateurs se voient accorder ou refuser l'accès au commutateur. La priorité des règles est indispensable pour faire correspondre les paquets aux règles, la correspondance des paquets étant établie sur une base de première correspondance. Le 1 correspond à la priorité la plus élevée.
- **Méthode de gestion** : sélectionnez la méthode de gestion pour laquelle la règle est définie. Les options sont les suivantes :
  - *Tout* : affecte toutes les méthodes de gestion à la règle.
  - *HTTP* : les utilisateurs demandant l'accès au commutateur répondant aux critères du profil d'accès HTTP se voient autoriser ou refuser l'accès.
  - *HTTP sécurisé (HTTPS)* : les utilisateurs demandant l'accès au commutateur répondant aux critères du profil d'accès HTTPS se voient autoriser ou refuser l'accès.
- **Action** : sélectionnez l'action rattachée à la règle. Les options sont les suivantes :
  - *Autoriser* : autorise l'accès au commutateur dans la mesure où l'utilisateur correspond aux paramètres du profil.
  - *Refuser* : refuse l'accès au commutateur dans la mesure où l'utilisateur correspond aux paramètres du profil.
- **S'applique à l'interface** : sélectionnez l'interface rattachée à la règle. Les options sont les suivantes :
  - *Tout* : s'applique à tous les ports, VLAN et LAG.
  - *Défini par l'utilisateur* : s'applique à l'interface sélectionnée.
- **Interface** : entrez le numéro d'interface si l'option Défini par l'utilisateur a été sélectionnée.
- **S'applique à l'adresse IP source** : sélectionnez le type d'adresse IP source auquel le profil d'accès s'applique. Le champ *Adresse IP source* est valide pour un sous-réseau. Sélectionnez l'une des valeurs suivantes :

- *Tout* : s'applique à tous les types d'adresses IP.
- *Défini par l'utilisateur* : s'applique uniquement aux types d'adresses IP définis dans les champs.

- **Version IP** : sélectionnez la version IP prise en charge pour l'adresse source, IPv6 ou IPv4.
- **Adresse IP** : saisissez l'adresse IP source.
- **Masque** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs suivants :
  - *Masque de réseau* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Longueur du préfixe* : sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l'adresse IP source.

ÉTAPE 7 Cliquez sur **Appliquer**. Le profil d'accès est écrit dans le fichier de Configuration d'exécution. Vous pouvez à présent sélectionner ce profil d'accès en tant que profil d'accès actif.

Définition de règles de profils

Les profils d'accès peuvent comporter jusqu'à 128 règles afin de déterminer qui est autorisé à gérer le commutateur ainsi qu'à y accéder et les méthodes d'accès pouvant être utilisées.

Chaque règle d'un profil d'accès comporte une action et des critères (un ou plusieurs paramètres) à faire correspondre. Une priorité est affectée à chaque règle. Les règles ayant la priorité la plus basse sont vérifiées en premier. Si le paquet entrant correspond à une règle, l'action associée à cette dernière est appliquée. Si aucune règle correspondante n'est trouvée dans le profil d'accès actif, le paquet est abandonné.

Par exemple, vous pouvez limiter l'accès au commutateur depuis toutes les adresses IP à l'exception de celles qui sont attribuées au centre de gestion informatique. Le commutateur peut ainsi continuer à être géré tout en bénéficiant d'un autre niveau de sécurité.

Pour ajouter des règles de profil à un profil d'accès :

ÉTAPE 1 Cliquez sur **Sécurité** > **Méthode d'accès de gestion** > **Règles de profils**. La page *Règles de profils* s'affiche.

ÉTAPE 2 Sélectionnez le champ Filtre et un profil d'accès. Cliquez sur **OK**.

Le profil d'accès sélectionné s'affiche dans la Table des règles de profil.

ÉTAPE 3 Cliquez sur **Ajouter** pour y ajouter une règle. La page *Ajouter une règle de profil* s'affiche.

ÉTAPE 4 Saisissez les paramètres.

- **Nom du profil d'accès** : sélectionnez un profil d'accès.
- **Priorité des règles** : saisissez la priorité des règles. Lorsque le paquet est mis en correspondance avec une règle, les groupes d'utilisateurs se voient accorder ou refuser l'accès au commutateur. La priorité des règles est indispensable pour faire correspondre les paquets aux règles, la correspondance des paquets étant établie sur une base de première correspondance.
- **Méthode de gestion** : sélectionnez la méthode de gestion pour laquelle la règle est définie. Les options sont les suivantes :
  - *Tout* : affecte toutes les méthodes de gestion à la règle.
  - *HTTP* : affecte un accès HTTP à la règle. Les utilisateurs demandant l'accès au commutateur répondant aux critères du profil d'accès HTTP se voient autoriser ou refuser l'accès.
  - *HTTP sécurisé (HTTPS)* : les utilisateurs demandant l'accès au commutateur répondant aux critères du profil d'accès HTTPS se voient autoriser ou refuser l'accès.
- **Action :** sélectionnez **Autoriser** pour autoriser les utilisateurs qui essaient d'accéder au commutateur en utilisant la méthode d'accès configurée depuis l'interface et la sourceIP définies dans cette règle. Ou sélectionnez **Refuser** pour refuser l'accès.
- **S'applique à l'interface** : sélectionnez l'interface rattachée à la règle. Les options sont les suivantes :
  - *Tout* : s'applique à tous les ports, VLAN et LAG.
  - *Défini par l'utilisateur :* s'applique uniquement au port, VLAN ou LAG sélectionné.

- **Interface** : entrez le numéro d'interface.
- **S'applique à l'adresse IP source** : sélectionnez le type d'adresse IP source auquel le profil d'accès s'applique. Le champ *Adresse IP source*est valide pour un sous-réseau. Sélectionnez l'une des valeurs suivantes :
  - *Tout* : s'applique à tous les types d'adresses IP.
  - *Défini par l'utilisateur* : s'applique uniquement aux types d'adresses IP définis dans les champs.
- **Version IP** : sélectionnez la version IP prise en charge pour l'adresse source : IPv6 ou IPv4.
- **Adresse IP** : saisissez l'adresse IP source.
- **Masque** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs :
  - *Masque de réseau :* sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Longueur du préfixe* : sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l'adresse IP source.

ÉTAPE 5 Cliquez sur **Appliquer**. La règle est ajoutée au profil d'accès.

Configuration des services TCP/UDP

La page *Services TCP/UDP* active les services TCP ou UDP sur le commutateur, généralement pour des raisons de sécurité.

Le commutateur fournit les services TCP/UDP suivants :

- **HTTP** : activé par défaut
- **HTTPS :** activé par défaut en usine

Les connexions TCP actives sont également affichées dans cette fenêtre.

Pour configurer les servicesTCP/UDP :

ÉTAPE 1 Cliquez sur **Sécurité** > **ServicesTCP/UDP**. La page *Services TCP/UDP* s'affiche.

ÉTAPE 2 Activez ou désactivez les services TCP/UDP suivants sur les services affichés.

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

La table des services TCP contient les champs suivants pour chaque service :

- **Nom de service** : méthode d'accès utilisée par le commutateur pour fournir le service TCP.
- **Type** : protocole IP utilisé par le service.
- **Adresse IP locale** : adresse IP locale via laquelle le commutateur propose le service.
- **Port local** : port TCP local via lequel le commutateur propose le service.
- **Adresse IP distante** : adresse IP de l'appareil distant qui demande le service.
- **Port distant :** port TCP de l'appareil distant qui demande le service.
- **État** : état du service.

La table des services UDP affiche les informations suivantes :

- **Nom de service** : méthode d'accès utilisée par le commutateur pour fournir le service UDP.
- **Type** : protocole IP utilisé par le service.
- **Adresse IP locale** : adresse IP locale via laquelle le commutateur propose le service.
- **Port local :** port UDP local via lequel le commutateur propose le service.
- **Instance d'application :** instance de service du service UDP (Par exemple, lorsque deux expéditeurs envoient des données vers la même destination.)

ÉTAPE 3 Cliquez sur **Appliquer**. Les services sont écrits dans le fichier de Configuration d'exécution.

Définition du contrôle des tempêtes

Lorsque des trames de Diffusion (Broadcast), Multidiffusion (Multicast) ou Monodiffusion inconnue (Unknown Unicast) sont reçues, elles sont dupliquées et une copie est envoyée à tous les ports de sortie possibles. Cela signifie dans la pratique qu'elles sont envoyées à tous les ports appartenant au VLAN approprié. De cette manière, une seule trame d'entrée est convertie en plusieurs trames, ce qui peut potentiellement occasionner une tempête de trafic.

La protection contre les tempêtes vous permet de limiter le nombre de trames entrant dans le commutateur et de définir les types de trames pris en compte dans le calcul de cette limite.

Si un seuil a été entré dans le système, le port bloque le trafic dès que le seuil est atteint. Le port reste bloqué jusqu'à ce que le débit du trafic passe en dessous de ce seuil. Il reprend ensuite normalement les opérations de transfert.

Pour définir le contrôle des tempêtes :

ÉTAPE 1 Cliquez sur **Sécurité** > **Contrôle des tempêtes**. La page *Contrôle des tempêtes* s'affiche.

Tous les champs de cette page sont décrits sur la page *Modifier le contrôle des tempêtes*, excepté pour le **Seuil de débit de contrôle des tempêtes (%)**. Il affiche le pourcentage de la bande passante totale disponible pour les paquets de Monodiffusion inconnue (Unknown Unicast), Multidiffusion (Multicast) et Diffusion (Broadcast) avant que le contrôle des tempêtes ne soit appliqué sur le port. La valeur par défaut est 10 % du débit maximal du port. Vous pouvez la définir sur la page *Modifier le contrôle des tempêtes*.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier**. La page *Modifier le contrôle des tempêtes* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Interface :** sélectionnez le port pour lequel activer le contrôle des tempêtes.
- **Contrôle des tempêtes :** sélectionnez cette option pour activer le contrôle des tempêtes.
- **Seuil de débit de contrôle des tempêtes :** saisissez le débit maximum auquel les paquets inconnus peuvent être transmis. La valeur par défaut de ce seuil est 10 000 pour les appareils FE et 100 000 pour les appareils GE.

- **Mode de contrôle des tempêtes :** sélectionnez l'un des modes suivants.
  - *Monodiffusion inconnue, multidiffusion et diffusion* : intègre le trafic de Monodiffusion inconnue (Unknown Unicast), Diffusion (Broadcast) et Multidiffusion (Multicast) au sein du seuil de la bande passante.
  - *Multidiffusion et diffusion* : intègre le trafic de Diffusion (Broadcast) et Multidiffusion (Multicast) au sein du seuil de la bande passante.
  - *Diffusion uniquement :* intègre uniquement le trafic de diffusion au sein du seuil de la bande passante.

ÉTAPE 4 Cliquez sur **Appliquer**. Le contrôle des tempêtes est modifié et le fichier de Configuration d'exécution est mis à jour.

Configuration de la sécurité des ports

Vous pouvez accroître la sécurité réseau en limitant l'accès à un port pour des utilisateurs disposant d'adresses MAC spécifiques. Les adresses MAC peuvent être apprises de façon dynamique ou configurées de manière statique.

La sécurité des ports surveille les paquets reçus et appris. L'accès aux ports verrouillés est limité aux utilisateurs disposant d'adresses MAC spécifiques.

La sécurité des ports dispose de quatre modes :

- **Verrouillage classique** : toutes les adresses MAC apprises sur le port sont verrouillées et le port n'apprend aucune nouvelle adresse MAC. Les adresses apprises ne sont pas soumises à un délai d'expiration ni à un réapprentissage.
- **Verrouillage dynamique limité**: le commutateur apprend des adresses MAC jusqu'à la limite configurée des adresses autorisées. Une fois la limite atteinte, le commutateur n'apprend pas d'adresses supplémentaires. Dans ce mode, les adresses sont soumises à un délai d'expiration ainsi qu'à un réapprentissage.
- **Sécurisé en permanence :** conserve les adresses MAC dynamiques actuellement associées au port et apprend au maximum le nombre d'adresses autorisées sur le port (défini par l'option Nombre max. d'adresses autorisées). Les opérations de réapprentissage et de délai d'expiration sont activées.

- **Suppression sécur. à la réinitialisation :** supprime les adresses MAC dynamiques actuellement associées au port après la réinitialisation. Les nouvelles adresses MAC peuvent être apprises en tant qu'adresses supprimées à la réinitialisation (Delete-On-Reset) jusqu'au nombre d'adresses autorisées sur le port. Les opérations de réapprentissage et de délai d'expiration sont désactivées.

