GUIDE D'ADMINISTRATION

Guide d'administration du commutateur administrable Cisco Small Business série 300

Commutateurs 10/100	SF 300-08, SF 302-08, SF 302-08MP, SF 302-08P, SF 300-24, SF 300-24P, SF 300-48, SF 300-48P
Commutateurs Gigabit	SG 300-10, SG 300-10MP, SG 300-10P, SG 300-20, SG 300-28, SG 300-28P, SG 300-52

Sommaire

1

Avant de commencer

Ce chapitre propose une introduction à l'interface utilisateur et englobe les rubriques suivantes :

- **Démarrage de l'utilitaire Web de configuration de commutateur**
- **Configuration du commutateur - Démarrage rapide**
- **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.

Restrictions s'appliquant aux navigateurs

Les restrictions suivantes s'appliquent aux navigateurs :

- Si vous utilisez Internet Explorer 6, vous ne pouvez pas utiliser directement une adresse IPv6 pour accéder au commutateur. Vous pouvez néanmoins utiliser le serveur DNS (Domain Name System) 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 link-local IPv6 pour accéder au commutateur à partir de votre navigateur.

Lancement de l'utilitaire de configuration

Pour ouvrir l'interface utilisateur :

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 *rubrique Connexion* s'ouvre.

REMARQUE Lorsque le commutateur utilise l'adresse IP par défaut définie en usine, sa LED 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 LED d'alimentation reste allumée.

Connexion

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 êtes invité à entrer un nouveau mot de passe.

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

ÉTAPE 1 Saisissez le nom d'utilisateur/le mot de passe. Le nom d'utilisateur/mot de passe par défaut est **cisco/cisco**. Le mot de passe peut comporter au maximum 32 caractères ASCII. Les règles de complexité du mot de passe sont décrites à la section **Définition de règles de complexité des mots 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 déjà enregistrée, reportez-vous à la section *Mettre à niveau/sauvegarder micrologiciel/langue*.

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

ÉTAPE 4 Saisissez le nouveau nom d'utilisateur/mot de passe et cliquez sur **Appliquer**.

Une fois la connexion établie, la *rubrique Avant de commencer* s'ouvre.

Si vous avez saisi un nom d'utilisateur ou un mot de passe erroné, un message d'erreur apparaît et la *rubrique Connexion* reste affichée sur la fenêtre. Si vous rencontrez des problèmes pour vous connecter, reportez-vous à la section **Lancement de l'utilitaire de configuration** du Guide d'administration du commutateur administrable Cisco Small Business série 300 pour plus d'informations.

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

Expiration du mot de passe

Expiration du mot de passe

La *rubrique 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

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

Une icône X rouge 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.

Lorsque vous cliquez sur **Enregistrer**, la *rubrique 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 *rubrique Connexion* s'ouvre en affichant un message indiquant l'état déconnecté. 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 *rubrique Avant de commencer.* Si vous n'avez pas sélectionné cette option, la page initiale est la *rubrique Avant de commencer.* Si vous avez sélectionné cette option, la page initiale est la *rubrique Récapitulatif du système*.

Configuration du commutateur - Démarrage rapide

Pour simplifier la configuration du commutateur, la *rubrique Avant de commencer* fournit des liens vers les pages les plus fréquemment utilisées afin de vous permettre d'y accéder rapidement.

Liens de la page Avant de commencer

Catégorie	Nom du lien (sur la page)	Page correspondante
Configuration initiale	Modifier l'adresse IP de l'appareil	*Rubrique Interface IPv4*
	Créer un VLAN	*Rubrique Créer un VLAN*
	Configurer les paramètres de port	*Rubrique Paramètres du port*

Liens de la page Avant de commencer (Suite)

Catégorie	Nom du lien (sur la page)	Page correspondante
État du commutateur	Récapitulatif du système	*Rubrique Récapitulatif du système*
	Statistiques des ports	*Rubrique Interface*
	Statistiques RMON	*Rubrique Statistiques*
	Afficher le journal	*Rubrique Mémoire RAM*
Accès rapide	Modifier le mot de passe de l'appareil	*Rubrique Comptes d'utilisateurs*
	Mettre à niveau le logiciel de l'appareil	*Mettre à niveau/sauvegarder micrologiciel/langue*
	Configuration de sauvegarde de l'appareil	*Rubrique Télécharger/ sauvegarder configuration/ journal*
	Créer une ACL basée sur MAC	*Rubrique ACL basée sur MAC*
	Créer une ACL basée sur IP	*Rubrique ACL basée sur IPv4*
	Configurer la QoS	*Rubrique Propriétés de QoS*
	Configurer la mise en miroir des ports	*Rubrique Mise en miroir des ports et VLAN*

Navigation dans les fenêtres

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

En-tête d'application

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 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. Cliquez sur **Enregistrer** pour afficher la *rubrique Copier/ enregistrer la configuration*. Enregistrez le type de fichier de Configuration d'exécution en le copiant sur le type de 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. Lors du redémarrage du commutateur, celui-ci copie le fichier de Configuration de démarrage sur la Configuration d'exécution et définit ses paramètres en fonction des données présentes dans la Configuration d'exécution.
Utilisateur	Cliquez pour afficher le nom de l'utilisateur connecté au commutateur. Le nom d'utilisateur par défaut est **cisco**. (Le mot de passe par défaut est également **cisco**.)
Se déconnecter	Cliquez pour vous déconnecter de l'utilitaire Web de configuration du commutateur.
À propos de	Cliquez pour afficher le nom du commutateur et son numéro de version.

Liens d'application (Suite)

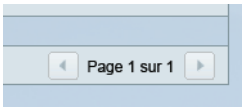
Nom du lien d'application	Description
Aide	Cliquez pour afficher l'aide en ligne.
Menu Langue	Sélectionnez une langue ou chargez un nouveau fichier de langue dans le commutateur. Si la langue requise s'affiche dans le menu, sélectionnez-la. Dans le cas contraire, sélectionnez **Télécharger une langue**. Pour plus d'informations sur l'ajout d'une nouvelle langue, reportez-vous à *Mettre à niveau/sauvegarder micrologiciel/ langue*.
	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 *rubrique Mémoire RAM*. Une fois que vous aurez accédé à cette page, l'icône d'état d'alerte Syslog ne s'affichera plus. Pour afficher la page en l'absence de message SYSLOG actif, suivez le chemin **État et statistiques** > **Afficher le journal** > **Mémoire RAM**.

Boutons de gestion

Boutons de gestion

La table suivante décrit les boutons couramment utilisés qui s'affichent sur différentes pages du système.

Boutons de gestion

Nom du bouton	Description
	Naviguez dans la table en utilisant les flèches droite et gauche lorsque cette table comporte plus de 50 entrées.
	Indique un champ obligatoire.

Boutons de gestion (Suite)

Nom du bouton	Description
Ajouter	Cliquez 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 *rubrique Copier/enregistrer la configuration* et enregistrer la Configuration d'exécution dans le type de fichier de 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 de Configuration de démarrage ou dans un autre type de fichier. Cliquez sur **Enregistrer** pour afficher la *rubrique Copier/enregistrer la configuration* et enregistrer la Configuration d'exécution dans le type de fichier de Configuration de démarrage sur le commutateur.
Annuler	Cliquez sur réinitialiser les modifications apportées à la page.
Effacer les compteurs de toutes les interfaces	Cliquez pour effacer les compteurs de statistiques de toutes les interfaces.
Effacer les compteurs de l'interface	Cliquez 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.

Boutons de gestion (Suite)

Nom du bouton	Description
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 cela est 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.
Supprimer	Sélectionnez l'entrée à supprimer dans la table et cliquez sur **Supprimer** pour valider l'opération. L'entrée est supprimée.
Détails	Cliquez pour afficher les détails associés à l'entrée sélectionnée sur la page principale.
Modifier	Sélectionnez l'entrée et cliquez sur **Modifier.** La rubrique *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.

2

Affichage des statistiques

Ce chapitre explique comment afficher les statistiques du commutateur.

Il englobe les sections suivantes :

- **Affichage de l'interface Ethernet**
- **Affichage des statistiques Etherlike**
- **Affichage des statistiques GVRP**
- **Affichage des statistiques EAP 802.1X**
- **Affichage de l'utilisation de la mémoire TCAM**
- **Gestion des statistiques RMON**

Affichage de l'interface Ethernet

La *Rubrique Interface* affiche les statistiques de trafic par 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, Multidiffusion et Diffusion).

Pour afficher les statistiques Ethernet :

ÉTAPE 1 Cliquez sur **État et statistiques** > **Interface**. La *rubrique Interface* s'ouvre.

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.
  - *15 s* : les statistiques sont actualisées toutes les 15 secondes.
  - *30 s* : les statistiques sont actualisées toutes les 30 secondes.
  - *60 s* : les statistiques sont actualisées toutes les 60 secondes.

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 unicast** : paquets unicast corrects reçus.
- **Paquets multicast** : paquets multicast corrects reçus.
- **Paquets broadcast** : paquets broadcast 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 unicast** : paquets unicast corrects transmis.
- **Paquets multicast** : paquets multicast corrects transmis.
- **Paquets broadcast** : paquets broadcast 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 *rubrique Etherlike* affiche les statistiques par port en fonction de la définition de la norme 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 (Niveau 1), qui pourraient perturber le trafic.

Pour afficher les statistiques Etherlike :

ÉTAPE 1 Cliquez sur **État et statistiques** > **Etherlike**. La *rubrique Etherlike* s'ouvre.

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 collision individuelle** : nombre de 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 dues à des collisions excessives.
- **Paquets de taille excessive** : paquets de plus de 1 518 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 depuis l'interface sélectionnée.

Pour effacer les compteurs de statistiques :

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

Affichage des statistiques GVRP

La *rubrique GVRP* affiche des informations se rapportant aux trames GVRP (GARP VLAN Registration Protocol, également appelé MVRP, Multiple VLAN Registration Protocol) envoyées ou reçues d'un port. GVRP est un protocole réseau de Niveau 2 basé sur des normes permettant la configuration automatique des informations VLAN sur les commutateurs. Il a été défini dans l'amendement 802.1ak apporté à la norme 802.1Q-2005.

Les statistiques GVRP d'un port ne s'affichent que si GVRP est activé globalement et sur le port. Ceci s'effectue dans la *rubrique GVRP*.

Pour afficher les statistiques GVRP :

ÉTAPE 1 Cliquez sur **État et statistiques** > **GVRP**. La *rubrique GVRP* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

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

Le pavé comptabilisant les attributs affiche les compteurs de différents types de paquets par interface.

- **Connexion (vide)** : nombre de paquets Connexion (vide) GVRP reçus/transmis.
- **Vide** : nombre de paquets Vide GVRP reçus/transmis.
- **Sortie (vide)** : nombre de paquets Sortie (vide) GVRP reçus/transmis.
- **Connexion** : nombre de paquets Connexion GVRP reçus/transmis.
- **Sortie** : nombre de paquets Sortie GVRP reçus/transmis.
- **Sortie (tous)** : nombre de paquets Sortie (tous) GVRP reçus/transmis.

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

- **ID de protocole non valide** : erreurs d'ID de protocole non valide.
- **Type d'attribut non valide** : erreurs de type d'attribut non valide.
- **Valeur d'attribut non valide** : erreurs de valeur d'attribut non valide.
- **Longueur d'attribut non valide** : erreurs de longueur d'attribut non valide.
- **Événement non valide** : événements non valides.

Pour effacer les compteurs, cliquez sur **Effacer les compteurs de l'interface**. Les compteurs de statistiques GVRP sont alors effacés.

Affichage des statistiques EAP 802.1X

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

Pour afficher les statistiques EAP :

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

ÉTAPE 2 Sélectionnez le **Port** interrogé pour ses 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** : trames EAPOL de début reçues sur le port.
- **Trames EAPOL de déconnexion reçues** : trames EAPOL de déconnexion reçues sur le port.
- **Trames ID/de réponse EAP reçues** : trames ID/de réponse EAP reçues sur le port.
- **Trames de réponse EAP reçues** : trames de réponse EAP reçues par le port (autres que les trames ID/de réponse).
- **Trames ID/de demande EAP transmises** : trames ID/de demande EAP transmises par le port.
- **Trames de demande EAP transmises** : trames de demande EAP transmises par le port.
- **Trames EAPOL non valides reçues** : trames EAPOL non reconnues 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 associé à la dernière trame EAPOL reçue.

Affichage de l'utilisation de la mémoire TCAM

L'architecture du commutateur utilise une mémoire ternaire adressable par contenu (TCAM,Ternary Content Addressable Memory) permettant de prendre en charge des recherches étendues de données au cours d'une brève période.

TCAM conserve les règles produites par d'autres processus, tels que les listes de contrôle d'accès (ACL, Access Control Lists) ou la QoS. 512 règles TCAM peuvent au maximum être allouées par l'ensemble des processus.

Certains processus allouent des règles lors de leur lancement. En outre, les processus qui s'initialisent lors du démarrage système utilisent une partie de leurs règles lors de ce processus de démarrage.

Pour afficher l'utilisation de la mémoire TCAM, cliquez sur **État et statistiques** > **Utilisation TCAM**. La *rubrique Utilisation TCAM* s'ouvre, affichant le pourcentage d'utilisation de la mémoire TCAM dans le système.

Cette page affiche **Utilisation TCAM**, le pourcentage de ressources TCAM utilisé.

Règles TCAM

La table Règles TCAM par processus répertorie tous les processus qui peuvent s'allouer des règles TCAM. Chaque processus dispose de sa propre stratégie d'allocation.

Règles TCAM par processus

Processus	Par port/ par commutateur	Allocation à l'activation	Limite maximale de processus	Règles TCAM max. utilisées par entrée utilisateur	Commentaires
Règles du mode avancé de QoS	Port	6/appareil	Aucune limite	1 ou 2 entrées TCAM par règle	
Règles de contrôle d'accès	Port	6/appareil	Aucune limite	1 ou 2 entrées TCAM par règle	
VLAN basé sur le protocole	Port	0	Aucune limite	1 ou 2	Les règles sont dupliquées pour les VLAN basés sur MAC.

Règles TCAM par processus (Suite)

Processus	Par port/ par commutateur	Allocation à l'activation	Limite maximale de processus	Règles TCAM max. utilisées par entrée utilisateur	Commentaires
VLAN basé sur MAC	Port	0	Aucune limite	Aucune limite	Les règles sont dupliquées pour les VLAN basés sur MAC.
DHCP Snooping	Commutateur	2/appareil	Aucune limite	8 entrées TCAM par règle de DHCP Snooping	
IP Source Guard	Port	0	Aucune limite	1 entrée TCAM par entrée IP Source Guard	
Inspection ARP	Commutateur	2/appareil	128	4 entrées TCAM par règle d'inspection ARP	
Limitation de débit VLAN	Les deux	0	255	1 règle globale par limite de débit VLAN	Une règle supplémentaire est créée pour chaque règle Autoriser de l'interface.

Gestion des statistiques RMON

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

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

Cette fonction vous permet de réaliser les actions suivantes :

- Afficher les statistiques (valeurs de compteurs) actuelles, c'est-à-dire depuis le dernier effacement. Vous pouvez également collecter les valeurs de ces compteurs sur une période puis afficher la table des données collectées, chaque ensemble collecté représentant une ligne individuelle de l'onglet *Historique*.
- Définir des changements intéressants dans les valeurs des compteurs, tels que « a atteint un certain nombre de collisions tardives » (définit l'alarme) puis définir l'action à mettre en œuvre lorsque cet événement se produit (journal, messages « trap » ou journal et messages « trap »).

Affichage des statistiques RMON

La *rubrique Statistiques* affiche des informations détaillées sur la taille des paquets ainsi que certaines informations sur les erreurs au niveau des couches physiques. Les informations sont présentées en vertu de la norme RMON.

Pour afficher les statistiques RMON :

ÉTAPE 1 Cliquez sur **RMON** > **Statistiques**. La *rubrique Statistiques* s'ouvre.

ÉTAPE 2 Sélectionnez l'**interface** pour laquelle les statistiques RMON 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 reçus, y compris les paquets erronés, ainsi que les paquets multicast et broadcast.

- **Paquets broadcast reçus** : nombre de paquets broadcast corrects reçus. Ce nombre n'inclut pas les paquets multicast.
- **Paquets multicast reçus** : nombre de paquets multicast 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 1 632 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 dont la taille dépassait 1 632 octets. Ce nombre exclut les bits de synchronisation, mais inclut les octets FCS qui comportaient une séquence FCS (Frame Check Sequence) erronée avec un nombre entier d'octets (Erreur FCS) ou une séquence FCS erronée avec un nombre non entier d'octets (Erreur d'alignement).
- **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 de 1 024 à 1 632 octets** : nombre de trames de 1 024 à 1 632 octets reçues.

ÉTAPE 4 Sélectionnez une autre interface dans le champ Interface. Les statistiques RMON s'affichent.

Configuration de l'historique RMON

La *rubrique Table de contrôle de l'historique* permet de collecter un journal de statistiques sur un port.

Vous pouvez configurer la fréquence d'échantillonnage, la quantité d'échantillons à stocker ainsi que le port à partir duquel recueillir les données. Une fois les données échantillonnées et stockées, elles s'affichent dans la *rubrique Table d'historique*, à laquelle vous pouvez accéder en cliquant sur **Table d'historique**.

Pour afficher les informations d'historique de contrôle RMON :

ÉTAPE 1 Cliquez sur **État et statistiques** > **RMON** > **Historique**. La *rubrique Table de contrôle de l'historique* s'ouvre.

Cette page affiche les champs suivants :

- **N° d'entrée d'historique** : numéro de l'entrée dans la table d'historique.
- **Interface source** : ID de l'interface à partir de laquelle les échantillons d'historique ont été recueillis.
- **Nombre maximum d'échantillons à conserver** : nombre maximum d'échantillons à stocker dans cette partie de la table d'historique.
- **Intervalle d'échantillonnage** : durée (en secondes) pendant laquelle des échantillons ont été collectés au niveau des ports. La plage du champ est comprise entre 1 et 3 600.
- **Propriétaire** : utilisateur ou station RMON ayant demandé les informations RMON. La plage du champ est comprise entre 0 et 20 caractères.
- **Nombre d'échantillons actuel** : de par la norme, RMON est autorisé à ne pas accepter tous les échantillons demandés et à limiter plutôt le nombre d'échantillons par demande. Ce champ représente donc le nombre d'échantillons réellement accordé à la demande, ce nombre étant égal ou inférieur à la valeur demandée.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter à l'historique RMON* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **Nouvelle entrée d'historique** : affiche le numéro de la nouvelle entrée de la table.
- **Interface source** : sélectionnez le type d'interface à partir de laquelle les échantillons d'historique doivent être recueillis.

- **Nombre maximum d'échantillons à conserver** : saisissez le nombre d'échantillons à stocker.
- **Intervalle d'échantillonnage** : saisissez la durée (en secondes) pendant laquelle des échantillons doivent être collectés au niveau des ports. La plage du champ est comprise entre 1 et 3 600.
- **Propriétaire** : saisissez l'utilisateur ou la station RMON ayant demandé les informations RMON. La plage du champ est comprise entre 0 et 20 caractères.

ÉTAPE 4 Cliquez sur **Appliquer**. L'entrée est ajoutée à la *rubrique Table de l'historique* et le commutateur est mis à jour.

Affichage de la table d'historique RMON

La *rubrique Table d'historique* affiche les échantillonnages réseau statistiques spécifiques à l'interface. Chaque entrée de table représente toutes les valeurs de compteurs compilées lors d'une même prise d'échantillon.

Pour afficher l'historique RMON :

ÉTAPE 1 Cliquez sur **RMON** > **Historique**. La *rubrique Table de l'historique* s'ouvre.

ÉTAPE 2 Cliquez sur **Table d'historique**. La *rubrique Table d'historique* s'ouvre.

ÉTAPE 3 Dans la liste **N° d'entrée d'historique**, sélectionnez un numéro d'entrée pour afficher les échantillons associés à cette entrée d'historique.

Les champs sont affichés pour l'échantillon sélectionné.

- **Propriétaire** : propriétaire de l'entrée dans la table d'historique.
- **N° d'échantillon** : les statistiques ont été récupérées de cet échantillon.
- **Événements d'abandon** : paquets abandonnés en raison d'un manque de ressources réseau lors de l'intervalle d'échantillonnage. Cela peut ne pas correspondre au nombre exacts de paquets abandonnés, mais plutôt au nombre de détections de paquets de ce type.
- **Octets reçus** : octets reçus, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **Paquets reçus** : paquets reçus, y compris les paquets erronés, ainsi que les paquets multicast et broadcast.

- **Paquets broadcast** : paquets broadcast corrects reçus. Ce nombre n'inclut pas les paquets multicast.
- **Paquets multicast** : paquets multicast corrects reçus.
- **Erreurs d'alignement et CRC** : erreurs d'alignement et CRC qui se sont produites.
- **Paquets de taille insuffisante** : paquets de taille insuffisante (moins de 64 octets) reçus.
- **Paquets de taille excessive** : paquets de taille excessive (plus de 1 632 octets) reçus.
- **Fragments** : fragments (paquets de moins de 64 octets) reçus, à l'exception des bits de synchronisation, mais incluant les octets FCS.
- **Jabotages** : nombre total de paquets reçus dont la taille dépassait 1 632 octets. Ce nombre exclut les bits de synchronisation, mais inclut les octets FCS qui comportaient une séquence FCS (Frame Check Sequence) erronée avec un nombre entier d'octets (Erreur FCS) ou une séquence FCS erronée avec un nombre non entier d'octets (Erreur d'alignement).
- **Collisions** : collisions reçues.
- **Utilisation** : pourcentage du trafic actuel de l'interface par rapport au trafic maximum pouvant être géré par cette dernière.

Définition du contrôle des événements RMON

La *rubrique Événements* permet de configurer des événements, qui sont des *actions* mises en œuvre lorsqu'une alarme est générée (les alarmes sont définies dans la *rubrique Alarmes*). Un événement peut correspondre à toute combinaison de journaux/messages « trap ».

Si l'action inclut la journalisation, les événements sont journalisés dans la *rubrique Table du journal d'événements*.

Pour afficher les événements RMON :

ÉTAPE 1 Cliquez sur **RMON** > **Événements**. La *rubrique Événements* s'ouvre.

Cette page affiche les événements précédemment définis.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter des événements RMON* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **Entrée d'événement** : affiche le numéro d'index d'entrée d'événement pour la nouvelle entrée.
- **Communauté** : saisissez la chaîne de communauté SNMP à inclure lors de l'envoi de messages « trap » (facultatif).
- **Description** : saisissez un nom pour l'événement. Ce nom est utilisé dans la *rubrique Ajouter une alarme RMON* pour joindre une alarme à un événement.
- **Type** : sélectionnez le type d'action que provoque cet événement. Les valeurs possibles sont :
  - *Aucun* : aucune action ne se produit lorsque l'alarme s'arrête.
  - *Journal* : ajoute une entrée de journal lorsque l'alarme s'arrête.
  - *Message « trap »* : envoie un message « trap » lorsque l'alarme s'arrête.
  - *Journal et message « trap »* : ajoute une entrée de journal et envoie un message « trap » lorsque l'alarme s'arrête.
- **Propriétaire** : saisissez l'appareil ou l'utilisateur ayant défini l'événement.

ÉTAPE 4 Cliquez sur **Appliquer**. L'événement RMON est ajouté et le commutateur mis à jour.

Affichage des journaux d'événements RMON

La *rubrique Table du journal d'événements* affiche le journal des événements (actions) qui se sont produits. Un événement peut être journalisé lorsqu'il est de type *Journal* ou *Journal et message « trap »*. L'action indiquée dans l'événement est mise en œuvre lorsque cet événement est lié à une alarme (voir la *rubrique Alarmes*) et que les conditions de l'alarme sont réunies.

ÉTAPE 1 Cliquez sur **RMON** > **Événements**. La *rubrique Événements* s'ouvre.

ÉTAPE 2 Cliquez sur **Table du journal d'événements** . La *rubrique Table du journal d'événements* s'ouvre.

Cette page affiche les champs suivants :

- **Événement** : numéro de l'entrée dans le journal d'événements.
- **N° de journal** : numéro du journal.

- **Heure de journalisation** : heure à laquelle l'entrée a été enregistrée dans le journal.
- **Description** : description de l'entrée du journal.

Définition des alarmes RMON

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

Une ou plusieurs alarmes sont liées à un événement. L'événement indique l'action à mettre en œuvre lorsque l'alarme se déclenche.

La *rubrique Alarmes* permet de configurer des alarmes et de les lier à des événements. Les compteurs d'alarme peuvent être contrôlés par des valeurs absolues ou par des changements (delta) dans les valeurs de ces compteurs.

Pour entrer des alarmes RMON :

ÉTAPE 1 Cliquez sur **RMON** > **Alarmes**. La *rubrique Alarmes* s'ouvre.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une alarme RMON* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **Entrée d'alarme** : affiche le numéro d'entrée de l'alarme.
- **Interface** : sélectionnez le type d'interface pour lequel les statistiques RMON s'affichent.
- **Nom du compteur** : sélectionnez la variable MIB qui indique le type d'occurrence mesuré.
- **Type d'échantillon** : sélectionnez la méthode d'échantillonnage pour générer une alarme. Les options disponibles sont les suivantes :
  - *Delta* : soustrait la valeur du dernier échantillon de la valeur actuelle. La différence est comparée au seuil. Si le seuil est franchi, une alarme est générée.

  - *Absolu* : si le seuil est franchi, une alarme est générée.
- **Seuil supérieur** : saisissez la valeur de compteur supérieure qui déclenche l'alarme de seuil supérieur.
- **Événement de hausse** : sélectionnez un événement, parmi ceux définis dans la Table des événements, à mettre en œuvre en cas de déclenchement d'un événement de hausse.
- **Seuil inférieur** : saisissez la valeur de compteur inférieure qui déclenche l'alarme de seuil inférieur.
- **Événement de baisse** : sélectionnez un événement, parmi ceux définis dans la Table des événements, à mettre en œuvre en cas de déclenchement d'un événement de baisse.
- **Alarme de démarrage** : sélectionnez le premier événement à partir duquel lancer la génération d'alarmes. La hausse est définie en franchissant le seuil en partant d'un seuil de faible valeur vers un seuil de valeur plus importante.
  - *Alarme de hausse* : une valeur de compteur en hausse déclenche l'alarme de seuil supérieur.
  - *Alarme de baisse* : une valeur de compteur en baisse déclenche l'alarme de seuil inférieur.
  - *Hausse et baisse* : des valeurs de compteur en hausse et en baisse déclenchent l'alarme.
- **Intervalle** : saisissez l'intervalle (en secondes) entre les alarmes.
- **Propriétaire** : saisissez le nom de l'utilisateur ou du système de gestion du réseau qui reçoit l'alarme.

ÉTAPE 4 Cliquez sur **Appliquer**. L'alarme RMON est ajoutée et le commutateur mis à jour.

3

Gestion des journaux système

Ce chapitre décrit la fonction Journal système, qui permet au commutateur de conserver plusieurs journaux indépendants. Chaque journal correspond à un ensemble de messages enregistrant les événements système.

Le commutateur génère les journaux locaux suivants :

- 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 journaliser des messages sur des serveurs SYSLOG de conservation de journaux sous la forme de messages « trap » SNMP et de messages SYSLOG.

Ce chapitre englobe les sections 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 *rubrique Paramètres des journaux* et indiquer si vous souhaitez ou non regrouper les messages de journaux.

Niveaux de sévérité

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*, indiqué par la lettre F). Par exemple, le message de journal « %INIT-I-InitCompleted: ... » a un niveau de sévérité correspondant à **I**, qui signifie *Informatif*.

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

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

Vous pouvez sélectionner des niveaux de sévérité différents pour les journaux de la mémoire RAM et flash. Ces journaux s'affichent respectivement dans la *rubrique Mémoire RAM* et la *rubrique 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 *rubrique 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 des messages SYSLOG. Si elle est activée, les messages « trap » et messages SYSLOG identiques et contigus sont

agrégés pour une période spécifique 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 commutateur est mis à jour.

Définition des paramètres de journalisation distante

La *rubrique Serveurs de journalisation distants* permet de définir les serveurs SYSLOG distants où sont envoyés les messages de journalisation (en utilisant 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 *rubrique Serveurs de journalisation distants* s'ouvre.

Cette page affiche la liste des serveurs de journalisation distants.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un serveur de journalisation distant* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **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 disponibles sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière unique l'hôte situé sur une seule liaison réseau. 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 entrée remplace l'adresse dans la configuration.

- *Globale* : l'adresse IPv6 est de type IPV6 de monodiffusion globale, visible et joignable depuis d'autres réseaux.

- **Interface de liaison locale** : sélectionnez dans la liste de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée).
- **Adresse IP de serveur de journalisation** : saisissez l'adresse du serveur auquel les journaux sont envoyés.
- **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 *rubrique Ajouter un serveur de journalisation distant* se ferme, le serveur SYSLOG est ajouté et le commutateur 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

Mémoire RAM

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

Le journal de la RAM est effacé lors du redémarrage du commutateur ou lorsque vous cliquez sur le bouton Effacer les journaux.

1. Cliquez sur **État et statistiques** > **Afficher le journal** > **Mémoire RAM**. La *rubrique Mémoire RAM* s'ouvre.

Cette page contient 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.

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

Mémoire flash

Mémoire flash

La *rubrique Mémoire flash* affiche, dans l'ordre chronologique, les messages enregistrés dans la mémoire flash. Le niveau de sévérité minimum à journaliser est configuré dans la *rubrique 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,

1. Cliquez sur **État et statistiques** > **Afficher le journal** > **Mémoire flash**. La *rubrique Mémoire flash* s'ouvre.

Cette page contient 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.

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

4

Gestion des fichiers système

Vous pouvez choisir le fichier de micrologiciel à partir duquel le commutateur démarrera. Vous pouvez également copier des types de fichiers en interne sur le commutateur ou depuis un appareil externe, un PC par exemple.

Les méthodes de transfert de fichiers disponibles sont les suivantes :

- Copie interne
- HTTP 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* et non en fonction d'un nom de fichier modifiable par l'utilisateur. Le contenu peut être copié d'un type de fichier 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 par un utilisateur dans un éditeur de texte tel que 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. Il s'agit du seul type de fichier que vous modifiez, en changeant des valeurs de paramètres via l'une des interfaces de configuration. Il doit en outre être enregistré manuellement pour pouvoir être conservé.

En cas de redémarrage du commutateur, la Configuration d'exécution est perdue. Lors du redémarrage du commutateur, ce type de fichier est copié de la Configuration de démarrage enregistrée dans la mémoire flash vers la Configuration d'exécution stockée dans la RAM.

Pour conserver toute modification apportée au commutateur, vous devez enregistrer la Configuration d'exécution dans la Configuration de démarrage ou dans un autre type de fichier si vous ne souhaitez pas que le commutateur redémarre avec cette configuration. Si vous avez enregistré la Configuration d'exécution dans la Configuration de démarrage, le commutateur recrée, lors de son redémarrage, une Configuration d'exécution qui inclut les modifications que vous avez apportées depuis le dernier enregistrement de la Configuration d'exécution dans la Configuration de démarrage.

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

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

- **Configuration de secours** : copie manuelle des définitions de paramètres assurant une protection en cas d'arrêt du système ou pour la maintenance d'un état de fonctionnement spécifique. Vous pouvez copier la Configuration miroir, la Configuration de démarrage ou la Configuration d'exécution sur un fichier de Configuration de secours. La Configuration de secours est conservée dans la mémoire flash et préservée en cas de redémarrage de l'appareil.

- **Configuration miroir** : une copie de la Configuration de démarrage, créée par le commutateur si :

  - 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 sur d'autres types de fichiers ou sur un autre appareil.

En cas de redémarrage du commutateur, les paramètres d'origine par défaut de la Configuration miroir sont restaurés. Outre cette particularité, la Configuration miroir se comporte de la même façon qu'une Configuration de secours, en fournissant une copie des valeurs de paramètres, copie qui sera conservée en cas de redémarrage du commutateur.

- **Micrologiciel** : le système d'exploitation. Plus communément appelé l'*image*.
- **Code de démarrage** : contrôle le démarrage de base du système et lance l'image du micrologiciel.
- **Fichier de langue** : le dictionnaire qui permet l'affichage des fenêtres 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**
- Afficher l'image du micrologiciel actuellement utilisée ou sélectionner l'image à utiliser lors du redémarrage suivant, comme décrit dans la section **Sélection de l'image active**
- Enregistrer les fichiers du commutateur dans 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 sur un autre type de fichier de configuration, comme décrit dans la section **Copie ou enregistrement des types de fichiers de configuration du commutateur**
- Télécharger un fichier de configuration d'un serveur TFTP sur le commutateur, comme décrit dans la section **Définition de la configuration automatique DHCP**

ATTENTION Sauf si la Configuration d'exécution est copiée manuellement sur la Configuration de démarrage, la Configuration de secours ou un fichier externe, toutes les modifications apportées depuis le dernier enregistrement du fichier sont perdues lors du redémarrage du commutateur. Nous vous conseillons d'enregistrer la Configuration d'exécution dans la Configuration de démarrage avant de vous déconnecter afin de conserver toute modification apportée au cours de cette session.

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

Lorsque vous cliquez sur **Enregistrer**, la *rubrique 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 vers la *rubrique Copier/enregistrer la configuration* sont masqués.

Ce chapitre décrit la façon dont les fichiers de configuration et les fichiers journaux sont gérés.

Il contient les rubriques suivantes :

- **Mettre à niveau/sauvegarder micrologiciel/langue**
- **Sélection de l'image active**
- **Téléchargement ou sauvegarde d'une configuration ou d'un journal**
- **Affichage des propriétés des fichiers de configuration**
- **Copie ou enregistrement des types de fichiers de configuration du commutateur**
- **Définition de la 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 un nouveau fichier de langue ou mettre à niveau un fichier de langue existant.

Les méthodes de transfert de fichiers suivantes sont activées :

- HTTP 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.)

Vous pouvez également accéder à la rubrique **Mettre à niveau/sauvegarder micrologiciel/langue** en sélectionnant **Télécharger une langue** dans le menu déroulant Langue qui s'affiche sur toutes les pages.

Téléchargement d'un nouveau fichier de micrologiciel ou de langue

Deux images de micrologiciel, **Image1** et **Image2**, sont stockées sur le commutateur. Une des images est identifiée en tant qu'*image active* et l'autre en tant qu'*image inactive*.

Lors de la mise à niveau du micrologiciel, la nouvelle image remplace toujours celle identifiée comme étant l'image inactive.

Une fois le nouveau micrologiciel téléchargé sur le commutateur, celui-ci continue de démarrer en utilisant l'image active (l'ancienne version) jusqu'à ce que vous changiez l'état de la nouvelle image en image active, en utilisant la procédure décrite dans la section **« Sélection de l'image active »**. Démarrez ensuite le commutateur en utilisant le processus décrit dans la section **Redémarrage du commutateur**.

Pour télécharger ou sauvegarder un fichier système ou de langue :

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

ÉTAPE 2 Cliquez sur la Méthode de transfert. Si vous avez sélectionné TFTP, passez à l'**ÉTAPE 3**. Si vous avez sélectionné HTTP, passez à l'**ÉTAPE 4**.

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

Sélectionnez l'**Action si enregistrement**.

Dans **Action si enregistrement**, si vous avez sélectionné *Mettre à niveau* pour spécifier que le type de fichier du commutateur doit être remplacé par une nouvelle version de ce type de fichier, située sur un serveur TFTP, procédez comme suit. Sinon, passez à la procédure suivante de cette étape.

a. **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**.)

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

c. **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options disponibles sont les suivantes :

- *Liaison locale* : l'adresse IPv6 identifie de manière unique l'hôte situé sur une seule liaison réseau. 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 entrée remplace l'adresse dans la configuration.
- *Globale* : l'adresse IPv6 est de type IPV6 de monodiffusion globale, visible et joignable depuis d'autres réseaux.

d. **Interface de liaison locale** : sélectionnez dans la liste de liaison locale (si IPv6 est utilisé).

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

f. **Nom du fichier source** : saisissez le nom du fichier source.

Dans **Action si enregistrement**, si vous avez sélectionné *Sauvegarder* pour spécifier qu'une copie du type de fichier doit être enregistrée dans un fichier sur un autre appareil, procédez comme suit :

a. **Type de fichier** : sélectionnez le type de fichier source. Seuls les types de fichiers valides peuvent être sélectionnés. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)

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

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

- *Liaison locale* : l'adresse IPv6 identifie de manière unique l'hôte situé sur une seule liaison réseau. 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 entrée remplace l'adresse dans la configuration.
- *Globale* : l'adresse IPv6 est de type IPV6 de monodiffusion globale, visible et joignable depuis d'autres réseaux.

d. **Interface de liaison locale** : sélectionnez dans la liste de liaison locale (si IPv6 est utilisé).

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

f. **Nom du fichier de destination** : saisissez le nom du fichier de destination. Les noms de fichiers ne peuvent pas comporter de barres obliques (\ ou /) ; la première lettre du nom du fichier ne doit pas être un point (.) ; et les noms de fichiers sur un serveur TFTP ne doivent pas dépasser 160 caractères. (Caractères valides : A-Z, a-z, 0-9, « . », « - », « _ »)

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

Sélectionnez l'**Action si enregistrement** : seules les actions activées peuvent être sélectionnées.

Dans **Action si enregistrement**, si vous avez sélectionné **Mettre à niveau** pour spécifier que le type de fichier du commutateur doit être remplacé par une nouvelle version de ce type de fichier, procédez comme suit.

a. **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**.)

b. **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.

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

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

Sélection de l'image active

Deux images de micrologiciel, **Image1** et **Image2**, sont stockées sur le commutateur. Une des images est identifiée en tant qu'*image active* et l'autre en tant qu'*image inactive*. Le commutateur démarre à partir de l'image que vous avez définie en tant qu'*image active*. Vous pouvez changer en *image active* l'image identifiée en tant qu'*image inactive*. (Vous pouvez redémarrer le commutateur en utilisant le processus décrit dans la section **Redémarrage du commutateur**.)

Pour sélectionner l'image active :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion de fichiers** > **Image active**. La *rubrique Image active* s'ouvre.

Cette page affiche les éléments suivants :

Image active : affiche le fichier image actuellement actif sur le commutateur.

Numéro de version de l'image active : affiche la version du micrologiciel de l'image active.

ÉTAPE 2 Sélectionnez l'image dans le menu **Image active après redémarrage** pour identifier l'image du micrologiciel utilisée en tant qu'image active une fois le commutateur redémarré. **Numéro de version de l'image active après redémarrage** affiche la version du micrologiciel de l'image active utilisée une fois le commutateur redémarré.

ÉTAPE 3 Cliquez sur **Appliquer**. La sélection de l'image active est mise à jour.

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

La *rubrique Télécharger/sauvegarder configuration/journal* permet la sauvegarde depuis des types de fichiers de configuration ou le journal flash du commutateur vers un fichier sur un autre appareil ou la restauration de types de fichiers de configuration depuis un autre appareil vers le commutateur.

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 *rubrique Télécharger/sauvegarder configuration/journal* s'ouvre.

ÉTAPE 2 Cliquez sur la Méthode de transfert.

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

Sélectionnez l'**Action si enregistrement**.

Dans **Action si enregistrement**, si vous avez sélectionné *Télécharger* pour spécifier que le fichier d'un autre appareil remplacera un type de fichier sur le commutateur, procédez comme suit. Sinon, passez à la procédure suivante de cette étape.

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

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

- *Liaison locale* : l'adresse IPv6 identifie de manière unique l'hôte situé sur une seule liaison réseau. 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 entrée remplace l'adresse dans la configuration.

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

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

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

e. **Nom du fichier source** : saisissez le nom du fichier source. Les noms de fichiers ne peuvent pas comporter de barres obliques (\ ou /) ; la première lettre du nom du fichier ne doit pas être un point (.) et les noms de fichiers sur le serveur TFTP ne peuvent dépasser 160 caractères. (Caractères valides : A-Z, a-z, 0-9, « . », « - », « _ »)

f. **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**.)

Dans **Action si enregistrement**, si vous avez sélectionné *Sauvegarder* pour spécifier qu'un type de fichier doit être copié sur un fichier d'un autre appareil, procédez comme suit :

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

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

- *Liaison locale* : l'adresse IPv6 identifie de manière unique l'hôte situé sur une seule liaison réseau. 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 entrée remplace l'adresse dans la configuration.

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

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

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

e. **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**.)

f. **Nom du fichier de destination** : saisissez le nom du fichier de destination. Les noms de fichiers ne peuvent pas comporter de barres obliques (\ ou /) ; la première lettre du nom du fichier ne doit pas être un point (.) ; et les noms de fichiers sur le serveur TFTP ne doivent pas dépasser 160 caractères. (Caractères valides : A-Z, a-z, 0-9, « . », « - », « _ »)

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

Sélectionnez l'**Action si enregistrement**.

Dans **Action si enregistrement**, si vous avez sélectionné *Télécharger* pour spécifier que le type de fichier du commutateur doit être remplacé par une nouvelle version de ce type de fichier à partir d'un fichier d'un autre appareil, 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.

Dans **Action si enregistrement**, si vous avez sélectionné *Sauvegarder* pour spécifier qu'un type de fichier doit être copié sur un fichier d'un autre appareil, 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. Cliquez sur **Appliquer**. La fenêtre **Téléchargement de fichier** s'affiche.

c. Cliquez sur **Enregistrer**. La fenêtre **Enregistrer sous** s'affiche.

d. Cliquez sur **Enregistrer**.