Lorsqu'une trame d'une nouvelle adresse MAC est détectée sur un port sur lequel elle n'est pas autorisée (le port est verrouillé de façon classique et une nouvelle adresse MAC est détectée ou bien le port est verrouillé de façon dynamique et le nombre maximal des adresses autorisées a été dépassé), il est fait appel au mécanisme de protection et l'une des actions suivantes peut s'appliquer :

- La trame est rejetée.
- La trame est transmise.
- Le port est fermé.

Lorsque l'adresse MAC sécurisée est détectée sur un autre port, la trame est transmise mais l'adresse MAC n'est pas apprise sur ce port.

Outre l'une de ces actions, vous pouvez également générer des messages « trap » ainsi qu'en limiter la fréquence ou le nombre afin d'éviter de surcharger les appareils.

REMARQUE Les messages « trap » sont des messages SYSLOG, non générés via SNMP.

REMARQUE Pour utiliser 802.1X sur un port, il doit être en mode Hôtes multiples ou Sessions multiples. La sécurité des ports ne peut pas être définie sur un port si ce dernier est un mode unique (reportez-vous à la page *802.1x, Authentification hôtes et sessions)*.

Pour configurer la sécurité des ports :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité des ports**. La page *Sécurité des ports* s'affiche. Page Sécurité des ports

ÉTAPE 2 Sélectionnez une interface à modifier et cliquez sur **Modifier**. La page *Modifier les paramètres d'interface de sécurité des ports* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Interface :** sélectionnez le nom de l'interface.
- **État de l'interface :** sélectionnez l'état de verrouillage du port.

- **Mode d'apprentissage :** sélectionnez le type de verrouillage du port. L'État de l'interface doit être déverrouillé pour que ce champ puisse être configuré. Le champ Mode d'apprentissage est uniquement activé si le champ *État de l'interface* est verrouillé. Pour modifier le Mode d'apprentissage, État de l'interface doit être désactivé. Une fois ce mode modifié, vous pouvez rétablir l'état de l'interface. Les options sont les suivantes :
  - *Verrouillage classique :* verrouille immédiatement le port, quel que soit le nombre d'adresses ayant déjà été apprises.
  - *Verrouillage dynamique limité*: verrouille le port en supprimant les adresses MAC dynamiques actuellement associées au port. Le port apprend au maximum le nombre d'adresses autorisées sur le port. Le réapprentissage et le délai d'expiration des adresses MAC sont activés.
  - *Sécurisé en permanence* : conserve les adresses MAC dynamiques actuellement associées au port et apprend au maximum le nombre d'adresses autorisées sur le port (défini par l'option **Nombre max. d'adresses autorisées**). Les opérations de réapprentissage et de délai d'expiration sont activées.
  - *Suppression sécur. à la réinitialisation* : supprime les adresses MAC dynamiques actuellement associées au port après la réinitialisation. Les nouvelles adresses MAC peuvent être apprises en tant qu'adresses supprimées à la réinitialisation (Delete-On-Reset) jusqu'au nombre d'adresses autorisées sur le port. Les opérations de réapprentissage et de délai d'expiration sont désactivées.
- **Nombre max. d'adresses autorisées :** saisissez le nombre maximum d'adresses MAC pouvant être apprises sur le port dans la mesure où le mode d'apprentissage *Verrouillage dynamique limité* est sélectionné. Le chiffre 0 indique que seules les adresses statiques sont prises en charge dans l'interface.
- **Action en cas de violation** : sélectionnez l'action à appliquer aux paquets qui arrivent sur un port verrouillé. Les options sont les suivantes :
  - *Abandonner* : abandonne les paquets en provenance d'une source non apprise.
  - *Transférer* : transfère les paquets en provenance d'une source inconnue sans apprendre l'adresse MAC.
  - *Arrêter* : abandonne les paquets en provenance d'une source non apprise et ferme le port. Le port reste fermé jusqu'à sa réactivation ou jusqu'au redémarrage du commutateur.

- **« Trap »** : sélectionnez cette option pour activer les messages « trap » lorsqu'un paquet est reçu sur un port verrouillé. Ceci est approprié pour les violations de verrouillage. Pour le Verrouillage classique, ceci correspondra à toute nouvelle adresse reçue. Pour le Verrouillage dynamique limité, cela correspondra à toute nouvelle adresse qui dépassera le nombre des adresses autorisées.

  REMARQUE Les messages « trap » sont des messages SYSLOG, non générés via SNMP.

- **Fréquence du/des message(s) « trap »** : saisissez la durée minimale qui s'écoulera entre deux messages « trap ».

ÉTAPE 4 Cliquez sur **Appliquer**. La sécurité des ports est modifiée et le fichier de Configuration d'exécution est mis à jour.

Configuration de 802.1X

Le contrôle d'accès basé sur les ports a pour effet de créer deux types d'accès sur les ports du commutateur. Un point d'accès active la communication non contrôlée, ceci indépendamment de l'état d'autorisation (*port non contrôlé*). L'autre point d'accès autorise la communication entre un hôte et le commutateur.

802.1x est une norme IEEE pour le contrôle d'accès réseau basé sur les ports. L'infrastructure 802.1X permet à un appareil (le demandeur) de demander l'accès à un port à partir d'un appareil distant (l'authentificateur) auquel il est connecté. Pour que le demandeur qui requiert l'accès au port puisse envoyer des données vers le port, il doit d'abord être authentifié et autorisé. Sinon, l'authentificateur supprime les données du demandeur.

L'authentification du demandeur est effectuée par un serveur RADIUS externe via l'authentificateur. Celui-ci contrôle le résultat de l'authentification.

Dans la norme 802.1x, un appareil peut être simultanément un demandeur et un authentificateur au niveau d'un port, et ainsi demander et accorder l'accès à un port. Cet appareil n'est toutefois que l'authentificateur ; il ne peut faire office de demandeur.

Il existe différents types de 802.1X :

- **802.1X à session unique :**
  - **Session unique/hôte unique :** dans ce mode, le commutateur en tant qu'authentificateur prend en charge une session 802.1x unique et accorde l'autorisation d'utiliser le port au demandeur autorisé. Tous les accès des autres appareils reçus du même port sont refusés tant que le demandeur autorisé utilise le port ou que l'accès ne s'effectue pas vers le VLAN non authentifié.
  - **Session unique/hôtes multiples** : applique la norme 802.1x. Dans ce mode, le commutateur en tant qu'authentificateur autorise tout périphérique à utiliser un port s'il en a reçu l'autorisation.
- **802.1X multi-sessions :** chaque appareil (demandeur) se connectant à un port doit être authentifié et autorisé par le commutateur (authentificateur), séparément, dans une session 802.1x distincte.

Le commutateur prend en charge le mécanisme d'authentification 802.1X, tel que décrit dans la norme pour authentifier et autoriser les demandeurs802.1X.

Flux de travail des paramètres 802.1X

Définissez les paramètres 802.1X comme suit :

- (Facultatif) Définissez un ou plusieurs VLAN statiques en tant que VLAN non authentifiés, comme décrit à la section **Définition des propriétés 802.1X**. Les appareils ou ports autorisés et non autorisés pour 802.1X peuvent toujours envoyer ou recevoir des paquets à ou depuis des VLAN non authentifiés.
- Définissez les paramètres 802.1X de chaque port à l'aide de la page *Modifier l'authentification des ports*.

Notez les éléments suivants :

- Vous pouvez sélectionner le champ VLAN invité pour que les trames entrantes non balisées soient dirigées vers le VLAN invité.
- Définissez les paramètres d'authentification des hôtes pour chaque port à l'aide de la page *Authentification des ports*.
- Affichez l'historique d'authentification 802.1X à l'aide de la page *Hôtes authentifiés*.

Définition des propriétés802.1X

La page *Propriétés 802.1X* permet d'activer 802.1X globalement et de définir la façon dont les ports sont authentifiés. Pour que 802.1X puisse fonctionner, il doit être activé à la fois globalement et individuellement sur chaque port.

Pour définir l'authentification basée sur les ports :

ÉTAPE 1 Cliquez sur **Sécurité** > **802.1X** > **Propriétés**. La page *Propriétés* apparaît.

ÉTAPE 2 Saisissez les paramètres.

- **Authentification basée sur les ports** : active ou désactive l'authentification 802.1X basée sur les ports.
- **Méthode d'authentification :** sélectionnez les méthodes d'authentification des utilisateurs. Les options sont les suivantes :
  - *RADIUS, aucune :* effectue tout d'abord l'authentification des ports en utilisant le serveur RADIUS. Si aucune réponse n'est reçue de ce serveur (par exemple s'il n'est pas actif), aucune authentification n'est réalisée et la session est autorisée.
  - *RADIUS :* authentifie l'utilisateur sur le serveur RADIUS. Si aucune authentification n'est effectuée, la session n'est pas autorisée.
  - *Aucune :* n'authentifie pas l'utilisateur. Autorise la session.

ÉTAPE 3 Cliquez sur **Appliquer**. Les propriétés 802.1X sont écrites dans le fichier de Configuration d'exécution.

Définition de l'authentification des ports 802.1X

La page *Authentification des ports* permet de définir les paramètres 802.1X pour chaque port. Puisque certaines modifications de la configuration ne sont possibles que si le port a l'état *Autorisation forcée* (par exemple, l'authentification des hôtes), il est recommandé de changer le contrôle du port en *Autorisation forcée* avant d'effectuer des modifications. Une fois la configuration terminée, rétablissez l'état précédent du contrôle de port.

REMARQUE Un port sur lequel 802.1X est défini ne peut pas devenir membre d'un LAG.

Pour définir l'authentification 802.1X :

ÉTAPE 1 Cliquez sur **Sécurité** > **802.1X** > **Authentification des ports**. La page *Authentification des ports* s'affiche.

Cette page affiche les paramètres d'authentification de tous les ports.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier**. La page *Modifier l'authentification des ports* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez un port.
- **Nom d'utilisateur** : affiche le nom d'utilisateur du port.
- **Contrôle de port actuel** : affiche l'état actuel de l'autorisation du port. Si l'état est *Autorisé*, le port est authentifié ou le *Contrôle de port administratif* est en *Autorisation forcée*. À l'inverse, si l'état est *Non autorisé*, le port est non authentifié ou le *Contrôle de port administratif* est en *Non-autorisation forcée*.
- **Contrôle de port administratif** : affiche l'état d'autorisation du port administratif. Les options sont les suivantes :
  - *Non-autorisation forcée :* refuse l'accès à l'interface en passant cette dernière en mode non autorisé. Le commutateur ne fournit pas de services d'authentification au client via l'interface.
  - *Automatique* : active l'authentification et l'autorisation basées sur les ports sur le commutateur. L'interface bascule entre un état autorisé ou non autorisé en fonction de l'échange d'authentification entre le commutateur et le client.
  - *Autorisation forcée :* autorise l'interface sans authentification.
- **Méthode d'authentification :** sélectionnez la méthode d'authentification pour le port. Les options sont les suivantes :
  - *802.1X uniquement :* l'authentification 802.1X est la seule méthode d'authentification appliquée sur le port.
- **Réauthentification périodique** : sélectionnez cette option pour autoriser les tentatives de réauthentification du port une fois la Période de réauthentification spécifiée expirée.
- **Période de réauthentification :** saisissez le délai (en secondes) au bout duquel le port sélectionné est réauthentifié.

- **Réauthentifier maintenant :** sélectionnez cette option pour permettre la réauthentification immédiate du port.
- **État de l'authentificateur** : affiche l'état défini de l'autorisation du port. Les options sont les suivantes :
  - *Autorisation forcée :* l'état du port contrôlé est défini sur Autorisation forcée (le trafic est transféré).