ÉTAPE 5 Cliquez sur **Appliquer** ou sur **Terminé**. Le fichier est mis à niveau ou sauvegardé sur le commutateur (en fonction du type de fichier).

Affichage des propriétés des fichiers de configuration

La *rubrique Propriétés des fichiers de configuration* permet d'afficher les types de fichiers de configuration ainsi que la date et l'heure de leur modification. Elle permet également de supprimer la Configuration de démarrage et/ou la Configuration de secours. Vous ne pouvez en revanche pas modifier les autres types de fichiers de configuration.

Pour afficher les propriétés des fichiers de configuration, cliquez sur **Administration** > **Gestion de fichiers** > **Propriétés des fichiers de configuration**. La *rubrique Propriétés des fichiers de configuration* s'ouvre.

Cette page affiche 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.

Pour effacer un fichier de configuration, sélectionnez-le et cliquez sur **Effacer les fichiers**.

Copie ou enregistrement des types de fichiers de configuration du commutateur

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 en tant que fichier sur un autre appareil.

La *rubrique Copier/enregistrer la configuration* permet de copier ou d'enregistrer un fichier de configuration dans un autre afin de le sauvegarder.

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 une configuration d'un type de fichier vers un autre :

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

ÉTAPE 2 Sélectionnez le **Nom du fichier source** à copier. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)

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

ÉTAPE 4 Cliquez sur **Appliquer**. Le fichier est copié et le commutateur est mis à jour.

Définition de la configuration automatique DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) permet de transmettre des informations de configuration (y compris l'adresse IP d'un serveur TFTP et un nom de fichier de configuration) aux hôtes d'un réseau TCP/IP. Par défaut, le commutateur est activé en tant que client DHCP.

Configuration automatique DHCP

Lorsque l'adresse IP est allouée ou renouvelée, par exemple lors d'un redémarrage ou dans le cas d'une demande explicite de renouvellement DHCP et dans la mesure où le commutateur et le serveur sont configurés en conséquence, le commutateur transfère vers le commutateur, un fichier de configuration du serveur TFTP identifié par DHCP. Ce processus est connu sous le nom de *configuration automatique*.

REMARQUE Si vous activez Configuration automatique DHCP sur un commutateur sur lequel le protocole DHCP est désactivé, vous devez activer ce dernier en suivant la procédure décrite dans la section **Adressage IP**.

La *rubrique Configuration automatique DHCP* configure le commutateur afin qu'il reçoive les informations DHCP pointant sur un serveur TFTP pour une configuration automatique ou une configuration manuelle du serveur TFTP et du fichier de configuration pour le cas où les informations ne seraient pas fournies dans un message DHCP.

Notez les limitations suivantes se rapportant au processus de mise à jour 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, les adresses IP doivent être liées 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 *rubrique Configuration automatique DHCP* s'ouvre.

ÉTAPE 2 Saisissez les valeurs appropriées.

- **Configuration automatique via DHCP** : sélectionnez ce champ pour activer ou désactiver le transfert automatique d'une configuration d'un serveur TFTP vers la Configuration de démarrage du commutateur.
- **Serveur TFTP de secours** : saisissez l'adresse IP du serveur TFTP à utiliser si aucune adresse IP de serveur TFTP n'a été spécifiée dans le message DHCP.
- **Fichier de configuration de secours** : saisissez le chemin et le nom du fichier à utiliser si aucun fichier de configuration n'a été spécifié dans le message DHCP.

La fenêtre affiche les éléments suivants :

- **Adresse IP du dernier serveur TFTP 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.

  L'Adresse IP du dernier serveur TFTP pour configuration automatique et le Dernier nom du fichier de configuration automatique sont comparés aux informations reçues de la part d'un serveur DHCP lors de la réception d'une adresse IP de configuration pour le commutateur. Si ces valeurs ne correspondent pas, le commutateur transfère le fichier de configuration du serveur TFTP identifié par le serveur DHCP dans le fichier de Configuration de démarrage puis initie un redémarrage. Si les valeurs correspondent, aucune action n'est initiée.

ÉTAPE 3 Cliquez sur **Appliquer**. La Configuration automatique DHCP est mise à jour.

5

Informations et opérations administratives générales

Ce chapitre indique comment afficher les informations relatives au système et configurer différentes options sur le commutateur.

Il contient les rubriques suivantes :

- **Informations système**
- **Modèles de commutateurs**
- **Redémarrage du commutateur**
- **Surveillance de l'état et de la température du ventilateur**
- **Définition du délai d'expiration en cas de session inactive**

Informations système

La *rubrique 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

Affichage du récapitulatif du système

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

La rubrique Récapitulatif du système affiche les informations se rapportant au système ainsi qu'au matériel.

Informations système :

- **Description du système** : présente une description du système.
- **Emplacement du système** : indique l'emplacement physique du commutateur. Cliquez sur **Modifier** pour accéder à la *rubrique Paramètres système* et entrer cette information.
- **Contact système** : nom d'une personne à contacter. Cliquez sur **Modifier** pour accéder à la *rubrique Paramètres système* et entrer cette information.
- **Nom d'hôte** : nom du commutateur. Cliquez sur **Modifier** pour accéder à la *rubrique Paramètres système* et entrer cette information. 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).
- **ID de l'objet système** : identification unique du fournisseur du sous-système de gestion du réseau contenu dans l'entité (utilisée dans SNMP).
- **Temps utilisation syst.** : temps qui s'est écoulé depuis le dernier redémarrage.
- **Heure actuelle** : heure actuelle du système.
- **Adresse MAC de base** : adresse MAC du commutateur.
- **Trames Jumbo** : état de prise en charge des trames Jumbo. Cette prise en charge peut être activée ou désactivée depuis la *rubrique Paramètres du port*.

Informations sur la version du matériel et du micrologiciel :

- **Description du modèle** : description du modèle de commutateur.
- **Numéro de série** : numéro de série.
- **PID VID** : référence de pièce et ID de version.
- **Version du micrologiciel (image active)** : numéro de version du micrologiciel de l'image active.
- **MD5 Checksum du micrologiciel (image active)** : MD5 Checksum de l'image active.
- **Version du micrologiciel (non active)** : numéro de version du micrologiciel de l'image non active. .
- **MD5 Checksum du micrologiciel (non active)** : MD5 Checksum de l'image non active.

- **Version de démarrage** : numéro de version de démarrage.
- **MD5 Checksum de démarrage** : MD5 Checksum de la version de démarrage.
- **Locale** : locale de la première langue (toujours définie sur Anglais).
- **Version de langue** : version du micrologiciel du paquet linguistique principal.
- **MD5 Checksum de langue** : MD5 Checksum du fichier de langue.
- **Locale** : locale de la seconde langue.
- **Version de langue** : version du micrologiciel du paquet linguistique secondaire.
- **MD5 Checksum de langue** : MD5 Checksum du fichier de langue secondaire.

État PoE général sur les modèles dotés de la fonctionnalité PoE :

- **Puissance maximale disponible (W)** : puissance maximale disponible pouvant être fournie par le PoE.
- **Consommation de l'alimentation principale (W)** : puissance PoE actuelle fournie aux périphériques PoE connectés.
- **État de fonctionnement du système** : mode d'alimentation du PoE.

Configuration des paramètres système

Pour accéder aux paramètres système :

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

ÉTAPE 2 Modifiez 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 :
  - *Valeurs par défaut* : le nom d'hôte par défaut (Nom du système) de ces commutateurs est *commutateur123456*, où 123456 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'hôtes ne peuvent pas être précédés ou 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).

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

Modèles de commutateurs

Tous les modèles peuvent être entièrement gérés via l'utilitaire Web de configuration du commutateur. Le Niveau 2 est le mode de fonctionnement par défaut de tous les appareils. En mode Niveau 2, le commutateur transfère les paquets en tant que pont VLAN-aware. En mode Niveau 3, le commutateur effectue à la fois un routage IPv4 et un pontage VLAN-aware.

Chaque modèle peut être configuré en mode Niveau 3 en utilisant l'interface console, décrite dans le chapitre **Interface de la console** du guide d'administration. Lorsque le commutateur fonctionne en mode Niveau 3, les contrôleurs de limite du débit VLAN et de QoS ne sont pas opérationnels. Les autres fonctionnalités du Mode avancé de QoS sont quant à elles opérationnelles.

Modèles de commutateurs administrables

Nom du modèle	ID du produit (PID)	Description	Ports	Puissance dédiée au PoE	Nbre de ports gérant PoE
SG 300-10	SRW2008-K9	10 ports Gigabit	g1-g10, 8 GE + 2 ports combo (GE/SFP)		
SG 300-10MP	SRW2008MP-K9	10 ports Gigabit PoE	g1-g10, 8 GE + 2 ports combo	124 W au maximum	8
SG 300-10P	SRW2008P-K9	10 ports Gigabit PoE	g1-g10, 8 GE + 2 ports combo	62 W au maximum	8

Modèles de commutateurs administrables (Suite)

Nom du modèle	ID du produit (PID)	Description	Ports	Puissance dédiée au PoE	Nbre de ports gérant PoE
SG 300-20	SRW2016-K9	20 ports Gigabit	g1-g20, 16 GE + 4 GE-2 logements SFP partagés		
SG 300-28	SRW2024-K9	28 ports Gigabit	g1-g28. 24 ports normaux et quatre ports spécifiques - liaisons montantes et ports combo		
SG 300-28P	SRW2024P-K9	28 ports Gigabit PoE	g1-g28. 24 ports normaux et quatre ports spécifiques - liaisons montantes et ports combo	180 W au maximum	24
SG 300-52	SRW2048-K9	52 ports Gigabit	g1-g52. 48 ports normaux et quatre ports spécifiques - liaisons montantes et ports combo		
SF 300-08	SRW208-K9	8 ports 10/100	e1-e8. 8 ports 10/100		
SF 302-08	SRW208G-K9	8 ports 10/100	e1-e8, g1-g2. 8 ports 10/1000 + deux ports 10/100/1000		
SF 302-08MP	SRW208MP-K9	8 ports 10/100 PoE	e1-e8, g1-g2. 8 ports 10/1000 + deux ports 10/100/1000	124 W au maximum	8
SF 302-08P	SRW208P-K9	8 ports 10/100 PoE	e1-e8, g1-g2. 8 ports 10/100 + deux ports 10/100/1000	62 W au maximum	8
SF 300-24	SRW224G4-K9	24 ports 10/100	e1-e24, g1-g4. 24 ports 10/100 normaux + quatre ports 10/100/1000 spécifiques - liaisons montantes et ports combo		
SF 300-24P	SRW224G4P-K9	24 ports 10/100 PoE	e1-e24, g1-g4. 24 ports 10/100 normaux + quatre ports 10/100/1000 spécifiques - liaisons montantes et ports combo	180 W au maximum	24
SF 300-48	SRW248G4-K9	48 ports Gigabit	e1-e48, g1-g4. 48 ports 10/100 normaux + quatre ports 10/100/1000 spécifiques - liaisons montantes et ports combo		
SF 300-48P	SRW248G4P-K9	48 ports 10/100 PoE	e1-e48, g1-g4. 48 ports 10/100 normaux + quatre ports 10/100/1000 spécifiques - liaisons montantes et ports combo	375 W au maximum	48

Redémarrage du commutateur

Certaines modifications apportées au niveau de 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, consultez la section **Fichiers et types de fichiers** du chapitre **Gestion des fichiers système**.

Vous pouvez sauvegarder la configuration en utilisant Administration > Copier/enregistrer la configuration ou cliquer sur **Enregistrer** en haut de la fenêtre. Vous pouvez également télécharger la configuration à partir d'un appareil distant. Pour plus d'informations, consultez la section **« Téléchargement ou sauvegarde d'une configuration ou d'un journal »** du chapitre **Gestion des fichiers système**.

Pour redémarrer le commutateur :

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

ÉTAPE 2 Cliquez sur l'un des boutons de redémarrage.

- **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. Lorsque cette action est sélectionnée, tout paramètre non enregistré dans un autre fichier est effacé.

ATTENTION Configuration automatique DHCP doit être désactivée (cette option est activée par défaut). Dans le cas contraire, un fichier de configuration pourrait être chargé depuis un serveur TFTP, à la place des paramètres d'origine par défaut.

Le commutateur est redémarré.

Surveillance de l'état et de la température du ventilateur

La *rubrique Santé* affiche l'état et la température du ventilateur du commutateur sur un SF 300-48P. Les modèles SG 300-28P, SF 300-24P et SG 300-52 affichent uniquement l'état du ventilateur.

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

La page Santé affiche les champs suivants :

- **État du ventilateur** : état du ventilateur.
- **Température** : température du commutateur.

Définition du délai d'expiration en cas de session inactive

Le *Délai d'expiration de session inactive* configure les intervalles de temps pendant lesquels les sessions de gestion peuvent rester inactives avant d'expirer et de nécessiter une nouvelle connexion de l'utilisateur pour rétablir une des sessions suivantes :

- **Délai d'expiration de session HTTP**
- **Délai d'expiration de session HTTPS**
- **Délai d'expiration de session de console**
- **Délai d'expiration de session Telnet**
- **Délai d'expiration de session SSH**

Pour saisir le délai d'expiration en cas de session inactive et ce pour différents types de sessions :

ÉTAPE 1 Cliquez sur **Administration** > **Délai d'expiration de session inactive**. La rubrique *Délai d'expiration de session inactive* s'ouvre.

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

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

6

Heure système

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. L'heure constitue également le seul système de référence entre tous les périphériques du réseau. Sans synchronisation de l'heure, la corrélation précise des fichiers journaux entre ces périphériques est difficile, voire même impossible.

Le suivi des failles de sécurité et l'utilisation du réseau font entre autre partie des raisons spécifiques. Il s'avère presque impossible de suivre les problèmes affectant un grand nombre de composants si les heures systèmes des journaux ne sont pas précises.

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

C'est pour ces raisons que l'heure configurée sur tous les périphériques du réseau nécessite 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 sur celle du serveur SNTP. Le commutateur fonctionne uniquement en tant que client SNTP et ne peut pas fournir de services d'heure à d'autres périphériques.

Ce chapitre décrit les options permettant de configurer l'heure système, le fuseau horaire et l'heure d'été (DST). Il contient les rubriques suivantes :

- **Options d'heure système**
- **Configuration de l'heure système**
- **Paramétrer SNTP**
- **Définition de l'authentification SNTP**

Options d'heure système

L'heure système peut être réglée manuellement par l'utilisateur ou dynamiquement à l'aide du serveur SNTP. 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 d'une certaine manière, à partir de DHCP, de SNTP, de valeurs définies manuellement ou si rien d'autre ne fonctionne, à partir des paramètres usine par défaut.

Heure

Les méthodes suivantes sont disponibles pour obtenir ou définir l'heure sur le commutateur :

- SNTP qui garantit une synchronisation de l'heure réseau précise du commutateur à la milliseconde près en utilisant un serveur SNTP comme source d'horloge.

  REMARQUE Sans synchronisation de l'heure, la corrélation précise des fichiers journaux entre périphériques est difficile, voire même impossible. Nous vous recommandons d'utiliser SNTP pour la source d'horloge.

- Saisie manuelle de l'heure système par l'utilisateur.
- Saisie de l'heure par l'ordinateur qui accède au commutateur via l'utilitaire de configuration de l'appareil. Si cette fonction est activée, le commutateur utilise l'heure système de l'ordinateur de configuration, sauf si l'heure a été manuellement configurée sur le commutateur par l'utilisateur ou si la prise en charge du serveur SNTP n'est pas disponible ou activée.

  REMARQUE La réception de l'heure depuis l'ordinateur de configuration du commutateur devrait être utilisée en dernier recours, comme par exemple, après une panne de courant ou lorsqu'aucune autre source d'horloge n'est disponible.

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 par l'utilisateur où le fuseau horaire et l'heure d'été définis manuellement deviennent les paramètres opérationnels, seulement si la configuration dynamique pour ces options est désactivée ou échoue.

Configuration de l'heure système

Utilisez la *rubrique Heure système* pour configurer l'heure, l'heure d'été, le fuseau horaire ainsi que la source d'horloge. Si l'heure est définie manuellement, saisissez-la ici.

ATTENTION Le commutateur n'a pas d'horloge interne qui met cette valeur à jour. 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 *rubrique Heure système* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

▪ **Source d'horloge** : sélectionnez la source utilisée pour définir l'horloge système.

- **Utiliser les paramètres locaux** : l'heure système est saisie manuellement ou prise sur l'ordinateur de configuration. Si ce bouton est sélectionné, saisissez les paramètres locaux.
- **Utiliser le serveur SNTP** : l'heure système est obtenue à partir d'un serveur SNTP. Ajoutez également un serveur SNTP et activez le mode de diffusion SNTP en utilisant la *rubrique Paramétrer SNTP*. Exécutez l'authentification des sessions SNTP en utilisant la *rubrique Authentification SNTP*.

- **Autre source d'horloge** : sélectionnez cette option pour définir la date et l'heure depuis cet ordinateur lorsque l'option Utiliser les paramètres locaux est sélectionnée.
- **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** à la *rubrique Interface IPv4*.

Paramètres locaux : l'heure locale est utilisée lorsqu'il n'existe aucune autre source de temps comme un serveur SNTP :

- **Date** : saisissez la date du système.
- **Heure locale** : saisissez l'heure système.
- **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 +1et celui pour New York est GMT - 5.
- **Heure d'été** : sélectionnez Heure d'été pour activer cette option.
- **Différence d'heure** : saisissez le nombre en minutes du changement d'heure causé par l'heure d'été.
- **Type d'heure d'été** : sélectionnez le mode de définition de l'heure d'été :
  - **États-Unis** : selon les dates utilisées aux États-Unis
  - **Europe** : selon les dates utilisées par l'Union Européenne et d'autres pays utilisant cette norme.
  - **Par dates** : manuellement, généralement pour un pays autre que les États-Unis ou un pays européen. Saisissez les paramètres suivants :
    - **De** : jour et heure de début de l'heure d'été.
    - **À** : jour et heure de fin de l'heure d'été.
    - **Récurrent** : l'heure d'été entre en vigueur à la même date chaque année. Saisissez les paramètres suivants :

      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 définies et le commutateur est mis à jour.

Les paramètres de temps s'affichent dans la section *Détails sur l'heure actuelle*.

Paramétrer SNTP

Un commutateur peut être configuré afin de synchroniser son horloge système avec un serveur SNTP en utilisant la *rubrique Paramétrer SNTP*.

REMARQUE Cette fonctionnalité nécessite que les serveurs DNS soient configurés sur le commutateur (voir la section **Définition de serveurs DNS**) pour fonctionner correctement.

Le commutateur prend en charge les modes suivants :

- Diffusion : le serveur SNTP diffuse 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.
- Mode Serveur SNTP monodiffusion : le commutateur envoie des requêtes de monodiffusion à la liste de serveurs SNTP configurés manuellement et attend une réponse.

Le commutateur est capable de disposer des deux modes activés en même temps et choisit la meilleure source de paramètres selon la strate la plus proche (distance par rapport à l'horloge de référence).

Pour définir les paramètres du serveur SNTP :

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

ÉTAPE 2 (Facultative) Sélectionnez **Réception de diffusion SNTP** > **Activer** pour écouter les paquets de synchronisation de la diffusion SNTP pour les informations d'heure système. Si cette option est sélectionnée, le système n'affiche pas le serveur SNTP à partir duquel les paramètres d'heure sont reçus.

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

- **Serveur SNTP** : adresse IP du serveur SNTP. Un maximum de huit serveurs SNTP peuvent être définis. Le serveur préféré est choisi selon le niveau de sa strate.
- **Intervalle d'interrogation** : intervalle (en secondes) auquel le serveur SNTP est interrogé pour les informations d'heure système. L'intervalle d'interrogation est de 1024 secondes.
- **ID de clé d'authentification** : l'identification de clé sert à communiquer entre le serveur SNTP et le commutateur.
- **Préférence** : priorité d'utilisation pour le serveur SNTP.
  - *Principal* : serveur disposant du niveau de strate le plus faible. Le niveau de strate représente la distance par rapport à l'horloge de référence. Les informations concernant l'heure sont puisées à partir de ce serveur.
  - *Secondaire* : serveur disposant du second niveau de strate le plus faible après celui du serveur principal. Sert de serveur de secours au serveur principal.
  - *En fonctionnement* : serveur SNTP qui envoie ou reçoit actuellement des informations SNTP.
- **État** : état du serveur SNTP. Les options disponibles sont les 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.

- **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.
- **Ecart** : 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 3 Cliquez sur **Ajouter** pour afficher la *rubrique Ajouter un serveur SNTP*.

ÉTAPE 4 Saisissez les paramètres suivants :

- **Définition du serveur** : sélectionnez cette option si le serveur SNTP sera identifié par son adresse IP ou si vous allez choisir 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 pas être routée et ne peut servir uniquement 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 entrée remplace l'adresse dans la configuration.

  - *Globale* : l'adresse IPv6 est d'un type global d'IPV6 de monodiffusion visible et accessible à partir d'autres réseaux.

- **Interface de liaison locale** : sélectionnez dans la liste de liaison locale (si le type d'adresse IPv6 Liaison locale est sélectionné).
- **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 SNTP 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 SNTP 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. (Créez des clés d'authentification en utilisant la *rubrique Authentification SNTP*.)

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

Définition de l'authentification SNTP

La *rubrique Authentification SNTP* permet la configuration des clés d'authentification utilisées pour communiquer avec un serveur SNTP nécessitant une authentification.

Lorsqu'une clé est créée, elle doit être liée à un ou plusieurs serveurs SNTP appropriés pour être authentifiée. Cette clé d'authentification peut également être utilisée pour l'authentification lors de la réception de la synchronisation de diffusion.

Des sessions SNTP peuvent nécessiter une authentification. Un serveur SNTP monodiffusion nécessitant une authentification doit être lié à une clé d'authentification lorsqu'il est ajouté en utilisant la *rubrique Ajouter un serveur SNTP*.

Pour définir une l'authentification SNTP :

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

ÉTAPE 2 Sélectionnez **Authentification SNTP** pour requérir 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 *rubrique 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** : cochez la case pour permettre au commutateur de recevoir les informations de synchronisation de diffusion uniquement à partir d'un serveur SNTP utilisant cette clé d'authentification.

ÉTAPE 6 Cliquez sur **Appliquer**. L'authentification SNTP est définie et le commutateur mis à jour.

7

Gestion des diagnostics de l'appareil

Ce chapitre 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.

Il contient 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 des CPU**

Test des ports cuivre

La *rubrique Ports cuivre* affiche les résultats des tests de câbles intégrés effectués sur les câbles en cuivre.

Deux types de tests sont utilisés :

- 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 100 mètres de long.
- Les tests s'appuyant sur la technologie DSP sont effectués sur des liaisons GE actives pour en mesurer la longueur.

ATTENTION Lorsqu'un port est testé, il est mis en l'état Inactif et les communications sont interrompues. Une fois le test terminé, le port revient en 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** > **Ports cuivre**. La *rubrique Ports cuivre* s'ouvre.

Cette page affiche les résultats des tests de base précédemment réalisés.

ÉTAPE 2 Pour effectuer un Test de base, sélectionnez un port dans la liste des ports et cliquez sur **Test de base**. Un message s'affiche, indiquant que le test amène brièvement la liaison en état inactif.

ÉTAPE 3 Cliquez sur **OK** pour confirmer que la liaison peut passer à l'état inactif ou sur **Annuler** pour abandonner le test.

Les résultats s'affichent sur la page :

- **Résultat de test** : les résultats du test du câble. Les valeurs possibles sont :
  - *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.
- **Longueur de câble** : longueur estimée du câble, uniquement disponible pour les liaisons 1 Gbit/s, à l'exception des ports combo. Consultez l'explication fournie à la section *Description de la longueur de câble*.

  REMARQUE La longueur du câble est « **Inconnu** » lorsque les fonctionnalités écologiques sont activées.
- **Dernière mise à jour** : heure à laquelle a été effectué le dernier test sur le port.

ÉTAPE 4 Pour effectuer le test avancé sur tous les ports GE, cliquez sur **Test avancé**. La *rubrique Fonction étendue câble en cuivre* s'ouvre.

REMARQUE Pour éviter d'obtenir des résultats inconnus au cours du Test avancé, réalisez au préalable le Test de base.

Cette page affiche les résultats du test le plus récent :

- **Port** : identificateur du port.
- **État du câble** : état du câble.
- **Vitesse** : vitesse de la liaison.
- **État de la liaison** : état Actif/Inactif actuel de la liaison.
- **Paire** : paires de fils de câble testées.
- **Distance au défaut** : distance entre le port et l'emplacement du câble où le problème a été détecté.
- **État** : état de la paire de fils. Rouge indique un défaut et Vert indique l'état OK.
- **Longueur de câble** : longueur du câble en mètres.

  Si la liaison est inactive, la technologie TDR est utilisée pour tester les ports GE et FE. Les mesures de longueur de câble sont précises à 3 ou 4 mètres près.

  Si la liaison est active, la technologie DSP est utilisée pour tester les ports GE. (La longueur des ports FE n'est pas testée.) Les valeurs renvoyées sont :

  - 1 : moins de 50 mètres
  - 2 : de 50 à 80 mètres
  - 3 : de 80 à 110 mètres
  - 4 : de 110 à 140 mètres
  - 5 : plus de 140 mètres
- **Canal** : canal du câble.
- **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.

ÉTAPE 5 Cliquez sur **Fermer** pour fermer la fenêtre.

Affichage de l'état des modules optiques

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

SFP compatibles MSA

Les émetteurs-récepteurs SFP FE (100 Mbit/s) suivants sont disponibles :

- 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 disponibles :

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

Pour afficher les résultats des tests optiques, cliquez sur **Administration** > **Diagnostics** > **État des modules optiques**. La *rubrique 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'ensemble d'un VLAN vers une connexion de surveillance réseau sur un autre port commuté. 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 affiche les paquets de données afin de diagnostiquer, de déboguer et de contrôler 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 provenant 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.

La mise en miroir VLAN n'est pas active sur un VLAN qui n'a pas été créé. Prenons un exemple : le VLAN 23 est créé par GVRP puis, pour une raison ou pour une autre, supprimé de la base de données des VLAN. Vous créez ensuite manuellement le VLAN 34 ainsi que la mise en miroir des ports, qui intègre le VLAN 23, le VLAN 34 ou les deux et supprimez par la suite le VLAN 34. L'état de la mise en miroir des ports est alors défini comme **Pas prêt**, les VLAN n'étant plus enregistrés dans la base de données.

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

Pour activer la mise en miroir des ports et VLAN :

ÉTAPE 1 Cliquez sur **Administration** > **Diagnostics** > **Mise en miroir des ports et VLAN**. La *rubrique 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, sortant du port ou les deux.
- **État** : indique si l'interface est active ou inactive.

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

ÉTAPE 3 Saisissez les paramètres :

- **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. Un port identifié en tant que port de destination de l'analyseur conserve cette fonction jusqu'à ce que toutes les entrées aient été supprimées.
- **Interface source** : sélectionnez un Port ou VLAN en tant que 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 et le commutateur mis à jour.

Affichage de l'utilisation des CPU

La *rubrique Utilisation des CPU* affiche l'utilisation des CPU du commutateur. Vous pouvez activer ou désactiver la surveillance de l'utilisation des CPU et configurer la fréquence de mise à jour du graphique.

Pour activer et afficher la surveillance de l'utilisation des CPU :

ÉTAPE 1 Cliquez sur **Administration** > **Diagnostics** > **Utilisation des CPU**. La *rubrique Utilisation des CPU* s'ouvre.

ÉTAPE 2 Sélectionnez **Utilisation des CPU** pour activer l'affichage des informations relatives à l'utilisation des ressources du CPU.

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

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

8

Configuration de la détection

Ce chapitre fournit des informations sur la configuration de la détection.

Il contient les rubriques suivantes :

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

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, HTTPs et Telnet. (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 pour un système en mode L2 (Layer 2, couche 2)

Bonjour pour un système en mode L2 (Layer 2, couche 2)

Lorsque le commutateur fonctionne en mode Layer 2, la détection Bonjour est activée au niveau global ; vous ne pouvez pas l'activer séparément pour chaque port ou chaque VLAN. Le commutateur annonce tous les services qui ont été activés par l'administrateur : HTTP, HTTPS, Telnet et SSH.

Lorsque vous activez à la fois la détection Bonjour et IGMP, l'adresse IP de multidiffusion de Bonjour est affichée dans la *rubrique Adresse IP du groupe de multidiffusion*.

Lorsque vous désactivez la détection Bonjour, le commutateur cesse toute annonce de type de service et ne répond à aucune demande de service émanant des applications de gestion réseau.

Pour activer Bonjour globalement lorsque le commutateur fonctionne en mode Layer 2 :

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

Bonjour pour un système en mode L3 (Layer 3, couche 3)

Bonjour pour un système en mode L3 (Layer 3, couche 3)

En mode Layer 3, chaque interface (VLAN, port ou LAG) peut recevoir une adresse IP. Lorsque vous activez Bonjour, le commutateur peut envoyer des paquets de détection Bonjour vers toutes les interfaces dotées d'une adresse IP. (Accédez à **Configuration IP** > **Interfaces de gestion et IP** > **Interface IPv4** pour configurer une adresse IP sur une interface.) Vous pouvez activer la détection Bonjour pour certaines interfaces précises.

Si une interface (un VLAN, par exemple) est supprimée, des paquets Goodbye sont envoyés pour désenregistrer les services annoncés par le commutateur auprès de la table de cache de voisinage sur le réseau local. (Reportez-vous à la table de contrôle des interfaces de détection Bonjour sur la page **Administration** > **Détection - Bonjour**. Si les services disponibles changent, ces modifications sont annoncées, ce qui désenregistre les services désactivés et enregistre les services activés. Si vous modifiez une adresse IP, cette modification est annoncée.

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

Si Bonjour est désactivé, le commutateur n'envoie aucune annonce de détection Bonjour et n'écoute pas les annonces de détection Bonjour envoyées par d'autres périphériques.

Pour configurer Bonjour lorsque le commutateur fonctionne en mode Layer 3 :

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

ÉTAPE 2 Sélectionnez les interfaces à activer ou désactiver, ainsi que celles à ajouter ou supprimer dans la table de contrôle des interfaces de détection Bonjour. La détection Bonjour ne peut être activée que sur les interfaces dotées d'une adresse IP.

ÉTAPE 3 Cliquez sur **Ajouter** pour activer une interface et l'ajouter à la table de contrôle des interfaces de détection Bonjour.

Cliquez sur **Supprimer** pour désactiver une interface et la supprimer de la table de contrôle des interfaces de détection Bonjour.

ÉTAPE 4 Cliquez sur **Appliquer**. Une fenêtre pop-up éclair (« popup ») s'affiche, indiquant si Bonjour a été correctement activé ou désactivé sur les interfaces concernées.

ÉTAPE 5 Cliquez sur **Appliquer**. Bonjour est activé ou désactivé sur les interfaces ajoutées.

Configuration de LLDP

Link Layer Discovery Protocol (LLDP) permet aux gestionnaires réseau d'effectuer le dépannage et d'améliorer la gestion du réseau en détectant des topologies et en assurant leur maintenance dans des environnements multifournisseurs. LLDP détecte le voisinage réseau en normalisant les méthodes de détection des périphériques réseau afin de s'annoncer auprès des autres systèmes et de stocker les informations détectées.

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

Le protocole LLDP fonctionne en mode Layer 2 en diffusant des trames de multidiffusion depuis chaque port. On les appelle PDU (Protocol Data Units, unités de données de protocole) ou PDU LLDP. Elles sont traitées par les périphériques qui reconnaissent le protocole LLDP. La PDU LLDP contient des TLV (combinaisons Type, Longueur, Valeur), qui stockent les informations diffusées par le périphérique. Vous pouvez configurer les types de TLV à diffuser.

Le protocole LLDP possède une extension nommée LLDP Media Endpoint Discovery (LLDP MED, détection d'extrémité de support), qui fournit et accepte des informations émanant de périphériques voix ou vidéo. Pour en savoir plus sur LLDP MED, reportez-vous à la section *Protocole LLDP MED*.

Flux de travail de configuration de LLDP

Voici des exemples d'actions qu'il est possible de réaliser avec la fonction LLDP :

1. Activer LLDP globalement (LLDP est activé par défaut) puis entrer des paramètres LLDP globaux comme l'intervalle d'envoi des mises à jour LLDP à l'aide de la *rubrique Propriétés LLDP*.
2. Configurer LLDP pour chaque interface à l'aide de la *rubrique Paramètres du port*.
3. Créer des stratégies réseau LLDP MED à l'aide de la *rubrique Stratégie réseau LLDP MED*.
4. Associer des stratégies réseau LLDP MED aux ports à l'aide de la *rubrique Paramètres des ports LLDP MED*.
5. Afficher les détails d'état des ports locaux LLDP à l'aide de la *rubrique Informations locales LLDP.*
6. Afficher les informations LLDP détectées depuis les voisins, notamment le port local, le nom système, la durée de vie, la description du système et les fonctions système, ceci à l'aide de la *rubrique Informations de voisinage LLDP*.
7. Afficher des informations statistiques liées à LLDP pour chaque interface à l'aide de la *rubrique Statistiques LLDP*.
8. Afficher les informations de surcharge à l'aide de la *rubrique Surcharge LLDP*.

Configuration des propriétés LLDP

La *rubrique Propriétés LLDP* vous permet de saisir les paramètres LLDP généraux. Cela inclut 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 *rubrique Propriétés LLDP* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **État LLDP** : sélectionnez l'état LLDP global sur le commutateur.

- **Intervalle d'annonce TLV** : définissez, en nombre de secondes, la fréquence d'envoi des mises à jour des annonces LLDP.
- **Intervalle de notification SNMP de changement de topologie** : saisissez le délai minimal entre deux notifications SNMP.
- **Multiplicateur de conservation** : saisissez la durée de conservation des paquets LLDP avant leur élimination, en multiples de l'intervalle d'annonce TLV. Par exemple, si l'intervalle d'annonce TLV est de 30 secondes et si le multiplicateur de conservation est 4, 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.

Pour consulter la description de LLDP MED, reportez-vous à la section *Protocole LLDP MED*.

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.

ÉTAPE 4 Cliquez sur **Appliquer**. Les propriétés LLDP sont définies.

Modification des paramètres de port LLDP

La *rubrique Paramètres du port* vous permet d'activer LLDP et la notification SNMP pour chaque port, ainsi que de saisir les TLV envoyées dans la PDU LLDP.

En définissant ces propriétés, il est possible de fournir divers types d'information aux périphériques qui prennent en charge le protocole LLDP.

Vous pouvez sélectionner les TLV LLDP MED à annoncer dans la *rubrique Paramètres des ports LLDP MED*.

Pour définir des paramètres de port LLDP :

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

Cette page affiche les informations LLDP des ports.

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

Cette page contient les champs suivants :

- **Interface** : sélectionnez le port à définir.
- **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 SNMP** : sélectionnez **Activer** pour envoyer des notifications aux destinataires de notification SNMP (système de gestion SNMP, par exemple) en cas de modification de la topologie.

  L'intervalle entre deux notifications est défini dans le champ Intervalle de notification SNMP de changement de topologie de la *rubrique Propriétés LLDP*. Définissez les destinataires des notifications SNMP en utilisant les options **SNMP** > **Destinataires de notifications v1,2** et/ou **SNMP** > **Destinataires de notifications v3**.
- **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 ou non sur le commutateur. Les fonctions 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 début 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 d'annonce de l'adresse IP de gestion au commutateur :
  - *Annonce automatique* : envoyez l'adresse IP de gestion actuelle au commutateur, qu'elle ait été acquise par DHCP ou manuellement.
  - *Aucun* : aucune annonce de l'adresse IP de gestion.
  - *Annonce manuelle* : sélectionnez cette option et l'adresse IP de gestion à annoncer. Il est recommandé de choisir cette option lorsque le commutateur fonctionne en mode Layer 3 et qu'il est configuré avec plusieurs adresses IP.
- **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 puis cliquez sur **Appliquer**. Les paramètres de port sont modifiés et le commutateur est mis à jour.

Protocole LLDP MED

LLDP Media Endpoint Discovery (LLDP MED) est une amélioration de LLDP qui fournit des fonctions supplémentaires de prise en charge des périphériques multimédias.

LLDP MED :

- Fournit des informations détaillées sur la topologie réseau, notamment les périphériques du réseau et leur emplacement. Par exemple, indique le téléphone IP connecté sur un port particulier, les logiciels exécutés sur un commutateur donné et le numéro des ports connectés à chaque PC.
- 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.
- Fournit des informations de dépannage. LLDP MED envoie des alertes aux gestionnaires réseau :
  - Conflits de débit de port et de mode duplex
  - Erreurs de configuration des stratégies QoS

REMARQUE Le commutateur *annonce* automatiquement la stratégie en fonction de votre configuration ; toutefois, vous devez également configurer manuellement le commutateur pour qu'il *utilise* cette stratégie.

Configuration d'une stratégie réseau LLDP MED

Une stratégie réseau LLDP MED est un ensemble de paramètres de configuration apparentés identifié par un numéro de stratégie réseau. Cet ensemble est chargé dans une TLV LLDP MED puis envoyé aux périphériques connectés au commutateur. Les périphériques connectés emploient ces informations pour envoyer un trafic tel que le définit la stratégie réseau. Par exemple, vous pouvez créer une stratégie pour les téléphones VoIP afin de leur demander :

- d'envoyer le trafic voix sur le VLAN 10 ;
- de marquer le trafic voix avec DSCP=63 ;
- de transmettre le trafic de données au commutateur (depuis le PC connecté au commutateur via le téléphone VoIP) sans modifier le trafic envoyé par le PC (en général, sans marquage).

Vous associez des stratégies réseau aux ports à l'aide de la *rubrique Paramètres des ports LLDP MED*. (L'administrateur doit créer les VLAN puis configurer leurs membres sur la base des spécifications des stratégies réseau LLDP-MED.)

Pour définir une stratégie réseau LLDP MED :

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

Cette page affiche les stratégies réseau précédemment créées.

ÉTAPE 2 Cliquez sur **Ajouter** pour ouvrir la *rubrique Ajouter une stratégie réseau LLDP MED*.

Cette page vous permet de définir une nouvelle stratégie.

ÉTAPE 3 Saisissez les valeurs appropriées.

- **Numéro de stratégie réseau** : sélectionnez le numéro de la stratégie à créer.
- **Application** : sélectionnez dans la liste le type d'application (type de trafic) pour lequel vous définissez la stratégie réseau :
  - **Voix**
  - **Signalisation vocale**
  - **Voix invité**
  - **Signalisation vocale invité**
  - **Voix, téléphone logiciel**
  - **Vidéoconférence**
  - **Lecture vidéo en continu**
  - **Signaux vidéo**
- **ID VLAN** : saisissez l'ID du VLAN auquel le trafic doit être envoyé.
- **Balise VLAN** : indiquez si le trafic doit être marqué ou non.
- **Priorité d'utilisateur** : sélectionnez le niveau de priorité qui sera accordé au trafic défini par cette stratégie réseau.
- **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 4 Cliquez sur **Appliquer**. La stratégie réseau est définie. Associez cette stratégie à un port à l'aide de la *rubrique Paramètres des ports LLDP MED*.

Configuration des paramètres de port LLDP MED

La *rubrique Paramètres des ports LLDP MED* vous permet de sélectionner des stratégies réseau, précédemment configurées dans la *rubrique Stratégie réseau LLDP MED*, afin de les annoncer sur le port. Vous pouvez aussi sélectionner les TLV LLDP MED à envoyer dans la PDU LLDP.

Pour configurer LLDP MED sur chaque port :

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

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

ÉTAPE 2 Sélectionnez un port puis cliquez sur **Modifier**. La *rubrique Modifier les paramètres de port LLDP MED* s'ouvre.

Cette page vous permet d'associer des stratégies LLDP MED à des ports.

ÉTAPE 3 Saisissez les paramètres.

- **Port** : sélectionnez le port à configurer. Après avoir configuré ce port et cliqué sur **Appliquer**, vous pouvez configurer un autre port sans revenir à la rubrique Paramètres des ports LLDP MED.
- **État LLDP MED** : Activez/désactivez LLDP MED sur ce port.
- **Notification SNMP** : indiquez si la notification SNMP doit être envoyée, port par port, lorsqu'une station de travail prenant en charge MED est détectée (un système de gestion SNMP, par exemple), lors d'un changement de topologie.
- **TLV facultatives disponibles** : sélectionnez les TLV que le commutateur peut publier en les déplaçant vers la liste *TLV facultatives sélectionnées*.
- **Stratégies réseau disponibles** : sélectionnez les stratégies LLDP MED que LLDP va publier en les déplaçant vers la liste Stratégies réseau sélectionnées. Vous les aviez précédemment créées dans la *rubrique Stratégie réseau LLDP MED*.

  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 civique 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 4 Cliquez sur **Appliquer**. Les paramètres de port LLDP MED sont modifiés et le commutateur mis à jour.

Affichage de l'état des ports LLDP

La *rubrique Table d'état des ports LLDP* affiche des informations globales concernant LLDP ainsi que sur l'état LLDP de chaque port.