    REMARQUE Si le port n'est pas en Non-autorisation forcée, il est en mode automatique et l'authentificateur affiche l'état de l'authentification en cours. Une fois le port authentifié, l'état indique Authentifié.
- **Période silencieuse :** saisissez le délai (en secondes) pendant lequel le commutateur reste en état silencieux après l'échec d'un échange d'authentification.
- **Renvoi d'EAP :** saisissez le nombre de secondes pendant lesquelles le commutateur attend une réponse à une demande/trame d'identité EAP (Extensible Authentication Protocol) du demandeur (client) avant de renvoyer la demande.
- **Demandes EAP max.** : saisissez le nombre maximum de demandes EAP pouvant être envoyées. Si aucune réponse n'est reçue après la période définie (délai pour demandeur), le processus d'authentification est relancé.
- **Délai pour demandeur :** saisissez le nombre de secondes qui s'écoulent avant que les demandes EAP soient renvoyées au demandeur.
- **Délai pour serveur :** saisissez le nombre de secondes qui s'écoulent avant que le commutateur renvoie une demande au serveur d'authentification.
- **Cause d'arrêt :** affiche la raison pour laquelle l'authentification du port a été arrêtée, si applicable.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres des ports sont écrits dans le fichier de Configuration d'exécution.

Définition de l'authentification des hôtes et sessions

La page *Authentification hôtes et sessions* permet de définir le mode de fonctionnement de 802.1X sur le port, ainsi que l'action à réaliser si une violation a été détectée.

Les modes 802.1X sont les suivants :

- **Unique** : un seul hôte autorisé peut accéder au port. (La Sécurité des ports ne peut pas être activée sur un port en mode hôte unique.)
- **Hôtes multiples (802.1X)** : plusieurs hôtes peuvent être associés à un seul port activé pour 802.1X. Seul le premier hôte doit être autorisé, puis le port est ouvert à tous ceux qui souhaitent accéder au réseau. En cas d'échec de l'authentification de l'hôte ou de réception d'un message EAPOL-logoff, tous les clients rattachés se voient refuser l'accès au réseau.
- **Sessions multiples** : permet à plusieurs hôtes autorisés spécifiques d'accéder au port. Chaque hôte est considéré comme s'il était le premier et seul utilisateur, et doit être authentifié. Le filtrage se fonde sur l'adresse MAC source.

Pour définir les paramètres 802.1X avancés pour les ports :

ÉTAPE 1 Cliquez sur **Sécurité** > **802.1X** > **Authentification hôtes et sessions**. La page *Authentification hôtes et sessions* s'affiche.

Les paramètres d'authentification 802.1X sont décrits pour tous les ports. Tous les champs à l'exception des suivants sont décrits sur la page *Modifier l'authentification hôte et session*.

- **État :** affiche l'état de l'hôte. Un astérisque indique que le port n'est pas relié ou est inactif. Les options sont les suivantes :
  - *Non autorisé* : le contrôle du port est soit en *Non-autorisation forcée* et la liaison du port est inactive soit en *Automatique* mais un client n'a pas été authentifié via le port.
  - *Autorisation forcée* : les clients disposent d'un accès total au port.
  - *Hôte unique verrouillé* : le contrôle du port est en *Automatique* et un seul client a été authentifié via le port.
  - *Pas d'hôte unique* : le contrôle du port est *Auto* et le mode Hôtes multiples est activé. Au moins un client a été authentifié.
  - *Pas en mode automatique* : le contrôle automatique du port n'est pas activé.

- **Nombre de violations :** affiche le nombre de paquets qui arrivent sur l'interface en mode hôte unique en provenance d'un hôte dont l'adresse MAC ne correspond pas à celle du demandeur.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier**. La page *Modifier l'authentification hôte et session* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : entrez un numéro de port pour lequel l'authentification des hôtes est activée.
- **Authentification des hôtes** : sélectionnez l'un des modes. Ces modes sont décrits ci-dessus dans *Définition de l'authentification hôtes et sessions*.

  REMARQUE Les champs suivants ne sont pertinents que si vous sélectionnez Individuelle dans le champ Authentification des hôtes.

Paramètres de violation d'hôte unique :

- **Action en cas de violation :** sélectionnez l'action à appliquer aux paquets arrivant en mode session unique/hôte unique en provenance d'un hôte dont l'adresse MAC ne correspond pas à celle du demandeur. Les options sont les suivantes :
  - *Protéger (Abandonner)* : abandonne les paquets.
  - *Restreindre (Transférer)* : transfère les paquets.
  - *Arrêter* : abandonne les paquets et ferme le port. Le port reste fermé jusqu'à sa réactivation ou jusqu'au redémarrage du commutateur.
- **Messages « trap »** (en cas de violation d'hôte unique) : sélectionnez cette option pour activer les messages « trap ».

  REMARQUE Les messages « trap » sont des messages SYSLOG, non liés à SNMP.
- **Fréquence des interruptions (en cas de violation d'hôte unique)** : définit la fréquence d'envoi des messages « trap » à l'hôte. Ce champ ne peut être défini que si plusieurs hôtes sont désactivés.

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

Affichage des hôtes authentifiés

Pour afficher des informations détaillées sur les utilisateurs authentifiés :

ÉTAPE 1 Cliquez sur **Sécurité** > **802.1X** > **Hôtes authentifiés**. La page *Hôtes authentifiés* s'affiche.

Cette page affiche les champs suivants :

- **Nom d'utilisateur** : nom des demandeurs authentifiés sur chaque port.
- **Port** : numéro du port.
- **Heure de session (JJ:HH:MM:SS)** : durée pendant laquelle le demandeur a été connecté au port.
- **Méthode d'authentification :** méthode utilisée pour l'authentification de la dernière session. Les options sont les suivantes :
  - *Aucun* : aucune authentification n'est appliquée ; l'autorisation est automatiquement accordée.
  - *RADIUS :* le demandeur a été authentifié par un serveur RADIUS.
- **Adresse MAC** : affiche l'adresse MAC du demandeur.

Prévention du déni de service

La prévention du *déni de service* (DoS) améliore la sécurité du réseau en empêchant les paquets présentant certains paramètres d'adresse IP de pénétrer dans le réseau.

SCT

Le commutateur Cisco est un commutateur avancé qui gère les types de trafic suivants, en plus du trafic de l'utilisateur final :

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

Le trafic non souhaité encombre le CPU et peut empêcher le commutateur de fonctionner normalement.

Le commutateur utilise la fonction Secure Core Technology (SCT) qui garantit que le commutateur reçoit et traite le trafic de gestion et de protocole, quel que soit le volume de trafic total reçu.

La fonction SCT est activée par défaut sur l'appareil et ne peut pas être désactivée.

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

La fonction SCT peut être contrôlée sur la page *Déni de service > Prévention du déni de service > Paramètres de la suite de sécurité* (bouton Détails).

Paramètres de la suite de sécurité de déni de service

REMARQUE Avant d'activer la prévention du déni de service (DoS), vous devez supprimer les liaisons de toutes les listes de contrôle d'accès (ACL, Access Control Lists) et stratégies de QoS avancées qui sont liées à un port. Les ACL et les stratégies de QoS avancées ne sont pas actives lorsque la protection contre le déni de service est activée sur un port.

Pour configurer les paramètres globaux de prévention du déni de service et contrôler la fonction SCT :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Paramètres de suite de sécurité**. La page *Paramètres de la suite de sécurité* s'affiche.

Mécanisme de protection CPU : Activé indique que la fonction SCT est activée.

ÉTAPE 2 Cliquez sur **Détails** en regard de **Utilisation du CPU** pour activer l'affichage des informations relatives à l'utilisation des ressources du CPU.

18

Utilisation de la fonction SSL

Cette section décrit la fonction Secure Socket Layer (SSL).

Elle contient les rubriques suivantes :

- **Présentation de SSL**
- **Configuration et paramètres par défaut**
- **Paramètres d'authentification de serveur SSL**

Présentation de SSL

La fonction Secure Socket Layer (SSL) permet d'ouvrir une session HTTPS sur l'appareil.

Une session HTTPS peut être ouverte avec le certificat par défaut qui est présent sur l'appareil.

Certains navigateurs génèrent des avertissements lors de l'utilisation d'un certificat par défaut, car ce certificat n'est pas signé par une autorité de certification (CA, Certification Authority). Il est recommandé d'utiliser un certificat signé par une CA de confiance.

Pour ouvrir une session HTTPS avec un certificat créé par l'utilisateur, procédez comme suit :

1. Générez un certificat.
2. Demandez que le certificat soit certifié par une CA.
3. Importez le certificat signé dans l'appareil.

Configuration et paramètres par défaut

Par défaut, le commutateur contient un certificat qui peut être modifié.

HTTPS est activé par défaut.

Paramètres d'authentification de serveur SSL

Il peut être nécessaire de générer un nouveau certificat pour remplacer le certificat par défaut présent sur l'appareil.

Pour créer un nouveau certificat, modifiez un certificat existant ou importez-en un :

ÉTAPE 1 Cliquez sur **Sécurité** > **Serveur SSL** > **Paramètres d'authentification de serveur SSL**. La page *Paramètres d'authentification de serveur SSL* s'affiche.

Les informations concernant les certificats 1 et 2 s'affichent dans la Table de clés de serveur SSL. Ces champs sont définis sur la page *Modifier*, excepté pour les champs suivants :

- **Valide du** : spécifie la date à partir de laquelle le certificat est valide.
- **Valide jusqu'au** : spécifie la date jusqu'à laquelle le certificat est valide.
- **Source du certificat** : spécifie si le certificat a été généré par le système (**Autogénéré**) ou l'utilisateur (**Défini par l'utilisateur**).

ÉTAPE 2 Sélectionnez un certificat actif.

ÉTAPE 3 Vous pouvez effectuer l'une des actions suivantes en cliquant sur le bouton approprié :

- **Modifier** : sélectionnez l'un des certificats et renseignez les champs suivants pour celui-ci :
  - **Regénérer une clé RSA** : sélectionnez-le pour regénérer la clé RSA.
  - **Longueur de clé** : entrez la longueur de la clé RSA à générer.
  - **Nom courant** : spécifie l'adresse IP ou l'URL complète de l'appareil. Si elle n'est pas indiquée, le système utilisera l'adresse IP la plus basse de l'appareil (lors de la génération du certificat).
  - **Unité organisationnelle** : spécifie l'unité organisationnelle ou le nom du service.

- **Nom de l'organisation** : spécifie le nom de l'organisation.
- **Lieu** : spécifie l'emplacement ou le nom de la ville.
- **État** : spécifie le nom de l'état ou de la province.
- **Pays** : spécifie le nom du pays.
- **Durée** : spécifie le nombre de jours de validité d'une certification.

▪ **Générer une demande de certificat** : générez une demande de certificat devant être signé par une CA.

- Renseignez les champs du certificat (identiques à ceux de la page *Modifier*).

ÉTAPE 4 Cliquez sur **Générer une demande de certificat**. Le système crée alors une clé qui doit être entrée dans la CA.

▪ **Importer un certificat** : une fois l'approbation reçue de la CA, entrez les éléments suivants :

- **ID de certificat** : sélectionnez le certificat actif.
- **Certificat** : copiez dans le certificat reçu.
- **Importer une paire de clés RSA** : sélectionnez cette option pour autoriser la copie dans la nouvelle paire de clés RSA.
- **Clé publique** : copiez dans la clé publique RSA.
- **Clé privée (chiffrée)** : sélectionnez et copiez dans la clé privée RSA sous forme chiffrée.
- **Clé privée (texte en clair)** : sélectionnez et copiez dans la clé privée RSA sous forme de texte en clair.
- **Afficher les données sensibles sous forme chiffrée** : cliquez sur ce bouton pour afficher cette clé sous forme chiffrée. Une fois que vous avez cliqué sur ce bouton, les clés privées sont écrites dans le fichier de configuration sous forme chiffrée (dès que vous cliquez sur **Appliquer**).

▪ **Détails** : affiche le certificat et la paire de clés RSA. Cela vous permet de copier le certificat et la paire de clés RSA vers un autre appareil (via la fonction copier/coller). Lorsque vous cliquez sur **Afficher les données sensibles sous forme chiffrée**, les clés privées apparaissent sous forme chiffrée.

ÉTAPE 5 Cliquez sur **Appliquer** pour appliquer les modifications dans la Configuration d'exécution.

19

Secure Sensitive Data

Secure Sensitive Data (SSD) est une architecture qui simplifie la protection des données confidentielles, comme les mots de passe et les clés, sur un appareil. Cette fonctionnalité utilise les mots de passe, le cryptage, le contrôle d'accès et l'authentification des utilisateurs afin de fournir une solution sécurisée pour la gestion des données confidentielles.

Elle a été étendue afin de protéger l'intégrité des fichiers de configuration, sécuriser le processus de configuration et prendre en charge la configuration automatique sans intervention SSD.