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

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 activées** : 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 la principale fonction de périphérique activée sur le 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** > **Propriétés**. La *rubrique Informations locales LLDP* s'ouvre.

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 2 Sélectionnez l'entrée voulue dans la liste **Port**.

Cette page contient les champs suivants :

Global

- **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 activées** : 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 ; généralement, une adresse Layer 3.
- **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 IEEE 802.3 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 ou non agrégée.
- **ID du port d'agrégation** : ID d'interface agrégée annoncé.

Détails MED

- **Fonctionnalités activées** : fonctions MED activées 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 d'extrémité 1** : indique une extrémité générique offrant des services LLDP de base.
  - **Classe d'extrémité 2** : indique un point d'extrémité multimédia offrant des services de lecture multimédia en continu, en plus des services de classe 1.
  - **Classe d'extrémité 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 bien** : ID du bien.

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 :

- **Civique** : adresse, ndont le nom de la rue.
- **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 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. Les valeurs disponibles sont les suivantes :
  - Marqué : indique que la stratégie réseau est définie pour les VLAN avec marquage.
  - Non marqué : indique que la stratégie réseau est définie pour les VLAN sans marquage.
- **Priorité d'utilisateur** : priorité d'utilisateur de la stratégie réseau.
- **DSCP** : DSCP de la stratégie réseau.

Affichage des informations LLDP des voisins

La *rubrique Informations de voisinage LLDP* affiche les informations reçues via le protocole LLDP depuis les 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 LLDP des voisins**. La *rubrique Informations de voisinage LLDP* s'ouvre.

Cette page contient 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 *rubrique Informations LLDP des voisins* s'ouvre.

Cette page contient 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 activées** : fonctions principales du périphérique. Les fonctions 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.

Adresse 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 interfaces Ethernet et l'injection de bits dans le réseau. Exemple : mode full duplex 100BASE-TX.

Alimentation 802.3 via MDI

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

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.

Détails MED

- **Fonctionnalités activées** : 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 d'extrémité 1* : indique un point d'extrémité générique offrant des services LLDP de base.

- *Classe d'extrémité 2* : indique un point d'extrémité multimédia offrant des services de lecture multimédia en continu, en plus des services de classe 1.
- *Classe d'extrémité 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 bien** : ID du bien.

VLAN et protocole 802.1

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

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

- **ID du 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 :

- **Civique** : adresse civique, dont le nom de la rue.
- **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 marquage.
- **Priorité d'utilisateur** : priorité d'utilisateur de la stratégie réseau.
- **DSCP** : DSCP de la stratégie réseau.

Accès aux statistiques LLDP

La *rubrique 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 *rubrique 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 aux paquets, ce qui peut créer des paquets surdimensionnés. Les informations ajoutées par LLDP sont divisées en divers groupes. Le commutateur transmet un maximum de groupes entiers, ce qui signifie qu'aucun groupe partiel n'est transmis.

La *rubrique Surcharge LLDP* affiche l'état de transmission du port ainsi que le nombre d'octets envoyés et le nombre d'octets restant à envoyer pour les TLV LLDP, ce pour chaque port.

Pour afficher les informations de surcharge LLDP :

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

Cette page contient les champs suivants, pour chaque port :

- **Interface** : identificateur de port.
- **Total (octets)** : nombre total des octets de chaque paquet.
- **Restant à envoyer (octets)** : nombre total des octets restant à ajouter au paquet.

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

ÉTAPE2 Pour afficher les détails de surcharge d'un port, sélectionnez-le et cliquez sur **Détails**. La *LLDP Overloading Details* 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 s'il y a surcharge.
- **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 de paquets envoyés, en octets.
- **Restant à envoyer (octets)** : nombre total des octets de paquet restant à transmettre.

9

Gestion des ports

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

Il inclut les rubriques suivantes :

- **Définition de la configuration de base des ports**
- **Configuration de l'agrégation de liaisons**
- **Flux de travail des LAG statiques et dynamiques**
- **Définition de la gestion des LAG**
- **Configuration de LACP**
- **Green Ethernet**

Flux de travail de gestion des ports

Flux de travail de gestion des ports

Pour configurer des ports, procédez comme suit :

1. Configurez le port dans la *rubrique Paramètres du port*.
2. Activez/désactivez le protocole de contrôle de l'agrégation de liaisons puis configurez les ports membres potentiels sur les LAG (Link Aggregation Groups, groupes d'agrégation de liaisons) appropriés dans la *rubrique Gestion des LAG*. Par défaut, aucun LAG ne comporte de port membre.
3. Configurez les paramètres Ethernet dont le débit et la négociation automatique pour les LAG dans la *rubrique Paramètres des LAG*.
4. Configurez les paramètres LACP des ports membres d'un LAG ou candidats à l'adhésion à un LAG dans la *rubrique LACP.*
5. Configurez les paramètres Green Ethernet globaux dans la *rubrique Propriétés*.

6. Configurez chaque port en mode d'économie d'énergie Green Ethernet dans la *rubrique Paramètres du port*.
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 *rubrique Paramètres du port* 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 voulus dans la *rubrique Modifier le paramètre de port*.

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

Pour configurer les paramètres des ports :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Paramètres des ports**. La *rubrique Paramètres du port* s'ouvre.

ÉTAPE 2 Sélectionnez **Trames Jumbo - Activer** pour prendre en charge les paquets des tailles allant jusqu'à 10 Ko. Si l'option **Trames Jumbo** n'est pas activée, le système prend en charge les tailles de paquets jusqu'à 1 632 octets.

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

Les modifications apportées à la configuration des trames Jumbo prennent effet *uniquement* après un enregistrement explicite de la configuration d'exécution dans le fichier de configuration de démarrage dans la *rubrique Copier/enregistrer la configuration* et après un redémarrage du commutateur.

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

ÉTAPE 5 Modifiez les paramètres suivants :

- **Port** : sélectionnez le numéro du port.
- **Description du port** : saisissez le nom défini par l'utilisateur pour ce port ou un commentaire.
- **Type de port** : affiche le type du port. Les options disponibles sont les suivantes :
  - *Ports cuivre* : les ports standard, non mixtes, prennent en charge les valeurs suivantes : 10M, 100M, 1000M (type : Cuivre).

  - *Ports cuivre mixtes* : un port mixte connecté à un câble cuivre CAT5 prend en charge les valeurs suivantes : 10M, 100M, 1000M (type : ComboC).
  - *Fibre mixte* : *port GBIC (Gigabit Interface Converter, convertisseur d'interface Gibabit) fibre SFP* dispose des valeurs suivantes : 100M et 1000M (type : ComboF).

- **État administratif** : indiquez si le port doit être opérationnel (Démarré) ou non opérationnel (Arrêté) au redémarrage du commutateur.
- **État opérationnel** : affiche l'état actuel de la connexion du port.
- **Réactiver un 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, des configurations d'ACL (Access Control List, liste de contrôle d'accès), BPDUGuard ou Root-Guard.
- **Négociation automatique** : sélectionnez cette option pour activer la négociation automatique sur le port. La négociation automatique permet à un port d'annoncer son débit de transmission, son mode duplex et ses fonctions de contrôle de flux à d'autres périphériques.
- **Négociation automatique opérationnelle** : affiche l'état actuel de la négociation automatique sur le port.
- **Débit de port administratif** : sélectionnez le débit configuré pour le port. Le type du port détermine les options de débit disponibles. Vous ne pouvez choisir *Débit administratif* 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. Les options disponibles sont les suivantes :
  - *Full (bidirectionnelle)* : l'interface prend en charge la transmission entre le commutateur et le client dans les deux directions simultanément.
  - *Half (unidirectionnelle)* : 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, obtenu par négociation.

- **Annonce automatique** : sélectionnez les fonctions que le port doit annoncer. Les options disponibles sont les suivantes :
  - *Capacité maximale* : tous les débits de port et tous les modes duplex sont acceptés.
  - *10 Half* : débit de 10 Mbits/s et mode half-duplex.
  - *10 Full* : débit de 10 Mbits/s et mode full duplex.
  - *100 Half* : débit de 100 Mbits/s et mode half-duplex.
  - *100 Full* : débit de 100 Mbits/s et mode full duplex.
  - *1000 Full* : débit de 1000 Mbits/s et mode full duplex.
- **Annonce opérationnelle** : affiche les fonctions actuellement publiées à l'attention du voisin du port pour démarrer le processus de négociation. Les options disponibles sont celles spécifiées dans le champ *Annonce administrative*.
- **Contre-pression** : sélectionnez le mode de contre-pression du port (utilisé en mode half-duplex) à appliquer pour ralentir le débit 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 l'appareil.
- **Contrôle de flux** : activez ou désactivez le contrôle de flux 802.3x ou activez la négociation automatique du contrôle de flux sur le port (uniquement en mode full duplex).
- **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 ports du commutateur sont câblés conformément aux normes TIA (Telecommunications Industry Association).

  Les options disponibles sont les suivantes :
  - *MDIX* : sélectionnez cette option pour relier ce commutateur à des concentrateurs ou à d'autres commutateurs via un câble droit. Ce commutateur échange ses paires d'émission et de réception. Vous pouvez donc le connecter à un autre commutateur ou à un autre concentrateur à l'aide d'un câble droit.
  - *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. Si l'autre périphérique prend en charge la fonction AutoMDX et que vous définissez le paramètre sur Auto, les périphériques concernés négocient généralement le brochage sur la base du type de câble qui relie les périphériques ainsi que sur la base de la configuration de brochage d'émission et de réception de chaque port.

- **MDI/MDIX opérationnel** : affiche le paramètre MDI/MDIX actuel.
- **Port protégé** : sélectionnez cette option pour définir ce port en tant que port protégé. (Un port protégé est également appelé PVE (Private VLAN Edge).) Les fonctions d'un port protégé sont les suivantes :
  - Les ports protégés fournissent une isolation Layer 2 (snooping) entre les diverses interfaces (ports Ethernet et LAG (Link Aggregation Groups, groupes d'agrégation de liaisons)) qui partagent le même domaine de diffusion (VLAN).
  - Les paquets reçus de ports protégés ne peuvent être transférés que vers des ports de sortie non protégés. Les règles de filtrage des ports protégés s'appliquent également aux paquets transférés par un logiciel comme les applications de traçage.
  - La protection des ports ne dépend pas de l'appartenance aux VLAN. Les périphériques connectés à des ports protégés ne peuvent pas communiquer entre eux, même s'ils sont membres du même VLAN.
  - Les ports et les LAG peuvent être munis ou non d'une protection.
- **Membre du LAG** : indique le nom du LAG dans la mesure où le port est membre d'un LAG.

ÉTAPE 6 Cliquez sur **Appliquer**. Les *paramètres de port* sont modifiés et le commutateur est mis à jour.

Pour configurer un autre port, sélectionnez-le dans le champ Port, en haut de la *rubrique Modifier le paramètre de port*.

Configuration de l'agrégation de liaisons

Le protocole LACP (Link Aggregation Control Protocol, protocole de contrôle de l'agrégation de liaisons) fait partie d'une spécification IEEE (802.3ad) qui vous permet de regrouper plusieurs ports physiques en un seul canal logique. L'agrégation de liaisons optimise l'utilisation des ports car elle relie plusieurs ports pour former un LAG (Link Aggregation Group, groupe d'agrégation de liaisons). 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. Vous configurez un LAG statique avec un groupe de ports qui restent toujours des membres actifs du LAG.
- *Dynamique* : un LAG est dynamique s'il est compatible LACP. Vous définissez un groupe de ports comme candidats à l'appartenance à un LAG dynamique. Le protocole LACP détermine les ports candidats au LAG qui sont des membres actifs. Les membres non actifs sont des ports *de réserve* prêts à remplacer un membre actif en cas de défaillance.

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 sur la base des informations d'en-tête de paquet Layer 2 ou Layer 3. Les paquets de multidiffusion se comportent de façon identique aux paquets de diffusion.

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

Les ports membres actifs d'un LAG sont définis de manière statique via une affectation explicite par l'utilisateur ou sélectionnés de manière dynamique par le protocole LACP (Link Aggregation Control Protocol, protocole de contrôle de l'agrégation de liaisons). Le processus de sélection LACP choisit les ports membres actifs du LAG après un échange d'informations LACP entre les périphériques locaux et distants.

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 huit LAG en charge.

Chaque LAG possède les caractéristiques suivantes :

- Tous les ports d'un LAG doivent disposer du même type de support.
- Pour que vous puissiez ajouter un port au LAG, il ne doit appartenir à aucun autre VLAN que le VLAN par défaut.
- Les ports d'un LAG ne doivent être affectés à aucun autre LAG.
- Il est impossible d'affecter plus de huit ports à un LAG statique. Il est également impossible de définir plus de 16 ports comme candidats à un LAG dynamique.
- Bien que cette fonction puisse être activée sur le LAG, vous devez désactiver la négociation automatique sur tous les ports d'un *LAG*.
- Lorsque vous ajoutez un port à la configuration d'origine du LAG, la configuration existante de ce port n'est plus appliquée car ce port adopte la configuration du LAG. 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.
- Tous les ports du LAG doivent avoir la même priorité 802.1p.

Flux de travail des LAG statiques et dynamiques

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

1. Configurez le LAG sélectionné en tant que LAG statique en désactivant LACP sur ce LAG. Affectez jusqu'à huit ports membres actifs au LAG statique. Pour ce faire, sélectionnez les ports et déplacez-les de la liste **Port** vers la liste **Membres du LAG**, dans la *rubrique Gestion des LAG*.
2. Configurez le débit et le contrôle de flux du LAG dans la *rubrique Paramètres des LAG*.

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

1. Configurez le LAG sélectionné en tant que LAG dynamique en activant LACP sur ce LAG. Affectez jusqu'à 16 ports candidats au LAG dynamique. Pour ce faire, sélectionnez les ports et déplacez-les de la liste **Port** vers la liste **Membres du LAG**, dans la *rubrique Gestion des LAG*.
2. Configurez le débit et le contrôle de flux du LAG dans la *rubrique Paramètres des LAG*.
3. Configurez les paramètres LACP des ports du LAG dans la *rubrique LACP*.

Définition de la gestion des LAG

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

ÉTAPE 1 Pour configurer la gestion des LAG, cliquez sur **Gestion des ports** > **Agrégation de liaisons** > **Gestion des LAG**. La *rubrique 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 et sur les adresses MAC source et cible pour les paquets non-IP.

ÉTAPE 3 Cliquez sur **Appliquer**. L'algorithme d'équilibrage de charge est défini et le commutateur mis à jour.

Définition des ports membres d'un LAG

La page Gestion des LAG vous permet de définir les ports membres d'un LAG.

ÉTAPE 1 Sélectionnez le LAG à configurer puis cliquez sur **Modifier**. La *rubrique 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.
- **Liste des ports** : déplacez les ports à affecter au LAG de la **liste des ports** à la liste **Membres du 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**. Les membres du LAG sont définis et le commutateur est mis à jour.

En modifiant le champ LAG, vous pouvez choisir un autre LAG afin de le configurer.

Configuration des paramètres de LAG

La *rubrique 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 en lançant la *rubrique Modifier les paramètres des LAG*.

Pour configurer le LAG :

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

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

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **LAG** : sélectionnez le numéro d'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 opérationnel (Démarré) ou non opérationnel (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 via des configurations ACL.
- **Négociation automatique administrative** : permet d'activer ou de désactiver la négociation automatique sur le LAG. La négociation automatique est un protocole établi entre deux partenaires de liaison qui permet à un LAG d'annoncer son débit 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 fonctions que le LAG doit annoncer. Les options disponibles sont les suivantes :
  - *Capacité maximale* : tous les débits de LAG et modes duplex sont acceptés.
  - *10 Full* : le LAG annonce un débit de 10 Mbits/s et le mode full duplex.
  - *100 Full* : le LAG annonce un débit de 100 Mbits/s et le mode full duplex.
  - *1000 Full* : le LAG annonce un débit de 1000 Mbits/s et le mode full duplex.

- **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*.
- **Annonce de voisin** : affiche les fonctions annoncées par le LAG voisin (celui auquel l'interface sélectionnée est connectée) pour lancer le processus de négociation. Les options disponibles sont celles spécifiées dans le champ *Annonce administrative*.
- **Contrôle de flux administratif** : activez ou désactivez le contrôle de flux ou activez la négociation automatique du contrôle de flux sur le LAG.
- **Contrôle de flux opérationnel** : affiche le paramètre de contrôle de flux actuel.
- **LAG protégé** : sélectionnez cette option pour définir ce LAG comme un port protégé pour l'isolation Layer 2. Consultez la description de la configuration des ports à la section **Flux de travail de gestion des ports** pour en savoir plus sur les ports et LAG protégés.

ÉTAPE 4 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

En modifiant le champ LAG, vous pouvez choisir un autre LAG afin de le configurer.

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.

Un groupe de canaux LACP peut comporter jusqu'à 16 ports Ethernet d'un même type. Huit ports (maximum) peuvent être actifs et jusqu'à huit ports peuvent être en mode de réserve. Si un groupe de canaux LACP 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 canal 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.

La priorité LACP est déduite du périphérique local ou distant conformément à la règle suivante : la valeur Priorité du système LACP locale est comparée à la priorité système LACP du périphérique distant. La priorité la plus faible est appliquée. Si les deux priorités sont identiques, les adresses MAC locale et distante sont comparées. Le niveau de priorité du périphérique muni de l'adresse MAC la plus basse est pris en compte.

Les règles supplémentaires de sélection des ports actifs ou de réserve d'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 *rubrique 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 *rubrique LACP* s'ouvre.

ÉTAPE 2 Saisissez la valeur **Priorité du système LACP** globale qui déterminera les ports candidats qui deviendront membres du LAG.

Cette page affiche les paramètres LACP de chaque port. Vous pouvez sélectionner et modifier le port voulu dans la *rubrique Modifier les paramètres*

ÉTAPE 3 Sélectionnez un port puis cliquez sur **Modifier**. La *rubrique Modifier les paramètres* s'ouvre.

ÉTAPE 4 Saisissez les valeurs pour les champs suivants :

- **Port** : sélectionne le numéro du port auquel les valeurs de délai et de priorité s'appliquent.
- **Priorité des ports LACP** : saisissez la valeur de priorité LACP du port.
- **Délai LACP** : indiquez si la transmission périodique des PDU LACP doit se produire à un rythme lent ou rapide, selon la préférence de délai LACP définie.

ÉTAPE 5 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

Vous pouvez choisir un autre port dans le champ Port afin de poursuivre les modifications.

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 réduit la consommation énergétique globale de deux manières :

- **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 Précédente 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.
- **Courte portée** : la longueur du câble est analysée et la consommation d'énergie est ajustée en fonction de cette longueur. Dans ce mode, un test de longueur VCT (Virtual Cable Tester, testeur de câble virtuel) est réalisé pour mesurer le câble. Si le câble est inférieur à une longueur (prédéfinie) donnée, le commutateur consomme 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 GE mixtes.

Les deux modes Green Ethernet (Détection d'énergie et Courte portée) doivent être globalement activés et configurés sur chaque port.

Il est possible de contrôler les économies d'énergie et la consommation électrique actuelle. 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.

Vous pouvez surveiller les économies d'énergie.

Les fonctions Green Ethernet sont définies pour chaque port, que ce dernier soit ou non membre d'un LAG.

Définition de propriétés Green Ethernet globales

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

Pour définir des propriétés Green Ethernet globales :

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

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **Mode Détection d'énergie** : permet d'activer ou de désactiver globalement le mode Détection d'énergie. Si ce mode change, un message est affiché.

  Le mode d'économie d'énergie change lorsque vous cliquez sur **OK**.

- **Courte portée** : permet d'activer ou de désactiver globalement le mode Courte portée s'il existe des ports GE sur le commutateur.

  REMARQUE La désactivation ou l'activation du mode Détection d'énergie déconnecte temporairement les connexions réseau.

- **Économies d'énergie** : affiche le pourcentage d'énergie économisé grâce au mode Green Ethernet.

- **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.

ÉTAPE 3 Cliquez sur **Appliquer**. Les *paramètres de port* sont modifiés et le commutateur est mis à jour.

Définition de propriétés Green Ethernet pour chaque port

La *rubrique Paramètres du port* affiche le mode d'économie d'énergie Green Ethernet actuel de chaque port et vous permet de sélectionner un port pour la configuration de Green Ethernet dans la *rubrique Modifier le paramètre de port*. Pour que les modes Green Ethernet fonctionnent sur un port, vous devez avoir activé ces modes globalement dans la *rubrique Propriétés.*

Pour définir les paramètres Green Ethernet de chaque port :

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

La *rubrique Paramètres du port* affiche les champs suivants :

- **N° d'entrée** : numéro de séquence de l'entrée dans la table.
- **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.

  REMARQUE Cette fenêtre affiche le paramètre Courte portée de chaque port. Pour autant, vous ne pouvez *pas activer* la fonction Courte portée tant qu'elle n'est pas activée globalement (utilisez la *rubrique Propriétés*). Pour activer globalement le mode Courte portée, reportez-vous à la section **Définition de propriétés Green Ethernet globales**.
- **Longueur de câble** : indique la longueur de câble détectée par VCT, en mètres.

ÉTAPE 2 Sélectionnez un **port** puis cliquez sur **Modifier**. *La rubrique 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 Choisissez d'activer ou de désactiver le mode Courte portée pour le port.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres Green Ethernet du port sont modifiés et le commutateur est mis à jour.

Sélectionnez un autre port pour l'afficher et le modifier.

10

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**.

Ce chapitre explique comment utiliser la fonctionnalité PoE.

Il contient les rubriques suivantes :

- **PoE sur le commutateur**
- **Configurer les 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.

Fonctionnalités PoE

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 ainsi de réduire de façon significative les coûts d'installation.

PoE peut être utilisé dans tout réseau d'entreprise déployant des appareils de puissance relativement faible connectés au LAN Ethernet et notamment :

- les téléphones IP,
- les points d'accès sans fil,
- les passerelles IP,
- les appareils de surveillance audio et vidéo à distance.

Fonctionnement de PoE

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 appareil PoE est situé à l'autre extrémité, cet appareil répond à ces impulsions.
- Classification : la négociation entre le PSE (Power Sourcing Equipment) et l'appareil alimenté (PD, Powered Device) débute après l'étape de détection. Au cours de la négociation, 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

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. Les valeurs de puissance par port ayant été configurées pour le mode Limite du port sont conservées ;
- de la limite de port maximale autorisée en tant que limite numérique par port en mW (mode Limite du port) ;
- de générer une message « trap » lorsqu'un PD essaie de consommer trop de puissance et du pourcentage de la puissance maximale auquel ce message « trap » 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 » SNMP.

Configurer les propriétés PoE

La *rubrique 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 *rubrique 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.
- **Messages « trap »** : permet d'activer ou de désactiver les messages « trap ». Si les « traps » sont activés, vous devez également activer SNMP et configurer au moins un destinataire de notification SNMP.
- **Seuil des « trap » d'alimentation** : saisissez le seuil d'utilisation sous la forme d'un pourcentage de la limite de puissance. Une alarme se déclenche si la puissance dépasse cette valeur.

Les compteurs suivants s'affichent :

- **Puissance nominale** : 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 - la quantité de puissance consommée.

Configurer la puissance, la priorité et la classe PoE

La *rubrique Paramètres PoE* affiche les informations PoE 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.

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. Ce mode est configuré dans la *rubrique 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. Ce mode est configuré dans la *rubrique Propriétés PoE*.

  Lorsque la puissance consommée sur le port dépasse la limite de classe, l'alimentation du port est désactivée.

Dans certains cas, le commutateur ne dispose pas de la puissance suffisante pour fournir simultanément à tous les ports la puissance allouée. Pour résoudre ce problème, affectez à la fois des limites et des priorités aux ports. Par exemple, 15,4 W sont autorisés sur les 48 ports mais seuls 24 d'entre eux peuvent être alimentés en même temps en raison de limitations de puissance. Dans ce cas, la priorité détermine les ports qui seront alimentés et ceux qui ne le seront pas même si aucun port ne se situe au-dessus de la limite et que des PD sont connectés sur chacun d'eux. Vous devez entrer ces priorités dans la *rubrique Paramètres PoE*.

Pour configurer les paramètres de port PoE :

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

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier**. La *rubrique Modifier les paramètres PoE* s'ouvre.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **Port** : 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.

- **Classe** : ce champ ne s'affiche que si le Mode d'alimentation Limite de classe est défini dans la *rubrique 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	15,4 W

- **Affectation de puissance** : ce champ ne s'affiche que si le Mode d'alimentation Limite du port est défini dans la *rubrique Propriétés PoE*. Saisissez la puissance affectée au port (en milliwatts). Cette plage est comprise entre 0 et 15 400.
- **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 définis et le commutateur est mis à jour.

11

Gestion des VLAN

Ce chapitre contient les sections suivantes :

VLAN

Un VLAN est un groupe logique qui permet aux périphériques qui lui sont connectés 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 VLAN. Un port est un membre balisé d'un VLAN si tous les paquets qui lui sont destinés disposent d'une balise VLAN. Un port peut être membre d'un ou plusieurs VLAN.

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, ce qui augmente sa taille maximum de 1518 à 1522. La balise contient un ID VLAN compris entre 1 et 4094 et une balise de priorité VLAN (VPT) comprise entre 0 et 7. Voir *Modes QoS* pour en savoir plus sur VPT.

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

Les VLAN fonctionnent au niveau de la Couche 2 (Layer 2). 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. Des périphériques de VLAN différents peuvent communiquer entre eux uniquement via des routeurs de Couche 3 (Layer 3). Un routeur IP, par exemple, est requis pour acheminer le trafic IP entre les VLAN si chaque VLAN représente un sous-réseau IP.

Le routeur IP peut être un routeur traditionnel où chacune de ses interfaces se connecte à un seul VLAN. Le trafic depuis et vers un routeur IP traditionnel doit être balisé VLAN. Le routeur IP peut être un routeur tenant compte du VLAN où chacune de ses interfaces peut se connecter à un ou plusieurs VLAN. Le trafic depuis et vers un routeur IP tenant compte du VLAN peut être balisé ou non balisé VLAN.

Les périphériques adjacents tenant compte du VLAN échangent des informations VLAN entre eux via le protocole GVRP (Generic VLAN Registration Protocol). En conséquence, les informations VLAN sont propagées via un réseau raccordé.

Les VLAN sur un périphérique peuvent être créés statistiquement ou dynamiquement en vertu des informations GVRP échangées par les périphériques. Un VLAN peut être statique ou dynamique (via GVRP), mais pas les deux. Pour en savoir plus sur GVRP, reportez-vous à la section *Paramètres GVRP*.

Certains VLAN peuvent avoir des rôles supplémentaires, notamment :

- VLAN voix : pour en savoir plus, reportez-vous à la section *VLAN voix*.
- VLAN invité : défini dans la *rubrique Modifier l'authentification VLAN.*
- VLAN par défaut : pour en savoir plus, reportez-vous à la section *Configuration des paramètres VLAN par défaut*.
- VLAN de gestion (dans des systèmes en mode Couche 2 (Layer 2)) : pour en savoir plus, reportez-vous à la section *Adressage IP Layer 2*.

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 de VLAN**.
3. Définissez la configuration VLAN par port à l'aide de la section **Configuration des paramètres d'interface VLAN**.
4. Assignez des interfaces aux VLAN à l'aide de la section **Configuration du port au VLAN** ou de la section **Configuration du VLAN au port**.
5. Vous pouvez afficher l'appartenance actuelle du port VLAN pour toutes les interfaces dans la section **Affichage de l'appartenance VLAN**.

Configuration des paramètres VLAN par défaut

Avec les paramètres usine par défaut, le commutateur crée automatiquement un VLAN 1 en tant que VLAN par défaut. Le statut 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 être utilisé pour un rôle spécial tel qu'un VLAN non authentifié ou un VLAN voix.
- 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.
- Les serveurs RADIUS ne peuvent pas assigner le VLAN par défaut aux demandeurs 802.1x via l'affectation avec VLAN dynamique.

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 *rubrique Paramètres VLAN par défaut* s'ouvre.

ÉTAPE 2 Saisissez la valeur du champ suivant :

- **ID VLAN par défaut actuel** : affiche l'ID VLAN par défaut actuel.
- **ID VLAN par défaut après réinitialisation** : 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 de VLAN

Vous pouvez créer un VLAN mais cela n'a aucun effet tant que le VLAN n'est pas manuellement ou dynamiquement lié à au moins un port. Les ports doivent toujours appartenir à un ou plusieurs VLAN. Le commutateur Cisco Sx300 prend en charge des VLAN 256, VLAN par défaut inclus.

Chaque VLAN doit être configuré avec un VID unique (ID VLAN) dont la valeur est comprise entre 1 et 4094. 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 jamais transférés à un port.

Pour créer un VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Créer un VLAN**. La *rubrique Créer un VLAN* s'ouvre.

La page de création des 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. Les options disponibles sont les suivantes :
  - *Dynamique* : le VLAN a été dynamiquement créé via le protocole GVRP (Generic VLAN Registration Protocol).
  - *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 *rubrique Ajouter/Modifier VLAN* s'ouvre.

La page active 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).

ÉTAPE 4 Cliquez sur **Appliquer** pour créer le ou les VLAN.

Configuration des paramètres d'interface VLAN

La *rubrique Paramètres d'interface* affiche et active la configuration des paramètres VLAN pour toutes les interfaces. Le commutateur Cisco Sx300 prend en charge des VLAN 256, VLAN par défaut inclus.

Pour configurer les paramètres VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres d'interface**. La *rubrique Paramètres d'interface* s'ouvre.

La page des paramètres d'interface répertorie tous les ports ou LAG ainsi que leurs paramètres VLAN.

ÉTAPE 2 Sélectionnez un type d'interface (Port ou LAG) puis cliquez sur **OK**.

ÉTAPE 3 Sélectionnez un port ou un LAG et cliquez sur **Modifier.** La *rubrique Modifier les paramètres d'interface* s'ouvre.

ÉTAPE 4 Saisissez les valeurs pour les champs suivants :

- **Interface** : sélectionnez un port ou un LAG.
- **Mode d'interface VLAN** : sélectionnez le mode d'interface du VLAN. Les options disponibles 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.
- **PVID** : 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. Les valeurs possibles sont :
  - *Tout admettre* : l'interface accepte tous les types de trames : trames non balisées, trames balisées et trames balisées de priorité.
  - *Admettre marquées uniquement* : l'interface accepte uniquement les trames balisées.
  - *Admettre non marquées 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.
- **Appartenance automatique en VLAN voix** : sélectionnez cette option pour activer Appartenance VLAN voix automatique. Lorsque cette option est activée sur une interface, le commutateur configure automatiquement l'interface comme membre du VLAN voix s'il détecte les paquets voix

entrants basés sur les OUI (Organizationally Unique Identifiers) de téléphonie configurés. La stratégie réseau LLDP-MED n'active pas le VLAN voix.

- **Mode QoS VLAN voix** : sélectionnez l'une des valeurs suivantes :
  - *Tout* : les valeurs de qualité de service (QoS) configurées sur le VLAN voix sont appliquées à toutes les trames entrantes qui sont 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 la trame entrante reçue sur l'interface, catégorisée comme VLAN voix et dont l'adresse MAC source est configurée avec l'OUI de téléphonie. (Les OUI de téléphonie sont configurées en suivant la procédure de la section **Configuration de l'OUI de téléphonie**.)

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres sont définis et le commutateur est mis à jour.

Définition de l'appartenance VLAN

La **rubrique port au VLAN**, la *rubrique VLAN au port et* la *rubrique Appartenance VLAN des ports* affichent les appartenances VLAN des ports dans diverses présentations. Vous pouvez utiliser la **rubrique port au VLAN** et la *rubrique VLAN au port* pour ajouter ou supprimer des appartenances VLAN.

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 ou apprendre dynamiquement les VLAN ainsi que leurs appartenances de port via le protocole GVRP (Generic VLAN Registration Protocol).

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 des périphériques d'interconnexion 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. Le port de sortie atteignant le nœud d'extrémité doit être un membre non balisé du VLAN.

Configuration du port au VLAN

Utilisez la **rubrique port au VLAN** pour afficher et configurer un VLAN et tout ses ports membres sur une seule page.

Pour mapper les ports ou les LAG à un VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Port au VLAN**. La **rubrique port au VLAN** s'ouvre.

ÉTAPE 2 Sélectionnez un VLAN et le type d'interface (Port ou LAG) puis cliquez sur **Aller** afin d'afficher ou de modifier la caractéristique du port relative au VLAN.

Le mode Port de chaque port ou LAG s'affiche dans son mode actuel (Accès, Liaison ou Général) configuré depuis la *rubrique 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 même à partir de l'enregistrement GVRP. Lorsqu'un port n'est pas membre d'un autre VLAN, l'activation de cette option sur le port l'intègre au VLAN interne 4095 (VID réservé).
- **Exclu** : l'interface n'est actuellement pas membre du VLAN. C'est le paramètre par défaut pour tous les ports et LAG. Le port peut rejoindre le VLAN via un enregistrement GVRP.
- **Marqué** : l'interface est un membre balisé du VLAN. Les trames du VLAN sont envoyées balisées à l'interface 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. Vous ne pouvez configurer que le PVID des ports généraux.

ÉTAPE 4 Cliquez sur **Appliquer**. Les interfaces sont assignées au VLAN et le commutateur est mis à jour.

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 du VLAN au port

Utilisez la *rubrique VLAN au port* pour mapper des ports à plusieurs VLAN dynamiques.

Pour assigner un port à plusieurs VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN au port**. La *rubrique VLAN au port* s'ouvre.

ÉTAPE 2 Sélectionnez un type d'interface (Port ou LAG) puis cliquez sur **Aller**. Les champs suivants s'affichent pour toutes les interfaces du type sélectionné :

- **Interface** : ID du port/LAG.
- **Mode** : mode de l'interface VLAN sélectionné dans la *rubrique Paramètres d'interface.*
- **VLAN** : menu déroulant qui affiche tous les VLAN dont l'interface est 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 *rubrique Connecter le VLAN au port* s'ouvre.

ÉTAPE 4 Saisissez les valeurs pour les champs suivants :

- **Interface** : sélectionnez un port/LAG.
- **Mode** : affiche le mode port VLAN sélectionné dans la *rubrique 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 marqué. Il ne peut cependant être sélectionné.

- **Balisage** : sélectionnez une des options de PVID/balisage suivantes :
  - *Marqué* : 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 le commutateur est mis à jour.

Affichage de l'appartenance VLAN

La *rubrique Appartenance VLAN des ports* affiche une liste des VLAN auxquels chaque port appartient.

Pour afficher l'appartenance VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Appartenance VLAN des ports**. La *rubrique Appartenance VLAN des ports* s'ouvre.

ÉTAPE 2 Sélectionnez un type d'interface (Port ou LAG) puis cliquez sur **Aller**.

La page d'appartenance VLAN des ports affiche l'appartenance opérationnelle des ports ou LAG :

- **numéro** du port.
- **Mode** : le mode port est défini dans la *rubrique Paramètres d'interface*.
- **PVID** : identificateur de port VLAN du VLAN auquel les trames non balisées entrantes sont assignées à l'entrée. Cette option suppose qu'aucun autre mécanisme d'affectation avec VLAN n'est utilisé, tel que les VLAN basés sur MAC.
- **VLAN** : VLAN auquel le port appartient.

Paramètres GVRP

Les périphériques adjacents tenant compte du VLAN peuvent s'échanger des informations VLAN via le protocole GVRP (Generic VLAN Registration Protocol). Le GVRP est basé sur le protocole GARP (Generic Attribute Registration Protocol) et propage des informations VLAN à travers le réseau raccordé.

Étant donné que GVRP requiert une prise en charge du balisage, le port doit être configuré en mode Liaison ou Général.

Lorsqu'un port est connecté à un VLAN via GVRP, il est ajouté au VLAN en tant que membre dynamique, sauf si cette action a été expressément interdite à la *rubrique VLAN au port*. Si le VLAN n'existe pas, il est dynamiquement créé lorsque la création de VLAN dynamiques est activée pour ce port.

Le GVRP doit être activé globalement et sur chaque port. Lorsqu'il est activé, il transmet et reçoit des GPDU (GARP Packet Data Units). Les VLAN définis mais non actifs ne sont pas propagés. Pour propager le VLAN, il doit être actif au moins sur un port.

Définition des paramètres GVRP

Pour définir les paramètres GVRP pour une interface :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres GVRP**. La *rubrique Paramètres GVRP* s'ouvre.

ÉTAPE 2 Sélectionnez **État global GVRP** pour activer globalement le GVRP.

ÉTAPE 3 Cliquez sur **Appliquer** pour définir l'état global GVRP.

ÉTAPE 4 Sélectionnez un type d'interface (Port ou LAG) puis cliquez sur **OK**. Les champs suivants s'affichent dans le tableau des paramètres GVRP.

- **Interface** : numéro du port/LAG.
- **État GVRP** : indique si le GVRP est activé/désactivé sur l'interface.
- **Création de VLAN dynamiques** : indique si la création de VLAN dynamiques est activée/désactivée sur l'interface. Si elle est désactivée, GVRP peut fonctionner mais de nouveaux VLAN ne sont pas créés.
- **Enregistrement GVRP** : indique si l'enregistrement VLAN via GVRP est activé ou désactivé sur le port.

ÉTAPE 5 Pour définir les paramètres GVRP pour un port, sélectionnez-le et cliquez sur **Modifier.** La *rubrique Modifier le paramètre GVRP* s'ouvre.

ÉTAPE 6 Saisissez les valeurs pour les champs suivants :

- **Interface** : sélectionnez l'interface (port ou LAG) à modifier.
- **État GVRP** : sélectionnez cette option pour activer GVRP sur cette interface.
- **Création de VLAN dynamiques** : sélectionnez cette option pour activer la création de VLAN dynamiques sur cette interface.
- **Enregistrement GVRP** : sélectionnez cette option pour activer l'enregistrement VLAN via GVRP sur cette interface.

ÉTAPE 7 Cliquez sur **Appliquer.** Les paramètres GVRP sont modifiés et le commutateur est mis à jour.

Groupes VLAN

Assignation de groupes VLAN basés sur MAC

Utilisez cette fonction afin d'assigner du trafic non balisé à partir d'adresses MAC spécifiques vers un VLAN spécifique pour les périphériques en mode Couche 2 (Layer 2). Cette affectation s'exécute par étapes :

1. Assignez l'adresse MAC à un ID de groupe (un identificateur créé à l'aide de la *rubrique Groupes basés sur MAC*).
2. Pour chaque interface, assignez le groupe VLAN à un VLAN en utilisant *rubrique Mappage de groupes au VLAN* (les interfaces doivent être en mode Général.)

Cette fonction est uniquement disponible lorsque le commutateur est en mode Couche 2 (Layer 2).

Le VLAN doit être créé puis lié à l'interface.

Pour assigner une adresse MAC à un groupe VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Groupes VLAN** > **Groupes basés sur MAC**. La *rubrique Groupes basés sur MAC* s'ouvre.

ÉTAPE 2 Cliquez sur **Ajouter.** La *rubrique Ajouter un groupe basé sur MAC* s'ouvre.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **Adresse MAC** : saisissez une adresse MAC à assigner à un groupe VLAN.

  REMARQUE Cette adresse ne peut pas être assignée à un autre groupe VLAN.

- **Masque** : saisissez l'une des informations suivantes :
  - *Hôte* : hôte source de l'adresse MAC
  - *Préfixe* de l'adresse MAC
- **ID de groupe** : saisissez un numéro d'ID de groupe VLAN créé par l'utilisateur.

ÉTAPE 4 Cliquez sur **Appliquer**. L'adresse MAC est assignée à un groupe VLAN.

Assignation d'un ID de groupe VLAN à un VLAN par interface

La *rubrique Mappage de groupes au VLAN* affiche les groupes basés sur MAC créés dans la *rubrique Groupes basés sur MAC.* Cette fonctionnalité est uniquement disponible lorsque le commutateur est en mode Couche 2 et le port en mode Général.

Pour assigner un ID de groupe VLAN à un VLAN par interface :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Groupes VLAN** > **Mappage de groupes vers VLAN**. La *rubrique Mappage de groupes au VLAN* s'ouvre.

La fenêtre affiche :

- **Interface** : type d'interface (port ou LAG), via lequel le trafic est reçu pour ce groupe.
- **ID de groupe** : groupe VLAN défini dans la *rubrique Groupes basés sur MAC*.
- **ID de VLAN** : le trafic est transféré depuis le groupe VLAN vers ce VLAN.

ÉTAPE 2 Cliquez sur **Ajouter**. La *Ajouter un mappage de groupe au VLAN* s'ouvre. (L'interface doit être en mode Général.)

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **Type de groupe** : indique que le groupe est basé sur adresse MAC.
- **Interface** : saisissez une interface (port ou LAG) via laquelle le trafic est reçu.
- **ID de groupe** : sélectionnez l'un des groupes VLAN définis dans la *rubrique Groupes basés sur MAC.*
- **ID de VLAN** : sélectionnez le VLAN vers lequel le trafic est transféré depuis le groupe VLAN.

  REMARQUE Pour chaque interface, vous pouvez sélectionner un groupe ou VLAN.

ÉTAPE 4 Cliquez sur **Appliquer** pour définir le mappage du groupe VLAN au VLAN. (Le VLAN basé sur adresse MAC ne lie pas dynamiquement le port au VLAN de groupe MAC ; l'interface pour laquelle le VLAN basé sur-MAC est défini doit être manuellement ajoutée à ce VLAN.)

VLAN voix

Le VLAN voix est utilisé lorsque le trafic depuis des téléphones ou équipements VoIP est assigné à un VLAN spécifique. Le commutateur peut automatiquement détecter et ajouter des ports membres au VLAN voix et assigner la QoS (Qualité de service) configurée aux paquets depuis le VLAN voix.

Attributs de la QoS

Les attributs de la QoS peuvent être assignés aux paquets VoIP (voix et signalisation) afin d'attribuer la priorité au trafic via le commutateur. Les attributs de la QoS peuvent être assignés par port aux paquets voix suivant deux modes :

- **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.
- **SRC** : les valeurs de QoS configurées pour le VLAN voix sont appliquées à la trame entrante reçue sur l'interface, catégorisée comme VLAN voix et son adresse MAC source est configurée avec l'OUI de téléphonie. (Les OUI de téléphonie sont configurés en suivant la procédure de la section **Configuration de l'OUI de téléphonie**.)

Dans les adresses MAC, les trois premiers octets contiennent un ID de fabricant, connu comme OUI (Organizationally Unique Identifier) et les trois derniers octets contiennent un ID de station unique. La classification d'un paquet de téléphones ou équipements VoIP est basée sur l'OUI de son adresse MAC source.

Les ports peuvent être assignés au VLAN voix comme suit :

- **Statique** : assigné manuellement au VLAN voix (décrit dans la section **Configuration des paramètres d'interface VLAN**).
- **Dynamique** : le port est identifié comme candidat pour rejoindre le VLAN voix. Lorsqu'un paquet muni d'une adresse MAC OUI source identifiant l'équipement à distance comme équipement voix est perçu sur le port, le port se connecte au VLAN voix en tant que port balisé. (Cette option est configurée à l'aide du processus décrit dans la section **Configuration des paramètres d'interface VLAN**.) Si le délai d'expiration de la dernière adresse MAC de téléphonie dépasse le délai d'expiration du VLAN voix, le port est supprimé du VLAN voix. Le délai d'expiration peut être modifié en utilisant la procédure décrite dans la section **Configuration des propriétés du VLAN voix**.

Les scénarios de réseau suivants sont pris en charge pour l'affectation dynamique :

- Un téléphone est configuré avec l'ID VLAN voix et envoie toujours des paquets balisés.
- Un téléphone envoie des paquets non balisés pour acquérir son adresse IP initiale. Une réponse du serveur DHCP local dirige le téléphone afin qu'il utilise l'ID VLAN voix. Le téléphone redémarre alors une session DHCP sur le VLAN voix (balisé).
- Si l'équipement voix prend en charge le protocole LLDP-MED, le commutateur envoie une stratégie de réseau LLDP-MED qui indique au téléphone comment envoyer les trames au commutateur (par exemple : balisé et balisé avec un VLAN spécifique).

Options de VLAN voix

Options de VLAN voix

Vous pouvez effectuer les opérations suivantes avec cette fonctionnalité :

- Activer ou désactiver le VLAN voix tel qu'indiqué dans la section **Configuration des propriétés du VLAN voix**/
- Créer un nouveau VLAN pour servir de VLAN voix en utilisant la *rubrique Créer un VLAN* ou configurer un VLAN existant tel qu'indiqué dans la section **Configuration des propriétés du VLAN voix**.
- Assigner des ports en tant que candidats au VLAN voix. (Cette option est configurée à l'aide du processus décrit dans la section **Configuration des paramètres d'interface VLAN**.)
- Assignez le mode QoS par port à l'un des éléments suivants :
  - Pour un port qui est déjà connecté au VLAN voix, tous les paquets sont assignés au VLAN voix tel qu'indiqué dans la section **Configuration des paramètres d'interface VLAN**.
  - Seuls les paquets qui proviennent des téléphones IP (basés sur le préfixe d'adresse MAC OUI source) en utilisant la procédure décrite dans la section **Configuration des paramètres d'interface VLAN**.
- Saisissez la CoS (classe de service) du VLAN voix (avec ou sans nouveau marquage du VPT du paquet) en utilisant la *rubrique Propriétés du VLAN voix*. Lorsque l'option de nouveau marquage est sélectionnée, le commutateur modifie la priorité 802.1p du paquet à la sortie. Paramétrez l'option de nouveau marquage telle qu'indiquée dans la section **Configuration des propriétés du VLAN voix**.
- Configurez et mettez à jour le tableau OUI de téléphonie avec un maximum de 128 entrées (chaque entrée est un numéro à trois octets) tel qu'indiqué dans la section **Configuration de l'OUI de téléphonie**. Le commutateur utilise le tableau pour déterminer si l'appartenance VLAN voix automatique du port est activée et si le port va se connecter au VLAN voix.
- Saisissez le délai d'expiration du VLAN voix tel qu'indiqué dans la section **Configuration des propriétés du VLAN voix**.

Contraintes du VLAN voix

Contraintes du VLAN voix

Les contraintes suivantes existent :

- Seul un VLAN voix est pris en charge.
- Le VLAN voix n'est pas pris en charge par l'Affectation avec VLAN dynamique.
- Le VLAN voix doit être un VLAN statique créé manuellement.
- Un VLAN défini en tant que VLAN voix ne peut être supprimé.
- Un nouvel ID VLAN peut être configuré pour le VLAN voix uniquement si le VLAN voix actuel n'a pas de ports candidats.
- Le VLAN voix ne peut être le VLAN invité.
- L'interface VLAN d'un port candidat peut être en mode Général ou Liaison.
- A l'exception de la décision QoS relative à la Stratégie/ACL, la décision QoS du VLAN voix a priorité sur toute autre décision QoS.
- La QoS du VLAN voix est appliquée aux 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 connue de la FDB (s'il n'existe aucun espace disponible dans la FDB, aucune action ne se produit).

Configuration des propriétés du VLAN voix

Utilisez la *rubrique Propriétés du VLAN voix* pour configurer globalement la fonction VLAN voix en paramétrant les éléments suivants :

- ID VLAN du VLAN voix
- Classe de trafic reçue par le trafic
- Intervalle de temps au cours duquel le port reste dans le VLAN voix après que la dernière trame VoIP ait été identifiée avec un OUI dans la table.

Pour activer la fonctionnalité sur un port, ce dernier doit être globalement activé dans la *rubrique Paramètres d'interface*.

Pour configurer des propriétés du VLAN voix :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **Propriétés**. La *rubrique Propriétés du VLAN voix* s'ouvre.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **État du VLAN voix** : sélectionnez ce champ pour activer la fonction VLAN voix.
- **ID VLAN voix** : sélectionnez le VLAN qui sera le VLAN voix.
- **Classe de service** : sélectionnez cette option pour ajouter un niveau de CoS aux paquets non balisés reçus sur le VLAN voix. Les valeurs possibles sont comprises entre 0 et 7, où 7 dispose de la priorité la plus élevée. 0 est utilisé dans le cadre d'un mode meilleur effort (best effort) et est automatiquement invoqué lorsqu'aucune autre valeur n'a été définie (par défaut).
- **Remarquer la CoS** : sélectionnez cette option pour réassigner le niveau de CoS aux paquets reçus sur le VLAN voix. Si cette option est sélectionnée, la priorité d'utilisateur extérieure sera la nouvelle CoS. Dans le cas contraire, la priorité d'utilisateur extérieure sera la CoS d'origine car le mode Liaison est utilisé.
- **Délai d'expiration d'appartenance automatique** : saisissez la durée après laquelle le port quitte le VLAN voix si aucun paquet voix n'est reçu. Le délai peut se situer entre 1 minute et 30 jours.

ÉTAPE 3 Cliquez sur **Appliquer**. Les propriétés du VLAN sont enregistrées et le commutateur est mis à jour.

Configuration de l'OUI de téléphonie

Les OUI (Organizationally Unique Identifiers) sont assignés 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 perçues.

La table globale OUI peut contenir jusqu'à 128 entrées.

Utilisez la *rubrique OUI de téléphonie* pour afficher les OUI existants et en ajouter de nouveaux.

Pour ajouter un nouvel OUI VLAN voix :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **OUI de téléphonie**. La *rubrique OUI de téléphonie* s'ouvre.

La page OUI de téléphonie affiche les champs suivants :

- **Téléphonie OUI** : six premiers chiffres de l'adresse MAC réservés pour les OUI.
- **Description** : description de l'OUI assigné à l'utilisateur.

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 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un OUI de téléphonie* s'ouvre.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **OUI de téléphonie** : saisissez un nouvel OUI.
- **Description** : saisissez un nom d'OUI.

ÉTAPE 4 Cliquez sur **Appliquer**. L'OUI est ajouté.

12

Configuration du protocole Spanning Tree

Le protocole Spanning Tree (STP) (IEEE802.1D et IEEE802.1Q) est activé par défaut, réglé sur le mode RSTP (Rapid Spanning Tree Protocol) et protège un domaine de diffusion de couche 2 contre la propagation d'orages en paramétrant sélectivement des liens sur le mode de réserve pour empêcher les boucles. En mode de réserve, ces liens ne transfèrent pas de données d'utilisateur pendant un moment. Ils sont automatiquement réactivés lorsque la topologie est modifiée pour relancer le transfert de données d'utilisateur.

Ce chapitre contient les sections suivantes :

Types de STP

Des boucles se produisent lorsque des routes alternatives existent entre les hôtes. Des boucles au sein d'un réseau étendu peuvent provoquer un transfert indéfini du trafic par les commutateurs de couche 2 et ainsi engendrer l'augmentation du trafic ainsi qu'un réseau moins efficace.

Le protocole STP fournit une topologie en arborescence pour l'agencement de commutateurs de couche 2 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.

  Même si le STP classique empêche la couche 2 de transférer des boucles dans une topologie de réseau générale, un délai inacceptable peut se produire avant la convergence. Cela signifie que les ponts ou commutateurs du réseau doivent choisir de transférer activement ou non le trafic à chacun de leurs ports.
- Le STP multiple (MSTP) détecte les boucles de couche 2 et tente de les réduire en empêchant le port impliqué de transférer le trafic. Étant donné que les boucles existent au niveau d'un domaine de couche 2, il peut se produire une situation où une boucle se crée dans le VLAN A mais pas dans le VLAN B. Si les deux VLAN sont définis sur un port X et STP souhaite réduire la boucle, le protocole stoppe le trafic sur tout le port, y compris celui du VLAN B alors que cela n'est pas nécessaire.

  MSTP résout ce problème en activant plusieurs instances STP afin de détecter et de réduire séparément les boucles à chaque instance. En associant les instances aux VLAN, chacune d'entre elles est associée au domaine de couche 2 sur lequel elle détecte et réduit les boucles. Cette opération permet par exemple lors d'une instance de stopper le trafic du VLAN A provoquant une boucle, tout en maintenant le trafic dans un autre domaine (tel que le VLAN B) où aucune boucle ne se produit.

  MSTP fournit une connectivité complète pour les paquets affectés à un VLAN. MSTP est basé sur RSTP. Par ailleurs, MSTP transmet des paquets assignés à divers VLAN via des régions MST différentes. Les régions MST agissent comme pont unique.

Configuration de l'état STP et des paramètres globaux

La *rubrique État STP et paramètres globaux* contient les paramètres permettant d'activer STP, RSTP ou MSTP. Pour connaître la configuration détaillée de chaque mode STP, consultez respectivement les *rubriques Paramètres d'interface STP*, Paramètres d'interface RSTP et *Propriétés MSTP* .

Pour définir l'état STP et les paramètres globaux :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **État STP et paramètres globaux**. La *rubrique État STP et paramètres globaux* 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 Bridge Protocol Data Unit (BPDU)** : sélectionnez la manière dont les paquets BPDU sont gérés lorsque STP est désactivé sur le port ou 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 de 4096. Par exemple 4096, 8192, 12 288, 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 en savoir plus, 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 du chemin racine** : coût du chemin 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**. Le commutateur est mis à jour muni des paramètres globaux STP.

Définition des paramètres d'interface du Spanning Tree

La *rubrique 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 sur cette page est active pour tous les types de protocole STP.

Pour configurer STP sur une interface :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **Paramètres d'interface STP**. La *rubrique Paramètres d'interface STP* s'affiche.

ÉTAPE 2 Sélectionnez une interface puis cliquez sur **Modifier**. La rubrique Modifier les paramètres d'interface s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez le numéro de port ou le LAG sur lequel le 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 disponibles 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.
- **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 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 peut connaître les adresses MAC.
  - Transfert : le port est en mode Transfert. Il peut transférer le trafic et prendre connaissance de nouvelles adresses MAC.
- **Rôle du port** : affiche le comportement du port.
- **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 modifiés et le commutateur est mis à jour.

Configuration des paramètres Rapid Spanning Tree

Le protocole Rapid Spanning Tree (RSTP) détecte et utilise les topologies du réseau qui permettent une convergence STP plus rapide sans créer de boucles de transfert.

La rubrique 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 ou MSTP.

Pour entrer les paramètres RSTP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **État STP et paramètres globaux**. La *rubrique État STP et paramètres globaux* s'affiche. Activez **RSTP**.

ÉTAPE 2 Cliquez sur **Spanning Tree** > **Paramètres d'interface RSTP**. La *rubrique Paramètres d'interface RSTP* s'ouvre :

ÉTAPE 3 Sélectionnez un port. (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 s'il a migré ou non vers RSTP ou MSTP. 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 ou MSTP, il communique avec lui respectivement via RSTP ou MSTP.

ÉTAPE 5 Sélectionnez une interface puis cliquez sur **Modifier**. La *rubrique Paramètres Rapid Spanning Tree* s'affiche.

ÉTAPE 6 Saisissez les paramètres.

- **Interface** : définissez l'interface et précisez le port ou LAG où RSTP doit être configuré.
- **Etat opérationnel 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 2 secondes).

- 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 une vitesse rapide.
- Auto : détermine automatiquement l'état du commutateur en utilisant les BPDU RSTP.

- **État opérationnel point à point** : affiche l'état de fonctionnement point à point si l'**État opérationnel point à point** est défini sur Auto.
- **Rôle** : affiche le rôle du port 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.
  - Secours : fournit un chemin de secours pour le chemin de port désigné vers les nœuds terminaux du Spanning Tree. Des ports de secours existent lorsque deux ports sont reliés dans une boucle par un lien point à point. Des ports de secours apparaissent également lorsqu'un LAN possède deux ou plusieurs connexions reliées 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 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 les nouvelles adresses MAC.
- Transfert : le port est en mode Transfert. Il peut transférer le trafic et prendre connaissance de nouvelles adresses MAC.

ÉTAPE 7 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

Multiple Spanning Tree

Le protocole Multiple Spanning Tree Protocol (MSTP) fournit des solutions à divers scénarios d'équilibrage des charges. Par exemple, un port A bloqué dans une instance STP peut être placé en mode Transfert dans une autre instance STP. La *rubrique Propriétés MSTP* contient des informations permettant de définir MSTP global.

Charge de travail MSTP

Pour configurer MSTP, effectuez les opérations suivantes :

1. Définissez le mode de fonctionnement STP sur MSTP tel qu'indiqué dans la section **Configuration de l'état STP et des paramètres globaux**.
2. Définissez les instances MST. Chaque instance MST calcule et établit une topologie sans boucles pour transmettre les paquets à partir des VLAN qui mappent à l'instance. Reportez-vous à la section **Mappage des VLAN à une instance MST**.
3. Associez ces instances MST aux VLAN en choisissant l'instance MST sera active dans un VLAN spécifique.
4. Pour configurer les attributs MSTP :
   - **Définition des propriétés MSTP**
   - **Définition des paramètres d'instance MSTP**
   - **Mappage des VLAN à une instance MST**
   - **Définition des paramètres de l'interface MSTP**

Définition des propriétés MSTP

Le protocole global Multiple Spanning Tree (MSTP) configure un Spanning Tree distinct pour chaque groupe VLAN et bloque tous les chemins alternatifs possibles sauf un, ceci dans chaque Spanning Tree. MSTP permet la formation de régions MST pouvant exécuter des instances MST multiples (MSTI). Des régions multiples et d'autres ponts STP sont interconnectés à l'aide d'un Spanning Tree commun unique (CST).

MSTP est totalement compatible avec les ponts RSTP dans la mesure où un BPDU MSTP peut être interprété par un pont RSTP en tant que BPDU RSTP. Cela assure non seulement une compatibilité avec les ponts RSTP sans modifier la configuration mais permet aussi à tous les ponts RSTP en dehors d'une région MSTP de percevoir la région comme un pont RSTP unique, ceci quel que soit le nombre de ponts MSTP dans la région.

Pour que deux ou plusieurs commutateurs soient dans la même région MST, ils doivent posséder les mêmes VLAN mappés sur une instance MST, le même numéro de révision de la configuration ainsi que le même nom de région.

Les commutateurs destinés à être dans la même région MST ne sont jamais séparés par des commutateurs d'une autre région MST. Si tel est le cas, la région se sépare en deux régions distinctes.

Ce mappage peut être effectué dans la *rubrique VLAN d'une instance MST*.

La configuration indiquée sur cette page s'applique si le mode STP du système est paramétré sur MSTP.

Pour définir MSTP :

ÉTAPE1 Cliquez sur **Spanning Tree** > **État STP et paramètres globaux**. La *rubrique État STP et paramètres globaux* s'affiche. Activez MSTP.

ÉTAPE 2 Cliquez sur **Spanning Tree** > **MSTP Propriétés**. La *rubrique Propriétés MSTP* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Nom de région** : définissez un nom de région MSTP.
- **Révision** : définissez un nombre non affecté d'un signe à 16 octets qui identifie la révision de la configuration MST actuelle. Ce champ est compris entre 0 et 65535.

- **Sauts max.** : définissez le nombre total des sauts se produisant dans une région spécifique avant la désactivation du BPDU. Lorsque le BPDU est désactivé, les informations du port sont obsolètes. Ce champ est compris entre 1 et 40.
- **Maître IST** : affiche le maître de la région.

ÉTAPE 4 Cliquez sur **Appliquer**. Les propriétés MSTP sont définies et le commutateur est mis à jour.

Mappage des VLAN à une instance MST

La *rubrique VLAN d'une instance MST* vous permet de mapper chaque VLAN à une instance Multiple Spanning Tree (MSTI). Pour que les périphériques soient dans la même région, le mappage des VLAN aux MSTI doit être identique.

REMARQUE Le même MSTI peut être mappé à plus d'un VLAN. Un VLAN ne peut lui être lié qu'à une instance MST.

La configuration indiquée sur cette page (et toutes les pages MSTP) s'applique si le mode STP du système est défini sur MSTP.

Sept instances MST peuvent au maximum être définies sur les commutateurs Cisco Small Business 300. Le commutateur mappe automatiquement à l'instance CIST (Core and Internal Spanning Tree) les VLAN qui ne sont pas explicitement mappés à l'une des instances MST. L'instance CIST est l'instance MST 0.

Pour relier des VLAN à des instances MSTP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **VLAN d'une instance MSTP**. La *rubrique VLAN d'une instance MST* s'affiche.

La rubrique VLAN d'une instance MSTP contient les champs suivants :

- **ID d'instance MSTP** : toutes les instances MSTP sont affichées.
- **VLAN** : tous les VLAN appartenant à l'instance MSTP sont affichés.

ÉTAPE 2 Pour ajouter un VLAN à une instance MSTP, sélectionnez l'instance MSTP puis cliquez sur **Modifier**. La *rubrique VLAN d'une instance MST* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **ID d'instance MSTP** : sélectionnez l'instance MSTP.

- **VLAN** : définissez les VLAN à mapper sur cette instance MSTP.
- **Action** : choisissez **Ajouter** (mapper) ou **Supprimer** le VLAN à/de l'instance MSTP.

ÉTAPE 4 Cliquez sur **Appliquer**. Les mappages MSTP VLAN sont définis et le commutateur est mis à jour.

Définition des paramètres d'instance MSTP

La *rubrique Paramètres d'instance MST* vous permet de configurer et d'afficher les paramètres par instance MSTP. C'est l'équivalent par instance des Configuration de l'état STP et des paramètres globaux.

Pour entrer les paramètres de l'instance MSTP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **Paramètres de l'instance MSTP**. La *rubrique Paramètres d'instance MST* s'affiche.

ÉTAPE 2 Saisissez les paramètres.

- **ID d'instance** : sélectionnez une instance MSTP à afficher et à définir.
- **VLAN inclus** : affiche les VLAN mappés à l'instance sélectionnée. Le mappage par défaut mappe tous les VLAN à l'instance CIST (Common and Internal Spanning Tree) (instance 0).
- **Priorité du pont** : définissez la priorité de ce pont pour l'instance MSTP sélectionnée.
- **ID du pont racine désigné** : affiche la priorité et l'adresse MAC du pont racine pour l'instance MSTP.
- **Port racine** : affiche le port racine de l'instance sélectionnée.
- **Coût du chemin racine** : affiche le coût du chemin racine de l'instance sélectionnée.
- **ID du pont** : affiche la priorité du pont et l'adresse MAC de ce commutateur pour l'instance sélectionnée.
- **Sauts restants** : affiche le nombre de sauts restant jusqu'à la prochaine destination.

ÉTAPE 3 Cliquez sur **Appliquer**. La configuration de l'instance MST est définie et le commutateur est mis à jour.

Définition des paramètres de l'interface MSTP

La *rubrique Paramètres d'interface MSTP* vous permet de configurer les paramètres MSTP du port pour chaque instance MSTP et d'afficher les informations actuellement connues par le protocole comme par exemple le pont désigné par instance MST.

Pour configurer les ports dans une instance MST :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **Paramètres d'interface MSTP**. La *rubrique Paramètres d'interface MSTP* s'affiche.

ÉTAPE 2 Saisissez les paramètres.

- **L'instance équivaut à** : sélectionnez l'instance MSTP à configurer.
- **Le type d'interface équivaut à** : choisissez d'afficher la liste des ports ou des LAG.

Les paramètres MSTP pour les interfaces de l'instance s'affichent.

ÉTAPE 3 Sélectionnez une interface puis cliquez sur **Modifier**. La rubrique Modifier les paramètres d'interface s'affiche.

ÉTAPE 4 Saisissez les paramètres.

- **ID d'instance** : sélectionnez l'instance MST à configurer.
- **Interface** : sélectionnez l'interface pour laquelle les paramètres MSTI doivent être définis.
- **Priorité d'interface** : définissez la priorité du port pour l'interface spécifiée et l'instance MST.
- **Coût de chemin** : définissez la contribution du port au coût du chemin racine ou utilisez la valeur par défaut. Le coût du chemin racine est le coût du commutateur pour le pont racine de l'instance MST spécifiée.

- **État du port** : affiche l'état MSTP du port spécifique sur une instance MST spécifique. Les paramètres sont définis comme suit :
  - Désactivé : STP est actuellement désactivé.
  - Blocage : le port sur cette instance est actuellement bloqué et ne peut ni transférer le trafic (à l'exception des données BPDU) ni connaître les adresses MAC.
  - Écoute : le port sur cette instance est en mode Écoute. Il ne peut ni transférer le trafic ni connaître les adresses MAC.
  - Apprentissage : le port sur cette instance est en mode Apprentissage. Il ne peut pas transférer le trafic mais peut peut connaissance de nouvelles adresses MAC.
  - Transfert : le port sur cette instance est en mode Transfert. Il peut transférer le trafic et prendre connaissance de nouvelles adresses MAC.
- **Rôle du port** : affiche le rôle du port ou du LAG, par port ou LAG par instance, assigné par l'algorithme MSTP afin de fournir les chemins STP :
  - Racine : le transfert des paquets vers cette interface fournit le chemin de coût inférieur pour transférer les paquets vers le périphérique 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 pour l'instance MST.
  - Secondaire : l'interface fournit un chemin alternatif depuis l'interface racine vers le périphérique racine.
  - Secours : l'interface fournit un chemin de secours pour le chemin de port désigné vers les nœuds terminaux du Spanning Tree. Des ports de secours existent lorsque deux ports sont reliés dans une boucle par un lien point à point. Des ports de secours apparaissent également lorsqu'un LAN possède deux ou plusieurs connexions reliées à un segment partagé.
  - Désactivé : l'interface ne participe pas au Spanning Tree.
- **Mode** : affiche le mode Spanning Tree actuel.
  - STP classique : active le STP classique sur le port.
  - STP rapide : active RSTP sur le port.
  - STP : active STP sur le port.

- **Type** : affiche le type MST du port.
  - Limite : un port de limite relie les ponts MST à un LAN dans une région éloignée. Si le port est un port de limite, il indique également si le périphérique de l'autre côté du lien fonctionne en mode RSTP ou STP.
  - Port maître : un port maître fournit une connectivité d'une région MSTP vers la racine CIST éloignée.
  - Interne : le port est un port interne.
- **ID de pont désigné** : affiche le numéro d'ID de pont qui connecte le lien ou le LAN partagé à la racine.
- **ID de port désigné** : affiche le numéro d'ID du port sur le pont désigné qui connecte le lien ou le LAN partagé à la racine.
- **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.
- **Sauts restants** : affiche le nombre de sauts restant jusqu'à la prochaine destination.
- **Transitions de transfert** : affiche le nombre de fois où le port est passé du mode Transfert au mode Blocage.

ÉTAPE 5 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

13

Gestion des tables d'adresses MAC

Les adresses MAC sont stockées avec les informations relatives aux VLAN et aux ports dans la table des *adresses statiques* ou la table des adresses *dynamiques*. Les adresses statiques sont configurées par l'utilisateur dans la Tables des adresses statiques et n'expirent pas. Les adresses MAC détectées dans les paquets arrivant sur le commutateur sont répertoriées dans la table des adresses dynamiques pour une période définie. Si aucune autre trame disposant de la même adresse MAC source n'apparaît sur le commutateur avant l'expiration de ce délai, l'entrée est supprimée de la table.

Lorsqu'une trame arrive sur le commutateur, celui-ci recherche une adresse MAC 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 sur la base d'une recherche effectuée dans les tables. Les trames adressées à une adresse MAC de destination n'ayant pas été trouvée dans les tables sont diffusées à tous les ports du VLAN approprié. Ces trames sont appelées trames de monodiffusion inconnue.

Le commutateur prend en charge un maximum de 8 000 adresses MAC statiques et dynamiques.

Cette section contient des informations relatives à la définition des tables d'adresses MAC statiques et dynamiques et englobe les rubriques suivantes :

- **Configuration d'adresses MAC statiques**
- **Adresses MAC dynamiques**
- **Définition d'adresses MAC réservées**

Configuration d'adresses MAC statiques

Les adresses statiques peuvent être affectées à une interface et un VLAN spécifiques sur le commutateur. Les adresses sont liées à l'interface affectée. Si une adresse statique est détectée sur une autre interface, cette adresse est ignorée et n'est pas enregistrée dans la table des adresses.

La *rubrique Adresses statiques* permet d'afficher les adresses MAC configurées de façon statique et de créer de nouvelles adresses MAC statiques.

Pour définir une adresse statique :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC** > **Adresses statiques**. La *rubrique Adresses statiques* s'ouvre.

La *rubrique Adresses statiques* affiche les adresses statiques définies.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une adresse statique* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **ID VLAN** : sélectionnez l'ID VLAN du port.
- **Adresse MAC** : saisissez l'adresse MAC de l'interface.
- **Interface** : sélectionnez une interface (port ou LAG) pour l'entrée.
- **État** : sélectionnez le mode de traitement de l'entrée. Les options disponibles sont les suivantes :
  - *Permanent* : l'adresse MAC statique n'est jamais supprimée de la table à l'expiration d'un délai et si elle est enregistrée dans la Configuration de démarrage elle est conservée après le redémarrage.
  - *Supprimer à la réinitialisation* : l'adresse MAC statique n'est jamais supprimée de la table à l'expiration d'un délai.
  - *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.

ÉTAPE 4 Cliquez sur **Appliquer**. Une nouvelle entrée est créée dans la table.

Adresses MAC dynamiques

La Table des adresses dynamiques contient les adresses MAC obtenues en surveillant les adresses source du trafic entrant dans le commutateur. Lorsque l'adresse de destination du trafic entrant est trouvée dans la base de données, les paquets destinés à cette adresse sont directement transmis au port associé. Dans le cas contraire, le trafic est transmis à tous les ports du VLAN de la trame.

Pour éviter le débordement de la table de pontage et libérer de l'espace pour les nouvelles adresses, une adresse MAC dynamique est supprimée de cette table si aucun trafic n'est reçu de cette adresse au cours d'un délai spécifique. Ce délai correspond au délai d'expiration.

Configuration des paramètres d'adresses MAC dynamiques

La *rubrique Paramètres des adresses dynamiques* permet d'indiquer le délai d'expiration de la table des adresses MAC.

Pour entrer le délai d'expiration des adresses dynamiques :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC** > **Paramètres des adresses dynamiques**. La *rubrique 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**. La Table des adresses MAC dynamiques est mise à jour.

Interrogation d'adresses dynamiques

La *rubrique Adresses dynamiques* permet d'interroger la table des adresses MAC dynamiques en fonction des critères suivants :

- Type d'interface
- Adresses MAC
- VLAN

Cette page affiche les adresses MAC acquises de façon dynamique. Vous pouvez effacer les adresses dynamiques de la table des adresses MAC et spécifier des critères d'interrogation afin d'afficher un sous-ensemble de la table comme les adresses MAC acquises via une interface spécifique. Vous pouvez également spécifier le mode de tri des résultats de l'interrogation. Si vous n'saisissez aucun critère de filtrage, toute la table s'affichera.

Pour interroger la table des adresses dynamiques :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC** > **Adresses dynamiques**. La *rubrique Adresses dynamiques* s'ouvre.

ÉTAPE 2 Dans le bloc *Filtre*, saisissez les critères d'interrogation suivants :

- **ID VLAN** : saisissez l'ID VLAN pour lequel la table est interrogée.
- **Adresse MAC** : saisissez l'adresse MAC pour laquelle la table est interrogée.
- **Interface** : sélectionnez l'interface au sujet de laquelle la table est interrogée. L'interrogation peut également rechercher des ports ou LAG spécifiques.
- **Clé de tri de la table des adresses dynamiques** : saisissez le champ en fonction duquel la table est triée. La table des adresses peut être triée en fonction de l'ID VLAN, de l'adresse MAC ou de l'interface.

ÉTAPE 3 Sélectionnez l'option souhaitée pour le tri de la Clé de tri de la table des adresses dynamiques.

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.

Définition d'adresses MAC réservées

Lorsque le commutateur reçoit une trame utilisant une adresse MAC de destination qui appartient à une plage réservée (conformément à la norme IEEE), cette trame peut être abandonnée ou pontée. La configuration peut être définie par adresse MAC réservée ou par adresse MAC réservée et type de trame, comme suit :

- Adresse MAC réservée, type de trame et Ethertype pour une trame de type EthertnetV2
- Adresse MAC réservée, type de trame et DSAP-SSAP pour une trame de type LLC
- Adresse MAC réservée, type de trame et PID pour une trame de type LLC-SNAP

Pour configurer une entrée pour une adresse MAC réservée :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC** > **Adresses MAC réservées**. La *rubrique Adresses MAC réservées* s'ouvre.

Cette page affiche les adresses MAC réservées.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une adresse MAC réservée* s'ouvre.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **Adresse MAC** : sélectionnez l'adresse MAC à réserver.
- **Type de trame** : sélectionnez un type de trame en fonction des critères suivants :
  - *Ethernet V2* : s'applique aux paquets Ethernet V2 avec l'adresse MAC spécifique.
  - *LLC* : s'applique aux paquets LLC (Logical Link Control) avec l'adresse MAC spécifique.
  - *LLC-SNAP* : s'applique aux paquets LLC-SNAP (Logical Link Control/ Sub-Network Access Protocol) avec l'adresse MAC spécifique.
  - *Tout* : s'applique à tous les paquets avec l'adresse MAC spécifique.

- **Action** : sélectionnez l'une des actions suivantes qui sera appliquée au paquet entrant correspondant aux critères sélectionnés :
  - *Abandonner* : supprime le paquet.
  - *Pont* : transfère le paquet à tous les membres du VLAN.

ÉTAPE 4 Cliquez sur **Appliquer**. Une nouvelle adresse MAC est réservée.

14

Configuration du transfert de multidiffusion

Ce chapitre décrit la fonction de transfert de multidiffusion. Il contient les rubriques suivantes :

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 rompre 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'IGMP v2 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 ces 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 provenant (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 où il reçoit 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

Fonctionnement de la multidiffusion

Dans un service de multidiffusion Layer 2, 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

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, ce commutateur analyse tous 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 provenant 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 sur les 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 activées :

- IGMP v1/v2/ v3
- MLD v1/v2
- Émetteur de requêtes de traçage IGMP Snooping simple

Vous devez disposer d'un émetteur de requêtes IGMP pour gérer le protocole IGMP sur un sous-réseau particulier. En général, le routeur de multidiffusion sert également d'émetteur de requêtes IGMP. Lorsqu'un sous-réseau inclut plusieurs émetteurs de requêtes IGMP, ces émetteurs choisissent l'un des leurs comme émetteur principal.

Vous pouvez configurer le Sx300 en tant qu'émetteur de requêtes IGMP de secours ou l'utiliser comme un émetteur de requêtes IGMP lorsqu'il n'existe aucun émetteur de requêtes IGMP standard. Le Sx300 ne dispose pas de toutes les fonctions d'un émetteur de requêtes IGMP.

Si vous configurez le commutateur en tant qu'émetteur de requêtes IGMP, il démarre s'il s'écoule 60 secondes sans qu'aucun trafic (requêtes) IGMP ne soit détecté depuis un routeur de multidiffusion. En présence d'autres émetteurs de requêtes IGMP, le commutateur peut cesser d'envoyer des requêtes (ou non), ceci en fonction des résultats du processus de sélection de l'émetteur de requêtes standard.

Propriétés d'adresse de multidiffusion

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 située 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 groupe de multidiffusion 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 leur 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 *rubrique Propriétés* vous 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 dans la *rubrique 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** : sur la base de l'adresse MAC de destination dans la trame Ethernet.

  REMARQUE Comme cela est mentionné à la section « Propriétés d'adresse de multidiffusion », il est possible de mapper une ou plusieurs adresses IP de groupe de multidiffusion 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** : sur la base de 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 assure le soutien d'un maximum de 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 *rubrique Propriétés* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **État du filtrage multidiffusion par ponts** : permet d'activer ou de désactiver le filtrage.
- **ID VLAN** : sélectionnez l'ID du VLAN voulu pour définir sa méthode de transfert.
- **Méthode de transfert pour IPv6** : définissez la méthode de transfert pour les adresses IPv6. Le matériel les utilise 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.

- **Méthode de transfert pour IPv4** : définissez la méthode de transfert pour les adresses IPv4. Le matériel les utilise 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.

ÉTAPE 3 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

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 *rubrique 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 cette base de données qui fournissent des informations de transfert statiques sur la base des adresses MAC de destination.
- Affichage de la liste de tous les ports/LAG membres de chaque ID de VLAN ou adresse MAC de group et indication de si le trafic doit ou non être transféré vers cette destination.

Pour afficher les informations en transfert, utilisez la *rubrique Adresse IP du groupe de multidiffusion* une fois en mode *Adresse de groupe IP* ou en mode *Groupe IP et source*.

Pour définir et afficher des groupes de multidiffusion MAC :

ÉTAPE 1 Cliquez sur **Multidiffusion > Adresse MAC de groupe**. La *rubrique 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.

ÉTAPE 4 Cliquez sur **Ajouter** pour ajouter une adresse MAC de groupe statique. La *rubrique 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 MAC de groupe** : définit l'adresse MAC du nouveau groupe de multidiffusion.

ÉTAPE 6 Cliquez sur **Appliquer** ; la MAC du groupe de multidiffusion est ajoutée et le commutateur est mis à jour.

Pour configurer et afficher l'enregistrement des interfaces au sein du groupe, sélectionnez une adresse puis cliquez sur **Détails**. La *rubrique Paramètres d'adresse de groupe MAC* s'ouvre.

La page affiche les éléments suivants :

- **ID VLAN** : ID de VLAN du groupe de multidiffusion.
- **Adresse MAC de groupe** : adresse MAC du groupe.

ÉTAPE 7 Sélectionnez dans le menu **Filtre : Type d'Interface** le port ou le LAG à afficher.

ÉTAPE 8 Cliquez sur **OK** pour afficher les membres (ports ou LAG).

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 commutateur est mis à jour.

Adresse IP de multidiffusion de groupe

La *rubrique Adresse IP du groupe de multidiffusion* ressemble à la *rubrique Adresse de groupe MAC* à la seule différence que les groupes de multidiffusion y sont identifiés par leurs adresses IP.

La *rubrique Adresse IP du groupe de multidiffusion* vous permet d'interroger et d'ajouter des IP de multidiffusion de groupes.

Pour définir et afficher des IP de multidiffusion de groupes :

ÉTAPE 1 Cliquez sur **Multidiffusion > Adresse IP de multidiffusion de groupe**. La *rubrique Adresse IP du groupe de multidiffusion* s'ouvre.

La page affiche toutes les adresses IP de multidiffusion de groupes apprises via le traçage (Snooping).

ÉTAPE 2 Saisissez les paramètres nécessaires pour le filtrage.

- **ID VLAN est égal à** : définissez l'ID de VLAN du groupe à afficher.
- **Version IP est égale à** : sélectionnez IPv6 ou IPv4.
- **Adresse IP de 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).
- **Adresse IP source est égale à** : définissez l'adresse IP source du périphérique émetteur. Si le mode est (S,G), saisissez la valeur S (indiquant l'expéditeur). Combinée à l'adresse IP de groupe, cette valeur définit l'ID de multidiffusion du groupe (S,G) à afficher. Si le mode est (*.G), saisissez un astérisque (*) pour indiquer que le groupe de multidiffusion n'est défini que par sa destination.

ÉTAPE 3 Cliquez sur **OK**. Les résultats s'affichent dans le bloc inférieur. Lorsque vous activez à la fois Bonjour et IGMP sur un commutateur 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 rubrique Paramètres d'interface d'IP 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 du nouveau groupe de multidiffusion.
- **Propre à la source** : indique que l'entrée contient une source spécifique et ajoute l'adresse correspondante dans le champ Adresse IP source. Dans le cas contraire, l'entrée est ajoutée sous la forme (*,G), c'est-à-dire une adresse IP de groupe associée à toutes les sources IP.
- **Adresse IP source** : définit l'adresse source à inclure.
- **Filtre : Type d'interface est égal à** : sélectionnez le port afin d'afficher les membres (ports ou LAG). Vous pouvez cliquer sur le bouton d'option **Statique** pour ajouter le port ou LAG spécifique concerné à l'IP de multidiffusion du groupe.

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 rubrique Paramètres d'interface d'IP de multidiffusion s'ouvre.

ÉTAPE 8 Saisissez les paramètres.

- **ID VLAN** : saisissez l'ID de VLAN du groupe à ajouter.
- **Version IP** : sélectionnez la version IP.
- **Adresse IP de multidiffusion de groupe** : saisissez l'adresse IP du nouveau groupe de multidiffusion.
- **Adresse IP source** : saisissez l'adresse de l'expéditeur. En mode (S,G), la source (S) de l'expéditeur est affichée. Combinée à l'adresse IP de groupe, cette valeur définit l'ID de multidiffusion du groupe (S,G). Si le mode est (*.G), l'astérisque (*) indique que le groupe de multidiffusion est défini par sa destination.

ÉTAPE 9 Cliquez sur **OK** pour afficher les membres du groupe (ports ou LAG).

ÉTAPE 10 Sélectionnez le type d'association de chaque interface. Les options disponibles sont les suivantes :

- *Statique* : rattache l'interface au groupe de multidiffusion en tant que membre statique.
- *Dynamique* : 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* : indique que le port n'est actuellement pas membre de ce groupe de multidiffusion sur ce VLAN.

ÉTAPE 11 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

Traçage IGMP Snooping

Pour prendre en charge le transfert de multidiffusion sélectif (IPv4), vous devez activer le filtrage multidiffusion par ponts. Vous devez aussi activer le traçage IGMP Snooping globalement ainsi que pour chacun des VLAN concernés.

Informations supplémentaires

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 dans la *rubrique 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.

L'émetteur de requêtes de traçage IGMP Snooping sert à prendre en charge un domaine de multidiffusion Layer 2 de commutateurs de traçage, en l'absence d'un routeur de multidiffusion. Par exemple, dans le cas où un serveur local fournit un contenu de multidiffusion alors que le routeur (s'il en existe un) de ce réseau ne prend pas en charge la multidiffusion.

Il ne doit exister qu'un seul émetteur de requêtes IGMP dans chaque domaine de multidiffusion Layer 2. Le commutateur prend en charge le choix de l'émetteur de requêtes IGMP basé sur les normes lorsqu'il existe plusieurs émetteurs de requêtes IGMP dans le domaine.

La vitesse de fonctionnement de l'émetteur de requêtes IGMP doit s'aligner sur celle des commutateurs dotés de fonctions de traçage IGMP Snooping. Les requêtes doivent être envoyées à un rythme qui corresponde à la durée de vie des entrées dans la table de traçage. Si les requêtes sont envoyées à un rythme inférieur à la durée de vie, l'abonné ne peut pas recevoir les paquets 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 *rubrique Traçage IGMP Snooping* s'ouvre.

La table de traçage IGMP Snooping affiche les informations IGMP Snooping des VLAN du commutateur. Les colonnes de cet affichage sont décrites à l'**ÉTAPE 4**.