Introduction

SSD protège les données confidentielles présentes sur un appareil, telles que les mots de passe et les clés, autorise et refuse l'accès aux données confidentielles sous forme chiffrée et de texte en clair en fonction des informations d'identification de l'utilisateur et des règles SSD, mais protège également contre toute altération des fichiers de configuration contenant des données confidentielles.

En outre, SSD permet la sauvegarde et le partage sécurisés des fichiers de configuration qui contiennent des données confidentielles.

SSD offre aux utilisateurs la flexibilité de configurer le niveau de protection souhaité pour leurs données confidentielles ; à savoir aucune protection des données confidentielles sous forme de texte en clair, une protection minimale avec un cryptage basé sur le mot de passe par défaut ou une protection améliorée avec un cryptage basé sur le mot de passe défini par l'utilisateur.

SSD accorde une autorisation en lecture sur les données confidentielles uniquement aux utilisateurs authentifiés et autorisés, et conformément aux règles SSD. Un appareil authentifie et autorise l'accès de gestion pour les utilisateurs par l'intermédiaire du processus d'authentification des utilisateurs.

Que vous utilisiez ou non SSD, il est recommandé qu'un administrateur sécurise le processus d'authentification par l'intermédiaire de la base de données d'authentification locale, et/ou sécurise la communication vers le serveur d'authentification externe (RADIUS et TACACS) utilisé dans le processus d'authentification des utilisateurs.

En résumé, SSD protège les données sensibles sur un appareil à l'aide des règles SSD, des propriétés SSD et de l'authentification des utilisateurs. Et les règles SSD, les propriétés SSD et les configurations d'authentification des utilisateurs sur l'appareil sont elles-mêmes des données protégées par SSD.

Gestion de SSD

La gestion SSD inclut un ensemble de paramètres de configuration qui définissent le traitement et la sécurité des données confidentielles. Les paramètres de configuration SSD eux-mêmes sont des données confidentielles et sont protégés par SSD.

Toute la configuration de SSD s'effectue via les pages SSD qui sont uniquement disponibles pour les utilisateurs disposant des autorisations appropriées (reportez-vous à la section **Règles SSD**).

Règles SSD

Les règles SSD définissent les autorisations en lecture et le mode de lecture par défaut attribués à une session utilisateur sur un canal de gestion.

Une règle SSD est identifiée de manière unique par son utilisateur et le canal de gestion SSD. Il peut y avoir différentes règles SSD pour le même utilisateur mais pour différents canaux. Inversement, il peut y avoir différentes règles pour le même canal, mais pour différents utilisateurs.

Les autorisations en lecture déterminent la façon dont les données confidentielles peuvent être affichées : sous forme chiffrée uniquement, sous forme de texte en clair uniquement, sous forme chiffrée ou de texte en clair, ou aucune autorisation d'afficher les données confidentielles. Les règles SSD elles-mêmes sont protégées en tant que données confidentielles.

Un appareil peut prendre en charge un total de 32 règles SSD.

Un appareil accorde à un utilisateur l'autorisation en lecture SSD de la règle SSD qui correspond le mieux à l'identité/aux informations d'identification de l'utilisateur et au type de canal de gestion à partir duquel l'utilisateur accède ou accédera aux données confidentielles.

À l'origine, un appareil comporte un ensemble de règles SSD par défaut. Un administrateur peut ajouter, supprimer et modifier des règles SSD comme il le souhaite.

REMARQUE Il se peut qu'un appareil ne puisse pas prendre en charge tous les canaux définis par SSD.

Éléments d'une règle SSD

Une règle SSD inclut les éléments suivants :

- **Type d'utilisateur** : les types d'utilisateur pris en charge dans l'ordre de préférence (de la plus haute à la plus basse) sont les suivants : (Si un utilisateur correspond à plusieurs règles SSD, la règle avec le Type d'utilisateur ayant la préférence la plus haute sera appliquée).
  - **Spécifique** : la règle s'applique à un utilisateur spécifique.
  - **Utilisateur par défaut (cisco)** : la règle s'applique à l'utilisateur par défaut (cisco).
  - **Niveau 15** : la règle s'applique aux utilisateurs ayant le niveau de privilège 15.
  - **Tous** : la règle s'applique à tous les utilisateurs.
- **Nom d'utilisateur** : si le type d'utilisateur est Spécifique, un nom d'utilisateur est requis.
- **Canal** type de canal de gestion SSD auquel la règle s'applique. Les types de canaux pris en charge sont :
  - **Sécurisé** : spécifie que la règle s'applique uniquement aux canaux sécurisés. Un appareil peut prendre en charge une partie ou l'ensemble des canaux sécurisés suivants :

interface du port de console, SCP, SSH et HTTPS.

- **Non sécurisé** : spécifie que cette règle s'applique uniquement aux canaux non sécurisés. Un appareil peut prendre en charge une partie ou l'ensemble des canaux non sécurisés suivants :
  Telnet, TFTP et HTTP.
- **SNMP XML sécurisé** : spécifie que cette règle s'applique uniquement au XML sur HTTPS **[Sx300-500]** avec confidentialité. Un appareil est susceptible de ne pas prendre en charge tous les canaux XML et SNMP sécurisés.
- **SNMP XML non sécurisé** : spécifie que cette règle s'applique uniquement au XML sur HTTP **[Sx300-500]**/ sans confidentialité. Un appareil est susceptible de ne pas prendre en charge tous les canaux XML et SNMP sécurisés.

- **Autorisation en lecture** : autorisations en lecture associées aux règles. Elles peuvent être les suivantes :
  - (Basse) **Exclure** : les utilisateurs ne sont pas autorisés à accéder aux données confidentielles sous quelque forme que ce soit.
  - (Moyenne) **Chiffré uniquement** : les utilisateurs sont autorisés à accéder aux données confidentielles sous forme chiffrée uniquement.
  - (Haute) **Texte en clair uniquement** : les utilisateurs sont autorisés à accéder aux données confidentielles sous forme de texte en clair uniquement. Les utilisateurs sont également autorisés à accéder aux paramètres SSD en lecture et en écriture.
  - (Très haute) **Les deux** : les utilisateurs ont les autorisations Chiffré et Texte en clair, et sont autorisés à accéder aux données confidentielles sous forme chiffrée et de texte en clair. Les utilisateurs sont également autorisés à accéder aux paramètres SSD en lecture et en écriture.

Chaque canal de gestion permet des autorisations en lecture spécifiques. Elles sont récapitulées dans le tableau suivant.

Tableau 1 Autorisations en lecture permises par canal de gestion

Canal de gestion	Options d'autorisation en lecture permises
Sécurisé	Les deux, Chiffré uniquement
Non sécurisé	Les deux, Chiffré uniquement

Tableau 1 Autorisations en lecture permises par canal de gestion

Canal de gestion	Options d'autorisation en lecture permises
SNMP XML sécurisé	Exclure, Texte en clair uniquement
SNMP XML non sécurisé	Exclure, Texte en clair uniquement

- **Mode de lecture par défaut** : tous les modes de lecture par défaut sont sujets à l'autorisation en lecture de la règle. Les options suivantes sont disponibles, mais certaines sont susceptibles d'être refusées en fonction de l'autorisation en lecture. Si l'autorisation en lecture définie par l'utilisateur pour un utilisateur est Exclure (par exemple), et que le mode de lecture par défaut est Chiffré, l'autorisation en lecture définie par l'utilisateur s'applique.
  - **Exclure** : n'autorise pas la lecture des données confidentielles.
  - **Chiffré** : les données confidentielles sont présentées sous forme chiffrée.
  - **Texte en clair** : les données confidentielles sont présentées sous forme de texte en clair.

  Chaque canal de gestion permet des autorisations en lecture spécifiques. Elles sont récapitulées dans le tableau suivant.

Tableau 2 Modes de lecture par défaut pour les autorisations en lecture

Autorisation en lecture	Mode de lecture par défaut autorisé
Exclure	Exclure
Chiffré uniquement	*Chiffré
Texte en clair uniquement	*Texte en clair
Les deux	*Texte en clair, Chiffré

* Le mode de lecture d'une session peut être temporairement changé sur la page *Propriétés* SSD si le nouveau mode de lecture n'enfreint pas l'autorisation en lecture.

REMARQUE Notez les éléments suivants :

- Le mode de lecture par défaut pour les canaux de gestion SNMP XML sécurisé et SNMP XML non sécurisé doit être identique à leur autorisation en lecture.

- L'autorisation en lecture est uniquement permise pour les canaux de gestion SNMP XML sécurisé et SNMP XML non sécurisé ; l'autorisation n'est pas permise pour les canaux sécurisés et non sécurisés standard.
- L'exclusion des données confidentielles dans les canaux de gestion SNMP XML sécurisé et SNMP XML non sécurisé indique que les données confidentielles sont présentées en tant que 0 (ce qui signifie une chaîne nulle ou numérique 0). Si l'utilisateur souhaite afficher les données confidentielles, la règle doit être changée en texte en clair.
- Par défaut, un utilisateur SNMPv3 ayant des autorisations de canaux confidentiels et XML-over-secure est considéré comme un utilisateur de niveau 15.
- Les utilisateurs SNMP sur un canal SNMP et XML non sécurisé (SNMPv1, v2 et v3 sans confidentialité) sont considérés comme Tous les utilisateurs.
- Il doit toujours y avoir au moins une règle avec une autorisation en lecture : Texte en clair uniquement ou Les deux, car seuls les utilisateurs qui disposent de ces autorisations peuvent accéder aux pages SSD.
- Les changements apportés au mode de lecture par défaut et aux autorisations en lecture d'une règle deviennent effectifs et sont appliqués aux utilisateurs concernés et au canal de toutes les sessions de gestion actives immédiatement, à l'exclusion de la session qui effectue les changements même si la règle est applicable. Lorsqu'une règle est changée (ajout, suppression, modification), un système met à jour toutes les sessions CLI/GUI concernées.

  REMARQUE Lorsque la règle SSD appliquée lors de la connexion à une session est modifiée à partir de cette session, l'utilisateur doit se déconnecter puis se reconnecter pour voir la modification.

Règles SSD et authentification des utilisateurs

SSD accorde une autorisation SSD uniquement aux utilisateurs authentifiés et autorisés, et conformément aux règles SSD. Un appareil dépend de son processus d'authentification des utilisateurs pour authentifier et autoriser l'accès de gestion. Pour protéger un appareil et ses données contre tout accès non autorisé, y compris les données confidentielles et les configurations SSD, il est recommandé de sécuriser le processus d'authentification des utilisateurs. Pour sécuriser le processus d'authentification des utilisateurs, vous pouvez utiliser la base de données d'authentification locale, mais aussi sécuriser la communication via les serveurs d'authentification externes, tels que les serveurs RADIUS et TACACS. La configuration de la communication sécurisée vers les serveurs d'authentification externes constitue des données confidentielles et est protégée par SSD.

REMARQUE Les informations d'identification des utilisateurs contenues dans la base de données d'authentification locale sont déjà protégées par un mécanisme non lié à SSD.

Si un utilisateur présent sur un canal exécute une action qui utilise un autre canal, l'appareil applique l'autorisation en lecture et le mode de lecture par défaut à partir de la règle SSD qui correspond aux informations d'identification des utilisateurs et à l'autre canal. Par exemple, si un utilisateur se connecte via un canal sécurisé et démarre une session de chargement TFTP, l'autorisation en lecture SSD de l'utilisateur sur le canal non sécurisé (TFTP) est appliquée.

Règles SSD par défaut

Les règles par défaut suivantes sont définies pour l'appareil :

Tableau 3 Règles SSD par défaut

Clé de règle		Action de règle	
Utilisateur	Canal	Autorisation en lecture	Mode de lecture par défaut
Niveau 15	SNMP XML sécurisé	Texte en clair uniquement	Texte en clair
Niveau 15	Sécurisé	Les deux	Chiffré
Niveau 15	Non sécurisé	Les deux	Chiffré
Tous	SNMP XML non sécurisé	Exclure	Exclure

Tableau 3 Règles SSD par défaut

Clé de règle		Action de règle	
Utilisateur	Canal	Autorisation en lecture	Mode de lecture par défaut
Tous	Sécurisé	Chiffré uniquement	Chiffré
Tous	Non sécurisé	Chiffré uniquement	Chiffré

Il est possible de modifier les règles par défaut, mais pas de les supprimer. Si les règles par défaut SSD ont été modifiées, elles peuvent être restaurées.

Remplacement du mode de lecture par défaut SSD de la session

Le système affiche les données confidentielles dans une session, sous forme chiffrée ou de texte en clair, en fonction de l'autorisation en lecture et du mode de lecture par défaut de l'utilisateur.

Le mode de lecture par défaut peut être temporairement remplacé tant que cela n'occasionne pas de conflit avec l'autorisation en lecture SSD de la session. Cette modification est effective immédiatement dans la session actuelle, jusqu'à ce que l'un des événements suivants se produise :

- L'utilisateur le change à nouveau.
- La session est terminée.
- L'autorisation en lecture de la règle SSD qui est appliquée à l'utilisateur de la session est modifiée et n'est plus compatible avec le mode de lecture actuel de la session. Dans ce cas, le mode de lecture de la session redevient le mode de lecture par défaut de la règle SSD.

Propriétés SSD

Les propriétés SSD sont un ensemble de paramètres qui, conjointement avec les règles SSD, définissent et contrôlent l'environnement SSD d'un appareil. L'environnement SSD comporte les propriétés suivantes :

- Contrôle de la façon dont les données confidentielles sont chiffrées.
- Contrôle du niveau de sécurité sur les fichiers de configuration.

- Contrôle de la façon dont les données confidentielles sont affichées dans la session en actuelle.

Mot de passe

Le mot de passe constitue la base du mécanisme de sécurité dans la fonction SSD. Il permet de générer la clé de cryptage et de décryptage des données confidentielles. Les commutateurs Sx200, Sx300, Sx500 et SG500x qui ont le même mot de passe peuvent décrypter mutuellement leurs données confidentielles qui ont été cryptées avec la clé générée à partir du mot de passe.

Un mot de passe doit respecter les règles suivantes :

- **Longueur** : entre 8 et 16 caractères.
- **Classes de caractères** : le mot de passe doit comporter au moins un caractère en majuscule, un caractère en minuscule, un chiffre et un caractère spécial (# ou $, par exemple).

Mot de passe par défaut et mot de passe défini par l'utilisateur

Tous les appareils disposent d'un mot de passe par défaut qui est transparent pour les utilisateurs. Le mot de passe par défaut ne s'affiche jamais dans le fichier de configuration ou la CLI/GUI.

Pour bénéficier d'une meilleure sécurité et d'une meilleure protection, un administrateur doit configurer SSD sur un appareil, afin qu'il utilise un mot de passe défini par l'utilisateur au lieu du mot de passe par défaut. Un mot de passe défini par l'utilisateur doit être gardé secret pour que la sécurité des données confidentielles sur l'appareil ne soit pas compromise.

Un mot de passe défini par l'utilisateur peut être configuré manuellement sous forme de texte en clair. Il peut aussi être issu d'un fichier de configuration (reportez-vous à la section Configuration automatique sans intervention SSD). Un appareil affiche toujours sous forme chiffrée les mots de passe définis par l'utilisateur.

Mot de passe local

Un appareil conserve un mot de passe local qui est celui de sa configuration d'exécution. SSD effectue normalement le cryptage et le décryptage des données confidentielles avec la clé générée à partir du mot de passe local.

Le mot de passe local peut être configuré pour être le mot de passe par défaut ou un mot de passe défini par l'utilisateur. Par défaut, le mot de passe local et le mot de passe par défaut sont identiques. Il peut être changé via des actions d'administration à partir de l'interface de ligne de commande (si disponible) ou de l'interface Web. Il est automatiquement remplacé par le mot de passe figurant dans le fichier de Configuration de démarrage lorsque la configuration de démarrage devient la configuration active de l'appareil. Lorsqu'un appareil est réinitialisé à ses valeurs par défaut, le mot de passe local est réinitialisé au mot de passe par défaut.

Contrôle du mot de passe du fichier de configuration

Le contrôle du mot de passe du fichier constitue une protection supplémentaire pour un mot de passe défini par l'utilisateur, et les données confidentielles qui sont chiffrées avec la clé générée à partir du mot de passe défini par l'utilisateur, dans les fichiers de configuration textuels.

Les modes de contrôle du mot de passe existants sont indiqués ci-après :

- **Sans restriction** (par défaut) : l'appareil inclut son mot de passe lors de la création d'un fichier de configuration. Cela permet à tout appareil qui accepte le fichier de configuration d'apprendre le mot de passe à partir du fichier.
- **Restreint** : l'appareil empêche l'exportation de son mot de passe vers un fichier de configuration. Le mode Restreint protège les données confidentielles chiffrées présentes dans un fichier de configuration contre les appareils qui ne disposent pas de mot de passe. Ce mode doit être utilisé lorsqu'un utilisateur ne souhaite pas exposer le mot de passe dans un fichier de configuration.

Une fois qu'un appareil a été réinitialisé à ses valeurs par défaut, son mot de passe local est réinitialisé au mot de passe par défaut. Ainsi, l'appareil ne pourra plus décrypter les données confidentielles chiffrées à partir d'un mot de passe défini par l'utilisateur qui a été entré depuis une session de gestion (GUI/CLI), ou dans tout fichier de configuration avec le mode Restreint, y compris les fichiers créés par l'appareil lui-même avant qu'il ne soit réinitialisé à ses valeurs par défaut. Cette situation reste inchangée tant que l'appareil n'est pas manuellement reconfiguré avec le mot de passe défini par l'utilisateur ou qu'il n'apprend pas le mot de passe défini par l'utilisateur à partir d'un fichier de configuration.

Contrôle de l'intégrité du fichier de configuration

Un utilisateur peut protéger un fichier de configuration contre toute altération ou modification en créant le fichier de configuration avec le Contrôle de l'intégrité du fichier de configuration. Il est recommandé d'activer le Contrôle de l'intégrité du fichier de configuration lorsqu'un appareil utilise un mot de passe défini par l'utilisateur et que le Contrôle du mot de passe du fichier de configuration est défini sur Sans restriction.

ATTENTION Toute modification apportée à un fichier configuration dont l'intégrité est protégée est considérée comme une altération.

Un appareil détermine si l'intégrité d'un fichier de configuration est protégée en examinant la commande Contrôle de l'intégrité du fichier dans le bloc de contrôle SSD du fichier. Si la protection de l'intégrité est définie pour un fichier, mais qu'un appareil détecte que l'intégrité du fichier n'est pas intacte, l'appareil refuse le fichier. Sinon, le fichier est accepté pour traitement ultérieur.

Un appareil vérifie l'intégrité d'un fichier de configuration textuel lorsque le fichier est téléchargé ou copié vers le fichier de Configuration de démarrage.

Mode de lecture

Chaque session comporte un mode de lecture. Il détermine la façon dont les données confidentielles s'affichent. Le mode de lecture peut être Texte en clair, auquel cas les données confidentielles apparaissent en texte normal ou Chiffré, auquel cas les données confidentielles apparaissent sous forme chiffrée.

Fichiers de configuration

Un fichier de configuration contient la configuration d'un appareil. Un appareil comporte un fichier de Configuration d'exécution, un fichier de Configuration de démarrage, un fichier de Configuration miroir (facultatif) et un fichier de Configuration de secours. Un utilisateur peut charger et télécharger un fichier de configuration de et vers un serveur de fichiers distant. Un appareil peut télécharger automatiquement sa configuration de démarrage à partir d'un serveur de fichiers distant pendant l'étape de configuration automatique via DHCP. Les fichiers de configuration stockés sur des serveurs de fichiers distants sont appelés des fichiers de configuration à distance.

Un fichier de Configuration d'exécution contient la configuration actuellement utilisée par un appareil. La configuration dans un fichier de Configuration de démarrage devient la configuration d'exécution une fois le redémarrage effectué. Les fichiers de Configuration d'exécution et de Configuration de démarrage ont un format interne. Les fichiers de Configuration miroir, de secours et à distance sont des fichiers textuels qui sont généralement stockés à des fins d'archivage, d'enregistrement ou de récupération. Lors de la copie, du chargement et du téléchargement d'un fichier de configuration source, un appareil convertit automatiquement le contenu source dans le format du fichier de destination si les deux fichiers ont un format différent.

Indicateur SSD de fichier

Lors de la copie du fichier de Configuration d'exécution ou de démarrage dans un fichier de configuration textuel, l'appareil génère et place l'indicateur SSD de fichier dans le fichier de configuration textuel pour indiquer si le fichier contient des données confidentielles sous forme chiffrée, des données confidentielles sous forme de texte en clair, ou s'il exclut les données confidentielles.

- L'indicateur SSD, s'il existe, doit se trouver dans le fichier d'en-tête de configuration.
- Une configuration textuelle qui n'inclut pas d'indicateur SSD ne contient normalement pas de données confidentielles.
- L'indicateur SSD permet d'appliquer les autorisations en lecture SSD à des fichiers de configuration textuels, mais il est ignoré lors de la copie des fichiers de configuration vers le fichier de Configuration d'exécution ou de démarrage.

L'indicateur SSD dans un fichier est défini conformément à l'instruction de l'utilisateur, au cours de la copie, pour inclure les données confidentielles sous forme chiffrée ou de texte en clair, ou exclure les données confidentielles d'un fichier.

Bloc de contrôle SSD

Lorsqu'un appareil crée un fichier de configuration textuel à partir de son fichier de Configuration de démarrage ou d'exécution, il insère un bloc de contrôle SSD dans le fichier si un utilisateur demande que le fichier doit inclure les données confidentielles. Le bloc de contrôle SSD, qui est protégé contre toute altération, contient les règles SSD et les propriétés SSD de l'appareil qui crée le fichier. Un bloc de contrôle SSD commence et finit respectivement avec « ssd-control-start » et « ssd-control-end ».

Fichier de Configuration de démarrage

L'appareil prend actuellement en charge la copie depuis les fichiers de Configuration d'exécution, de secours, miroir et à distance vers un fichier de Configuration de démarrage. Les configurations définies dans la configuration de démarrage sont effectives et deviennent la configuration d'exécution une fois le redémarrage effectué. Un utilisateur peut récupérer les données confidentielles sous forme chiffrée ou de texte en clair à partir d'un fichier de Configuration de démarrage, sujet à l'autorisation en lecture SSD et au mode de lecture SSD actuel de la session de gestion.

L'accès en lecture aux données confidentielles dans la configuration de démarrage sous toutes ses formes est exclu si le mot de passe défini dans le fichier de Configuration de démarrage diffère du mot de passe local.

SSD ajoute les règles suivantes lors de la copie des fichiers de Configuration de secours, miroir et à distance vers le fichier de Configuration de démarrage :

- Une fois qu'un appareil a été réinitialisé à ses valeurs par défaut, toutes ses configurations y compris les règles et les propriétés SSD sont réinitialisées à leurs valeurs par défaut.
- Si un fichier de configuration source contient des données confidentielles chiffrées, mais pas de bloc de contrôle SSD, l'appareil refuse le fichier source et la copie échoue.
- S'il n'y a pas de bloc de contrôle SSD dans le fichier de configuration source, la configuration SSD définie dans le fichier de Configuration de démarrage est réinitialisée à ses valeurs par défaut.
- Si un mot de passe est présent dans le bloc de contrôle SSD du fichier de configuration source, l'appareil refuse le fichier source, et la copie échoue s'il y a des données confidentielles chiffrées dans le fichier qui ne sont pas chiffrées par la clé générée à partir du mot de passe dans le bloc de contrôle SSD.

- S'il y a un bloc de contrôle SSD dans le fichier de configuration source et que le fichier échoue lors du contrôle d'intégrité SSD et/ou lors du contrôle d'intégrité du fichier, l'appareil refuse le fichier source et la copie échoue.
- S'il n'y a aucun mot de passe dans le bloc de contrôle SSD du fichier de configuration source, toutes les données confidentielles chiffrées dans le fichier doivent être chiffrées soit par la clé générée à partir du mot de passe local, soit par la clé générée à partir du mot de passe par défaut, mais pas par les deux. Sinon, le fichier source est refusé et la copie échoue.
- L'appareil configure le mot de passe, le contrôle du mot de passe et l'intégrité du fichier le cas échéant à partir du bloc de contrôle SSD dans le fichier de configuration source vers le fichier de Configuration de démarrage. Il configure le fichier de Configuration de démarrage avec le mot de passe qui est utilisé pour générer la clé permettant de décrypter les données confidentielles dans le fichier de configuration source. Toutes les configurations SSD introuvables sont réinitialisées à leurs valeurs par défaut.
- S'il y a un bloc de contrôle SSD dans le fichier de configuration source et que le fichier contient des données confidentielles sous forme de texte en clair, à l'exclusion des configurations SSD dans le bloc de contrôle SSD, le fichier est accepté.