ÉTAPE 2 Vérifiez l'état d'activation (ou de désactivation) du traçage IGMP Snooping.

L'option État IGMP Snooping permet au périphérique qui surveille le trafic réseau de déterminer les hôtes qui ont demandé à recevoir le trafic de multidiffusion. Le commutateur exécute le traçage IGMP Snooping si vous avez activé à la fois IGMP Snooping et le filtrage multidiffusion par ponts.

ÉTAPE 3 Sélectionnez un VLAN puis cliquez sur **Modifier**. La *rubrique Modifier IGMP Snooping* s'ouvre.

Il ne doit exister qu'un seul émetteur de requêtes IGMP par réseau. Le commutateur prend en charge le choix de l'émetteur de requêtes IGMP basé sur les normes. Certaines des valeurs des paramètres de fonctionnement de cette table sont envoyées par l'émetteur de requêtes choisi. Les autres valeurs sont dérivées du commutateur.

ÉTAPE 4 Saisissez les paramètres.

- **ID VLAN** : sélectionnez l'ID du VLAN où le traçage IGMP Snooping est défini.
- **État IGMP Snooping** : activez ou désactivez la surveillance du trafic réseau pour déterminer les hôtes qui ont demandé à recevoir le trafic de multidiffusion. Le commutateur exécute le traçage IGMP Snooping uniquement si vous avez activé à la fois IGMP Snooping et le filtrage multidiffusion par ponts.
- **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** : affiche l'intervalle de requête du dernier membre, envoyé 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.
- **État de l'émetteur de requêtes IGMP** : permet d'activer ou de désactiver l'émetteur de requêtes IGMP.
- **Adresse IP source de l'émetteur de requêtes administratif** : sélectionnez l'adresse IP source de l'émetteur de requêtes IGMP. Il peut s'agir de l'adresse IP du VLAN ou de l'adresse IP de gestion.
- **Adresse IP source de l'émetteur de requêtes opérationnel** : affiche l'adresse IP source de l'émetteur de requêtes choisi.
- **Version de l'émetteur de requêtes IGMP** : sélectionnez la version IGMP utilisée si le commutateur devient l'émetteur de requêtes choisi. Sélectionnez IGMPv3 s'il existe des commutateurs et/ou des routeurs de multidiffusion dans le VLAN qui réalise le transfert de multidiffusion IP propre à la source.

ÉTAPE 5 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

Traçage MLD Snooping

Pour prendre en charge le transfert de multidiffusion sélectif (IPv6), vous devez activer le filtrage multidiffusion par ponts. Vous devez aussi activer le traçage MLD Snooping globalement ainsi que pour chacun des VLAN concernés.

REMARQUE Le commutateur ne prend en charge le traçage MLD Snooping que sur les VLAN statiques. Le traçage MLD Snooping n'est pas pris en charge sur les VLAN dynamiques.

Le commutateur exploite cette fonction pour construire 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.

Informations supplémentaires

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 destination IPv6.
- 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. Toutefois, seules les définitions statiques sont conservées si vous redémarrez le système.

Pour activer le traçage MLD Snooping :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **MLD Snooping**. La *rubrique MLD Snooping* s'ouvre.

ÉTAPE 2 Activez ou désactivez l'option **État MLD Snooping**. L'option État MLD Snooping permet au périphérique qui surveille le trafic réseau de déterminer les hôtes qui ont demandé à recevoir du trafic de multidiffusion. Le commutateur exécute le traçage MLD Snooping si vous avez activé à la fois MLD Snooping et le filtrage multidiffusion par ponts.

La table de traçage MLD Snooping affiche les informations MLD Snooping des VLAN du commutateur. Pour consulter une description des colonnes de cette table, reportez-vous à l'**ÉTAPE 3**.

ÉTAPE 3 Sélectionnez un VLAN puis cliquez sur **Modifier**. La *rubrique 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 ce port. Le commutateur surveille le trafic réseau pour déterminer les hôtes qui ont demandé à recevoir du trafic de multidiffusion. Vous ne pouvez activer le traçage MLD Snooping que si le filtrage multidiffusion par ponts a été activé dans la *rubrique Propriétés*.
- **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 l'intervalle de requête que le commutateur doit appliquer s'il ne peut pas dériver la valeur des messages envoyés par l'émetteur de requêtes choisi.
- **Intervalle de requête opérationnelle** : intervalle en secondes qui sépare 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 commutateur est mis à jour.

IP de multidiffusion de groupes IGMP/MLD

La page IP de multidiffusion de groupes IGMP/MLD affiche l'adresse IPv4 et IPv6 de groupes que le commutateur apprend des messages IGMP/MLD qu'il trace (Snooping).

Il peut exister des différences entre les informations affichées sur cette page et, par exemple, celles affichées sur la *rubrique 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 *rubrique 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 vers lesquels le flux de multidiffusion correspondant est transféré.

- **Ports exclus** : liste des ports non membres du groupe.
- **Mode de compatibilité** : version d'enregistrement IGMP/MLD la plus ancienne que le commutateur reçoit des hôtes à l'adresse IP du groupe.

Port 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 ports de routeur de multidiffusion lorsqu'il transfère les flux de multidiffusion et les messages d'enregistrement IGMP/MLD. Cela est indispensable pour que tous les routeurs de multidiffusion puissent, à leur tour, transférer les flux de multidiffusion et propager les messages d'enregistrement vers d'autres sous-réseaux.

Cette page vous permet de configurer de manière statique (ou de détecter de manière dynamique) les ports connectés aux routeurs Mrouter.

Pour définir des ports de routeur de multidiffusion :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Port de routeur de multidiffusion**. La *rubrique 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 que vous décrivez.
- **IPv4 ou IPv6 est égal 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 interface. Les options disponibles sont les suivantes :

- *Statique* : le port est configuré de manière statique en tant que port de routeur de multidiffusion.

- *Dynamique* : 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 routeur de multidiffusion, même s'il reçoit des requêtes IGMP ou MLD. Si l'option **Détection automatique des ports MRouter** est activée sur ce port, la configuration échoue.
- *Aucun* : le port n'est actuellement pas un port de routeur de multidiffusion.

ÉTAPE 5 Cliquez sur **Appliquer** pour mettre à jour le commutateur.

Définition de la multidiffusion Tout transférer

La *rubrique Tout transférer* active et affiche la configuration des ports et/ou LAG qui doivent recevoir l'ensemble du flux de multidiffusion provenant d'un VLAN spécifique. Cette fonction exige que vous activiez le filtrage multidiffusion par ponts dans la *rubrique Propriétés*. Si cette fonction est désactivée, tout le trafic de multidiffusion est envoyé à tous les ports du commutateur.

Vous pouvez configurer 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 *rubrique 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 l'interface à définir en mode Tout transférer à l'aide des méthodes suivantes :

- *Statique* : le port reçoit tous les flux de multidiffusion.
- *Dynamique* : (Non applicable).
- *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 commutateur est mis à jour.

Définition de 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 manière statique. Qu'ils aient été appris dynamiquement ou configurés de façon statique, ces groupes de multidiffusion sont considérés comme enregistrés. Cela permet au commutateur de transférer les trames de multidiffusion (depuis un groupe de multidiffusion enregistré) uniquement vers les ports membres du groupe de multidiffusion concerné. Le commutateur transfère les trames de multidiffusion (depuis un groupe de multidiffusion enregistré) uniquement vers les ports enregistrés dans ce groupe de multidiffusion.

La *rubrique 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 *rubrique 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.
- **N° d'entrée** : numéro de l'entrée dans la table de multidiffusion non enregistrée.
- **Interface** : affiche l'ID de l'interface.
- **Multidiffusion non enregistrée** : affiche l'état de transfert de l'interface sélectionnée. Les valeurs disponibles sont les 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 **Modifier**. La *rubrique Modifier la multidiffusion non enregistrée* s'ouvre.

ÉTAPE 4 Remplissez le champ Multidiffusion non enregistrée.

- **Interface** : sélectionnez l'interface à modifier.
- **Multidiffusion non enregistrée** : définissez l'état de transfert de l'interface sélectionnée. Les options disponibles sont les suivantes :
  - *Transfert* : active le transfert des trames de multidiffusion non enregistrée vers l'interface sélectionnée.
  - *Filtrage* : active le filtrage des trames de multidiffusion non enregistrée sur l'interface sélectionnée.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres sont enregistrés et le commutateur est mis à jour.

15

Configuration des informations IP

Les adresses d'interface IP peuvent être configurées manuellement par l'utilisateur ou automatiquement via un serveur DHCP. Ce chapitre fournit des informations sur la définition des adresses IP du commutateur.

Il contient les rubriques suivantes :

- **Interfaces de gestion et IP**
- **Définition du routage statique IPv4**
- **Activation du proxy ARP**
- **Définition du relais UDP**
- **Relais DHCP**
- **Configuration d'ARP**
- **DNS (Domain Name System, système de noms de domaine)**

Interfaces de gestion et IP

Le paramètre d'usine par défaut défini pour 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 DHCPDECLINE (Refus DHCP) au serveur DHCP qui lui a 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 par défaut.

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. En mode Layer 2, seul le VLAN de gestion peut être configuré avec une adresse IP statique ou dynamique. En mode Layer 3, vous pouvez configurer jusqu'à 32 interfaces (ports, LAG et/ou VLAN) du commutateur avec une adresse IP statique ou dynamique. Les sous-réseaux IP dont font partie ces adresses IP sont appelés sous-réseaux IP à connexion directe.

Les règles d'affectation d'adresse IP au commutateur sont les suivantes :

- En mode Layer 2, 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 du 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 DHCPREQUEST (Demande DHCP).
- 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.

Gestion d'IPv6

Internet Protocol version 6 (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 tunnel exploite 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 IPv6 Ethertype.

Adressage IP

Le commutateur peut fonctionner en mode Layer 2 ou en mode Layer 3.

- En mode Layer 2, le commutateur fonctionne en tant que commutateur reconnaissant les VLAN Layer 2, sans aucune fonction de routage.
- En mode Layer 3, le commutateur possède des fonctions de routage en plus des fonctions du mode Layer 2.

  En mode Layer 3, le commutateur ne prend pas en charge les VLAN MAC, l'affectation dynamique de VLAN, la limite de débit VLAN, la protection DoS de débit SYN, ni les gestionnaires de stratégie de QoS avancé.

Pour configurer le commutateur afin qu'il fonctionne dans l'un ou l'autre mode, vous utilisez l'interface de console, décrite au chapitre **Interface de la console** du guide d'administration.

Les sections suivantes décrivent les différences qui existent entre l'adressage IP en mode Layer 2 et en mode Layer 3.

Adressage IP Layer 2

Adressage IP Layer 2

En mode 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 à l'aide d'une adresse IP statique ou via DHCP. Vous configurez l'adresse IP statique et la passerelle par défaut pour le mode Layer 2 dans la *rubrique Interface IPv4*. En mode Layer 2, 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, VLAN 1 est le VLAN de gestion mais vous pouvez modifier ce paramètre. Lorsqu'il fonctionne en mode Layer 2, le commutateur n'est accessible à l'adresse IP configurée que via son VLAN de gestion.

Adressage IP Layer 3

Adressage IP Layer 3

En mode Layer 3, le commutateur peut posséder plusieurs adresses IP. Chaque adresse IP peut être affectée aux ports, LAG ou VLAN spécifiés. Vous configurez ces adresses IP dans la *rubrique Interface IPv4* pour le mode Layer 3. Cela fournit davantage de souplesse réseau que le mode Layer 2, qui ne permet de configurer qu'une seule adresse IP. Lorsqu'il fonctionne en mode Layer 3, le commutateur est accessibles à toutes ses adresses IP depuis les interfaces correspondantes.

Aucune route prédéfinie par défaut n'est fournie en mode Layer 3. Vous devez définir une route par défaut pour gérer le commutateur à distance. Toutes les passerelles par défaut affectées par DHCP sont stockées en tant que routes par défaut. De plus, vous pouvez définir manuellement des routes par défaut. Vous utilisez pour ce faire la *rubrique Routes statiques IP*.

REMARQUE Vous ne pouvez faire passer le commutateur du mode Layer 2 au mode Layer 3 qu'à l'aide de l'interface de console. Lors de cette opération, tous les paramètres de configuration reprennent leurs valeurs par défaut. Pour en savoir plus sur l'interface de console, reportez-vous au chapitre **Interface de la console** du guide d'administration.

Toutes les adresses IP configurées sur le commutateur ou qui lui sont affectées sont également appelées « adresses IP de gestion » dans ce guide.

Les sections suivantes présentent des informations de configuration pertinentes à la fois pour le mode Layer 2 et le mode Layer 3.

Définition de l'interface IPv4 lorsque le commutateur fonctionne en mode Layer 2

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 *rubrique Interface IPv4* s'ouvre.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **VLAN de gestion** : sélectionnez le VLAN de gestion utilisé pour accéder au commutateur via telnet ou l'interface Web graphique (GUI). VLAN1 est le VLAN de gestion par défaut.
- **Type d'adresse IP** : sélectionnez l'une des options suivantes :
  - **Dynamique** : détection de l'adresse IP via DHCP sur le VLAN de gestion.
  - **Statique** : définition manuelle d'une adresse IP.

Si vous utilisez une adresse IP statique, configurez les champs suivants.

- **Adresse IP** : saisissez l'adresse IP puis remplissez 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** : sélectionnez Défini par l'utilisateur puis 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, sélectionnez les champs suivants, qui sont alors activés :

- **Renouveler l'adresse DHCP** : l'adresse IP dynamique du commutateur peut être renouvelée à tout moment après son affectation par le serveur DHCP. Selon la configuration de votre serveur DHCP, le commutateur peut recevoir une nouvelle adresse IP après le renouvellement, ce qui provoquera une perte de connexion de votre session sur l'interface graphique.
- **Configuration automatique via DHCP** : affiche l'état de la fonction de configuration automatique. Vous configurez la configuration DHCP automatique à l'aide de l'option *Administration* > *Gestion de fichiers* > *Configuration automatique DHCP*.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres d'interface IPv4 sont définis et le commutateur mis à jour.

Définition de l'interface IPv4 lorsque le commutateur fonctionne en mode Layer 3

Vous utilisez la *rubrique Interface IPv4* lorsque le commutateur fonctionne en mode Layer 3 : Ce mode permet de configurer plusieurs adresses IP pour la gestion du commutateur et fournit des services de routage.

L'adresse IP peut être configurée sur une interface de port, de LAG ou de VLAN.

Lorsqu'il fonctionne en mode Layer 3, le commutateur route le trafic entre les sous-réseaux IP à connexion directe configurés sur le commutateur. Le commutateur continue à servir de pont pour le trafic entre les périphériques appartenant au même VLAN. Vous pouvez configurer des routes IPv4 supplémentaires pour le routage vers des sous-réseaux sans connexion directe, dans la *rubrique Routes statiques IP*.

REMARQUE Le logiciel de commutateur consomme un seul ID de VLAN (VID) pour chaque adresse IP configurée sur un port ou un LAG. Le commutateur utilise le premier VID non encore utilisé, à partir de 4094.

Pour configurer des adresses IPv4 :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces de gestion et IP** > **Interface IPv4.** La *rubrique Interface IPv4* s'ouvre.

Cette page contient les champs suivants :

- **Interface** : interface pour laquelle l'adresse IP est définie.

- **Type d'adresse IP** : adresse IP définie comme statique ou DHCP.
  - *Statique* : saisie manuelle.
  - *DHCP* : réception depuis le serveur DHCP.
- **Adresse IP** : adresse IP configurée pour l'interface.
- **Masque** : masque d'adresse IP configuré.
- **État** : résultats de la vérification d'unicité de l'adresse IP.
  - *Aucune entrée* : adresse IP inconnue.
  - *Provisoire* : aucun résultat final pour la vérification d'unicité de l'adresse IP.
  - *Valide* : contrôle de collision d'adresse IP terminé, aucune collision détectée.
  - *Valide-Doublon* : contrôle de collision d'adresse IP terminé, une adresse IP en double a été détectée.
  - *Doublon sans validité* : doublon d'adresse IP détecté pour l'adresse IP par défaut.

ÉTAPE 2 **Cliquez sur Ajouter.** La *rubrique Ajouter une interface IPv4* s'ouvre.

ÉTAPE 3 Sélectionnez l'un des champs suivants :

- **Interface** : sélectionnez Port, LAG ou VLAN comme interface associée à cette configuration IP puis choisissez une valeur pour l'interface dans la liste.
- **Type d'adresse IP** : sélectionnez l'une des options suivantes :
  - **Adresse IP dynamique** : réception de l'adresse IP depuis un serveur DHCP.
  - **Adresse IP statique** : saisissez l'adresse IP.

ÉTAPE 4 Si vous avez choisi d'utiliser une adresse statique, saisissez l'**adresse IP** de l'interface.

ÉTAPE 5 Saisissez le masque réseau ou la longueur de préfixe correspondant à cette adresse IP.

- **Masque réseau** : masque IP pour cette adresse.
- **Longueur du préfixe** : longueur du préfixe d'adresse IPv4.

ÉTAPE 6 Cliquez sur **Appliquer.** Les paramètres d'adresse IPv4 sont définis et le commutateur est mis à jour.

Définition de la configuration globale IPv6

La *rubrique Configuration globale IPv6* indique la fréquence des messages d'erreur ICMP IPv6 générés par le commutateur.

Pour définir des paramètres IPv6 globaux :

ÉTAPE 1 En mode Layer 2, cliquez sur **Administration** > **Interface de gestion** > **Configuration globale IPv6**.

En mode Layer 3, cliquez sur **Configuration IP** > **Interfaces de gestion et IP** > **Configuration globale IPv6**.

La *rubrique Configuration globale IPv6* s'ouvre.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **Intervalle limite de débit ICMPv6** : saisissez le délai limite.
- **Taille de bucket limite de débit ICMPv6** : saisissez le nombre maximal de messages d'erreur ICMP que le commutateur peut envoyer au cours de chaque intervalle.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres d'adresse IPv6 sont définis et le commutateur mis à jour.

Définition d'une interface IPv6

La *rubrique Interfaces IPv6* affiche les paramètres d'interface IPv6 du commutateur et vous *permet* de configurer cette interface. 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'extrémité IPv6.

Une interface de tunnel est configurée avec une adresse IPv6 sur la base des paramètres définis dans la *rubrique Tunnel IPv6*.

Pour configurer des interfaces IPv6 :

ÉTAPE 1 En mode Layer 2, cliquez sur **Administration** > **Interface de gestion** > **Interfaces IPv6**.
En mode Layer 3, cliquez sur **Configuration IP** > **Interfaces de gestion et IP** > **Interfaces IPv6**.

La *rubrique Interfaces IPv6* s'ouvre.

Cette page affiche les interfaces IPv6 déjà configurées.

ÉTAPE 2 Cliquez sur **Ajouter** pour créer une nouvelle interface IPv6, c'est-à-dire pour définir l'interface sur laquelle IPv6 est activé. La *rubrique Ajouter une interface IPv6* s'ouvre.

ÉTAPE 3 Saisissez les valeurs.

- **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 des nouvelles adresses IPv6 Unicast avant de les 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 des adresses IPv6** : active la configuration automatique des adresses à partir du serveur DHCP. La configuration automatique des adresses est un processus avec ou sans conservation d'état (DHCP). 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.
- **Envoyer des messages ICMPv6** : active la génération de messages concernant les destinations injoignables.

ÉTAPE 4 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 5 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 En mode Layer 2, cliquez sur **Administration** > **Interface de gestion** > **Adresses IPv6**.
En mode Layer 3, cliquez sur **Configuration IP** > **Interfaces de gestion et IP** > **Adresses IPv6**.

La *rubrique Adresse IPv6* s'ouvre.

ÉTAPE 2 Sélectionnez une interface puis cliquez sur **OK**. L'interface s'affiche dans la table des adresses IPv6.

ÉTAPE 3 Cliquez sur **Ajouter**. La rubrique Ajouter une adresse IPv6 s'ouvre.

ÉTAPE 4 Saisissez les valeurs pour les champs.

- **Interface IPv6** : affiche l'interface où l'adresse est automatiquement complétée sur la base du filtre.
- **Type d'adresse IPv6** : sélectionnez Liaison locale ou Globale comme type d'adresse IPv6 à ajouter.
  - *Liaison locale* : l'adresse IPv6 identifie de manière unique l'hôte situé sur une seule liaison réseau. 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 prise en charge. S'il existe une adresse locale de liaison sur l'interface, cette entrée remplace l'adresse dans la configuration.
  - *Globale* : l'adresse IPv6 est de type IPV6 de monodiffusion globale, visible et joignable depuis 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** : longueur du préfixe IPv6 global est une valeur décimale de 0 à 128 indiquant 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 commutateur est mis à jour.

Définition d'une liste de routeurs IPv6 par défaut

La *rubrique Liste des routeurs par défaut IPv6* vous permet de configurer et d'afficher les adresses de routeur IPv6 par défaut. Cette liste peut être vide ou contenir un ou plusieurs routeurs candidats au rôle de routeur par défaut pour le trafic non local. 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 interface IP, toutes les adresses IP de routeur par défaut sont supprimées.
- Il est impossible de supprimer des adresses IP dynamiques.
- Un message d'alerte s'affiche lorsque vous tentez d'insérer plus d'une adresse définie par l'utilisateur.
- Un message d'alerte s'affiche lorsque vous tentes d'insérer une adresse d'un type autre qu'une liaison locale « fe80: ».

Pour définir un routeur par défaut :

ÉTAPE 1 En mode Layer 2, cliquez sur **Administration** > **Interface de gestion** > **Liste des routeurs par défaut IPv6**.
En mode Layer 3, cliquez sur **Configuration IP** > **Interfaces de gestion et IP** > **Liste des routeurs par défaut IPv6**.

La *rubrique Liste des routeurs par défaut IPv6* s'ouvre.

Cette page contient 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** : la configuration du routeur par défaut 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 *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 la durée prédéfinie indiquée par *Délai de retard*. 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 *rubrique 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'adresse IP du routeur par défaut statique dans le champ Adresse IPv6 du routeur par défaut.

ÉTAPE 4 Cliquez sur **Appliquer**. Le routeur par défaut est défini et le commutateur mis à jour.

Configuration de tunnels IPv6

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. Vous devez activer et configurer manuellement le tunnel ISATAP. Vous définissez ensuite manuellement une interface IPv6 sur ce tunnel ISATAP. Enfin, 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 processus DNS.

Pour configurer un tunnel IPv6 :

ÉTAPE 1 En mode Layer 2, cliquez sur **Administration** > **Interface de gestion** > **Tunnel IPv6**.
En mode Layer 3, cliquez sur **Configuration IP** > **Interfaces de gestion et IP** > **Tunnel IPv6**.

La *rubrique Tunnel IPv6* s'ouvre.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **Numéro du tunnel** : affiche le numéro de domaine du routeur de tunnel automatique.
- **Type du tunnel** : toujours affiché en tant qu'ISATAP.
- **Adresse IPv4 source** : désactive le tunnel ISATAP ou l'active sur une interface IPv4. L'adresse IPv4 de l'interface IPv4 sélectionnée sera utilisée 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* : désactive le tunnel ISATAP.
- *Manuel* : configuration manuelle d'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** : sert à 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 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 défini et le commutateur mis à jour.

Définition des informations sur les voisins IPv6

La *rubrique 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 ARP IPv4. 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 En mode Layer 2, cliquez sur **Administration** > **Interface de gestion** > **Voisins IPv6**.
En mode Layer 3, cliquez sur **Configuration IP** > **Interfaces de gestion et IP** > **Voisins IPv6**.

La *rubrique Voisins IPv6* s'ouvre.

ÉTAPE 2 Sélectionnez une option **Effacer la table** afin d'effacer certaines adresses IPv6 (ou toutes) de la table de voisinage IPv6.

- *Statique uniquement* : permet de supprimer les entrées d'adresse IPv6 statiques.
- *Dynamique uniquement* : permet de supprimer les entrées d'adresse IPv6 dynamiques.
- *Dynamique et statique* : permet de supprimer 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 configuration des informations de cache de détection du voisinage (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.
  - *Accessible* : 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 Cliquez sur **Ajouter**. La *rubrique Ajouter un voisin IPv6* s'ouvre.

La *rubrique Ajouter un voisin IPv6* fournit des informations pour l'ajout d'un voisin à surveiller.

ÉTAPE 4 Saisissez les valeurs pour 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 commutateur est mis à jour.

Modification d'un voisin IPv6

Pour modifier un voisin IPv6 :

ÉTAPE 1 En mode Layer 2, cliquez sur **Administration** > **Interface de gestion** > **Voisins IPv6**.
En mode Layer 3, cliquez sur **Configuration IP** > **Interfaces de gestion et IP** > **Voisins IPv6**.

La *rubrique Voisins IPv6* s'ouvre.

ÉTAPE 2 Sélectionnez une interface puis cliquez sur **Modifier**. La *rubrique Modifier le voisin IPv6* s'ouvre.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **Adresse IPv6** : sélectionnez une adresse IPv6 valide.
- **Adresse MAC** : sélectionnez l'adresse MAC mappée sur l'adresse IPv6 spécifiée.
- **Type** : sélectionnez le type d'informations de cache de détection du voisinage.
  - *Statique* : entrées de cache de détection du voisinage statiques.
  - *Dynamique* : entrées de cache de détection du voisinage dynamiques.

ÉTAPE 4 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

Affichage des tables de routage IPv6

La *rubrique Table de routage IPv6* affiche la table des routes IPv6. La table contient une seule route par défaut (adresse IPv6 ::0), qui utilise le routeur par défaut sélectionné dans la liste des routeurs par défaut IPv6 afin d'envoyer des paquets aux périphériques de destination qui ne font pas partie du même sous-réseau IPv6 que le 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 en mode Layer 2, cliquez sur **Administration** > **Interface de gestion** > **Routes IPv6**. En mode Layer 3, cliquez sur **Configuration IP** > **Interfaces de gestion et IP** > **Routes IPv6**.

La *rubrique Table de routage 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 servant à 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.
- **Mesure** : 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 au cours duquel 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* : adresse IPv6 configurée manuellement pour le commutateur.
  - *Dynamique* : la destination est rattachée à l'adresse du sous-réseau IPv6 de façon indirecte. Cette entrée a été obtenue de manière dynamique via le protocole ICMP.

Définition du routage statique IPv4

Lorsque le commutateur fonctionne en mode Layer 3, cette page vous permet de configurer et d'activer des routes IPv4 statiques sur le commutateur. Lors du routage du trafic, le saut suivant est déterminé à l'aide de l'algorithme LPM (Longest Prefix Match, correspondance avec le préfixe le plus long). L'adresse IPv4 d'une destination peut correspondre à plusieurs routes dans la table des routes IPv4 statiques. Le commutateur utilise la route qui correspond au masque de sous-réseau le plus élevé, c'est-à-dire au préfixe le plus long.

Pour définir une route IP statique :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Routes statiques IPv4**.

La *rubrique Routes statiques IP* s'ouvre.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une route statique* s'ouvre.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **Préfixe IP de destination** : saisissez le préfixe d'adresse IP de la destination.
- **Masque** : sélectionnez et saisissez des informations dans l'un des champs suivants :
  - **Masque réseau** : préfixe de route IP pour l'adresse IP de destination.

- **Longueur du préfixe** : préfixe de route IP pour l'adresse IP de destination.

- **Adresse IP du routeur de saut suivant** : saisissez l'adresse ou l'alias IP du saut suivant sur la route.

  REMARQUE Vous ne pouvez pas configurer de route statique via un sous-réseau IP à connexion directe dans lequel le commutateur obtient son adresse IP d'un serveur DHCP.

- **Type de route** : sélectionnez le type de route approprié.

  - *Rejeter* : rejette la route indiquée et stoppe tout routage vers le réseau de destination, sur toutes les passerelles. Cela garantit l'élimination de toutes les trames qui arrivent avec l'IP de destination de cette route.

  - *Distant* : indique que la route est située sur un chemin distant.

- **Mesure** : Saisissez la distance administrative jusqu'au saut suivant. La plage valide est 1–255.

ÉTAPE 4 Cliquez sur **Appliquer**. La route IP statique est ajoutée et le commutateur est mis à jour.

Activation du proxy ARP

La technique de proxy ARP est utilisée par un périphérique situé sur un sous-réseau IP donné pour répondre aux requêtes ARP qui concernent une adresse située hors de ce réseau.

Le proxy ARP reconnaît la destination du trafic et répond en suggérant une autre adresse MAC. Le proxy ARP sert en pratique à rediriger le trafic LAN de l'hôte de destination vers un autre. Le trafic capturé est alors généralement routé par le proxy vers la destination prévue via une autre interface ou à l'aide d'un tunnel.

Ce processus (une requête ARP demande une adresse IP différente, en vue du proxy, déclenchant une réponse de la part du nœud qui envoie sa propre adresse MAC) est parfois appelé publication.

Cette page vous permet de configurer l'état de la fonction de proxy ARP. Une fois que vous l'avez activée sur cette page, elle est activée pour toutes les interfaces IP.

Pour activer le proxy ARP sur le commutateur :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Proxy ARP**.

La *rubrique Proxy ARP* s'ouvre.

ÉTAPE 2 Sélectionnez **Proxy ARP** pour permettre au commutateur de répondre aux requêtes ARP concernant des nœuds distants avec l'adresse MAC du commutateur.

ÉTAPE 3 Cliquez sur **Appliquer**. Le proxy ARP est activé et le commutateur est mis à jour.

Définition du relais UDP

La fonction de relais UDP n'est disponible que lorsque le commutateur fonctionne en mode Layer 3. En général, les commutateurs ne routent pas les paquets de diffusion IP d'un sous-réseau IP à un autre. Toutefois, si vous le configurez à cet effet, le commutateur peut relayer des paquets de diffusion UDP spécifiques reçus de ses interfaces IPv4 vers des adresses IP de destination particulières.

Pour configurer le relais des paquets UDP reçus d'une interface IPv4 donnée vers un port UDP de destination particulier, ajoutez un relais UDP :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Relais UDP**. La *rubrique Relais UDP* s'ouvre.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un relais UDP* s'ouvre.

ÉTAPE 3 Sélectionnez l'**interface IP source** vers laquelle le commutateur doit relayer les paquets de diffusion UDP sur la base du port UDP de destination configuré. L'interface choisie doit être l'une des interfaces IPv4 configurées sur le commutateur.

ÉTAPE 4 Saisissez le numéro du **port UDP de destination** des paquets que le commutateur doit relayer. La plage valide est 1-65535.

ÉTAPE 5 Saisissez l'**adresse IP de destination** qui doit recevoir les paquets UDP relayés. Si ce champ contient 0.0.0.0, les paquets UDP sont éliminés. Si ce champ contient 255.255.255.255, des paquets UDP sont envoyés à toutes les interfaces IP.

ÉTAPE 6 Cliquez sur **Appliquer**. Les paramètres de relais UDP sont définis et le commutateur est mis à jour.

Relais DHCP

Le commutateur peut agir en tant qu'agent de relais DHCP, qui écoute les messages DHCP et les relaie entre serveurs et clients DHCP résidant sur des sous-réseaux IP ou des VLAN distincts.

Description du relais DHCP

Vous devez activer le relais DHCP à la fois globalement et pour chaque VLAN.

En mode Layer 2, le commutateur peut relayer les messages DHCP reçus d'un VLAN vers un ou plusieurs serveurs DHCP configurés. Lorsque le relais DHCP reçoit un message DHCP d'une station de travail, il ajoute l'option 82 à la trame pour mémoriser le VLAN et le port d'entrée. Lorsqu'un serveur DHCP répond, la fonction supprime l'option 82 de la trame et utilise cette option pour déterminer l'endroit où la station de travail est connectée. Dans ce mode, le relais DHCP élimine toutes les trames DHCP reçues des stations de travail contenant déjà l'option 82.

En mode Layer 3, le commutateur peut relayer les messages DHCP reçus de ses interfaces IPv4 vers un ou plusieurs serveurs DHCP configurés. Le commutateur insère l'adresse IPv4 dans le paramètre giaddr du message avant de le relayer vers les serveurs. Il utilise l'adresse IPv4 de commutateur de l'interface qui reçoit le message. Le commutateur emploie la valeur giaddr figurant dans la réponse pour déterminer comment transférer la réponse au client DHCP.

Limites du relais DHCP

En mode Layer 2, le commutateur insère sa propre option 82 DHCP, ainsi que des informations sur le VLAN et le port d'entrée, dans le message DHCP qu'il reçoit des clients DHCP. C'est pourquoi les serveurs DHCP doivent prendre en charge l'option 82 DHCP. Le commutateur élimine les messages DHCP contenant l'option 82 qu'il reçoit des clients DHCP.

En mode Layer 3, cette fonction ne peut être activée que sur les interfaces IPv4.

Définition des propriétés du relais DHCP

La *rubrique Propriétés* vous permet de configurer l'état du relais DHCP sur le commutateur ainsi que les adresses IP du serveur DHCP vers lequel les messages DHCP sont relayés.

Pour utiliser cette fonction, vous devez activer le relais DHCP sur l'interface d'entrée où les messages DHCP doivent être relayés. Cette opération peut être effectuée à partir de la *rubrique Interfaces de relais DHCP*.

L'option 82 insère des informations supplémentaires dans les paquets envoyés depuis l'hôte. Le serveur DHCP transmet les informations de configuration à des hôtes sur un réseau TCP/IP. Cela permet au serveur DHCP de limiter l'allocation d'adresses aux hôtes autorisés. Vous ne pouvez activer DHCP avec option 82 que si le relais DHCP est activé.

Pour configurer la fonction relais DHCP :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Relais DHCP** > **Propriétés**. La *rubrique Propriétés* s'ouvre.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **Relais DHCP** : sélectionnez cette option pour activer/désactiver le relais DHCP.
- **Option 82** : sélectionnez Option 82 pour activer l'insertion de l'adresse MAC du périphérique et des paramètres d'entrée dans les paquets dans le but d'identifier le périphérique. Vous ne pouvez configurer cette option qu'en mode Layer 3.
- **Table des serveurs DHCP** : affiche la liste des serveurs DHCP.

ÉTAPE 3 Cliquez sur **Ajouter** pour entrer l'adresse IP du serveur DHCP. La *rubrique Ajouter propriétés DHCP* s'ouvre.

ÉTAPE 4 Saisissez la valeur du champ suivant :

- **Version IP** : indique que seul IPv4 est pris en charge.
- **Adresse IP du serveur DHCP** : saisissez l'adresse IP du serveur DHCP.

ÉTAPE 5 Cliquez sur **Appliquer**. Le serveur DHCP est défini et le commutateur mis à jour.

Utilisez la *rubrique Interfaces de relais DHCP* pour configurer les interfaces qui prennent le relais DHCP en charge.

Définition des interfaces de relais DHCP

Cette page vous permet de configurer les interfaces de port, LAG ou VLAN qui prennent en charge les fonctions de relais DHCP. Pour que le relais DHCP fonctionne, vous devez également l'activer globalement dans la *rubrique Propriétés*.

Pour définir les interfaces de relais DHCP :

ÉTAPE 1 Cliquez sur **Configuration IP > Relais DHCP > Interfaces de relais DHCP**. La *rubrique Interfaces de relais DHCP* s'ouvre.

Cette page affiche l'interface où le relais DHCP est défini, ainsi que l'adresse IP. En mode Layer 3, les options incluent des ports, des LAG ou des VLAN ; en mode Layer 2, seuls les VLAN sont disponibles.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une interface DHCP (Layer 2)* s'ouvre.

ÉTAPE 3 Saisissez la valeur d'**interface**.

- Si le commutateur fonctionne en mode Layer 2, sélectionnez le VLAN où le relais DHCP doit être activé.
- Si le commutateur fonctionne en mode Layer 3, sélectionnez le type d'interface (port, VLAN ou LAG).

ÉTAPE 4 Cliquez sur **Appliquer**. L'interface de relais DHCP est définie et le commutateur est mis à jour.

Configuration d'ARP

Le commutateur gère une table ARP (Address Resolution Protocol, protocole de résolution d'adresse) pour tous les périphériques connus résidant sur ses sous-réseaux IP à connexion directe. Un sous-réseau IP à connexion directe désigne un sous-réseau sur lequel 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.

La *rubrique Table ARP* vous permet de consulter les entrées ARP dynamiques apprises par le commutateur, de modifier la durée de vie d'une entrée ARP, d'effacer des entrées ARP et d'ajouter ou de supprimer des entrées ARP statiques.

REMARQUE En mode Layer 2, les informations de mappage adresse IP-adresse MAC de la table ARP servent à transférer le trafic provenant du commutateur. En mode Layer 3, les informations de mappage servent au routage Layer 3 et au transfert du trafic généré.

Pour définir les tables ARP :

ÉTAPE 1 Cliquez sur **Configuration IP** > **ARP**. La *rubrique Table ARP* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **Délai d'expiration des entrées ARP** : saisissez le nombre de secondes de conservation des adresses dynamiques 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. À la fin de cette durée de vie, l'adresse dynamique concernée 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 d'entrée 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* : les adresses dynamiques sont supprimées en fonction de la durée de vie configurée pour les entrées ARP.

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 3 Cliquez sur **Appliquer.** Les paramètres ARP globaux sont modifiés et le commutateur est mis à jour.

ÉTAPE 4 Cliquez sur **Ajouter**. La *rubrique Ajouter entrées ARP (Layer 3)* s'ouvre.

ÉTAPE 5 Saisissez les paramètres.

- **Version IP** : format d'adresse IP pris en charge par l'hôte. Seul IPv4 est pris en charge.
- **Interface** : interface IPv4 du commutateur.
  - Pour les périphériques en mode Layer 2, il existe un seul sous-réseau IP à connexion directe, toujours situé sur le VLAN de gestion. Toutes les adresses statiques et dynamiques de la table ARP résident sur le VLAN de gestion.
  - Pour les périphériques en mode Layer 3, vous pouvez configurer une interface IPv4 sur un port, un LAG ou un VLAN. Sélectionnez l'interface voulue dans la liste des interfaces IPv4 configurées sur le commutateur.
- **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 définie et le commutateur est mis à jour.

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

La *rubrique Serveur DNS* vous permet de configurer les serveurs DNS ainsi que le domaine par défaut que le commutateur utilise.

Pour configurer des serveurs DNS :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Système de noms de domaine** > **Serveurs DNS**. La *rubrique Serveur DNS* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **DNS** : sélectionnez cette option pour activer le commutateur en tant que client DNS et lui permettre de traduire 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 (1–158 caractères). Le commutateur ajoute cette information à tous les noms de domaine non entièrement qualifiés, les transformant ainsi en noms de domaine entièrement qualifiés (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 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** : indique le serveur DNS actif. 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 **Ajouter**. La *rubrique Ajouter un serveur DNS* s'ouvre.

ÉTAPE 4 Saisissez les paramètres.

- **Version IP** : sélectionnez Version 6 pour IPv6 ou Version 4 pour IPv4.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options disponibles sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière unique l'hôte situé sur une seule liaison réseau. Une adresse locale de liaison possède le préfixe **FE80**, ne peut être routée et peut servir à la communication que

sur le réseau local. Une seule adresse locale de liaison est prise en charge. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplace l'adresse dans la configuration.

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

- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, sélectionnez si la réception s'effectue via VLAN2 ou ISATAP.
- **Adresse IP du serveur DNS** : saisissez l'adresse IP du serveur DNS.
- **État du serveur DNS - Actif** : sélectionnez cette option pour activer le nouveau serveur DNS.

ÉTAPE 5 Cliquez sur **Appliquer**. Le serveur DNS est ajouté et le commutateur est mis à jour.

Mappage d'hôtes DNS

Le commutateur enregistre dans le 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 une vérification de ces entrées statiques, suivie d'une recherche dans le cache DNS local et se termine par l'envoi de demandes au serveur DNS externe.

La *rubrique Mappage d'hôtes* vous permet de configurer des mappages statiques entre noms d'hôte DNS et adresses IP.

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 *rubrique Mappage d'hôtes* s'ouvre.

Cette page contient les champs suivants :

- **Nom d'hôte** : nom de domaine défini par l'utilisateur, maximum 158 caractères.
- **Adresse IP** : adresse IP correspondant au nom d'hôte.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique 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 de manière unique l'hôte situé sur une seule liaison réseau. 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 prise en charge. S'il existe une adresse locale de liaison sur l'interface, cette entrée remplace l'adresse dans la configuration.
  - *Globale* : l'adresse IPv6 est de type IPV6 monodiffusion globale, visible et joignable depuis d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, sélectionnez si la réception s'effectue via VLAN2 ou ISATAP.
- **Nom d'hôte** : saisissez un nom de domaine, maximum 158 caractères.
- **Adresse IP** : saisissez une adresse IPv4 ou jusqu'à quatre adresses IPv6 pour l'hôte. Les adresses 2 à 4 sont des adresses de secours.

ÉTAPE 4 Cliquez sur **Appliquer**. L'hôte DNS est ajouté et le commutateur mis à jour.