Fichier de Configuration d'exécution

Un fichier de Configuration d'exécution contient la configuration actuellement utilisée par l'appareil. Un utilisateur peut récupérer les données confidentielles sous forme chiffrée ou de texte en clair à partir d'un fichier de Configuration d'exécution, sujet à l'autorisation en lecture SSD et au mode de lecture SSD actuel de la session de gestion. L'utilisateur peut changer la configuration d'exécution en copiant les fichiers de Configuration de secours ou miroir, à travers d'autres actions de gestion via CLI, XML, [Sx300-500]etc.

Un appareil applique les règles suivantes lorsqu'un utilisateur change directement la configuration SSD dans la configuration d'exécution :

- Si l'utilisateur qui a ouvert la session de gestion ne dispose pas des autorisations SSD (à savoir les autorisations en lecture Les deux ou Texte en clair uniquement), l'appareil refuse toutes les commandes SSD.
- En cas de copie à partir d'un fichier source, l'indicateur SSD de fichier, l'intégrité du bloc de contrôle SSD et l'intégrité du fichier SSD ne sont ni vérifiés ni appliqués.

- En cas de copie à partir d'un fichier source, la copie échoue si le mot de passe contenu dans le fichier source est sous forme de texte en clair. Si le mot de passe est chiffré, il est ignoré.
- Lors de la configuration directe du mot de passe (pas de copie de fichier), dans la configuration d'exécution, le mot de passe contenu dans la commande doit être saisi sous forme de texte en clair. Sinon, la commande est refusée.
- Les commandes de configuration contenant des données confidentielles chiffrées, qui sont chiffrées avec la clé générée à partir du mot de passe local, sont configurées dans la configuration d'exécution. Sinon, la commande de configuration échoue et n'est pas intégrée au fichier de Configuration d'exécution.

Fichier de configuration de secours et miroir

Un appareil génère fréquemment son fichier de Configuration miroir à partir du fichier de Configuration de démarrage si le service de configuration miroir automatique est activé. Un appareil génère toujours un fichier de Configuration miroir avec des données confidentielles chiffrées. Par conséquent, l'indicateur SSD de fichier dans un fichier de Configuration miroir indique toujours que le fichier contient des données confidentielles chiffrées.

Par défaut, le service de configuration miroir automatique est activé. Pour activer ou désactiver la configuration miroir automatique, cliquez sur **Administration > Gestion de fichiers > Propriétés des fichiers de configuration**.

Un utilisateur peut afficher, copier et charger les fichiers complets de Configuration miroir et de secours, sujets à l'autorisation en lecture SSD, au mode de lecture actuel dans la session et à l'indicateur SSD de fichier dans le fichier source comme suit :

- S'il n'y a pas d'indicateur SSD de fichier dans un fichier de Configuration miroir ou de secours, tous les utilisateurs sont autorisés à accéder au fichier.
- Un utilisateur disposant de l'autorisation en lecture Les deux peut accéder à tous les fichiers de Configuration miroir et de secours. Toutefois, si le mode de lecture actuel de la session est différent de l'indicateur SSD de fichier, l'utilisateur reçoit un message indiquant que cette action n'est pas autorisée.

- Un utilisateur disposant de l'autorisation Texte en clair uniquement peut accéder aux fichiers de Configuration miroir et de secours si leur indicateur SSD de fichier affiche les données confidentielles Exclure ou Texte en clair uniquement.
- Un utilisateur disposant de l'autorisation Chiffré uniquement peut accéder aux fichiers de Configuration miroir et de secours si leur indicateur SSD de fichier affiche les données confidentielles Exclure ou Chiffré.
- Un utilisateur disposant de l'autorisation Exclure ne peut pas accéder aux fichiers de Configuration miroir et de secours si leur indicateur SSD de fichier affiche les données confidentielles Chiffré ou Texte en clair.

L'utilisateur ne doit pas changer manuellement l'indicateur SSD de fichier en cas de conflit (le cas échéant) avec les données confidentielles dans le fichier. Sinon, les données confidentielles sous forme de texte en clair peuvent être exposées de manière inattendue.

Configuration automatique sans intervention des données confidentielles

La configuration automatique sans intervention SSD est la configuration automatique des appareils cible contenant des données confidentielles. Elle ne nécessite pas de préconfigurer manuellement les appareils cible avec le mot de passe dont la clé permet de crypter les données confidentielles.

L'appareil prend actuellement en charge la Configuration automatique, qui est activée par défaut. Lorsque la Configuration automatique est activée sur un appareil et que l'appareil reçoit les options DHCP qui spécifient un serveur de fichiers et un fichier de démarrage, l'appareil télécharge le fichier de démarrage (fichier de configuration à distance) dans le fichier de Configuration de démarrage à partir d'un serveur de fichiers, puis redémarre.

> **REMARQUE** Le serveur de fichiers peut être spécifié par les champs bootp siaddr et sname, ainsi que l'option DHCP 150 et statiquement configuré sur l'appareil.

L'utilisateur peut en toute sécurité configurer automatiquement les appareils cible contenant des données confidentielles, en créant d'abord le fichier de configuration qui doit être utilisé dans la configuration automatique à partir d'un appareil qui contient les configurations. L'appareil doit être configuré et défini pour :

- Crypter les données confidentielles dans le fichier

- Assurer l'intégrité du contenu du fichier
- Inclure les règles SSD et les commandes de configuration d'authentification sécurisées qui contrôlent et sécurisent correctement l'accès aux appareils et aux données confidentielles

Si le fichier de configuration a été généré avec un mot de passe utilisateur et que le contrôle du mot de passe du fichier SSD est Restreint, le fichier de configuration qui en résulte peut être configuré automatiquement pour les appareils cible souhaités. Néanmoins, pour que la configuration automatique réussisse avec un mot de passe défini par l'utilisateur, les appareils cible doivent être préconfigurés manuellement avec le même mot de passe que celui de l'appareil qui génère les fichiers, ce qui ne correspond donc pas à une configuration sans intervention.

Si l'appareil qui crée le fichier de configuration est défini sur le mode de contrôle du mot de passe Sans restriction, l'appareil inclut le mot de passe dans le fichier. Par conséquent, l'utilisateur peut configurer automatiquement les appareils cible, y compris les appareils neufs ou définis à leurs paramètres par défaut, avec le fichier de configuration sans devoir manuellement préconfigurer les appareils cible avec le mot de passe. Il s'agit là d'une configuration sans intervention, car les appareils cible apprennent le mot de passe directement à partir du fichier de configuration.

Canaux de gestion SSD

Les appareils peuvent être gérés via des canaux de gestion comme telnet, SSH et web. SSD classe les canaux en différentes types en fonction de leur sécurité et/ou leurs protocoles : sécurisé, non sécurisé, SNMP XML sécurisé et SNMP XML non sécurisé.

Le tableau suivant indique si chaque canal de gestion est considéré par SSD comme sécurisé ou non sécurisé. S'il est non sécurisé, le tableau indique le canal sécurisé parallèle.

Sécurité des canaux de gestion

Canaux de gestion

Canal de gestion	Type de canal de gestion SSD	Canal de gestion sécurisé parallèle
GUI/HTTP	Non sécurisé	GUI/HTTPS
GUI/HTTPS	Sécurisé	
XML/HTTP	SNMP XML non sécurisé	XML/HTTPS
XML/HTTPS	SNMP XML sécurisé	
TFTP	Non sécurisé	[Sx300-500]
Transfert de fichier basé sur HTTP	Non sécurisé	Transfert de fichier basé sur HTTPS
Transfert de fichier basé sur HTTPS	Sécurisé	

Interface de ligne de commande (CLI) et récupération du mot de passe

L'interface de ligne de commande (CLI) est uniquement accessible aux utilisateurs dont les autorisations en lecture sont Les deux ou Texte en clair uniquement. Les autres utilisateurs n'y ont pas accès. Les données confidentielles contenues dans l'interface de ligne de commande (CLI) s'affichent toujours sous forme de texte en clair.

La récupération du mot de passe est actuellement activée à partir du menu de démarrage et permet à l'utilisateur de se connecter au terminal sans authentification. Si SSD est pris en charge, cette option est uniquement autorisée lorsque le mot de passe local est identique au mot de passe par défaut. Si un appareil est configuré avec un mot de passe défini par l'utilisateur, l'utilisateur ne peut pas activer la récupération du mot de passe.

Configuration de SSD

La configuration de la fonction SSD est décrite aux pages suivantes :

- Vous pouvez définir les propriétés SSD sur la page *Propriétés*.
- Vous pouvez définir les règles SSD sur la page *Règles SSD*.

Propriétés SSD

Seuls les utilisateurs qui disposent de l'autorisation en lecture SSD Texte en clair uniquement ou Les deux sont autorisés à définir les propriétés SSD.

Pour définir les propriétés SSD globales :

ÉTAPE 1 Cliquez sur **Sécurité** > **Gestion sécurisée des données confidentielles** > **Propriétés**. La page *Propriétés* apparaît. Le champ suivant est affiché :

- **Type de mot de passe local actuel** : indique si le mot de passe par défaut ou un mot de passe défini par l'utilisateur est actuellement utilisé.

ÉTAPE 2 Renseignez les champs **Paramètres persistants** suivants :

- **Contrôle du mot de passe du fichier de configuration** : sélectionnez une option, comme indiqué à la section **Contrôle du mot de passe du fichier de configuration**.
- **Contrôle de l'intégrité du fichier de configuration** : sélectionnez cette fonction pour l'activer. Reportez-vous à la section **Contrôle de l'intégrité du fichier de configuration**.

ÉTAPE 3 Sélectionnez un mode de lecture pour la session actuelle (reportez-vous à **Éléments d'une règle SSD**).

Pour changer le mot de passe local :

ÉTAPE 4 Cliquez sur **Modifier le mot de passe local**, puis entrez un nouveau **Mot de passe local** :

- **Par défaut** : utilisez le mot de passe par défaut de l'appareil.
- **Défini par l'utilisateur (texte en clair)** : saisissez et confirmez un nouveau mot de passe.

Règles SSD

Seuls les utilisateurs qui disposent de l'autorisation en lecture SSD Texte en clair uniquement ou Les deux sont autorisés à définir les règles SSD.

Pour configurer les règles SSD :

ÉTAPE 1 Cliquez sur **Sécurité** > **Gestion sécurisée des données confidentielles** > **Règles SSD**. La page *Règles SSD* apparaît.

Les règles actuellement définies sont affichées.

ÉTAPE 2 Pour ajouter une nouvelle règle, cliquez sur **Ajouter**. Renseignez les champs suivants :

- **Utilisateur** : définit le ou les utilisateurs auxquels la règle s'applique : Sélectionnez une des options suivantes :
  - *Utilisateur spécifique* : sélectionnez et entrez le nom d'utilisateur spécifique auquel cette règle s'applique (cet utilisateur ne doit pas nécessairement être défini).
  - *Utilisateur par défaut (cisco)* : indique que cette règle s'applique à l'utilisateur par défaut.
  - *Niveau 15* : indique que cette règle s'applique à tous les utilisateurs ayant le niveau de privilège 15.
  - *Tous* : indique que cette règle s'applique à tous les utilisateurs.
- **Canal** : définit le niveau de sécurité du canal d'entrée auquel la règle s'applique : Sélectionnez une des options suivantes :
  - *Sécurisé* : indique que cette règle s'applique uniquement aux canaux sécurisés (console, [Sx300-500]SSH et HTTPS), mais pas les canaux[Sx300-500] XML.
  - *Non sécurisé* : indique que cette règle s'applique uniquement aux canaux non sécurisés (Telnet, TFTP et HTTP), mais pas aux canaux [Sx300-500] XML.
  - *SNMP XML sécurisé* : indique que cette règle s'applique uniquement au XML sur HTTPS [Sx300-500] avec confidentialité.
  - *SNMP XML non sécurisé* : indique que cette règle s'applique uniquement au XML sur HTTP ou [Sx300-500] sans confidentialité.