16

Configuration de la sécurité

Ce chapitre décrit différents aspects de la sécurité et du contrôle d'accès. Le système gère différents types de sécurité. 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. Cette liste présente les différents types de fonctions de sécurité décrits dans ce chapitre :

L'autorisation d'administrer le commutateur est détaillée dans les sections suivantes :

- **Définition d'utilisateurs**
- **Configuration de TACACS+**
- **Configuration des paramètres RADIUS**
- **Authentification de l'accès de gestion**
- **Profils d'accès**
- **Configuration des services TCP/UDP**

La protection contre les attaques dirigées vers le CPU du commutateur est détaillée dans les sections suivantes :

- **Configuration des services TCP/UDP**
- **Définition du contrôle des tempêtes**

Le contrôle d'accès des utilisateurs finaux au réseau via le commutateur est détaillé dans les sections suivantes :

- **Authentification de l'accès de gestion**
- **Profils d'accès**
- **Définition d'utilisateurs**
- **Configuration de TACACS+**
- **Configuration des paramètres RADIUS**

- Configuration de la sécurité des ports
- 802.1X

La protection contre d'autres utilisateurs du réseau est détaillée dans les sections suivantes. Il s'agit d'attaques qui transitent par le commutateur, mais qui ne sont pas dirigées vers ce dernier.

- Prévention du déni de service
- Configuration des services TCP/UDP
- Définition du contrôle des tempêtes
- Configuration de la sécurité des ports

Définition d'utilisateurs

Dans ce contexte, un utilisateur est un administrateur système ou un super-utilisateur qui gère le commutateur.

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 êtes invité à entrer un nouveau mot de passe.

Définition de comptes d'utilisateurs

La *rubrique Comptes d'utilisateurs* permet d'entrer des utilisateurs supplémentaires autorisés à gérer le commutateur ou à modifier les mots de passe d'utilisateurs existants.

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 *rubrique Comptes d'utilisateurs* s'affiche.

Cette page affiche les utilisateurs définis dans le système.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un nouvel utilisateur ou sur **Modifier** pour en modifier un. La *rubrique Ajouter (ou Modifier) le compte d'utilisateur* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Nom d'utilisateur** : saisissez un nouveau nom d'utilisateur.
- **Mot de passe** : saisissez un mot de passe. Si la robustesse et la complexité du mot de passe sont définies, le mot de passe doit se conformer à ces directives. Cette configuration est présentée dans la section **Définition de règles de complexité des mots de passe**.
- **Confirmer le mot de passe** : saisissez à nouveau fois le mot de passe.
- **Mesure de la robustesse du mot de passe** : affiche le niveau de robustesse du mot de passe. La stratégie de robustesse et de complexité du mot de passe est configurée dans la *rubrique Robustesse du mot de passe*.

ÉTAPE 4 Cliquez sur **Appliquer**. L'utilisateur est ajouté et le commutateur mis à jour.

Définition de règles de complexité des mots de passe

Les mots de passe sont utilisés pour authentifier les utilisateurs accédant au commutateur. La gestion des mots de passe comprend la définition des règles générales de complexité des mots de passe et les mots de passe spécifiques aux utilisateurs. La longueur minimale du mot de passe, le nombre de classes de caractères et l'exigence de créer un nouveau mot de passe différent de l'ancien représentent différents aspects de la complexité des mots de passe.

La *rubrique Robustesse du mot de passe* permet de définir la complexité des mots de passe, ainsi que la durée pendant laquelle le mot de passe est valide.

Pour définir les règles de complexité des mots de passe :

ÉTAPE 1 Cliquez sur **Sécurité** > **Robustesse du mot de passe**. La *rubrique Robustesse du mot de passe* s'affiche.

ÉTAPE 2 Sélectionnez **Activer Paramètres de complexité du mot de passe** pour appliquer des règles de complexité minimales aux mots de passe.

ÉTAPE 3 Saisissez les paramètres.

- **Longueur minimale du mot de passe** : saisissez le nombre minimum de caractères requis pour les mots de passe.
- **Nombre minimum de classes de caractères** : saisissez le nombre minimum de classes de caractères dont doit se composer un mot de passe : caractères minuscules (1), majuscules (2), numériques (3) ou spéciaux (4).

- **Le nouveau mot de passe doit être différent de l'actuel** : si cette option est sélectionnée, le nouveau mot de passe ne pourra pas être identique au mot de passe actuel.
- **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) au bout de laquelle l'utilisateur devra modifier le mot de passe. La valeur par défaut est de 180 jours.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres du mot de passe sont définis et le commutateur est mis à jour.

Configuration de TACACS+

Le commutateur est un client TACACS+ *(Terminal Access Controller Access Control System)* qui s'appuie sur un serveur TACACS+ afin de fournir une sécurité centralisée en autorisant et en authentifiant les utilisateurs qui essaient d'accéder au commutateur et de l'administrer.

TACACS+ fournit les services suivants :

- **Authentification** : assure l'authentification des administrateurs se connectant au commutateur en utilisant des noms d'utilisateur et des mots de passe définis par l'utilisateur.
- **Autorisation** : effectuée au moment de la connexion. Une fois la session d'authentification terminée, une session d'autorisation commence en utilisant le nom d'utilisateur authentifié. Le serveur TACACS+ vérifie ensuite les privilèges de l'utilisateur.

Le protocole TACACS+ garantit l'intégrité du réseau, via des échanges de protocoles cryptés entre l'appareil et le serveur TACACS+.

TACACS+ est uniquement pris en charge sur IPv4.

Les serveurs TACACS+ ne peuvent pas être utilisés en tant que serveurs d'authentification 802.1X pour vérifier les informations des utilisateurs réseau cherchant à se connecter aux réseaux via le commutateur.

Certains serveurs TACACS+ prennent en charge une connexion unique qui permet à l'appareil de recevoir toutes les informations sur une même connexion. Si le serveur TACACS+ ne prend pas cette fonction en charge, l'appareil rétablit les connexions multiples.

Configuration des paramètres TACACS+ par défaut

La *rubrique TACACS+* permet d'ajouter, de supprimer et de modifier les serveurs TACACS+. Vous pouvez définir les paramètres par défaut, par exemple la chaîne de clé utilisée pour crypter les communications avec le serveur TACACS+. Un utilisateur doit être configuré sur le serveur TACACS+ avec un niveau de privilège 15 pour se voir accorder l'autorisation d'administrer le commutateur.

Pour définir un serveur TACACS+ et des paramètres d'authentification par défaut pour ce serveur :

ÉTAPE 1 Cliquez sur **Sécurité** > **TACACS+**. La *rubrique TACACS+* s'affiche.

La Table des serveurs TACACS+ affiche les paramètres par défaut et les serveurs TACACS+ précédemment définis.

ÉTAPE 2 Saisissez la **Chaîne de clé** par défaut. Il s'agit de la clé d'authentification et de cryptage utilisée pour communiquer avec les serveurs TACACS+. Le commutateur peut être configuré de façon à utiliser cette clé ou à utiliser une clé pour un serveur individuel (procédure décrite dans la section **Ajout d'un serveur TACACS+**). Si vous n'saisissez pas de chaîne de clé dans ce champ, la clé du serveur individuel devra correspondre à la clé de cryptage utilisée par le serveur TACACS+. Si vous saisissez une chaîne de clé dans ce champ ainsi qu'une chaîne de clé pour un serveur TACACS+ individuel, la chaîne de clé configurée pour le serveur TACACS+ individuel sera prioritaire.

ÉTAPE 3 Dans le champ **Délai de réponse**, saisissez la durée qui s'écoule avant l'expiration de la connexion entre le commutateur et le serveur TACACS+. Si aucune valeur n'est indiquée dans la *rubrique Ajouter un serveur TACACS+* d'un serveur spécifique, la valeur de ce champ sera utilisée.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres TACACS+ et le commutateur sont mis à jour.

Ajout d'un serveur TACACS+

ÉTAPE 1 Cliquez sur **Sécurité** > **TACACS+**. La *rubrique TACACS+* s'affiche.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un serveur TACACS+* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Adresse IP du serveur** : saisissez l'adresse IP du serveur TACACS+.
- **Priorité** : saisissez le niveau de priorité de ce serveur, qui sera utilisé pour définir l'ordre d'utilisation des différents serveurs TACACS+. Zéro correspond au serveur TACACS disposant de la priorité la plus élevée : il s'agit du serveur qui sera utilisé en premier. Si le commutateur ne parvient pas à établir de session avec le serveur possédant la priorité la plus élevée, il essaiera avec le serveur disposant du niveau de priorité suivant.
- **Chaîne de clé** : saisissez la clé d'authentification et de cryptage du serveur TACACS+. La clé doit correspondre à la clé de cryptage configurée sur le serveur TACACS+. Sélectionnez **Valeurs par défaut** pour utiliser la chaîne de clé définie sous les paramètres TACACS+ par défaut.
- **Délai de réponse** : saisissez la durée qui s'écoule avant l'expiration de la connexion entre le commutateur et le serveur TACACS+. Sélectionnez **Valeurs par défaut** pour utiliser la valeur par défaut affichée sur la page.
- **Port IP d'authentification** : saisissez le numéro de port via lequel s'opère la session TACACS+. Le port 49 est utilisé par défaut.
- **Connexion unique** : sélectionnez cette option pour activer une connexion ouverte unique entre le commutateur et le serveur TACACS+.

ÉTAPE 4 Cliquez sur **Appliquer**. Le serveur TACACS+ est ajouté et le commutateur est mis à jour.

Configuration des paramètres 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 qui s'appuie sur un serveur RADIUS pour fournir une sécurité centralisée, en autorisant et en authentifiant les utilisateurs qui essaient d'accéder au commutateur et de l'administrer.

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.

Utilisez cette page pour activer la configuration des paramètres de serveur RADIUS utilisés par le commutateur pour communiquer avec les serveurs.

Pour définir les paramètres RADIUS par défaut :

ÉTAPE 1 Cliquez sur **Sécurité** > **RADIUS**. La *rubrique RADIUS* s'affiche.

La table RADIUS affiche les paramètres spécifiques de chaque serveur RADIUS défini.

ÉTAPE 2 Saisissez les paramètres RADIUS par défaut. Les valeurs entrées dans les *Paramètres par défaut* s'appliquent à tous les serveurs. Si aucune valeur n'est entrée pour un serveur spécifique, le commutateur utilise les valeurs indiquées dans ces champs.

- **Version IP** : affiche la version IP prise 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 utilisée par défaut pour l'authentification et le cryptage des attributs RADIUS communiqués entre le commutateur et le serveur RADIUS. La clé doit correspondre à celle configurée sur le serveur RADIUS. Une chaîne de clé est utilisée pour

crypter les communications à l'aide de MD5. Une clé configurée pour un serveur RADIUS individuel est prioritaire par rapport à la clé par défaut (utilisée si aucune clé n'a été fournie pour un serveur individuel).

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres RADIUS du commutateur sont mis à jour.

Ajout d'un serveur RADIUS

ÉTAPE 1 Cliquez sur **Sécurité** > **RADIUS**. La *rubrique RADIUS* s'affiche.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un serveur RADIUS* s'affiche.

Cette page comporte des champs qui doivent être renseignés individuellement pour un serveur.

ÉTAPE 3 Renseignez les champs correspondant à chaque serveur. Pour utiliser les valeurs par défaut entrées dans la *rubrique RADIUS*, sélectionnez **Valeurs par défaut**.

- **Version IP** : sélectionnez la version IP de l'adresse IP du serveur RADIUS.
- **Adresse IP du serveur** : saisissez l'adresse du serveur RADIUS.
- **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 commencera 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 attributs RADIUS communiqués entre le commutateur et le serveur RADIUS. La clé doit correspondre à celle configurée sur le serveur RADIUS individuel. Si ce champ n'est pas renseigné, 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 aucune valeur n'est entrée dans ce champ, le commutateur utilise la valeur de délai par défaut.
- **Port d'authentification** : saisissez le numéro de port UDP du serveur RADIUS pour les demandes d'authentification.
- **Port de connexion** : saisissez le numéro de port UDP du serveur RADIUS pour les demandes de connexion.

- **Nombre de tentatives** : saisissez le nombre de demandes qui seront envoyées au serveur RADIUS avant que le système considère qu'une défaillance s'est produite. Sélectionnez **Valeurs par défaut** pour utiliser 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. Sélectionnez **Valeurs par défaut** pour utiliser 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 disponibles sont les suivantes :
  - *Connexion* : le serveur RADIUS est utilisé pour authentifier les utilisateurs qui souhaitent administrer le commutateur.
  - *802.1X* : le serveur RADIUS est utilisé pour l'authentification dans le contrôle d'accès 802.1X.
  - *Tout* : le serveur RADIUS est utilisé pour authentifier l'utilisateur qui souhaite administrer le commutateur et pour l'authentification dans le contrôle d'accès 802.1X.

ÉTAPE 4 Cliquez sur **Appliquer**. Le serveur RADIUS est ajouté et le commutateur est mis à jour.

Authentification de l'accès de gestion

Vous pouvez affecter des méthodes d'authentification aux méthodes d'accès de gestion et notamment à SSH, console, Telnet, HTTP et HTTPS. Cette authentification peut être effectuée au niveau local ou sur un serveur externe, tel qu'un serveur TACACS+ ou RADIUS.

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 *rubrique 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.
- *TACACS+* : l'utilisateur est authentifié sur le serveur TACACS+. Vous devez avoir configuré un ou plusieurs serveurs TACACS+.
- *Aucun* : l'utilisateur est autorisé à accéder au commutateur sans avoir été authentifié.
- *Local* : le nom d'utilisateur et le mot de passe sont comparés aux données stockées sur le commutateur local. Ces paires nom d'utilisateur-mot de passe sont définies dans la *rubrique Comptes d'utilisateurs*.

  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.

Profils d'accès

L'authentification d'accès de gestion configure les méthodes d'authentification à utiliser pour authentifier et autoriser les utilisateurs à partir de différentes méthodes d'accès de gestion. Les profils d'accès de gestion limitent l'accès de gestion à partir d'interfaces et/ou de sources spécifiques.

Seuls les utilisateurs qui passent avec succès à la fois le profil d'accès actif et l'authentification d'accès de gestion se voient accorder un accès de gestion au commutateur.

Règles, filtres et éléments des profils d'accès

Les profils d'accès se composent de règles gérant l'autorisation d'accès au commutateur. Chaque profil d'accès peut se composer d'une ou de plusieurs règles. Les règles sont exécutées dans l'ordre c'est-à-dire en, 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 :
  - Telnet
  - Telnet sécurisé (SSH)
  - HTTP (Hypertext Transfer Protocol)
  - HTTP sécurisé (HTTPS)
  - Simple Network Management Protocol (SNMP, protocole simple de gestion de réseau)
  - Tous les éléments ci-dessus
- **Action** : permet d'autoriser ou de refuser l'accès à une interface ou à une adresse source.
- **Interface** : les ports, LAG ou VLAN autorisés ou non à accéder à l'utilitaire Web de configuration du commutateur.
- **Adresse IP source** : adresses ou sous-réseaux IP. L'accès aux méthodes de gestion peut différer selon les groupes d'utilisateurs. Par exemple, un groupe d'utilisateurs pourrait être en mesure d'accéder au module du commutateur uniquement via une session HTTPS tandis qu'un autre serait en mesure d'y accéder en utilisant des sessions HTTPS et Telnet.

Profil d'accès actif

La *rubrique Profils d'accès* affiche les profils d'accès et tous les profils d'accès créés par des utilisateurs. Un seul profil d'accès peut être actif sur le commutateur et toute tentative d'accès à ce dernier doit respecter les règles du profil d'accès actif.

La recherche dans le profil d'accès actif s'effectue en utilisant une méthode de première correspondance. Le commutateur cherche si le profil d'accès actif autorise de façon explicite l'accès de gestion au commutateur. 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.

Si un profil d'accès limité à la console a été activé, une connexion directe de la station de gestion au port physique de la console situé sur le commutateur constitue le seul moyen de le désactiver.

Une fois qu'un profil d'accès a été défini, des règles supplémentaires peuvent être ajoutées ou modifiées via la *rubrique Règles de profils*.

Affichage, ajout ou activation d'un profil d'accès

Pour afficher, ajouter ou sélectionner un autre profil d'accès actif :

ÉTAPE 1 Cliquez sur **Sécurité** > **Méthode d'accès de gestion** > **Profils d'accès**. La *rubrique 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.

Un message d'avertissement s'affiche si vous avez sélectionné Console uniquement. Si vous poursuivez, vous serez immédiatement déconnecté de l'utilitaire Web de configuration du commutateur et ne pourrez plus accéder au commutateur que via le port console.

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 *rubrique Ajouter un profil d'accès*. Cette page vous permet de configurer un nouveau profil ainsi qu'une règle. Accédez à la section **Définition de règles de profils** pour obtenir des instructions sur la conception d'une règle.

ÉTAPE 5 Saisissez les paramètres.

- **Nom du profil d'accès** : saisissez un nom pour votre profil d'accès. Ce nom peut comporter jusqu'à 32 caractères.
- **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 utilisateurs disposant de ce profil d'accès peuvent uniquement accéder au commutateur en utilisant la méthode de gestion sélectionnée. Les options disponibles sont les suivantes :
  - *Tout* : affecte toutes les méthodes de gestion à la règle.
  - *Telnet* : les utilisateurs demandant l'accès au commutateur et répondant aux critères du profil d'accès Telnet se voient autoriser ou refuser l'accès.
  - *Secure Telnet (SSH)* : les utilisateurs demandant l'accès au commutateur et répondant aux critères du profil d'accès SSH se voient autoriser ou refuser l'accès.
  - *HTTP* : affecte un accès HTTP à la règle. Les utilisateurs demandant l'accès au commutateur et répondant aux critères du profil d'accès HTTP se voient autoriser ou refuser l'accès.
  - *Secure HTTP (HTTPS)* : les utilisateurs demandant l'accès au commutateur et répondant aux critères du profil d'accès HTTPS se voient autoriser ou refuser l'accès.
  - *SNMP* : les utilisateurs demandant l'accès au commutateur et répondant aux critères du profil d'accès SNMP se voient autoriser ou refuser l'accès.

- **Action** : sélectionnez l'action rattachée à la règle. Les options disponibles 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 disponibles 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.
- **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 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 6 Cliquez sur **Appliquer**. Le profil d'accès est créé et le commutateur mis à jour. 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 définir des règles de profils :

ÉTAPE 1 Cliquez sur **Sécurité** > **Méthode d'accès de gestion** > **Règles de profils**. La *rubrique 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 *rubrique 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 disponibles sont les suivantes :
  - *Tout* : affecte toutes les méthodes de gestion à la règle.
  - *Telnet* : les utilisateurs demandant l'accès au commutateur et répondant aux critères du profil d'accès Telnet se voient autoriser ou refuser l'accès.

- *Secure Telnet (SSH)* : les utilisateurs demandant l'accès au commutateur et répondant aux critères du profil d'accès Telnet se voient autoriser ou refuser l'accès.
- *HTTP* : affecte un accès HTTP à la règle. Les utilisateurs demandant l'accès au commutateur et répondant aux critères du profil d'accès HTTP se voient autoriser ou refuser l'accès.
- *Secure HTTP (HTTPS)* : les utilisateurs demandant l'accès au commutateur et répondant aux critères du profil d'accès HTTPS se voient autoriser ou refuser l'accès.
- *SNMP* : les utilisateurs demandant l'accès au commutateur et répondant aux critères du profil d'accès SNMP se voient autoriser ou refuser l'accès.

- **Action** : sélectionnez **Autoriser** pour autoriser les utilisateurs qui essaient d'accéder au commutateur en utilisant la méthode d'accès configurée depuis l'interface et la source IP définies dans cette règle. Ou sélectionnez **Refuser** pour refuser l'accès.
- **S'applique à l'interface** : sélectionnez l'interface rattachée à la règle. Les options disponibles 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.
- **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 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 *rubrique Services TCP/UDP* active les services basés sur TCP ou UDP sur le commutateur, généralement pour des raisons de sécurité.

Le commutateur fournit les services TCP/UDP suivants :

- Telnet : désactivé en usine par défaut
- SSH : désactivé en usine par défaut
- HTTP : activé en usine par défaut
- HTTPS : désactivé en usine par défaut
- SNMP : désactivé en usine par défaut

Les connexions TCP actives s'affichent également dans cette fenêtre.

Pour configurer les services TCP/UDP :

ÉTAPE 1 Cliquez sur **Sécurité** > **Services TCP/UDP**. La *rubrique Services TCP/UDP* s'affiche.

ÉTAPE 2 Activez ou désactivez les services TCP/UDP sur les services affichés.

La table des services TCP affiche les informations suivantes :

- **Nom du service** : méthode d'accès de gestion via laquelle le commutateur propose le service.
- **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 du service** : méthode d'accès de gestion via laquelle le commutateur propose le service.
- **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 vers la même destination).

ÉTAPE 3 Cliquez sur **Appliquer**. Les services sont ajoutés et le commutateur est mis à jour.

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. Ainsi, une trame d'entrée se transforme en un grand nombre de trames, créant un risque de tempête.

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.

Lorsqu'un seuil (limite) est entré dans le système, le port ignore le trafic une fois ce seuil 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 *rubrique Contrôle des tempêtes* s'affiche.

Cette page affiche les paramètres de contrôle des tempêtes pour tous les ports.

Tous les champs de cette page sont décrits dans la *rubrique Modifier le contrôle des tempêtes*, à l'exception du **Seuil de débit de contrôle des tempêtes (%)**. Il affiche le pourcentage de la bande passante totale disponible pour les paquets de monodiffusion inconnue, de multidiffusion et de diffusion avant l'application du contrôle des tempêtes au niveau du port. La valeur par défaut correspond à 10 % du débit maximum du port ; elle est définie dans la *rubrique Modifier le contrôle des tempêtes*.

ÉTAPE 2 Sélectionnez un port puis cliquez sur **Modifier**. La *rubrique Modifier le contrôle des tempêtes* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Port** : 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.
- **Mode de contrôle des tempêtes** : sélectionnez l'un des modes suivants :
  - *Monodiffusion inconnue, Multidiffusion et Diffusion* : intègre l'ensemble du trafic de monodiffusion inconnue, de multidiffusion et de diffusion au sein du seuil de la bande passante.
  - *Multidiffusion et Diffusion* : intègre le trafic de diffusion et de multidiffusion 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 commutateur 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 deux 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 cette limite atteinte, le commutateur n'apprend aucune adresse supplémentaire. Dans ce mode, les adresses sont soumises à un délai d'expiration ainsi qu'à un réapprentissage.

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 Si vous souhaitez utiliser 802.1X sur un port, il doit être en mode Hôtes multiples (voir la *rubrique 802.1x, Authentification hôtes et sessions)*.

La *rubrique Sécurité des ports* affiche les paramètres de sécurité de tous les ports et LAG et permet de les modifier.

Pour configurer la sécurité des ports :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité des ports**. La *rubrique Sécurité des ports* s'affiche.

Cette page affiche, en fonction du type d'interface sélectionné, des informations pour l'ensemble des ports ou des LAG .

ÉTAPE 2 Sélectionnez une interface à modifier et cliquez sur **Modifier**. La *rubrique 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 n'est activé que 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 le verrouillage de l'interface. Les options disponibles 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.
- **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. Cette plage est comprise entre 0 et 256. 0 constitue la valeur par défaut ; elle indique que seules les adresses statiques seront activées sur l'interface.
- **Action en cas de violation** : sélectionnez l'action à appliquer aux paquets qui arrivent sur un port verrouillé. Les options disponibles 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 paquetsen 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 « traps » lorsqu'un paquet est reçu sur un port verrouillé. Ceci est approprié pour les violations de verrouillage. Pour le Verrouillage classique, ceci correspondra à toute nouvelle adresse reçue. Pour le Verrouillage dynamique limité, cela correspondra à toute nouvelle adresse qui dépassera le nombre des adresses autorisées.

- **Fréquence du/des « Trap(s) »** : saisissez la durée minimale (en secondes) qui s'écoulera entre deux « traps ».

ÉTAPE 4 Cliquez sur **Appliquer**. La sécurité des ports est modifiée et le commutateur mis à jour.

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 l'hôte et le commutateur.

802.1X est une norme IEEE relative au 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. Ce n'est qu'une fois que le demandeur est authentifié et autorisé qu'il peut envoyer des données à ce port. Dans le cas contraire, l'authentificateur ignore les données du demandeur sauf si celles-ci sont envoyées à un VLAN invité et/ou à des VLAN non authentifiés.

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** :
  - **A1** : session unique/hôte unique. Dans ce mode, le commutateur, en tant qu'authentificateur, prend en charge une session 802.1X et accorde l'autorisation d'utiliser le port au demandeur autorisé au niveau d'un port. Toute demande d'accès effectuée par les autres appareils à partir du même port est refusée jusqu'à ce que le demandeur autorisé n'utilise plus le port ou si l'accès s'effectue vers le VLAN non authentifié ou le VLAN invité.
  - Session unique / hôtes multiples : respecte la norme 802.1X. Dans ce mode, le commutateur, en tant qu'authentificateur, autorise tout appareil à utiliser un port tant que l'autorisation a été accordée à un demandeur au niveau du port.
- **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. Il s'agit du seul mode qui prend en charge l'affectation dynamique de VLAN (ADV).

Affectation dynamique de VLAN (ADV)

L'affectation dynamique de VLAN (ADV) est également appelée affectation de VLAN RADIUS dans ce guide. Lorsqu'un port est en mode Sessions multiples et compatible ADV, le commutateur ajoute automatiquement le port en tant que membre non marqué du VLAN affecté par le serveur RADIUS lors du processus d'authentification. Le commutateur classe les paquets non marqués vers le VLAN affecté si ces paquets proviennent des appareils ou ports authentifiés et autorisés.

Pour qu'un appareil soit authentifié et autorisé sur un port compatible ADV :

- Le serveur RADIUS doit authentifier l'appareil et lui affecter de façon dynamique un VLAN.
- Le VLAN affecté ne doit pas correspondre au VLAN par défaut et doit avoir été créé au niveau du commutateur.
- Le commutateur ne doit pas être configuré pour utiliser à la fois une ADV et un groupe VLAN basé sur MAC.
- Un serveur RADIUS doit prendre en charge l'ADV avec les attributs RADIUS tunnel-type (64) = VLAN (13), tunnel-media-type (65) = 802 (6) et tunnel-private-group-id = un ID VLAN.

Méthodes d'authentification

Les méthodes d'authentification peuvent être :

- 802.1X : le commutateur prend en charge le mécanisme d'authentification tel que décrit dans la norme pour authentifier et autoriser les demandeurs 802.1X.
- Basées sur MAC : le commutateur peut être configuré pour utiliser ce mode afin d'authentifier et d'autoriser les appareils qui ne prennent pas en charge la norme 802.1X. Le commutateur émule le rôle du demandeur de la part des appareils non compatibles 802.1X et utilise l'adresse MAC des appareils en tant que nom d'utilisateur et mot de passe lors de la communication avec les serveurs RADIUS. Les adresses MAC du nom d'utilisateur et du mot de passe doivent être saisies en minuscules et ne comporter aucun caractère de délimitation (par exemple : aaccbb55ccff). Pour utiliser l'authentification basée sur MAC au niveau d'un port :
  - Un VLAN invité doit être défini.
  - Le port doit être compatible avec le VLAN invité.
  - Les paquets du premier demandeur sur le port avant l'obtention de l'autorisation doivent être non marqués.

Vous pouvez configurer un port pour qu'il utilise l'authentification 802.1X, basée sur MAC ou 802.1X et basée sur MAC. Si un port est configuré pour utiliser à la fois l'authentification 802.1X et l'authentification basée sur MAC, le demandeur 802.1X est prioritaire par rapport aux appareils non compatibles avec la norme 802.1X. Le demandeur 802.1X devance un appareil autorisé mais non compatible 802.1X sur un port configuré avec une session unique.

VLAN non authentifiés et le VLAN invité

Les VLAN non authentifiés et le VLAN invité fournissent l'accès aux services qui ne nécessitent pas que les ports ou appareils d'abonnement disposent d'une authentification et d'une autorisation basées sur MAC ou 802.1X.

Un VLAN non authentifié est un VLAN qui autorise l'accès via des appareils ou ports autorisés et non autorisés. Vous pouvez configurer un ou plusieurs VLAN pour qu'ils soient non authentifiés en suivant les instructions présentées dans la section **Création de VLAN** du chapitre **Configuration de la sécurité**. Un VLAN non authentifié est doté des caractéristiques suivantes :

- Il doit s'agir d'un VLAN statique ; il ne peut correspondre au VLAN invité ni au VLAN par défaut.
- Les ports membres doivent être configurés manuellement en tant que membres marqués.

- Les ports membres doivent être des ports réseau et/ou généraux. Un port d'accès ne peut pas être membre d'un VLAN non authentifié.

Le VLAN invité, s'il est configuré, est un VLAN statique doté des caractéristiques suivantes :

- Il doit être défini manuellement à partir d'un VLAN statique existant.
- Il est automatiquement disponible, mais uniquement pour les ports d'appareils ou appareils non autorisés qui sont connectés et sur lesquels le VLAN invité est activé.
- Si le VLAN invité est activé sur un port, le commutateur ajoute automatiquement ce dernier en tant que membre non marqué du VLAN invité lorsque le port n'est pas autorisé et supprime le port du VLAN invité lorsque le premier demandeur du port est autorisé.
- Le VLAN invité ne peut être utilisé en tant que VLAN voix ni en tant que VLAN non authentifié.

Le commutateur utilise également le VLAN invité pour le processus d'authentification sur les ports configurés avec le mode Sessions multiples et l'authentification basée sur MAC. Vous devez donc configurer un VLAN invité avant de pouvoir utiliser le mode d'authentification MAC.

Flux de travail des paramètres 802.1X

Flux de travail des paramètres 802.1X

Définissez les paramètres 802.1X comme suit :

1. Définissez une ou plusieurs périodes depuis la *rubrique Période* utilisée dans la *rubrique Modifier l'authentification des ports. Cette étape est facultative.*
2. Définissez un ou plusieurs VLAN statiques en tant que VLAN non authentifiés, tel que décrit dans 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. *Cette étape est facultative.*
3. Définissez les paramètres 802.1X pour chaque port depuis la *rubrique Modifier l'authentification des ports*. Notez les éléments suivants :
   a. Sur cette page, l'ADV peut être activée sur un port en sélectionnant le champ Affectation VLAN RADIUS.
   b. Vous pouvez sélectionner le champ VLAN invité pour que les trames entrantes non marquées soient dirigées vers le VLAN invité.

4. Définissez les paramètres d'authentification des hôtes pour chaque port depuis la *rubrique Port d'authentification*.
5. Affichez l'historique d'authentification 802.1X à partir de la *rubrique Hôtes authentifiés*.

Définition des propriétés 802.1X

La *rubrique Propriétés 802.1x* permet d'activer 802.1X globalement. 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 *rubrique Propriétés 802.1x* s'affiche.

ÉTAPE 2 Saisissez les paramètres.

- **Authentification basée sur les ports** : permet d'activer ou de désactiver l'authentification 802.1X basée sur les ports.
- **Méthode d'authentification** : sélectionnez les méthodes d'authentification des utilisateurs. Les options disponibles 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 réalisée, la session n'est pas autorisée.
  - *Aucune* : n'authentifie pas l'utilisateur. Autorise la session.
- **VLAN invité** : sélectionnez cette option pour permettre l'utilisation d'un VLAN invité pour les ports non autorisés. Si un VLAN invité est activé, tous les ports non autorisés se connectent automatiquement au VLAN sélectionné dans le champ *ID du VLAN invité*. Si un port est par la suite autorisé, il est supprimé du VLAN invité.
- **ID du VLAN invité** : sélectionnez le VLAN invité dans la liste des VLAN.

- **Délai d'expiration VLAN invité** : définissez une période :
  - Une fois la connexion établie, si le logiciel ne détecte pas le demandeur 802.1X ou si l'authentification a échoué, le port est ajouté au VLAN invité, uniquement une fois le *Délai d'expiration VLAN invité* atteint.
  - Si l'état du port passe d'*Autorisé* à *Non autorisé*, le port est ajouté au VLAN invité, uniquement une fois le délai d'expiration du *VLAN invité* atteint.

La Table d'authentification des VLAN affiche tous les VLAN et indique si l'authentification a été activée sur chacun d'eux.

ÉTAPE 3 Cliquez sur **Appliquer**. Les propriétés 802.1X sont modifiées et le commutateur est mis à jour.

Configuration de VLAN non authentifiés

Configuration de VLAN non authentifiés

Lorsqu'un port est compatible 802.1X, les ports ou appareils non autorisés ne peuvent accéder à un VLAN que si ce dernier est un VLAN invité ou un VLAN non authentifié. Vous pouvez transformer un VLAN statique en un VLAN non authentifié en suivant la procédure décrite dans la section **Définition des propriétés 802.1X** en permettant aux appareils ou ports autorisés et non autorisés pour 802.1X d'envoyer ou de recevoir des paquets à ou depuis des VLAN non authentifiés. Vous devez ajouter manuellement l'appartenance VLAN des ports via la rubrique Port vers VLAN.

ÉTAPE 1 Cliquez sur **Sécurité** > **802.1X** > **Propriétés**. La *rubrique Propriétés 802.1x* s'affiche.

ÉTAPE 2 Sélectionnez un VLAN et cliquez sur **Modifier**. La *rubrique Modifier l'authentification VLAN* s'affiche.

ÉTAPE 3 Sélectionnez un VLAN.

ÉTAPE 4 Vous pouvez également décocher **Authentification** pour faire du VLAN un VLAN non authentifié.

ÉTAPE 5 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

Définition de l'authentification des ports 802.1X

La *rubrique Port d'authentification* permet la configuration de plusieurs des paramètres 802.1X pour chaque port. Une partie des modifications de configuration, parmi lesquelles la méthode d'authentification, n'est possible que si le port est en *Autorisation forcée*. Nous vous recommandons donc de passer le contrôle de port sur *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 *rubrique Port d'authentification* s'affiche.

Cette page affiche les paramètres d'authentification de tous les ports.

Modification des paramètres d'authentification des ports 802.1X

ÉTAPE 1 Cliquez sur **Sécurité** > **802.1X** > **Authentification des ports**. La *rubrique Port d'authentification* s'affiche.

ÉTAPE 2 Sélectionnez un port puis cliquez sur **Modifier**. La *rubrique Modifier l'authentification des ports* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Port** : 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 disponibles 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.
- **Affectation VLAN RADIUS** : sélectionnez cette option pour activer l'affectation dynamique de VLAN sur le port sélectionné. L'affectation dynamique de VLAN n'est possible que si le mode 802.1X est défini sur Sessions multiples. (Une fois l'authentification réalisée, le port se connecte au VLAN demandeur en tant que port non marqué dans ce VLAN.)

ASTUCE Pour que la fonctionnalité d'affectation dynamique de VLAN fonctionne, le commutateur a besoin que le serveur RADIUS envoie les attributs suivants (tel que défini dans la RFC 3580) :

[64] Tunnel-Type = VLAN (type 13)

[65] Tunnel-Medium-Type = 802 (type 6)

[81] Tunnel-Private-Group-Id = ID VLAN

- **VLAN invité** : sélectionnez cette option pour indiquer que l'utilisation d'un VLAN invité précédemment défini est activée pour le commutateur. Les options disponibles sont les suivantes :
  - *Sélectionné* : permet d'utiliser un VLAN invité pour les ports non autorisés. Si un VLAN invité est activé, le port non autorisé se connecte automatiquement au VLAN sélectionné dans le champ *ID du VLAN invité* de la *rubrique Authentification des ports 802.1X*.

    Après un échec d'authentification et si le VLAN invité est activé au niveau global sur le port indiqué, le VLAN invité est automatiquement affecté aux ports non autorisés en tant que VLAN non marqué.
  - *Supprimé* : désactive le VLAN invité sur le port.

- **Méthode d'authentification** : sélectionnez la méthode d'authentification pour le port. Les options disponibles sont les suivantes :
  - *802.1X uniquement* : l'authentification 802.1X est la seule méthode d'authentification appliquée sur le port.
  - *MAC uniquement* : le port est authentifié en fonction de l'adresse MAC du demandeur. Seules huit authentifications basées sur MAC peuvent être utilisées sur le port.
  - *802.1X et MAC* : l'authentification 802.1X et l'authentification basée sur MAC sont appliquées sur le commutateur. L'authentification 802.1X est prioritaire.

  REMARQUE Pour que l'authentification MAC réussisse, le nom d'utilisateur et le mot de passe du demandeur du serveur RADIUS doivent correspondre à l'adresse MAC du demandeur. L'adresse MAC doit être en minuscules et saisie sans les séparateurs « : » ou « - », par exemple : 0020aa00bbcc.
- **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 disponibles sont les suivantes :
  - *Autorisation forcée* : l'état du port contrôlé est défini sur Autorisation forcée (le trafic est transféré).
  - *Non-autorisation forcée* : l'état du port contrôlé est défini sur Non-autorisation forcée (le trafic est abandonné).

    REMARQUE Si l'état est du port n'est pas Autorisation forcée ou 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** : affecte une limite au temps d'autorisation d'utilisation du port spécifique si 802.1X a été activé (Authentification basée sur les ports est coché).
- **Nom de période** : sélectionnez le profil qui spécifie la période.

- **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 du port sont définis et le commutateur est mis à jour.

Définition de l'authentification des hôtes et sessions

La *rubrique Authentification hôtes et sessions* permet de définir le mode de fonctionnement de 802.1X sur le port et l'action à mettre en œuvre en cas de détection d'une violation.

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 rattachés à un même port compatible 802.1X. Seul le premier hôte doit être autorisé ; le port est ensuite totalement accessible 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 un certain nombre d'hôtes spécifiques autorisés 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 *rubrique Authentification hôtes et sessions* s'affiche.

Les paramètres d'authentification 802.1X sont définis pour tous les ports. Tous les champs, à l'exception de ceux qui suivent, sont décrits dans la rubrique *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 disponibles sont les suivantes :
  - *Non autorisé* : soit le contrôle du port est en *Non-autorisation forcée* et la liaison du port est inactive soit le contrôle du port est 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.
  - *Hôte multiple (802.1X)* : le contrôle du port est en *Automatique* et le mode Hôtes multiples est activé. Au moins un client a été authentifié.
  - *Sessions multiples* : le contrôle du port est en *Automatique* et le mode Sessions multiples est activé. Au moins une session a été authentifiée.
  - *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, provenant d'un hôte dont l'adresse MAC ne correspond pas à celle du demandeur.

ÉTAPE 2 Sélectionnez un port puis cliquez sur **Modifier**. La *rubrique Modifier l'authentification hôte et session* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Port** : saisissez un numéro de port pour lequel l'authentification des hôtes est activée.

- **Authentification des hôtes** : sélectionnez un des modes décrits ci-dessus, dans *Définition de l'authentification des hôtes et sessions*.
- **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 disponibles sont les suivantes :
  - *Abandonner* : abandonne les paquets.
  - *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 « traps »** : sélectionnez cette option pour activer les « traps ».
- **Fréquence des « traps »** : définit la fréquence d'envoi des interruptions à l'hôte. Ce champ ne peut être défini que si plusieurs hôtes sont désactivés.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres sont définis et le commutateur est mis à jour.

Affichage des hôtes authentifiés

La *rubrique Hôtes authentifiés* affiche des informations détaillées sur les utilisateurs ayant été authentifiés. Ces informations incluent notamment le nom d'utilisateur ayant servi à authentifier l'utilisateur, l'adresse MAC de la station et la durée de la connexion de l'utilisateur.

Pour afficher des informations détaillées sur les utilisateurs authentifiés :

ÉTAPE 1 Cliquez sur **Sécurité** > **802.1X** > **Hôtes authentifiés**. La *rubrique Hôtes authentifiés* s'affiche.

Cette page contient les champs suivants :

- **Nom d'utilisateur** : nom des demandeurs authentifiés sur chaque port.
- **Port** : numéro du port.
- **Durée de session (JJ:HH:MM:SS)** : durée pendant laquelle le demandeur était connecté au port.

- **Méthode d'authentification** : méthode utilisée pour l'authentification de la dernière session. Les options disponibles 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.

Définition de périodes

La *rubrique Période* permet de définir la période pendant laquelle 802.1X est actif sur les ports compatibles 802.1X. Une période doit être configurée à l'aide d'heures absolues de début et de fin. Si une période se compose d'une période absolue mais d'aucune plage récurrente et qu'elle est configurée sur un port compatible 802.1X, 802.1X est actif sur le port de l'heure absolue de début jusqu'à l'heure absolue de fin.

Si une période comprend à la fois des périodes absolues et des plages récurrentes, le port n'est activé que si l'heure de début absolue et la période récurrente ont été atteintes. Le port est désactivé une fois l'une des périodes atteintes. La période récurrente est ajoutée à la période absolue depuis la *rubrique Plage récurrente*.

Si une période comprend une ou plusieurs périodes récurrentes et qu'elle est configurée sur un port compatible 802.1X, 802.1X est actif sur le port au cours de la ou des périodes définies dans la ou les plages récurrentes qui se situent également entre l'heure de début et de fin absolue de la période.

Lorsqu'un port compatible 802.1X est en dehors de sa période affectée et/ou de sa période récurrente, 802.1X est désactivé et son état équivaut à Non-autorisation forcée.

Le commutateur prend au maximum 20 périodes absolues en charge.

Toutes les spécifications horaires sont interprétées comme étant en heure locale (l'heure d'été n'a aucune incidence).

Pour garantir que les entrées de périodes prendront effet aux heures souhaitées, l'horloge logicielle doit être définie par l'utilisateur ou par le protocole SNTP. Dans le cas contraire, la période ne sera pas appliquée.

20 plages au total peuvent être définies.

Vous pouvez par exemple utiliser cette fonctionnalité si vous souhaitez limiter aux heures ouvrables l'accès des ordinateurs au réseau. En dehors de cette période, ils seront verrouillés et l'accès au reste du réseau sera bloqué.

Pour ajouter une période absolue :

ÉTAPE 1 Cliquez sur **Sécurité** > **802.1X** > **Période**. La *rubrique Période* s'affiche.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une période absolue* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Nom de période** : saisissez un nom pour la période.
- **Heure de début absolue** : définissez l'heure de début absolue :
- *Immédiat* : cliquez pour indiquer que la période commence une fois qu'elle a été créée.
- *Date* et *Heure* : sélectionnez la date et l'heure de début absolues.
- **Heure de fin absolue** : définissez l'heure de fin absolue :
- *Infini* : cliquez pour indiquer que la période ne se termine jamais.
- *Date* et *Heure* : sélectionnez la date et l'heure de fin absolues.

ÉTAPE 4 Cliquez sur **Appliquer**. La période est créée.

Définition d'une plage récurrente

La *rubrique Plage récurrente* permet de créer une plage récurrente qui peut ensuite être ajoutée à une période précédemment définie (créée dans la *rubrique Période*).

Toutes les spécifications horaires sont interprétées comme étant en heure locale (l'heure d'été n'a aucune incidence).

Pour ajouter une plage récurrente :

ÉTAPE 1 Cliquez sur **Sécurité** > **802.1X** > **Plage récurrente**. La *rubrique Plage récurrente* s'affiche.

Cette page affiche les plages récurrentes ayant été définies.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une plage récurrente* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Nom de période** : sélectionnez la période à laquelle la plage récurrente sera ajoutée.
- **Heure de début récurrente** : saisissez le jour de la semaine et l'heure auxquels la plage récurrente commence.
- **Heure de fin récurrente** : saisissez le jour de la semaine et l'heure auxquels la plage récurrente se termine.

ÉTAPE 4 Cliquez sur **Appliquer**. La plage récurrente est ajoutée à la période.

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. La prévention du déni de service élimine les paquets comportant des en-têtes ou un contenu connus pour indiquer des intentions malveillantes.

La prévention du déni de service permet aux gestionnaires de réseaux de réaliser les tâches suivantes :

- refuser les paquets qui contiennent des adresses IP réservées (*rubrique Adresses martiennes*) ;
- empêcher les connexions TCP à partir d'une interface spécifique (*rubrique Filtrage SYN*) et fixer un débit maximal pour les paquets (*rubrique Protection du débit SYN)* ;
- configurer le blocage de certains paquets ICMP (*rubrique Filtrage ICMP*) ;
- abandonner les paquets IP fragmentés provenant d'une interface spécifique (*rubrique Filtrage de fragments IP*) ;
- interdire les attaques de Distribution Stacheldraht, du cheval de Troie Invasor et du cheval de Troie Back Orifice.

Paramètres de la suite de sécurité de déni de service

La fonctionnalité Prévention du déni de service est un ensemble de règles prédéfinies qui protègent le réseau contre les attaques malveillantes. Les *rubrique Paramètres de suite de sécurité* de *Déni de service* permettent d'activer la suite de sécurité.

Les pages Déni de service permettent de filtrer le trafic. Cela permet de protéger le réseau contre un Déni de service et des attaques de type Déni de service distribué.

REMARQUE Avant d'activer la Prévention du déni de service, 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 accéder aux paramètres globaux de prévention du déni de service :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Paramètres de suite de sécurité**. La *rubrique Paramètres de suite de sécurité* s'affiche.

ÉTAPE 2 Sélectionnez **Protection contre les DoS** pour activer la fonctionnalité Prévention du déni de service.

- **Désactiver** : désactive la fonctionnalité.
- **Protection de niveau système** : interdit les attaques de Distribution Stacheldraht, du cheval de Troie Invasor et du cheval de Troie Back Orifice.
- **Protection de niveau système et de niveau interface** : interdit les attaques de type Adresse martienne, SYN, ICMP et Fragments IP.

ÉTAPE 3 Si vous sélectionnez la Protection de niveau système ou la Protection de niveau système et de niveau interface, activez une ou plusieurs des options de Protection contre les DoS suivantes :

- **Distribution Stacheldraht** : abandonne les paquets TCP dont le port TCP source est 16660.
- **Cheval de Troie Invasor** : abandonne les paquets TCP dont le port TCP de destination est 2140 et le port TCP source 1024.
- **Cheval de Troie Back Orifice** : abandonne les paquets UDP dont le port UDP de destination est 31337 et le port UDP source 1024.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres de la suite de sécurité de Prévention du déni de service sont définis et le commutateur est mis à jour.

ÉTAPE 5 Si la Protection de niveau interface est sélectionnée, cliquez sur le bouton **Modifier** approprié pour configurer la protection souhaitée.

Définition d'adresses martiennes

La *rubrique Adresses martiennes* permet de saisir les adresses qui indiquent une attaque si elles sont détectées sur le réseau.

Le commutateur prend en charge un ensemble d'adresses martiennes réservées qui sont incorrectes du point de vue du protocole IP. Les adresses martiennes réservées activées regroupent les éléments suivants :

- Les adresses définies comme étant incorrectes dans la *rubrique Adresses martiennes*.
- Certaines des adresses sont incorrectes du point de vue du protocole, par exemple les adresses de bouclage et notamment les plages suivantes :
  - **0.0.0.0/8 (à l'exception de 0.0.0.0/32 en tant qu'adresse source)** : les adresses situées dans ce bloc font référence aux hôtes source de ce réseau.
  - **127.0.0.0/8** : utilisée en tant qu'adresse de bouclage d'hôte Internet.
  - **192.0.2.0/24** : utilisée en tant que réseau de test TEST-NET dans la documentation et les exemples de codes.
  - **224.0.0.0/4 (en tant qu'adresse IP source)** : utilisée dans les affectations d'adresses de multidiffusion IPv4, anciennement connue sous le nom d'espace d'adressage de classe D.
  - **240.0.0.0/4 (à l'exception de 255.255.255.255/32 en tant qu'adresse de destination)** : plage d'adresses réservées, anciennement connue sous le nom d'espace d'adressage de classe E.

Vous pouvez également ajouter de nouvelles adresses martiennes pour la protection contre les DoS. Les paquets présentant une adresse martienne sont abandonnés.

Pour définir des adresses martiennes :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Adresses martiennes**. La *rubrique Adresses martiennes* s'affiche.

ÉTAPE 2 Sélectionnez Adresses martiennes réservées et cliquez sur **Appliquer** pour inclure les adresses martiennes réservées dans la liste Protection de niveau

système. La liste des adresses martiennes réservées s'affiche dans la Table des adresses martiennes.

ÉTAPE 3 Pour ajouter une adresse martienne, cliquez sur **Ajouter**. La *rubrique Ajouter des adresses martiennes* s'affiche.

ÉTAPE 4 Saisissez les paramètres.

- **Version IP** : indique la version IP prise en charge. À l'heure actuelle, la prise en charge n'est proposée que pour IPv4.
- **Adresse IP** : saisissez les adresses IP martiennes pour lesquelles la Prévention du déni de service est activée. Les valeurs disponibles sont les suivantes :
  - **De la liste réservée** : sélectionnez une adresse IP bien connue dans la liste réservée.
  - **Nouvelle adresse IP** : saisissez une adresse IP.
- **Masque** : saisissez le masque de l'adresse IP afin de définir la plage des adresses IP pour laquelle la Prévention du déni de service sera activée. Les valeurs disponibles sont les suivantes :
  - **Masque de réseau** : le masque de réseau est présenté dans un format décimal séparé par des points.
  - **Longueur du préfixe** : saisissez le préfixe de l'adresse IP afin de définir la plage des adresses IP pour laquelle la Prévention du déni de service sera activée.

ÉTAPE 5 Cliquez sur **Appliquer**. Les adresses martiennes sont définies et le commutateur est mis à jour.

Définition du filtrage SYN

La *rubrique Filtrage SYN* permet de filtrer les paquets TCP qui comportent un indicateur SYN et qui sont destinés à une adresse IP et/ou à un port spécifiques.

Pour définir le filtrage SYN :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Filtrage SYN**. La *rubrique Filtrage SYN* s'affiche.

Cette page affiche les filtres SYN existants.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un filtrage SYN* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez l'interface sur laquelle le filtre est défini.
- **Adresse IPv4** : saisissez l'adresse IP pour laquelle le filtre est défini ou sélectionnez *Toutes les adresses*.
- **Masque de réseau** : saisissez le masque de réseau pour lequel le filtre est activé au format d'adresse IP.
- **Port TCP** : sélectionnez le port TCP de destination filtré :
  - *Ports connus* : sélectionnez un port dans la liste.
  - *Défini par l'utilisateur* : saisissez un numéro de port.
  - *Tous les ports* : sélectionnez cette option pour indiquer que tous les ports seront filtrés.

ÉTAPE 4 Cliquez sur **Appliquer**. Le filtre SYN est défini et le commutateur est mis à jour.

Définition de la protection du débit SYN

La *rubrique Protection du débit SYN* permet de limiter au niveau du débit le nombre de paquets SYN à l'entrée. Cela limite l'incidence des attaques de déni de service, par exemple d'une saturation SYN sur des serveurs en limitant au niveau du débit le nombre de nouvelles connexions.

Pour définir la protection du débit SYN :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Protection du débit SYN**. La *rubrique Protection du débit SYN* s'affiche.

Cette page affiche la protection du débit SYN actuellement définie par interface.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une protection du débit SYN* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez l'interface à partir de laquelle la protection du débit sera définie.
- **Adresse IP** : saisissez l'adresse IP pour laquelle la protection du débit SYN est définie ou sélectionnez *Toutes les adresses*. Si vous saisissez l'adresse IP, saisissez également le masque ou la longueur du préfixe.

- **Masque de réseau** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs suivants :
  - *Masque* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau dans 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.
- **Limite du débit SYN** : saisissez le nombre des paquets SYN autorisés.

ÉTAPE 4 Cliquez sur **Appliquer**. La protection du débit SYN est définie et le commutateur est mis à jour.

Définition du filtrage ICMP

La *rubrique Filtrage ICMP* permet de bloquer les paquets ICMP provenant de certaines sources. Cela peut permettre de réduire la charge du réseau en cas d'attaque de déni de service de type saturation ICMP.

Pour définir le filtrage ICMP :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Filtrage ICMP**. La *rubrique Filtrage ICMP* s'affiche.

Cette page affiche les règles en fonction desquelles les paquets ICMP sont bloqués sur chaque interface.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un filtrage ICMP* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez l'interface sur laquelle le filtrage ICMP est défini.
- **Adresse IP** : saisissez l'adresse IPv4 pour laquelle le filtrage des paquets ICMP est activé ou sélectionnez *Tout* pour bloquer les paquets ICMP provenant de toutes les adresses source. Si vous saisissez l'adresse IP, saisissez également le masque ou la longueur du préfixe.
- **Masque de réseau** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs suivants :
  - *Masque* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau dans 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 4 Cliquez sur **Appliquer**. Le filtrage ICMP est défini et le commutateur mis à jour.

Définition du blocage IP fragmenté

La *rubrique IP fragmenté* permet de bloquer les paquets IP fragmentés.

Pour définir le blocage IP fragmenté :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Filtrage de fragments IP**. La *rubrique Filtrage de fragments IP* s'affiche.

Cette page affiche le blocage d'adresses IP fragmentées par interface.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une filtrage de fragments IP* s'affiche.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez l'interface sur laquelle la fragmentation IP est définie.
- **Adresse IP** : saisissez un réseau IP à partir duquel les paquets IP fragmentés sont filtrés ou sélectionnez **Tout** pour bloquer les paquets IP fragmentés provenant de toutes les adresses. Si vous saisissez l'adresse IP, saisissez également le masque ou la longueur du préfixe.
- **Masque de réseau** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs suivants :
  - *Masque* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau dans 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 4 Cliquez sur **Appliquer**. La fragmentation IP est définie et le commutateur mis à jour.

17

Contrôle d'accès

La fonction de liste de contrôle d'accès (ACL, Access Control List) fait partie intégrante du mécanisme de sécurité. Les définitions ACL sont un des mécanismes utilisés pour définir les flux de trafic auxquels une Qualité de service (QoS) spécifique doit être attribuée. Pour plus d'informations, consultez la section **Configuration du QoS** du chapitre **Configuration du QoS (Qualité de service)**.

Les ACL permettent aux gestionnaires de réseaux de définir des modèles (filtres et actions) pour le trafic entrant. Les paquets entrant dans le commutateur au niveau d'un port ou LAG disposant d'une ACL active sont soit acceptés, soit refusés.

Ce chapitre contient les sections suivantes :

- **Listes de contrôle d'accès**
- **Définition d'ACL basées sur MAC**
- **ACL basées sur IPv4**
- **ACL basées sur IPv6**
- **Définition d'une liaison ACL**

Listes de contrôle d'accès

Une liste de contrôle d'accès (ACL, Access Control List) est une liste ordonnée d'actions et de filtres de classification. Chaque règle de classification, englobant l'action correspondante, est appelée élément de contrôle d'accès (ACE, Access Control Element).

Chaque ACE est composé de filtres qui déterminent les groupes de trafic et les actions associées. Une seule ACL peut contenir un ou plusieurs ACE, qui sont comparés au contenu des trames entrantes. Une action DENY (REFUSER) ou PERMIT (AUTORISER) est appliquée aux trames dont le contenu correspond au filtre.

Le commutateur prend en charge un maximum de 512 ACL et de 512 ACE.

Lorsqu'un paquet correspond à un filtre ACE, l'action ACE est appliquée et le traitement de cette ACL est arrêté. Si le paquet ne correspond pas au filtre ACE, l'ACE suivant est traité. Si tous les ACE d'une ACL ont été traités sans trouver de correspondance et qu'il existe une autre ACL, celle-ci est traitée de manière similaire. Si aucune correspondance n'est trouvée sur l'ensemble des ACE de toutes les ACL appropriées, le paquet est abandonné (action par défaut). En raison de cette action d'abandon par défaut, vous devez ajouter de façon explicite dans l'ACL des ACE visant à autoriser l'ensemble du trafic, y compris le trafic de gestion, tel que telnet, HTTP ou SNMP, dirigé vers le commutateur lui-même.

Si IGMP/MLD Snooping est activé sur un port lié à une ACL, ajoutez dans cette dernière des filtres ACE pour transférer les paquets IGMP/MLD vers le commutateur. Dans le cas contraire, IGMP/MLD Snooping échouera au niveau du port.

Les ACE étant appliqués selon une méthode de première correspondance, l'ordre dans lequel ils apparaissent dans l'ACL est important. Les ACE sont traités de manière séquentielle, en commençant par le premier.

Les ACL peuvent être utilisées pour la sécurité, par exemple en autorisant ou en refusant certains flux de trafic, ainsi que pour la classification et la hiérarchisation du trafic en mode avancé de QoS.

REMARQUE Un port peut être sécurisé avec des ACL ou configuré avec une stratégie de QoS avancée ; il n'est toutefois pas possible d'employer ces deux méthodes.

Il ne peut y avoir qu'une seul ACL par port, à une exception près : il est possible d'associer à la fois une ACL basée sur IP et une ACL basée sur IPv6 à un port unique. Pour associer plusieurs ACL à un port, vous devez utiliser une stratégie comportant un ou plusieurs mappages de classe (class-map) (voir *Configuration d'une table de stratégies en mode avancé de QoS*). Les types suivants d'ACL peuvent être définis (selon la partie de l'en-tête de la trame qui est examinée) :

- ACL MAC : examine les champs de niveau 2 uniquement, comme décrit dans la section *Définition d'ACL basées sur MAC*
- ACL IP : examine le niveau 3 de trames IP, comme décrit dans la section *ACL basées sur IPv4*
- ACL IPv6 : examine le niveau 3 de trames IPv4, comme décrit dans la section *Définition d'ACL basées sur IPv6*

Si une trame correspond au filtre d'une ACL, elle est définie en tant que flux portant le nom de cette ACL. En mode avancé de QoS, il est possible de faire référence à ces trames en utilisant ce nom de flux et la QoS peut être appliquée à ces dernières (voir *Mode de QoS avancé*).

Création d'un flux de travail d'ACL

Pour créer des ACL et les associer à une interface, procédez comme suit :

1. Créez un ou plusieurs des types d'ACL suivants :
    a. ACL basée sur MAC en utilisant la *rubrique ACL basée sur MAC* et la *rubrique ACE basé sur MAC*
    b. ACL basée sur IP en utilisant la *rubrique ACL basée sur IPv4* et la *rubrique ACE basé sur IPv4*
    c. ACL basée sur IPv6 en utilisant la *rubrique ACL basée sur IPv6* et la *rubrique ACE basé sur IPv6*
2. Associez l'ACL avec les interfaces en utilisant la *rubrique Liaison ACL*.

Modification d'un flux de travail d'ACL

Vous ne pouvez modifier une ACL que si elle n'est pas en cours d'utilisation. La procédure suivante décrit la suppression de la liaison d'une ACL, préalable nécessaire à sa modification :

- Si l'ACL n'appartient pas à une « class-map » Mode avancé de QoS, mais qu'elle a été associée à une interface, supprimez sa liaison avec l'interface en utilisant la *rubrique Liaison ACL*.
- Si l'ACL fait partie de la « class-map » et qu'elle n'est pas liée à une interface, vous pouvez la modifier.
- Si l'ACL fait partie d'une « class-map » contenue dans une stratégie liée à une interface, vous devez supprimer la liaison comme suit :
    - Supprimez la liaison entre la stratégie contenant la « class-map » et l'interface en utilisant *Liaison de stratégies*.
    - Supprimez de la stratégie la « class-map » contenant l'ACL en utilisant la *Configuration d'une stratégie* (**mode édition**).
    - Supprimez la « class-map » contenant l'ACL, en utilisant *Définition d'un mappage de classe*.

Une fois ces étapes menées à bien, vous pouvez modifier l'ACL, en suivant la procédure décrite dans les sections de ce chapitre.

Définition d'ACL basées sur MAC

Les ACL basées sur MAC sont utilisées pour filtrer le trafic basé sur les champs du Layer 2 (niveau 2, couche 2). Ces ACL vérifient toutes les trames à la recherche d'une correspondance.

Les ACL basées sur MAC sont définies dans la *rubrique ACL basée sur MAC*. Leurs règles sont définies dans la *rubrique ACE basé sur MAC*.

Pour définir une ACL basée sur MAC :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACL basée sur MAC**. La *rubrique ACL basée sur MAC* s'ouvre.

Cette page affiche une liste de toutes les ACL basées sur MAC actuellement définies.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une ACL basée sur MAC* s'ouvre.

ÉTAPE 3 Saisissez le nom de la nouvelle ACL dans le champ **Nom de l'ACL**. Les noms d'ACL font la distinction entre les minuscules et les majuscules.

ÉTAPE 4 Cliquez sur **Appliquer**. L'ACL basée sur MAC est ajoutée et le commutateur mis à jour.

Ajout de règles à une ACL basée sur MAC

Pour ajouter des règles (ACE) à une ACL :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACE basé sur MAC**. La *rubrique ACE basé sur MAC* s'ouvre.

ÉTAPE 2 Sélectionnez une ACL et cliquez sur **OK**. Les ACE de l'ACL sont répertoriés.

ÉTAPE 3 Cliquez sur **Ajouter**. La *rubrique Ajouter un ACE basé sur MAC* s'ouvre.

ÉTAPE 4 Saisissez les paramètres.

- **Nom de l'ACL** : affiche le nom de l'ACL à laquelle un ACE est ajouté.
- **Priorité** : permet d'entrer la priorité de l'ACE. Les ACE disposant d'une priorité plus élevée sont traités en premier. Le 1 correspond à la priorité la plus élevée.

- **Action** : sélectionnez l'action à appliquer en cas de correspondance. Les options disponibles sont les suivantes :
  - *Autoriser* : transfère les paquets qui répondent aux critères de l'ACE.
  - *Refuser* : abandonne les paquets qui répondent aux critères de l'ACE.
  - *Arrêter* : abandonne les paquets qui répondent aux critères de l'ACE et désactive le port à partir duquel les paquets ont été reçus. Vous pouvez réactiver ces ports via la *rubrique Paramètres des ports*.
- **Adresse MAC de destination** : sélectionnez *Indiffér.* si toutes les adresses de destination sont possibles ou *Défini par l'utilisateur* pour entrer une adresse de destination ou une plage d'adresses de destination.
- **Valeur de l'adresse MAC de destination** : saisissez l'adresse MAC avec laquelle l'adresse MAC de destination sera mise en correspondance et saisissez également, le cas échéant, son masque.
- **Masque générique MAC de destination** : saisissez le masque pour définir une plage d'adresses MAC. Veuillez noter que ce masque est différent de ceux employés à d'autres fins comme un masque de sous-réseau. Ici, définir un octet avec **1** signifie « sans importance » et **0** implique masquer cette valeur. Par exemple, la valeur « FFFFFF000000 » indique que seuls les trois premiers octets de l'adresse MAC de destination seront utilisés.
- **Adresse MAC source** : sélectionnez *Indiffér.* si toutes les adresses source sont possibles ou *Défini par l'utilisateur* pour entrer une adresse source ou une plage d'adresses source.
- **Valeur de l'adresse MAC source** : saisissez l'adresse MAC avec laquelle l'adresse MAC source sera mise en correspondance et saisissez également, le cas échéant, son masque.
- **Masque générique MAC source** : saisissez le masque afin de définir une plage d'adresses MAC.
- **ID VLAN** : saisissez la partie ID VLAN de la balise VLAN à mettre en correspondance.
- **802.1p** : sélectionnez **Inclure** pour utiliser 802.1p.
- **Valeur 802.1p** : saisissez la valeur 802.1p à ajouter à la balise VPT.
- **Masque 802.1p** : saisissez le masque générique à appliquer à la balise VPT.
- **Ethertype** : saisissez l'Ethertype de trame à mettre en correspondance.

ÉTAPE 5 Cliquez sur **Appliquer**. L'ACE basé sur MAC est défini et le commutateur mis à jour.

ACL basées sur IPv4

Les ACL basées sur IPv4 servent à vérifier les paquets IPv4. Les autres types de trames, tels que les ARP, ne sont pas vérifiés.

Les champs suivants peuvent être mis en correspondance :

- Protocole IP (à partir du nom pour les protocoles bien connus ou directement à partir de la valeur)
- Ports source/de destination pour le trafic TCP/UDP
- Valeurs des balises pour les trames TCP
- Type et code ICMP et IGMP
- Adresses IP source/de destination (y compris les caractères génériques)
- Valeur DSCP/IP Precedence

REMARQUE Les ACL sont également utilisées en tant qu'éléments de base pour les définitions de flux relatifs à la gestion de la QoS par flux (voir *Mode de QoS avancé*).

La *rubrique ACL basée sur IPv4* permet d'ajouter des ACL au système. Leurs règles sont définies dans la *rubrique ACE basé sur IPv4*.

Les ACL IPv6 sont définies dans la *rubrique ACL basée sur IPv6*.

Définition d'une ACL basée sur IPv4

Pour définir une ACL basée sur IPv4 :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACL basée sur IPv4**. La *rubrique ACL basée sur IPv4* s'ouvre.

Cette page affiche toutes les ACL basées sur IPv4 actuellement définies.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une ACL basée sur IPv4* s'ouvre.

ÉTAPE 3 Saisissez le nom de la nouvelle ACL dans le champ **Nom de l'ACL**. Les noms font la distinction entre les minuscules et les majuscules.

ÉTAPE 4 Cliquez sur **Appliquer**. L'ACL basée sur IPv4 est définie et le commutateur mis à jour.

Ajout de règles (ACE) à une ACL basée sur IPv4

Pour ajouter des règles (ACE) à une ACL basée sur IPv4 :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACE basé sur IPv4**. La *rubrique ACE basé sur IPv4* s'ouvre.

ÉTAPE 2 Sélectionnez une ACL et cliquez sur **OK**. Tous les ACE IP actuellement définies pour l'ACL sélectionnée s'affichent.

ÉTAPE 3 Cliquez sur **Ajouter**. La *rubrique Ajouter ACE basé sur IPv4* s'ouvre.

ÉTAPE 4 Saisissez les paramètres.

- **Nom de l'ACL** : affiche le nom de l'ACL.
- **Priorité** : permet d'entrer la priorité. Les ACE disposant d'une priorité plus élevée seront traitées en priorité.
- **Action** : sélectionnez l'action affectée au paquet correspondant à l'ACE. Les options disponibles sont les suivantes :
  - *Autoriser* : transfère les paquets qui répondent aux critères de l'ACE.
  - *Refuser* : abandonne les paquets qui répondent aux critères de l'ACE.
  - *Arrêter* : abandonne le paquet qui répond aux critères de l'ACE et désactive le port auquel le paquet était adressé. Les ports sont réactivés à partir de la rubrique *Gestion des ports*.
- **Protocole** : choisissez de créer une ACE en fonction d'un protocole ou d'un ID de protocole spécifique. Sélectionnez *Tout (IP)* pour accepter tous les protocoles IP. Sinon, sélectionnez un des protocoles suivants dans la liste déroulante :
  - *ICMP* : *Internet Control Message Protocol*
  - *IGMP* : *Internet Group Management Protocol*
  - *IP in IP* : encapsulation IP in IP
  - *TCP* : Transmission Control Protocol

- *EGP* : Exterior Gateway Protocol
- *IGP* : Interior Gateway Protocol
- *UDP* : User Datagram Protocol
- *HMP* : Host Mapping Protocol
- *RDP* : Reliable Datagram Protocol
- *IDPR* : Inter-Domain Policy Routing Protocol
- *IPV6* : tunnellisation IPv6 sur IPv4
- *IPV6:ROUT* : fait correspondre les paquets appartenant à la *route IPv6 sur IPv4 via une passerelle*
- *IPV6:FRAG* : fait correspondre les paquets appartenant à l'en-tête de fragment IPv6 sur IPv4
- *IDRP* : Inter-Domain Routing Protocol
- *RSVP* : ReSerVation Protocol
- *AH* : *Authentication Header (En-tête d'authentification)*
- *IPV6:ICMP* : Internet Control Message Protocol
- *EIGRP* : *Enhanced Interior Gateway Routing Protocol*
- *OSPF* : *Open Shortest Path First*
- *IPIP* : *IP in IP*
- *PIM* : *Protocol Independent Multicast*
- *L2TP* : Layer 2 *Tunneling Protocol*
- *ISIS* : protocole spécifique à IGP

- **ID protocole de mise en correspondance** : au lieu de sélectionner le nom, saisissez l'ID du protocole.
- **Adresse IP source** : sélectionnez *Indiffér.* si toutes les adresses source sont acceptables ou *Défini par l'utilisateur* pour entrer une adresse source ou une plage d'adresses source.
- **Valeur de l'adresse IP source** : saisissez l'adresse IP avec laquelle l'adresse IP source sera mise en correspondance.

- **Masque générique IP source** : saisissez le masque pour définir une plage d'adresses IP.
- **Adresse IP de destination** : sélectionnez *Indiffér.* si toutes les adresses de destination sont acceptables ou *Défini par l'utilisateur* pour entrer une adresse de destination ou une plage d'adresses de destination.
- **Valeur de l'adresse IP de destination** : saisissez l'adresse IP avec laquelle l'adresse IP de destination sera mise en correspondance.
- **Masque générique IP de destination** : saisissez le masque pour définir une plage d'adresses IP.
- **Port source** : sélectionnez une des options suivantes :
  - *Indiffér.* : correspond à tous les ports source.
  - *Unique* : saisissez un seul port TCP/UDP source avec lequel les paquets sont mis en correspondance. Ce champ n'est actif que si TCP ou UDP est sélectionné dans le menu déroulant Sélectionner dans la liste.
  - *Plage* : sélectionnez une plage de ports source TCP/UDP avec lesquels le paquet est mis en correspondance. Huit plages de ports différentes peuvent être configurées (partagées entre les ports source et de destination). Les protocoles TCP et UDP disposent chacun de huit plages de ports.
- **Port de destination** : sélectionnez l'une des valeurs disponibles (identiques à celles du champ Port source décrit ci-dessus).

  REMARQUE Vous devez spécifier le protocole IP de l'ACE avant de pouvoir entrer le port source et/ou de destination.
- **Indicateurs TCP** : sélectionnez un ou plusieurs indicateurs TCP avec lesquels filtrer les paquets. Les paquets filtrés sont transmis ou abandonnés. Le filtrage de paquets par des indicateurs TCP améliore le contrôle des paquets et ainsi la sécurité du réseau.
- **Type de service** : **type de service du paquet IP.**
  - **Indiffér.** : tout type de service
  - **DSCP en correspondance** : DSCP (Differentiated Serves Code Point) à mettre en correspondance
  - **IP Precedence en correspondance**

- **ICMP** : si le protocole IP de l'ACL est ICMP, sélectionnez le type de message ICMP utilisé afin de filtrer. Sélectionnez le type de message en fonction de son nom ou saisissez le numéro du type de message :
  - *Indiffér.* : tous les types de message sont acceptés.
  - *Sélectionner dans la liste* : permet de sélectionner le type de message en fonction de son nom.
  - *Type ICMP de mise en correspondance* : numéro du type de message à utiliser afin de filtrer.
- **Code ICMP** : les messages ICMP peuvent disposer d'un champ de code indiquant comment gérer le message. Sélectionnez l'une des options suivantes pour indiquer si le filtrage s'effectuera en fonction de ce code :
  - *Indiffér.* : tous les codes sont acceptés.
  - *Défini par l'utilisateur* : saisissez un code ICMP afin de filtrer.
- **IGMP** : si l'ACL est basée sur IGMP, sélectionnez le type de message IGMP à utiliser afin de filtrer. Sélectionnez le type de message en fonction de son nom ou saisissez le numéro du type de message :
  - *Indiffér.* : tous les types de message sont acceptés.
  - *Sélectionner dans la liste* : permet de sélectionner le type de message en fonction de son nom.
  - *Type IGMP de mise en correspondance* : numéro du type de message qui sera utilisé afin de filtrer.

ÉTAPE 5 Cliquez sur **Appliquer**. L'ACE basé sur IPv4 est défini et le commutateur mis à jour.

ACL basées sur IPv6

La *rubrique ACL basée sur IPv6* affiche les ACL IPv6 existantes, qui vérifient le trafic purement IPv6 et permet également d'en créer. Les ACL IPv6 ne vérifient pas les paquets IPv6 sur IPv4 ou ARP.

REMARQUE Les ACL sont également utilisées en tant qu'éléments de base pour les définitions de flux relatifs à la gestion de la QoS par flux (voir *Mode de QoS avancé*).

Définition d'une ACL basée sur IPv6

Pour définir une ACL basée sur IPv6 :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACL basée sur IPv6**. La *rubrique ACL basée sur IPv6* s'ouvre.

Cette fenêtre affiche la liste des ACL définies et leur contenu.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une ACL basée sur IPv6* s'ouvre.

ÉTAPE 3 Saisissez le nom de la nouvelle ACL dans le champ **Nom de l'ACL**. Les noms font la distinction entre les minuscules et les majuscules.

ÉTAPE 4 Cliquez sur **Appliquer**. L'ACL basée sur IPv6 est définie et le commutateur est mis à jour.

Définition d'une règle (ACE) pour une ACL basée sur IPv6 :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACE basé sur IPv6**. La *rubrique ACE basé sur IPv6* s'ouvre.

Cette fenêtre affiche les ACE (règles) d'une ACL spécifiée (groupe de règles).

ÉTAPE 2 Sélectionnez une ACL et cliquez sur **OK**. Tous les ACE IP actuellement définies pour l'ACL sélectionnée s'affichent.

ÉTAPE 3 Cliquez sur **Ajouter**. La *rubrique Ajouter un ACE basé sur IPv6* s'ouvre.

ÉTAPE 4 Saisissez les paramètres.

- **Nom de l'ACL** : affiche le nom de l'ACL à laquelle un ACE est ajouté.
- **Priorité** : permet d'entrer la priorité. Les ACE disposant d'une priorité plus élevée seront traitées en priorité.
- **Action** : sélectionnez l'action affectée au paquet correspondant à l'ACE. Les options disponibles sont les suivantes :
  - *Autoriser* : transfère les paquets qui répondent aux critères de l'ACE.
  - *Refuser* : abandonne les paquets qui répondent aux critères de l'ACE.
  - *Arrêter* : abandonne les paquets qui répondent aux critères de l'ACE et désactive le port auquel les paquets étaient adressés. Les ports sont réactivés à partir de la rubrique *Gestion des ports*.

- **Protocole** : sélectionnez cette option pour créer une ACE basé sur un protocole spécifique. Sélectionnez *Tout (IPv6)* pour accepter tous les protocoles IP. Sinon, sélectionnez l'un des protocoles suivants :
  - *TCP* : Transmission Control Protocol. Permet à deux hôtes de communiquer et d'échanger des flux de données. TCP garantit la livraison des paquets et également que les paquets seront transmis et reçus dans l'ordre dans lequel ils ont été envoyés.
  - *UDP* : User Datagram Protocol. Transmet les paquets mais ne garantit pas leur livraison.
  - *ICMP* : fait correspondre les paquets au protocole ICMP (Internet Control Message Protocol).
- **ID protocole de mise en correspondance** : saisissez l'ID du protocole avec lequel établir la correspondance.
- **Adresse IP source** : sélectionnez *Indiffér.* si toutes les adresses source sont acceptables ou *Défini par l'utilisateur* pour entrer une adresse source ou une plage d'adresses source.
- **Valeur de l'adresse IP source** : saisissez l'adresse IP avec laquelle l'adresse IP source sera mise en correspondance et saisissez également, le cas échéant, son masque.
- **Longueur du préfixe IP source** : saisissez la longueur du préfixe de l'adresse IP source.
- **Adresse IP de destination** : sélectionnez *Indiffér.* si toutes les adresses de destination sont acceptables ou *Défini par l'utilisateur* pour entrer une adresse de destination ou une plage d'adresses de destination.
- **Valeur de l'adresse IP de destination** : saisissez l'adresse IP avec laquelle l'adresse IP de destination sera mise en correspondance et saisissez également, le cas échéant, son masque.
- **Longueur du préfixe IP de destination** : saisissez la longueur du préfixe de l'adresse IP.
- **Port source** : sélectionnez une des options suivantes :
  - *Indiffér.* : correspond à tous les ports source.
  - *Unique* : saisissez un seul port TCP/UDP source avec lequel les paquets sont mis en correspondance. Ce champ n'est actif que si TCP ou UDP est sélectionné dans le menu déroulant Sélectionner dans la liste.

- *Plage* : sélectionnez une plage de ports source TCP/UDP avec lesquels le paquet est mis en correspondance.

- **Port de destination** : sélectionnez l'une des valeurs disponibles. (Elles sont identiques à celles du champ Port source décrit ci-dessus.)

  REMARQUE Vous devez spécifier le protocole IPv6 de l'ACL avant de pouvoir configurer le port source et/ou de destination.

- **Indicateurs TCP** : sélectionnez un ou plusieurs indicateurs TCP avec lesquels filtrer les paquets. Les paquets filtrés sont transmis ou abandonnés. Le filtrage de paquets par des indicateurs TCP améliore le contrôle des paquets et ainsi la sécurité du réseau.

  - Défini : une correspondance est établie si l'indicateur est Défini.
  - Non défini : une correspondance est établie si l'indicateur est Non défini.
  - Sans importance : ignore l'indicateur TCP.

- **Type de service** : type de service du paquet IP.

- **ICMP** : si l'ACL est basée sur ICMP, sélectionnez le type de message ICMP à utiliser afin de filtrer. Sélectionnez le type de message en fonction de son nom ou saisissez le numéro du type de message. Si tous les types de message sont acceptés, sélectionnez *Indiffér.*.

  - *Indiffér.* : tous les types de message sont acceptés.
  - *Sélectionner dans la liste* : permet de sélectionner le type de message en fonction de son nom dans la liste déroulante.
  - *Type ICMP de mise en correspondance* : numéro du type de message qui sera utilisé afin de filtrer.

- **Code ICMP** : les messages ICMP peuvent disposer d'un champ de code indiquant comment gérer le message. Sélectionnez l'une des options suivantes pour indiquer si le filtrage s'effectuera en fonction de ce code :

  - *Indiffér.* : tous les codes sont acceptés.
  - *Défini par l'utilisateur* : saisissez un code ICMP afin de filtrer.

ÉTAPE 5 Cliquez sur **Appliquer**.

Définition d'une liaison ACL

Lorsqu'une ACL est liée à une interface, ses règles ACE sont appliquées aux paquets qui arrivent au niveau de cette interface. Les paquets qui ne correspondent à aucune des ACE de l'ACL sont mis en correspondance avec une règle par défaut, dont l'action consiste à abandonner les paquets sans correspondance.

Bien que chaque interface ne puisse être liée qu'à une seule ACL, plusieurs interfaces peuvent être liées à la même ACL en les regroupant dans une « policy-map » (principes directeurs) puis en liant cette dernière à l'interface.

Une fois qu'une ACL est liée à une interface, elle ne peut être éditée, modifiée ou supprimée qu'une fois enlevée de tous les ports auxquels elle est liée ou sur lesquels elle est utilisée.

Pour lier une ACL à une interface :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **Liaison ACL**. La *rubrique Liaison ACL* s'ouvre.

ÉTAPE 2 Sélectionnez comme type d'interface **Ports/LAG** (Port ou LAG).

ÉTAPE 3 Cliquez sur **OK**. La liste des ports/LAG s'affiche. Pour chaque type d'interface sélectionné, toutes les interfaces de ce type sont affichées avec la liste de leurs ACL actuelles :

- **Interface** : identificateur d'interface.
- **ACL MAC** : les ACL de type MAC qui sont liées à l'interface (le cas échéant).
- **ACL IPv4** : les ACL de type IPv4 qui sont liées à l'interface (le cas échéant).
- **ACL IPv6** : les ACL de type IPv6 qui sont liées à l'interface (le cas échéant).

  REMARQUE Pour supprimer la liaison de toutes les ACL au niveau d'une interface, sélectionnez cette dernière puis cliquez sur **Supprimer**.

ÉTAPE 4 Sélectionnez une interface puis cliquez sur **Modifier**. La *rubrique Modifier la liaison ACL* s'ouvre.

ÉTAPE 5 Sélectionnez l'**interface** à laquelle les ACL doivent être liées.

ÉTAPE 6 Sélectionnez une des options suivantes :

- **Sélectionner une ACL basée sur MAC** : sélectionnez une ACL basée sur MAC à lier à l'interface.
- **Sélectionner une ACL basée sur IPv4** : sélectionnez une ACL basée sur IPv4 à lier à l'interface.

- **Sélectionner une ACL basée sur IPv6** : sélectionnez une ACL basée sur IPv6 à lier à l'interface.

ÉTAPE 7 Cliquez sur **Appliquer**. La liaison des ACL est modifiée et le commutateur est mis à jour.

REMARQUE Si aucune ACL n'est sélectionnée, l'ACL ou des ACL précédemment liée(s) à l'interface est ou sont supprimée(s).

18

Configuration du 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.

Ce chapitre contient les sections suivantes :

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.

Modes QoS

Modes QoS

Le mode QoS sélectionné s'applique à toutes les interfaces du système.

- Mode de base — CoS (Class of Service, classe de service).

  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 valeur VPT (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 valeur TC (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.

  Le champ d'en-tête auquel faire confiance est entré dans la *rubrique Paramètres globaux*. Pour chaque valeur de ce champ, une file d'attente de sortie est désignée comme destinataire de l'envoi de la trame (dans la *rubrique CoS/802.1p vers file d'attente* ou dans la *rubrique DSCP vers file d'attente*, selon que le mode de confiance choisi est CoS/802.1p ou DSCP).

- Mode avancé — QoS (Quality of Service, qualité de service) pour chaque flux.

  En mode avancé, la QoS de chaque flux est constitué d'un mappage de classe et d'un gestionnaire de stratégie :

- Le mappage de classe définit le type de trafic d'un flux et contient une ou plusieurs ACL. Les paquets correspondant à ces ACL appartiennent au flux.
- Le gestionnaire de stratégie applique la QoS configuré à un flux. La configuration de QoS d'un flux peut regrouper une file d'attente de sortie, les valeurs DSCP ou CoS/802.1p et les actions à appliquer au trafic hors profil (excédent).

▪ Mode Désactivé

Dans ce mode, tout le trafic est mappé sur une seule file d'attente de type « meilleur effort » (best effort) et aucun type de trafic n'est prioritaire sur les autres.

Vous ne pouvez activer qu'un seul mode à la fois. Lorsque le système est configuré pour fonctionner en mode de QoS avancé, les paramètres du mode de base de QoS sont inactifs et inversement.

Lorsque vous changez de mode, les événements suivants se produisent :

- Lorsque vous passez du mode de QoS avancé à un autre mode, les définitions de profil de stratégie et les mappages de classe sont supprimés. Les ACL directement liées aux interfaces restent liées.
- Lorsque vous passez du mode de base de QoS au mode avancé, la configuration du mode de confiance QoS sur le mode De base n'est pas conservée.
- Lorsque vous désactivez la QoS, les paramètres de lissage (shaping) et de file d'attente (paramètre de bande passante WRR/SP) sont réinitialisés sur leurs valeurs par défaut.

Tous les autres éléments de configuration définis par l'utilisateur restent intacts.