- **Autorisation en lecture** : autorisations en lecture associées aux règles. Elles peuvent être les suivantes :
  - *Exclure* : autorisation en lecture la plus basse. Les utilisateurs ne sont pas autorisés à accéder aux données confidentielles sous quelque forme que ce soit.
  - *Texte en clair uniquement* : autorisation en lecture de niveau plus élevé que la précédente. Les utilisateurs sont autorisés à accéder aux données confidentielles sous forme de texte en clair uniquement.
  - *Chiffré uniquement* : autorisation en lecture de niveau moyen. Les utilisateurs sont autorisés à accéder aux données confidentielles sous forme chiffrée uniquement.
  - *Les deux (Texte en clair et Chiffré)* : autorisation en lecture la plus haute. Les utilisateurs ont les autorisations Chiffré et Texte en clair, et sont autorisés à accéder aux données confidentielles sous forme chiffrée et de texte en clair.
- **Mode de lecture par défaut** : tous les modes de lecture par défaut sont sujets à l'autorisation en lecture de la règle. Les options suivantes sont disponibles, mais certaines sont susceptibles d'être refusées en fonction de l'autorisation en lecture de la règle.
  - *Exclure* : n'autorise pas la lecture des données confidentielles.
  - *Chiffré* : les données confidentielles sont présentées sous forme chiffrée.
  - *Texte en clair* : les données confidentielles sont présentées sous forme de texte en clair.

ÉTAPE 3 Les actions suivantes peuvent être effectuées :

- **Restaurer les valeurs par défaut** : rétablit les valeurs d'origine d'une règle par défaut qui a été modifiée par l'utilisateur.
- **Restaurer toutes les règles par défaut** : rétablit les valeurs d'origine de toutes les règles par défaut qui ont été modifiées par l'utilisateur et supprime toutes les règles définies par l'utilisateur.

20

Configuration de la QoS (Qualité de service)

La fonction QoS (Quality of Service, qualité de service) est appliquée à l'ensemble du réseau pour garantir que le trafic réseau est géré en fonction des critères fixés et que les données voulues reçoivent un traitement préférentiel.

Cette rubrique aborde les points suivants :

- **Fonctions et composants QoS**
- **Configuration de la QoS - Général**
- **Gestion des statistiques de QoS**

Fonctions et composants QoS

La fonction QoS permet d'optimiser les performances du réseau.

La QoS fournit les éléments suivants :

- Classification du trafic entrant en différentes classes sur la base d'attributs, notamment :
  - Configuration du périphérique
  - Interface d'entrée
  - Contenu des paquets
  - Combinaison de ces attributs

La QoS inclut :

- **Classification du trafic** : permet de marquer chaque paquet entrant comme appartenant à un flux de trafic spécifique, sur la base du contenu de ce paquet et/ou du port. Cette classification est réalisée à l'aide d'une ACL (Access Control List, liste de contrôle d'accès). Seul le trafic répondant aux critères d'ACL est soumis à la classification CoS ou QoS.
- **Affectation à des files d'attente matérielles** — Affecte les paquets entrants à des files d'attente de transfert. Les paquets sont envoyés à une file d'attente particulière pour gestion en tant que fonction de la classe de trafic à laquelle ils appartiennent.
- **Autre attribut de gestion de classe de trafic** — Applique des mécanismes QoS à diverses classes, y compris la gestion de bande passante.

Fonctionnement de QoS

Lors de l'utilisation de la fonction QoS, tout le trafic d'une même classe reçoit un traitement identique, à savoir l'action unique de QoS consistant à déterminer la file d'attente de sortie sur le port de sortie, ceci sur la base de la valeur QoS indiquée dans la trame entrante. En mode Layer 2, il s'agit de la valeurVPT (VLAN Priority Tag, balise de priorité de VLAN)802.1p. En mode Layer 3, le système utilise la valeur DSCP (Differentiated Service Code Point, point de code de service différencié) pour IPv4 et la valeurTC (Traffic Class, classe de trafic) pour IPv6. Lorsqu'il fonctionne en mode De base, le commutateur fait confiance à cette valeur de QoS affectée en externe. La valeur de QoS affectée en externe à un paquet détermine sa classe de trafic et la QoS.

Vous pouvez entrer le type de champ d'en-tête de confiance sur la page *Paramètres globaux*. Pour chaque valeur de ce champ, une file d'attente de sortie est désignée, indiquant la file d'attente choisie pour l'envoi de la trame sur la page *CoS/802.1p vers file d'attente* ou la page *DSCP vers file d'attente* (selon que le mode de confiance choisi est CoS/802.1p ou DSCP).

Flux de travail de QoS

Pour définir les paramètres de QoS généraux, procédez comme suit :

ÉTAPE 1 Activez QoS dans la page *Propriétés QoS* pour sélectionner le mode de confiance. Activez ensuite QoS sur les ports dans la page *Paramètres d'interface*.

ÉTAPE 2 Attribuez à chaque interface une priorité CoS ou DSCP par défaut, via la page *Propriétés de QoS*.

ÉTAPE 3 Attribuez une méthode de planification (Priorité stricte ou WRR) et une valeur d'allocation de bande passante WRR aux files d'attente de sortie, via la page *File d'attente*.

ÉTAPE 4 Désignez une file d'attente de sortie pour chaque valeur IP DSCP/TC sur la page *DSCP vers file d'attente*. Si le commutateur fonctionne en mode de confiance DSCP, les paquets entrants sont placés dans les files d'attente de sortie en fonction de leur valeurDSCP/TC.

ÉTAPE 5 Associez une file d'attente de sortie à chaque prioritéCoS/802.1p. Si le commutateur fonctionne en mode de confiance CoS/802.1, tous les paquets entrants sont placés dans les files d'attente de sortie prévues en fonction de la priorité CoS/802.1 des paquets. Pour ce faire, utilisez la page *CoS/802.1p vers file d'attente*.

ÉTAPE 6 Saisissez les limites de bande passante et de débit dans les pages suivantes :

a. Définissez le lissage en sortie pour chaque file d'attente sur la page *Modelage de sortie par file d'attente.*

b. Définissez la limite de vitesse d'entrée et le taux de modelage en sortie pour chaque port sur la page *Bande passante.*

Configuration de la QoS - Général

La rubrique *Propriétés de QoS* contient des champs permettant d'activer QoS et de sélectionner le mode de confiance à utiliser. En outre, vous pouvez définir la priorité CoS ou la valeur DSCP par défaut de chaque interface.

Configuration des propriétés QoS

Pour activer QoS :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Propriétés de QoS**. La page *Propriétés de QoS* s'affiche.

ÉTAPE 2 Activez QoS sur le commutateur.

ÉTAPE 3 Sélectionnez un mode de confiance (CoS/802.1p ou DSCP), puis cliquez sur **Appliquer**.

ÉTAPE 4 Si vous avez sélectionné DSCP, passez à l'**ÉTAPE 6** ; si vous avez sélectionné CoS, procédez à l'étape suivante :

ÉTAPE 5 Sélectionnez **Port/LAG** et cliquez sur **Ok** pour afficher/modifier tous les ports/LAG sur le périphérique ainsi que leurs informations de CoS.

Les champs suivants sont affichés pour tous les ports/LAG :

- **Interface** — Type de l'interface.
- **CoS par défaut** — Valeur VPT par défaut pour les paquets entrants qui ne possèdent pas de balise VLAN. La valeur CoS par défaut est 0. Elle s'applique uniquement aux trames non balisées si *CoS de confiance* est sélectionné.

Sélectionnez **Restaurer les valeurs par défaut** pour rétablir le paramètre de CoS par défaut défini en usine pour cette interface.

ÉTAPE 6 Cliquez sur **Table de substitution DSCP** pour saisir les valeurs DSCP. La *Table de substitution DSCP* s'affiche.

ÉTAPE 7 DSCP en entrée affiche la valeur DSCP du paquet entrant qui doit à nouveau être marqué d'une autre valeur. Sélectionnez la nouvelle valeur DSCP qui remplacera la valeur entrante.

Sélectionnez Restaurer les valeurs par défaut pour restaurer les valeurs DSCP d'origine.

ÉTAPE 8 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Pour définir une QoS sur une interface, sélectionnez-la et cliquez sur **Modifier**. La page *Modifier la configuration CoS de l'interface* s'affiche.

ÉTAPE 1 Saisissez les paramètres.

- **Interface :** sélectionnez le port ou LAG.
- **CoS par défaut** — Sélectionnez la valeur de CoS (Class-of-Service, classe de service) à affecter aux paquets entrants qui ne possèdent pas de baliseVLAN. La plage valide va de 0 à 7.

ÉTAPE 2 Cliquez sur **Appliquer**. La valeur CoS par défaut de l'interface est écrite dans le fichier de Configuration d'exécution.

Paramètres QoS de l'interface

La page *Paramètres d'interface* vous permet de configurer la QoS sur chaque port du commutateur, comme suit :

QoS désactivée sur l'interface — Tout le trafic entrant sur le port est mappé sur la file d'attente Meilleur effort (Best effort) et aucune classification/attribution de priorité n'est effectuée.

QoS activée sur le port — Le trafic d'entrée sur le port reçoit un ordre de priorité qui dépend du mode de confiance configuré à l'échelle du système, à savoir CoS/802.1p ou DSCP.

Pour entrer les paramètres de QoS de chaque interface :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Paramètres d'interface**. La page *Paramètres d'interface* s'affiche.

ÉTAPE 2 Sélectionnez **Port** ou **LAG** pour afficher la liste des ports ou LAG.

La liste des ports/LAG s'affiche. **État deQoS** indique si la QoS est activée sur l'interface.

ÉTAPE 3 Sélectionnez une interface et cliquez sur **Modifier**. La page *Modifier les paramètres d'interface de QoS* s'affiche.

ÉTAPE 4 Sélectionnez le **port** ou l'interface **LAG**.

ÉTAPE 5 Cliquez pour activer ou désactiver l'**état de QoS** pour cette interface.

ÉTAPE 6 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Configuration de files d'attente de QoS

Le commutateur prend en charge quatre files d'attente pour chaque interface. La file d'attente numéro quatre est celle qui dispose de la priorité la plus élevée. La file d'attente numéro un est celle dont la priorité est la plus faible.

Il existe deux façons de déterminer le mode de gestion du trafic dans les files d'attente : Priorité stricte et WRR (Weighted Round Robin, technique du tourniquet pondéré).

Priorité stricte — Le trafic sortant émanant de la file d'attente de priorité la plus élevée est transmis en premier. Le trafic des files d'attente de priorité(s) plus faible(s) n'est traité qu'après transmission des files d'attente de priorité(s) supérieure(s), ce qui donne le niveau de priorité le plus élevé au trafic de la file d'attente portant le numéro le plus élevé.

Weighted Round Robin (WRR) — En mode WRR, le nombre de paquets envoyés depuis la file d'attente est proportionnel à la pondération de cette file d'attente (plus la pondération est élevée, plus le nombre de trames transmises est important). Par exemple, si les quatre files d'attente sont toutes de type WRR et que les pondérations par défaut sont appliquées, la file d'attente 1 reçoit 1/15 de la bande passante (en supposant que toutes les files d'attente sont saturées et qu'il y a encombrement), la file d'attente 2 en reçoit 2/15, la file d'attente 3 en reçoit 4/15 et la file d'attente 4 reçoit 8/15 de la bande passante. Le type d'algorithme WRR utilisé sur le périphérique n'est pas l'algorithme standard DWRR (Deficit WRR, WRR avec déficit) mais l'algorithme SDWRR (Shaped Deficit WRR, WRR avec déficit lissé).

Vous pouvez sélectionner les modes de mise en file d'attente sur la page *File d'attente.* Lorsque la mise en file d'attente se fait par priorité stricte, l'ordre de priorité définit l'ordre de traitement des files d'attente, en commençant par la file d'attente4 (celle dont la priorité est la plus élevée), puis en passant à la file d'attente de niveau immédiatement inférieur à la fin du traitement de chaque file.

Lorsque la mise en file d'attente est de type WRR (Weighted Round Robin), chaque file d'attente est traitée jusqu'à ce que son quota soit atteint. Le système passe ensuite à une autre file d'attente.

Il est également possible d'affecter une WRR à certaines des files d'attente de priorité plus faible tout en maintenant le traitement Priorité stricte pour des files d'attente de niveau(x) plus élevé(s). Dans ce cas, le trafic des files d'attente à priorité stricte est toujours envoyé avant celui des files d'attente WRR. Le trafic des files d'attente WRR n'est transféré que lorsque les files d'attente à priorité stricte sont vides. (La portion relative en provenance de chaque file d'attente WRR dépend de sa pondération.)

Pour sélectionner la méthode de priorité et entrer les données WRR :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **File d'attente**. La page *File d'attente* apparaît.

ÉTAPE 2 Saisissez les paramètres.

- **File d'attente** — Affiche le numéro de la file d'attente.
- **Méthode de planification :** Sélectionnez une des options suivantes :
  - *Priorité stricte* — La planification du trafic de la file d'attente sélectionnée et de toutes les files d'attentes supérieures est strictement basée sur la priorité de chaque file d'attente.
  - *WRR* — La planification du trafic de la file d'attente sélectionnée se base sur une WRR. Chaque période est divisée entre les files d'attente WRR qui ne sont pas vides (celles qui ont des descripteurs de sortie). Ceci ne s'applique que lorsque les files d'attente à priorité stricte sont vides.
  - *Pondération WRR* — Si vous choisissez WRR, saisissez la pondérationWRR attribuée à la file d'attente.
  - *% de bande passante WRR* — Affiche la quantité de bande passante affectée à la file d'attente. Ces valeurs représentent un pourcentage de la pondération WRR.

ÉTAPE 3 Cliquez sur **Appliquer**. Les files d'attente sont configurées et le fichier de Configuration d'exécution est mis à jour.

Mappage CoS/802.1p vers une file d'attente

La page *CoS/802.1p vers file d'attente* mappe des priorités 802.1p sur des files d'attente de sortie. La table CoS/802.1p vers file d'attente détermine les files d'attente de sortie des paquets entrants sur la base de la priorité 802.1p figurant dans leurs balisesVLAN. Pour les paquets entrants non balisés, la priorité 802.1p utilisée est la prioritéCoS/802.1p par défaut affectée aux ports d'entrée.

Files d'attente de mappage par défaut

Valeurs 802.1p (0 à 7, 7 étant la valeur la plus élevée)	File d'attente (4 files numérotées de 1 à 4, 4 étant la priorité la plus élevée)	File d'attente (2 files d'attente : Normal et Élevé)	Notes
0	1	Normal	À l'arrière-plan
1	1	Normal	Meilleur effort (Best effort)
2	2	Normal	Excellent effort
3	3	Normal	Application critique SIP pour téléphone LVS
4	3	Normal	Vidéo
5	4	Élevée	Voix Valeur par défaut de téléphone IP Cisco
6	4	Élevée	Contrôle de l'interfonctionnement RTP pour téléphone LVS
7	4	Élevée	Contrôle du réseau

En modifiant le mappage CoS/802.1p à file d'attente, la méthode de planification des files d'attente ainsi que l'allocation de la bande passante, il est possible d'obtenir la qualité de service voulue sur un réseau.

Le mappage CoS/802.1p vers file d'attente est applicable seulement si le mode de confiance est CoS/802.1p et que les paquets appartiennent à des flux CoS de confiance.

La file d'attente 1 a la plus basse priorité et la file d'attente 4 a la plus haute priorité.

Pour mapper des valeurs de CoS sur des files d'attente de sortie :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **CoS/802.1p vers file d'attente**. La page *CoS/802.1p vers file d'attente* s'affiche.

ÉTAPE 2 Saisissez les paramètres.

- **802.1p** — Affiche les valeurs de balise de priorité 802.1p à affecter à une file d'attente de sortie, où 0 est la priorité la plus faible et 7 la plus élevée.
- **File d'attente de sortie** — Sélectionnez la file d'attente de sortie sur laquelle la priorité 802.1p est mappée. Le système prend en charge quatre files d'attente de sortie, parmi lesquelles la File d'attente 4 dispose de la priorité la plus élevée et la File d'attente 1 de la priorité la plus faible.

ÉTAPE 3 Pour chaque priorité 802.1p, sélectionnez la file d'attente de sortie sur laquelle elle est mappée.

ÉTAPE 4 Cliquez sur **Appliquer**. Les valeurs de priorité 801.1 vers les files d'attente sont mappées et le fichier de Configuration d'exécution est mis à jour.

Mappage DSCP à file d'attente

La page DSCP (IP *Differentiated Services Code Point*, point de code de service différenciéIP) vers file d'attente mappe des valeurs DSCP sur des files d'attente de sortie. La table DSCP vers file d'attente détermine la file d'attente de sortie des paquetsIP entrants sur la base de leur valeur DSCP. La valeur VPT (VLAN Priority Tag, marquage de priorité VLAN) du paquet reste inchangée.

En modifiant simplement le mappage DSCP à file d'attente, la méthode de planification des files d'attente ainsi que l'allocation de bande passante, il est possible d'obtenir la qualité de service voulue sur un réseau.

Le mappage DSCP vers file d'attente s'applique aux paquets IP si le mode de confiance est DSCP.

Les paquets nonIP sont toujours classifiés comme appartenant à la file d'attente Meilleur effort (Best effort).

Pour créer des mappages DSCP à file d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **DSCP vers file d'attente**. La page *DSCP vers file d'attente* s'affiche.

La page *DSCP vers file d'attente* contient **DSCP d'entrée**. Il affiche la valeur DSCP du paquet entrant et la classe associée.

ÉTAPE 2 Sélectionnez la **file d'attente de sortie** (file d'attente de transfert du trafic) sur laquelle la valeur DSCP est mappée.

ÉTAPE 3 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Configuration de la bande passante

La page *Bande passante* permet aux utilisateurs de définir deux valeurs (Limite de vitesse d'entrée et Taux de modelage en sortie), qui déterminent la quantité de trafic que le système peut recevoir et envoyer.

La limite de vitesse d'entrée indique le nombre de bits par seconde que l'interface d'entrée peut recevoir. La bande passante dépassant cette limite est éliminée.

Les valeurs suivantes sont entrées pour le lissage en sortie (egress shaping) :

- L'option Débit minimal garanti (CIR) définit la quantité moyenne maximale de données que le système est autorisé à envoyer à l'interface de sortie, en bits par seconde.
- L'option Taille de rafale garantie (CBS) indique la rafale de données que le système est autorisé à envoyer même au-delà de la valeur CIR. Cette valeur est exprimée en nombre d'octets de données.

Pour indiquer la limite de bande passante :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Bande passante**. La page *Bande passante* apparaît.

La page *Bande passante* affiche les informations de bande passante de chaque interface.

La colonne % indique la limite de débit entrant pour le port divisée par la quantité totale de bande passante du port.

ÉTAPE 2 Sélectionnez une interface et cliquez sur **Modifier**. La page *Modifier la bande passante* apparaît.

ÉTAPE 3 Sélectionnez le **port ou l'interface LAG**.

ÉTAPE 4 Remplissez les champs pour l'interface sélectionnée :

- **Limite de débit d'entrée** — Sélectionnez cette option pour activer la limite de débit d'entrée, que vous définissez ensuite dans le champ situé au-dessous.
- **Limite de débit d'entrée** — Saisissez la quantité maximale de bande passante autorisée sur l'interface.

  REMARQUE Les deux champs **Limite de vitesse d'entrée** ne s'affichent pas lorsque le type d'interface est LAG.
- **Taux de lissage en sortie (egress shaping)** — Sélectionnez cette option pour activer le lissage en sortie (egress shaping) sur le port.
- **Débit minimal garanti (CIR)** — Saisissez la quantité maximale de bande passante de l'interface de sortie.
- **Taille de rafale garantie (CBS)** — Saisissez la taille maximale de rafale de données de l'interface de sortie, en octets. Cette quantité de données peut être envoyée même si cela provoque un dépassement temporaire de la limite de la bande passante autorisée.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres de bande passante sont écrits dans le fichier de Configuration d'exécution.

Configuration du lissage en sortie par file d'attente

Outre la limitation du débit de transmission de chaque port, que vous configurez sur la page *Bande passante,* le commutateur peut limiter le débit de transmission des trames en sortie sélectionnées pour chaque file d'attente et pour chaque port. La limitation du débit en sortie est réalisée par lissage (shaping) de la charge de sortie.

Le commutateur limite toutes les trames, à l'exception des trames de gestion. Toutes les trames non limitées sont ignorées dans le calcul du débit, ce qui signifie que leur taille n'est pas incluse dans la limite totale.

Vous pouvez désactiver le lissage (shaping) du débit en sortie pour chaque file d'attente.

Pour définir le lissage en sortie (egress shaping) pour chaque file d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Modelage de sortie par file d'attente**. La page *Modelage de sortie par file d'attente* s'affiche.

La page *Modelage de sortie par file d'attente* affiche la limite de débit et la taille de rafale applicables à chaque file d'attente.

ÉTAPE 2 Sélectionnez un type d'interface (Port ou LAG) et cliquez sur **OK**. La liste des ports/LAG s'affiche.

ÉTAPE 3 Sélectionnez un port/LAG et cliquez sur **Modifier**. La page *Modelage de sortie par file d'attente* s'affiche.

Cette page vous permet de lisser la sortie pour un maximum de quatre files d'attente sur chaque interface.

ÉTAPE 4 Sélectionnez l'**interface** voulue.

ÉTAPE 5 Pour chacune des files d'attente nécessaires, remplissez les champs suivants :

- **Activer le lissage** : sélectionnez cette option pour activer le modelage en sortie sur cette file d'attente.
- **Débit minimal garanti (CIR)** — Saisissez le débit maximal (CIR) en kilobits par seconde (kbits/s). Le CIR est la quantité maximale moyenne de données pouvant être envoyée.
- **Taille de rafale garantie (CBS)** — Saisissez la taille maximale de rafale (CBS), en octets. Le CBS indique la taille maximale de rafale de données dont l'envoi est autorisé même si cela dépasse le CIR.

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

Gestion des statistiques de QoS

Sur cette page, vous pouvez gérer les statistiques de files d'attente.

Affichage des statistiques de file d'attente

La page *Statistiques de files d'attente* affiche les statistiques concernant les files d'attente, dont le nombre de paquets transférés et éliminés, ceci sur la base de l'interface, de la file d'attente et de la priorité d'élimination.

REMARQUE Les statistiques de QoS ne sont affichées que lorsque le commutateur fonctionne en mode QoS avancé. Vous effectuez la modification sous **Général** > **Propriétés de QoS**.

Pour afficher les statistiques de file d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Statistiques de QoS** > **Statistiques de file d'attente**. La page *Statistiques de files d'attente* s'affiche.

Cette page affiche les champs suivants :

- **Taux d'actualisation :** sélectionnez la durée qui s'écoule avant l'actualisation des statistiques Ethernet de l'interface. Les options disponibles sont les suivantes :
  - *Aucune actualisation :* les statistiques ne sont pas actualisées.
  - *15s :* les statistiques sont actualisées toutes les 15 secondes.
  - *30s :* les statistiques sont actualisées toutes les 30 secondes.
  - *60s :* les statistiques sont actualisées toutes les 60 secondes.
- **Jeu de compteurs** — Les options disponibles sont les suivantes :
  - *Jeu1* — Affiche les statistiques du jeu1, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) élevée.

- *Jeu2* — Affiche les statistiques du jeu2, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) faible.

- **Interface** — Interface à laquelle correspondent les statistiques de file d'attente affichées.
- **File d'attente** — File d'attente d'où proviennent les paquets transférés ou éliminés, la file étant pleine (tail drop).
- **Priorité d'élimination** — Les paquets portant la priorité d'élimination la plus faible ont davantage de chances d'être conservés.
- **Nombre total de paquets :** nombre de paquets transférés ou éliminés, la file étant pleine (tail drop).
- **Paquets éliminés :** pourcentage de paquets éliminés, la file étant pleine (tail drop).

ÉTAPE 2 Cliquez sur **Ajouter**. La page *Ajouter des statistiques de files d'attente* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Jeu de compteurs** — Sélectionnez le jeu voulu :
  - *Jeu1* — Affiche les statistiques du jeu1, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) élevée.
  - *Jeu2* — Affiche les statistiques du jeu2, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) faible.
- **Interface** — Sélectionnez les ports auxquels correspondent les statistiques affichées. Les options sont les suivantes :
  - *Port :* sélectionnez le port pour lequel vous voulez afficher les statistiques, pour le numéro d'unité sélectionné.
  - *Tous les ports* — L'écran affiche les statistiques pour tous les ports.
- **File d'attente** — Sélectionnez la file d'attente pour laquelle vous voulez afficher les statistiques.
- **Priorité d'élimination** — Saisissez la priorité d'élimination, c'est-à-dire la probabilité de suppression des paquets.

ÉTAPE 4 Cliquez sur **Appliquer.** Le compteur de statistiques de files d'attente est ajouté et le fichier de Configuration d'exécution est mis à jour.