Flux de travail de QoS

Flux de travail de QoS

Pour configurer les paramètres de QoS généraux, procédez comme suit :

1. Choisissez le mode de QoS (De base, Avancé ou Désactivé, comme le décrit la section **« Modes QoS »**) du système, dans la *rubrique Propriétés de QoS.* Les étapes de flux de travail suivantes décrites ici considèrent que vous avez choisi d'activer la QoS.
2. Affectez à chaque interface une priorité CoS/802.1p par défaut, dans la *rubrique Propriétés de QoS*.

3. Affectez une méthode de planification (Priorité stricte ou WRR) et une valeur d'allocation de bande passante WRR aux files d'attente de sortie, dans la *rubrique File d'attente*.
4. Désignez une file d'attente de sortie pour chaque valeur IP DSCP/TC au sein de la rubrique *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 valeur DSCP/TC.
5. Associez une file d'attente de sortie à chaque priorité CoS/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. Utilisez pour cela la *rubrique CoS/802.1p vers file d'attente*.
6. Si nécessaire (uniquement pour le trafic Layer 3), affectez une file d'attente à chaque valeur DSCP/TC dans la *rubrique DSCP vers file d'attente.*
7. Saisissez les limites de bande passante et de débit dans les pages suivantes :
    a. Définissez le lissage en sortie (egress shaping) pour chaque file d'attente dans la *rubrique Lissage en sortie par file d'attente.*
    b. Définissez la limite de débit d'entrée et le lissage en sortie (egress shaping) pour chaque port dans la *rubrique Bande passante.*
    c. Définissez la limite de débit d'entrée du VLAN dans la *rubrique Limite de débit d'entrée VLAN*
8. Configurez le mode sélectionné en réalisant l'une des opérations suivantes :
    a. Configurez le mode de base comme le décrit la section *Flux de travail de configuration du mode de base de QoS*
    b. Configurez le mode avancé comme le décrit la section *Flux de travail de configuration du mode de QoS avancé*

Configuration du QoS

Affichage des propriétés de QoS

Affichage des propriétés de QoS

La rubrique *Propriétés de QoS* contient des champs permettant de définir le mode de QoS du système (De base, Avancé ou Désactivé, comme le décrit la section « Modes QoS »). En outre, vous pouvez définir la priorité CoS par défaut de chaque interface.

Pour sélectionner le mode de QoS :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Propriétés de QoS**. La *rubrique Propriétés de QoS* s'ouvre.

ÉTAPE 2 Sélectionnez le **mode de QoS** (Désactiver, De base ou Avancé) à activer sur le commutateur et cliquez sur **Appliquer**.

ÉTAPE 3 Sélectionnez **Port/LAG** pour afficher/modifier tous les ports/LAG et 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 n'ont pas de balise VLAN. Le CoS par défaut est 0. La valeur par défaut s'applique seulement aux trames non marquées, uniquement lorsque le système fonctionne en mode de base et que l'option de *confiance CoS* est sélectionnée dans la *rubrique Paramètres globaux*.

Sélectionnez **Restaurer les valeurs par défaut** pour rétablir le paramètre de CoS par défaut défini en usine pour cette interface.

Modification de la valeur de CoS par défaut de l'interface

Modification de la valeur de CoS par défaut de l'interface

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Propriétés de QoS**. La *rubrique Propriétés de QoS* s'ouvre.

ÉTAPE 2 Sélectionnez une interface puis cliquez sur **Modifier**. La *rubrique Modifier la configuration CoS de l'interface* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** — Sélectionnez l'interface.
- **CoS par défaut** — Sélectionnez la valeur de CoS (Class-of-Service, classe de service) à affecter aux paquets entrants qui ne possèdent pas de balise VLAN. La plage valide va de 0 à 7.

ÉTAPE 4 Cliquez sur **Appliquer**. La valeur de CoS par défaut de l'interface est définie et le commutateur mis à jour.

Configurer de files d'attente de QoS

Modes de mise en file d'attente

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 de la file 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 sélectionnez les modes de mise en file d'attente dans la *rubrique 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'attente 4 (celle dont la priorité est la plus élevée) puis et 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 provenant 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 *rubrique File d'attente* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **File d'attente** — Affiche le numéro de la file d'attente.
- **Méthode de planification :** Sélectionnez l'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 pondération WRR attribuée à la file d'attente.

- **% de bande passante WRR —** Affiche la quantité de bande passante affectée à la file d'attente. Ces valeurs représentent un pourcentage de la pondération WRR.

ÉTAPE 3 Cliquez sur **Appliquer**. Les files d'attente sont configurées et le commutateur est mis à jour.

Mappage CoS/802.1p vers file d'attente

La *rubrique 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 leur balise VLAN. Pour les paquets entrants non marqués, la priorité 802.1p utilisée est la priorité CoS/802.1p par défaut affectée aux ports d'entrée.

Files d'attente de mappage par défaut

Valeurs 802.1p (0-7, 7 étant la valeur la plus élevée)	File d'attente (4 files numérotées 1 à 4, 4 étant la priorité la plus élevée)	File d'attente (2 files d'attente : Normal et Élevé)	Remarques
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	Elevée	Voix Valeur par défaut de téléphone IP Cisco
6	4	Elevée	Contrôle de l'interfonctionnement RTP pour téléphone LVS
7	4	Elevée	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 à file d'attente s'applique uniquement si l'une des conditions suivantes est remplie :

- Le commutateur est en mode de base de QoS et en mode de confiance CoS/802.1p
- Le commutateur est en mode de QoS avancé et les paquets appartiennent à des flux en mode de confiance CoS/802.1p

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 *rubrique CoS/802.1p vers file d'attente* s'ouvre.

ÉTAPE 2 Saisissez les paramètres.

- **802.1p** — Affiche les valeurs de marquage 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.
- **Restaurer les valeurs par défaut** — Cliquez pour restaurer pour l'ensemble des files d'attente les valeurs par défaut d'usine relatives au mappage CoS/802.1p à file d'attente.

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 sont mappées sur les files d'attente et le commutateur est mis à jour.

Mappage DSCP à file d'attente

La rubrique DSCP (*Differentiated Services Code Point*, point de code de service différencié IP) 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 paquets IP entrants sur la base de leur valeur DSCP. La valeur VPT (VLAN Priority Tag, marquage de priorité VLAN) du paquet reste inchangée.

En modifiant simplement le mappage DSCP 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 à file d'attente s'applique aux paquets IP si :

- le commutateur est en mode de base de QoS et en mode de confiance DSCP ou
- le commutateur est en mode de QoS avancé et les paquets appartiennent à des flux en mode de confiance DSCP.

Les paquets non IP 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 *rubrique DSCP vers file d'attente* s'ouvre.

La *rubrique DSCP vers file d'attente* contient le champ **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 commutateur est mis à jour.

Configuration de la bande passante

La *rubrique Bande passante* permet aux gestionnaires réseau de définir deux ensembles de valeurs, qui déterminent la quantité de trafic que le système peut recevoir et envoyer.

Limite de débit d'entrée

La limite de débit d'entrée indique le nombre de bits par seconde que l'interface d'entrée peut recevoir. La bande passante dépassant cette limite est éliminée.

Les valeurs suivantes sont entrées pour le lissage en sortie (egress shaping) :

- L'option Débit minimal garanti (CIR) définit la quantité moyenne maximale de données que le système est autorisé à envoyer à l'interface de sortie, en bits par seconde.
- L'option Taille de rafale garantie (CBS) indique la rafale de données que le système est autorisé à envoyer même au-delà de la valeur CIR. Cette valeur est exprimée en nombre d'octets de données.

Pour indiquer la limite de bande passante :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Bande passante**. La *rubrique Bande passante* s'ouvre.

La *rubrique Bande passante* affiche les informations de bande passage 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 puis cliquez sur **Modifier**. La *rubrique Modifier la bande passante* s'ouvre.

ÉTAPE 3 Sélectionnez l'interface (**Port/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.

- **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 bande passante autorisée.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres de bande passante sont modifiés et le commutateur est mis à jour.

Configuration du lissage en sortie pour chaque file d'attente

Outre la limitation du débit de transmission de chaque port, que vous configurez dans la *rubrique 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 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 du débit en sortie pour chaque file d'attente.

Pour définir le lissage en sortie pour chaque file d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Lissage en sortie par file d'attente**. La *rubrique Lissage en sortie par file d'attente* s'ouvre.

La *rubrique Lissage en 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) puis cliquez sur **OK**. La liste des ports/LAG s'affiche.

ÉTAPE 3 Sélectionnez un port/LAG puis cliquez sur **Modifier**. La *rubrique Modifier le modelage en sortie par file d'attente* s'ouvre.

Cette page vous permet de modeler 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** — Sélectionnez cette option pour activer le lissage en sortie (egress shaping) 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 modifiés et le commutateur est mis à jour.

Configuration de la limite de débit VLAN

REMARQUE La fonction de limite de débit VLAN n'est disponible que lorsque le commutateur fonctionne en mode Layer 3.

La limitation du débit pour chaque VLAN, que vous réalisez dans la *rubrique Limite de débit d'entrée VLAN*, permet de limiter le trafic sur les VLAN. La limitation de débit QoS (configurée dans la rubrique *Table des stratégies*) est prioritaire par rapport à la limitation du débit VLAN. Par exemple, si un paquet est soumis à la fois à des limites de débit QoS et à des limites de débit VLAN et que ces limites entrent en conflit, les limites de débit QoS sont prioritaires.

Lorsque vous configurez des limites de débit d'entrée VLAN, cela limite le trafic agrégé de tous les ports du commutateur.

Vous configurez les limites de débit VLAN au niveau du périphérique et ces limites sont appliquées séparément pour chaque périphérique du réseau. Si le système inclut plusieurs périphériques (par exemple, si un réseau comprend 2 commutateurs 10/100 Cisco 24 ports participant au même VLAN), les valeurs limites de débit VLAN définies sont affectées séparément à chaque périphérique.

Pour définir la limite de débit d'entrée VLAN :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Limite de débit d'entrée VLAN**. La *rubrique Limite de débit d'entrée VLAN* s'ouvre.

Cette page affiche la table des limites de débit d'entrée VLAN.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une limite de débit d'entrée VLAN* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **ID VLAN** — Sélectionnez un VLAN.
- **Débit minimal garanti (CIR)** — Saisissez la quantité moyenne maximale de données qui peut être acceptée sur le VLAN, en kilo-octets par seconde.
- **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. Cette valeur ne peut pas être saisie pour un LAG.

ÉTAPE 4 Cliquez sur **Appliquer**. La limite de débit VLAN est ajoutée et le commutateur est mis à jour.

Évitement de l'encombrement TCP

La *rubrique Évitement de l'encombrement TCP* vous permet d'activer un algorithme d'évitement de l'encombrement TCP. Cet algorithme casse ou évite la synchronisation TCP globale sur un nœud encombré lorsque l'encombrement est dû au fait que plusieurs sources envoient des paquets munis de mêmes nombres d'octets.

Pour configurer l'évitement de l'encombrement TCP :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Évitement de l'encombrement TCP**. La *rubrique Évitement de l'encombrement TCP* s'ouvre.

ÉTAPE 2 Cliquez sur **Activer** pour activer l'évitement de l'encombrement TCP puis cliquez sur **Appliquer**.

Mode de base de QoS

En mode de base de QoS, vous pouvez définir un domaine spécifique du réseau en qualité de domaine de confiance. Dans ce domaine, les paquets sont marqués avec la priorité 802.1p et/ou DSCP afin de signaler le type de service qu'ils nécessitent. Les nœuds du domaine utilisent ces champs pour affecter les paquets à une file d'attente de sortie spécifique. La classification initiale des paquets et le marquage de ces champs s'effectuent dans les données d'entrée du domaine de confiance.

Flux de travail de configuration du mode de base de QoS

Flux de travail de configuration du mode de base de QoS

Pour configurer le mode de base de QoS, procédez comme suit :

1. Sélectionnez le mode de base pour le système dans la *rubrique Propriétés de QoS.*
2. Sélectionnez le comportement de confiance dans la *rubrique Paramètres globaux*. Le commutateur prend en charge le mode de confiance CoS/802.1p et le mode de confiance DSCP. Le mode de confiance CoS/802.1p utilise la priorité 802.1p figurant dans le balise VLAN. Le mode de confiance DSCP utilise la valeur DSCP figurant dans l'en-tête IP.
3. S'il existe un port qui fait exception et ne doit pas faire confiance au marquage CoS entrant, désactivez l'état QoS sur ce port dans la *rubrique Paramètres d'interface.*

   Activez ou désactivez le mode de confiance sélectionné au niveau global sur les divers ports dans la *rubrique Paramètres d'interface*. Si un port est désactivé sans mode de confiance, tous ses paquets d'entrée sont transférés en mode Meilleur effort (Best effort). Il est recommandé de désactiver le mode de confiance sur les ports où les valeurs CoS/802.1p et/ou DSCP des paquets entrants ne sont pas dignes de confiance. Dans le cas contraire, cela peut avoir un impact négatif sur les performances de votre réseau.

Configuration des paramètres globaux

La *rubrique Paramètres globaux* contient des informations concernant l'activation du mode de confiance sur le commutateur (reportez-vous au champ *Mode de confiance* ci-dessous). Cette configuration est active lorsque le mode de QoS est De base. Les paquets entrant dans un domaine QoS sont classifiés à la bordure du domaine QoS.

Pour définir la configuration de mode de confiance :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de base de QoS** > **Paramètres globaux**. La *rubrique Paramètres globaux* s'ouvre.

ÉTAPE 2 Sélectionnez le **mode de confiance** à appliquer lorsque le commutateur est en mode de base. Si le niveau de CoS et le marquage DSCP d'un paquet sont mappés sur des files d'attente distinctes, le mode de confiance détermine la file d'attente à laquelle ce paquet doit être affecté :

- **CoS/802.1p** — Le trafic est mappé sur des files d'attente en fonction du champ VPT du balise VLAN ou en fonction de la valeur par défaut CoS/802.1p définie pour chaque port (si le paquet entrant ne comporte aucune balise VLAN). Vous configurez le mappage VPT vers file d'attente réel dans la rubrique CoS/802.1p vers file d'attente.
- **DSCP** — Tout le trafic IP est mappé sur des files d'attente en fonction du champ DSCP de l'en-tête IP. Vous pouvez configurer le mappage DSCP à file d'attente réel dans la rubrique DSCP vers file d'attente. Si le trafic n'est pas de type IP, il est mappé sur la file d'attente Meilleur effort (Best effort).

ÉTAPE 3 Sélectionnez **Remplacer DSCP d'entrée** pour remplacer les valeurs DSCP d'origine des paquets entrants par d'autres, d'après la table de substitution DSCP. Lorsque la fonction Remplacer DSCP d'entrée est activée, le commutateur utilise les nouvelles valeurs DSCP pour la mise en file d'attente des données en sortie. Il remplace également les valeurs DSCP d'origine figurant dans les paquets par les nouvelles valeurs DSCP.

REMARQUE La trame est mappée sur une file d'attente en sortie à l'aide de la nouvelle valeur réécrite et non de la valeur DSCP d'origine.

ÉTAPE 4 Si vous avez activé l'option **Remplacer DSCP d'entrée**, cliquez sur **Table de substitution DSCP** pour reconfigurer le DSCP. La *rubrique Table de substitution DSCP* s'ouvre.

Pour en savoir plus sur cette page, reportez-vous à la rubrique *Mappage DSCP hors profil*, car cette page contient les mêmes champs.

ÉTAPE 5 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

Paramètres QoS de l'interface

La *rubrique 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** > **Mode de base de QoS** > **Paramètres d'interface**. La *rubrique Paramètres d'interface* s'ouvre.

ÉTAPE 2 Sélectionnez **Port** ou **LAG** pour afficher la liste des ports ou celle des LAG.

La liste des ports/LAG s'affiche. **État de QoS** indique si la QoS est activée sur l'interface.

ÉTAPE 3 Sélectionnez une interface puis cliquez sur **Modifier**. La *Modifier les paramètres d'interface de QoS* s'ouvre.

ÉTAPE 4 Sélectionnez l'interface (**Port** ou **LAG**).

ÉTAPE 5 Cliquez pour activer ou désactiver l'**état de QoS** pour cette interface.

ÉTAPE 6 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

Mode de QoS avancé

Les trames qui correspondent à une ACL et sont autorisées à entrer sur le système sont implicitement marquées du nom de l'ACL qui a donné cette autorisation. Vous pouvez alors appliquer des actions de QoS en mode avancé à ces flux.

En mode de QoS avancé, le commutateur utilise des stratégies pour prendre en charge la QoS pour chaque flux. Une stratégie et ses composants possèdent les caractéristiques et les relations suivantes :

- Une stratégie contient un ou plusieurs mappages de classe.

- Un mappage de classe définit un flux associé à une ou plusieurs ACL. Les paquets qui correspondent uniquement aux règles d'ACL (ACE) d'un mappage de classe avec l'action Autoriser (transfert) sont considérés comme appartenant au même flux et sont soumis à la même QoS. Ainsi, une stratégie contient un ou plusieurs flux, chacun avec une QoS définie par l'utilisateur.
- La QoS d'un mappage de classe (flux) est exercée par le gestionnaire de stratégie associé. Il existe deux types de gestionnaire de stratégie : le gestionnaire de stratégie individuelle et le gestionnaire de stratégie d'agrégats. Chaque gestionnaire de stratégie est configuré avec une spécification de QoS. Le gestionnaire de stratégie individuelle applique la QoS à un seul mappage de classe, c'est-à-dire à un seul flux, en se fondant sur la spécification de QoS qu'il contient. Le gestionnaire de stratégie d'agrégats applique la QoS à un ou plusieurs mappages de classe (flux). Un gestionnaire de stratégie d'agrégats peut prendre en charge des mappages de classe issus de plusieurs stratégies.
- La QoS est appliquée à chaque flux par liaison des stratégies aux ports voulus. Vous pouvez lier une stratégie et ses mappages de classe à un ou plusieurs ports mais chaque port ne peut être lié qu'à une seule stratégie.

Remarques :

- Les gestionnaires de stratégies individuelles et d'agrégats sont disponibles lorsque le commutateur fonctionne en mode Layer 2.
- Une ACL peut être configurée sur un ou plusieurs mappages de classe, quelles que soient les stratégies.
- Un mappage de classe ne peut appartenir qu'à une seule stratégie.
- Lorsqu'un mappage de classe utilisant un gestionnaire de stratégie individuelle est lié à plusieurs ports, chaque port possède sa propre instance de gestionnaire de stratégie individuelle ; chacune applique la QoS du mappage de classe (flux) sur un port, indépendamment des autres ports.
- Un gestionnaire de stratégie d'agrégats applique la QoS à tous les flux, de façon agrégée, ceci sans tenir compte ni des stratégies ni des ports.

Les paramètres de QoS avancé se composent de trois parties :

- Définition des règles à mettre en correspondance. Toutes les trames qui correspondent à un groupe unique de règles sont considérées comme constituant un *flux*.
- Définition des actions à appliquer aux trames de chaque flux qui correspondent aux règles.

- Liaison de combinaisons règles-action à une ou plusieurs interfaces.

Flux de travail de configuration du mode de QoS avancé

Flux de travail de configuration du mode de QoS avancé

Pour configurer le mode de QoS avancé, procédez comme suit :

1. Sélectionnez le mode avancé pour le système dans la *rubrique Propriétés de QoS.*
2. Si les valeurs DSCP internes sont différentes de celles utilisées dans les paquets entrants, mappez les valeurs externes sur des valeurs internes dans la *rubrique Marquages DSCP.*
3. Créez des ACL, comme le décrit la section *Flux de travail de création d'une ACL*.
4. Si des ACL ont été définies, créez des mappages de classe et associez-leur ces ACL dans la *rubrique Mappage de classe.*
5. Créez une stratégie dans la rubrique Table des stratégies puis associez cette stratégie à un ou plusieurs mappages de classe dans la rubrique Mappages de classe de stratégies. Vous pouvez également spécifier la QoS, si nécessaire, en affectant un gestionnaire de stratégie à un mappage de classe lors de l'opération d'affectation de ce mappage à la stratégie.

   Gestionnaire de stratégie individuelle — Créez une stratégie pour associer un mappage de classe à un gestionnaire de stratégie individuelle, dans la *rubrique Mappages de classe de stratégies* et dans la *rubrique Mappage de classe.* Dans la stratégie, définissez le gestionnaire de stratégie individuelle.

   Gestionnaire de stratégie d'agrégats — Créez une action de QoS pour chaque flux afin d'envoyer toutes les trames concordantes au même gestionnaire de stratégie (d'agrégats), dans la *rubrique Gestionnaire de stratégie d'agrégats*. Créez une stratégie pour associer un mappage de classe à ce gestionnaire de stratégie d'agrégats, dans la *rubrique Mappages de classe de stratégies.*
6. Liez la stratégie à une interface dans la *rubrique Liaison de stratégies.*

Configuration du nouveau marquage du DSCP hors profil

Lorsque vous associez un gestionnaire de stratégie à un mappage de classe (flux), vous pouvez définir l'action à exécuter lorsque la quantité de trafic de ce flux dépasse la limite définie par la QoS. La portion du trafic qui provoque ce dépassement de la limite de QoS du flux est appelée *paquets hors profil*.

Si l'action appliquée en cas de dépassement est DSCP hors profil, le commutateur remappe la valeur DSCP d'origine des paquets IP hors profil sur une nouvelle valeur, sur la base de la table Mappage DSCP hors profil. Le commutateur emploie les nouvelles valeurs pour affecter des ressources et des files d'attente de sortie à ces paquets. Il remplace aussi physiquement la valeur DSCP d'origine figurant dans les paquets hors profil par la nouvelle valeur DSCP.

Pour utiliser l'action de dépassement DSCP hors profil, remappez la valeur DSCP dans la table Mappage DSCP hors profil. Sinon, l'action est Null, car la valeur DSCP de la table remappe le paquet sur lui-même, selon les valeurs par défaut définies en usine.

Cliquez sur *Qualité de service > Mode avancé de QoS > Mappage DSCP hors profil*. La rubrique Marquage DSCP hors profil s'ouvre. En mode De base, permettez au réglage « Remplacer DSCP d'entrée » de modifier les valeurs DSCP d'entrée et de sortie du commutateur.

Description et exemple

Cette fonction modifie les marquages DSCP du trafic entrant commuté entre des domaines de QoS de confiance. En modifiant les valeurs DSCP utilisées dans un domaine, vous définissez la priorité de ce type de trafic sur la valeur DSCP utilisée dans l'autre domaine pour identifier le même type de trafic.

Ces paramètres sont actifs lorsque le système fonctionne en mode de base de QoS. Une fois activés, ils s'appliquent à l'échelle globale.

Par exemple : Supposez qu'il existe trois niveaux de service : Argent, Or et Platine et que les valeurs DSCP entrantes utilisées pour marquer ces niveaux soient respectivement 10, 20 et 30. Si ce trafic est transféré vers un autre fournisseur de services offrant les mêmes niveaux de service mais que ce fournisseur emploie les valeurs DSCP 16, 24 et 48, le **mappage DSCP hors profil** remplace les valeurs entrantes au fur et à mesure qu'elles sont mappées sur les valeurs sortantes.

Pour mapper des valeurs DSCP :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Mappage DSCP hors profil**. La *rubrique Mappage DSCP hors profil* s'ouvre Le champ **DSCP en entrée** affiche la valeur DSCP des paquets entrants qui doit être marquée à nouveau à l'aide d'une autre valeur.

ÉTAPE 2 Sélectionnez la valeur **DSCP en sortie** correspondant à l'endroit sur lequel la valeur entrante est mappée.

ÉTAPE 3 Cliquez sur **Appliquer**. Le commutateur est mis à jour avec la nouvelle table des nouveaux marquages DSCP.

Définition d'un mappage de classe

Un mappage de classe définit un flux de trafic doté d'ACL (Access Control List, liste de contrôle d'accès). Vous pouvez combiner une ACL MAC, une ACL IP et une ACL IPv6 en un même mappage de classe. Les mappages de classe sont configurés pour mettre en correspondance des critères de paquet sur une base 1-à-1 ou une base 1-à-n. La correspondance est établie avec les paquets selon la méthode du « premier qui convient » : l'action associée au premier mappage de classe reconnu comme correspondant aux critères est appliquée par le système. Les paquets correspondant au même mappage de classe sont considérés comme appartenant au même flux.

REMARQUE La définition de mappages de classe n'a aucun effet sur la QoS ; il s'agit d'une étape intermédiaire nécessaire pour que les mappages de classe puissent être utilisés ultérieurement.

Si vous avez besoin d'ensembles de règles plus complexes, vous pouvez regrouper plusieurs mappages de classe en un grand groupe, appelé stratégie (reportez-vous à la section **Configuration d'une stratégie**).

La *rubrique Mappage de classe* affiche la liste des mappages de classe définis et des ACL qui les constituent ; elle vous permet aussi d'ajouter/de supprimer des mappages de classe.

Pour définir un mappage de classe :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Mappage de classes**. La *rubrique Mappage de classe* s'ouvre.

Cette page affiche les mappages de classe déjà définis.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un mappage de classes* s'ouvre.

Vous ajoutez un nouveau mappage de classe en sélectionnant une ou plusieurs ACL et en attribuant un nom au mappage de classe. Si un mappage de classe inclut deux ACL, vous pouvez spécifier que les trames doivent correspondre à ces deux ACL ou bien demander qu'elles correspondent à au moins une des deux ACL sélectionnées.

ÉTAPE 3 Saisissez les paramètres.

- **Nom du mappage de classe** — Saisissez le nom du nouveau mappage de classe.
- **Type d'ACL recherché** — Critères qu'un paquet doit satisfaire pour être considéré comme appartenant au flux défini dans le mappage de classe. Les options disponibles sont les suivantes :
  - **IP** — Un paquet doit correspondre à l'une des ACL IP du mappage de classe.
  - **MAC** — Un paquet doit correspondre à l'ACL MAC du mappage de classe.
  - **IP et MAC** — Un paquet doit correspondre à la fois à l'ACL IP et à l'ACL MAC du mappage de classe.
  - **IP or MAC** — Un paquet doit correspondre soit à l'ACL IP, soit à l'ACL MAC du mappage de classe.
- **IP** — Sélectionnez l'ACL IPv4 ou IPv6 pour ce mappage de classe.
- **MAC** — Sélectionnez l'ACL MAC pour ce mappage de classe.
- **ACL préférée** — Indiquez si les paquets sont d'abord comparés à une ACL IP ou à une ACL MAC.

ÉTAPE 4 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

Gestionnaires de stratégie QoS

Vous pouvez mesurer le débit de trafic qui correspond à un ensemble prédéfini de règles et mettre en place des limites. Par exemple, vous pouvez limiter le débit de trafic de transfert de fichiers autorisé sur un port.

Pour ce faire, vous utilisez les ACL du ou des mappages de classe pour faire correspondre le trafic voulu. Vous utilisez ensuite un gestionnaire de stratégie pour faire fonctionner la QoS sur le trafic concordant.

REMARQUE Les gestionnaires de stratégie QoS ne sont pas pris en charge lorsque le commutateur fonctionne en mode Layer 3.

Un gestionnaire de stratégie est configuré avec une spécification de QoS. Il existe deux types de gestionnaire de stratégie :

- **Gestionnaire de stratégie individuelle (standard)** — Le gestionnaire de stratégie individuelle applique la QoS à un seul mappage de classe et à un seul flux, sur la base de la spécification de QoS qu'il contient. Lorsqu'un mappage de classe utilisant un gestionnaire de stratégie individuelle est lié à plusieurs ports, chaque port possède sa propre instance de gestionnaire de stratégie individuelle ; chacune applique la QoS du mappage de classe (flux) à des ports qui sont normalement indépendants les uns des autres. Vous créez un gestionnaire de stratégie individuelle dans la *rubrique Mappages de classe de stratégies.*
- **Gestionnaire de stratégie d'agrégats** — Le gestionnaire de stratégie d'agrégats applique la QoS à un ou plusieurs mappages de classe ainsi qu'à un ou plusieurs flux. Un gestionnaire de stratégie d'agrégats peut prendre en charge des mappages de classe issus de plusieurs stratégies. Un gestionnaire de stratégie d'agrégats applique la QoS à tous les flux, de façon agrégée, sans tenir compte des stratégies ni des ports. Vous créez un gestionnaire de stratégie d'agrégats dans la *rubrique Gestionnaire de stratégie d'agrégats.*

  Vous créez un gestionnaire de stratégie d'agrégats si vous prévoyez de la partager entre plusieurs classes.

Chaque gestionnaire de stratégie est défini avec sa propre spécification de QoS, par combinaison des paramètres suivants :

- Débit maximal autorisé, appelé CIR (Committed Information Rate, débit minimal garanti), mesuré en kbits/s.
- Quantité de trafic, mesurée en octets, appelée CBS (Committed Burst Size, taille de rafale garantie). Il s'agit du trafic autorisé à transiter sous forme de rafale temporaire, même s'il dépasse le débit maximal défini.
- Action à appliquer aux trames qui dépassent les limites (appelées trafic hors profil), à savoir s'il faut transmettre ces trames telles quelles, les éliminer ou les transmettre, mais en les remappant sur une valeur DSCP qui les marque comme trames de priorité faible pour tous les traitements suivants sur le périphérique.

Vous affectez un gestionnaire de stratégie à un mappage de classe lorsque vous ajoutez ce mappage à une stratégie. Si vous choisissez un gestionnaire de stratégie d'agrégats, vous devez le créer dans la *rubrique Gestionnaire de stratégie d'agrégats*.

Définition de gestionnaires de stratégie d'agrégats

Le gestionnaire de stratégie d'agrégats applique la QoS à un ou plusieurs mappages de classe et donc à un ou plusieurs flux. Un gestionnaire de stratégie d'agrégats peut prendre en charge des mappages de classe issus de différentes stratégies et applique la QoS à tous les flux, de façon agrégée, sans tenir compte des stratégies ni des ports.

REMARQUE Le commutateur ne prend en charge les gestionnaires de stratégie individuelle et d'agrégat que lorsqu'il fonctionne en mode Layer 2.

Pour définir un gestionnaire de stratégie d'agrégats :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Gestionnaire de stratégie d'agrégats**. La *rubrique Gestionnaire de stratégie d'agrégats* s'ouvre.

Cette page affiche les gestionnaires de stratégie d'agrégats existants.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un gest. de stratégie d'agrégats* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **Nom du gestionnaire de stratégie d'agrégats** — Saisissez le nom du gestionnaire de stratégie d'agrégats.
- **Débit minimal garanti en entrée** (CIR) — Saisissez la bande passante maximale autorisée, en bits par seconde. Reportez-vous à la description de la *rubrique Bande passante*.
- **Taille de rafale garantie en entrée (CBS)** — Saisissez la taille maximale de rafale (même si elle dépasse la valeur CIR), en octets. Reportez-vous à la description de la *rubrique Bande passante*.
- **Action si dépassement** — Sélectionnez l'action à appliquer aux paquets entrants qui dépassent le seuil CIR. Les options disponibles sont les suivantes :
  - *Transférer* — Les paquets qui dépassent la limite CIR définie sont transférés.
  - *Éliminer* — Les paquets qui dépassent la limite CIR définie sont éliminés.
  - *DSCP hors profil* — Les valeurs DSCP des paquets qui dépassent la limite CIR définie sont remappées sur d'autres, d'après la table Mappage DSCP hors profil.

ÉTAPE 4 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

Configuration d'une stratégie

La *rubrique Table des stratégies* affiche la liste des stratégies de QoS avancé définies sur le système. Cette page vous permet également de créer et de supprimer des stratégies. Seules les stratégies liées à une interface sont actives (reportez-vous à la *rubrique Liaison de stratégies*).

Chaque stratégie est constituée des éléments suivants :

- Un ou plusieurs mappages de classe d'ACL, qui définissent les flux de trafic dans la stratégie.
- Un ou plusieurs agrégats qui appliquent la QoS aux flux de trafic dans la stratégie.

Après avoir ajouté une stratégie, vous pouvez ajouter des mappages de classe dans la *rubrique Mappages de classe de stratégies.*

Pour ajouter une stratégie de QoS :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Table des stratégies**. La *rubrique Mappages de classe de stratégies* s'ouvre.

Cette page affiche la liste des stratégies définies.

ÉTAPE 2 Cliquez sur **Table de mappages de classe de stratégie** pour afficher la *rubrique Mappages de classe de stratégies*.
OU
Cliquez sur **Ajouter** pour ouvrir la *rubrique Ajouter une stratégie*.

ÉTAPE 3 Saisissez le nom de la nouvelle stratégie dans le champ prévu à cet effet.

ÉTAPE 4 Cliquez sur **Appliquer**. Le profil de stratégie QoS est ajouté et le commutateur est mis à jour.

Mappages de classe de stratégies

Vous pouvez ajouter un ou plusieurs mappages de classe à une stratégie. Un mappage de classe défini le type des paquets qui sont considérés comme appartenant au même flux de trafic.

REMARQUE Il est impossible de configurer un gestionnaire de stratégie sur un mappage de classe lorsque le commutateur fonctionne en mode Layer 3. Le commutateur ne prend en charge les gestionnaires de stratégie qu'en mode Layer 2.

Pour ajouter un mappage de classe à une stratégie :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Mappages de classe de stratégies**. La *rubrique Mappages de classe de stratégies* s'ouvre.

ÉTAPE 2 Sélectionnez une stratégie dans le filtre puis cliquez sur **OK**. Tous les mappages de classe de cette stratégie sont affichés.

ÉTAPE 3 Pour ajouter un nouveau mappage de classe, cliquez sur **Ajouter**. La *rubrique Ajouter un plan de classe de stratégies* s'ouvre.

ÉTAPE 4 Saisissez les paramètres.

- **Nom de la stratégie** — Indique la stratégie à laquelle vous ajoutez le mappage de classe.
- **Nom du mappage de classe** — Sélectionnez le mappage de classe existant à associer à la stratégie. Vous créez les mappages de classe dans la *rubrique Mappage de classe*.
- **Type d'action** — Sélectionnez l'action à appliquer concernant la valeur CoS/802.1p et/ou DSCP d'entrée de tous les paquets concordants.
  - **Aucun** — Permet d'ignorer la valeur CoS/802.1p et/ou DSCP d'entrée. Les paquets concordants sont envoyés en mode Meilleur effort (Best effort).
  - **Faire confiance à CoS/802.1p, DSCP** — Si vous sélectionnez cette option, le commutateur fait confiance aux valeurs CoS/802.1p et DSCP du paquet concordant. S'il s'agit d'un paquet IP, le commutateur place le paquet dans la file d'attente de sortie en fonction de la valeur DSCP détectée et du contenu de la table DSCP vers file d'attente. Sinon, la file d'attente de sortie du paquet dépend de la valeur CoS/802.1p de ce paquet et du contenu de la table CoS/802.1p vers file d'attente.
  - **Définir** — Si vous sélectionnez cette option, le système utilise le contenu saisi dans le champ **Nouvelle valeur** afin de déterminer la file d'attente de sortie des paquets concordants comme suit :

    Si la nouvelle valeur (0..7) est une priorité CoS/802.1p, utilisez la valeur de priorité ainsi que le contenu de la table CoS/802.1p vers file d'attente afin de déterminer la file d'attente de sortie de tous les paquets concordants.

    Si la nouvelle valeur (0..63) est une valeur DSCP, utilisez la nouvelle valeur DSCP ainsi que le contenu de la table DSCP vers file d'attente afin de déterminer la file d'attente de sortie des paquets IP concordants.

Sinon, le système utilise la nouvelle valeur (1..4) comme numéro de file d'attente de sortie pour tous les paquets concordants.

- **Type de gest. de stratégie** — Disponible uniquement en mode Layer 2. Sélectionnez le type de gestionnaire de stratégie pour votre stratégie. Les options disponibles sont les suivantes :
  - *Aucun* — Aucune stratégie n'est utilisée.
  - *Individuel* — La stratégie est associée à un gestionnaire de stratégie individuelle..
  - *Agrégat* — La stratégie est associée à un gestionnaire de stratégie d'agrégats.
- **Gestionnaire de stratégie d'agrégats** — Disponible uniquement en mode Layer 2. Si **Type de stratégie** est configuré sur *Agrégat*, sélectionnez un gestionnaire de stratégie d'agrégats précédemment défini (dans la *rubrique Gestionnaire de stratégie d'agrégats*).

Si **Type de gest. de stratégie** indique *Individuelle*, saisissez les paramètres de QoS suivants :

- **Débit minimal garanti en entrée (CIR)** — Saisissez la valeur CIR, en kilobits par seconde. Reportez-vous à la description de la *rubrique Bande passante*.
- **Taille de rafale garantie en entrée (CBS)** — Saisissez la valeur CBS, en octets. Reportez-vous à la description de la *rubrique Bande passante*.
- **Action si dépassement** — Sélectionnez l'action à appliquer aux paquets entrants qui dépassent le seuil CIR. Les options disponibles sont les suivantes :
  - *Aucun* — Aucune action.
  - *Éliminer* — Les paquets qui dépassent la limite CIR définie sont éliminés.
  - *DSCP hors profil* — Les paquets IP qui dépassent la limite CIR définie sont transférés avec une nouvelle valeur DSCP, tirée de la table Mappage DSCP hors profil.

ÉTAPE 5 Cliquez sur **Appliquer**.

Liaison de stratégies

La *rubrique Liaison de stratégies* indique le profil de stratégie lié à chaque port. Lorsqu'un profil de stratégie est lié à un port spécifique, il est actif sur ce port. Vous ne pouvez configurer qu'un seul profil de stratégie sur chaque port mais il possible de lier un même profil à plusieurs ports.

Lorsque vous liez une stratégie à un port, ce dernier filtre et applique la QoS au trafic en entrée qui correspond aux flux définis au sein de cette stratégie. La stratégie ne s'applique pas au trafic en sortie sur le même port.

Pour modifier une stratégie, vous devez d'abord la supprimer (annuler la liaison) de tous les ports auxquels elle est liée.

Pour définir une liaison de stratégie :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Liaison de stratégies**. La *rubrique Liaison de stratégies* s'ouvre.

ÉTAPE 2 Sélectionnez un **nom de stratégie**.

ÉTAPE 3 Sélectionnez le **type d'interface** affecté à la stratégie.

ÉTAPE 4 Cliquez sur **Appliquer**. La liaison de stratégie QoS est définie et le commutateur est mis à jour.

Gestion des statistiques de QoS

Affichage des statistiques d'un gestionnaire de stratégie

Un gestionnaire de stratégie individuelle est lié à un mappage de classe issu d'une seule stratégie. Un gestionnaire de stratégie d'agrégats est lié à un ou plusieurs mappages de classe, issus d'une ou plusieurs stratégies.

Affichage des statistiques d'un gestionnaire de stratégie individuelle

Affichage des statistiques d'un gestionnaire de stratégie individuelle

La *rubrique Statistiques de gestionnaire de stratégie individuelle* indique le nombre de paquets hors profil ou conformes au profil reçus depuis une interface, qui répondent aux conditions définies dans le mappage de classe d'une stratégie.

REMARQUE Cette page n'est pas disponible lorsque le commutateur fonctionne en mode Layer 3.

Pour afficher les statistiques du gestionnaire de stratégie :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Statistiques de QoS** > **Statistiques de gestionnaire de stratégie individuelle.** La *rubrique Statistiques de gestionnaire de stratégie individuelle* s'ouvre.

Cette page contient les champs suivants :

- **Interface** — Interface à laquelle correspondent les statistiques affichées.
- **Stratégie** — Stratégie à laquelle correspondent les statistiques affichées.
- **Mappage de classe** — Mappage de classe auquel correspondent les statistiques affichées.
- **Octets dans le profil** — Nombre d'octets conformes au profil reçus.
- **Octets hors profil** — Nombre d'octets hors profil reçus.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter des statistiques de gest. de stratégie individuelle* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** — Sélectionnez l'interface pour laquelle cumuler les statistiques.
- **Nom de la stratégie** — Sélectionnez le nom de la stratégie.
- **Nom du mappage de classe** — Sélectionnez le nom du mappage de classe.

ÉTAPE 4 Cliquez sur **Appliquer**. Une demande de statistiques supplémentaire est créée et le commutateur est mis à jour.

Affichage des statistiques d'un gestionnaire de stratégie d'agrégats

Affichage des statistiques d'un gestionnaire de stratégie d'agrégats

Pour afficher les statistiques d'un gestionnaire de stratégie d'agrégats :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Statistiques de QoS** > **Statistiques de gestionnaire de stratégie d'agrégats**. La *rubrique Statistiques de gestionnaire de stratégie d'agrégats* s'ouvre.

Cette page contient les champs suivants :

- **Nom du gestionnaire de strat. d'agrégats** — Gestionnaire de stratégie sur lequel les statistiques sont fondées.
- **Octets dans le profil** — Nombre de paquets conformes au profil reçus.
- **Octets hors profil** — Nombre de paquets hors profil reçus.

ÉTAPE 2 Cliquez sur **Ajouter** pour ouvrir la *rubrique Ajouter des statistiques de gest. de stratégie d'agrégats*.

ÉTAPE 3 Sélectionnez un **nom du gestionnaire de strat. d'agrégats**, parmi les gestionnaires de stratégie précédemment créés afin d'afficher les statistiques correspondantes.

ÉTAPE 4 Cliquez sur **Appliquer**. Une demande de statistiques supplémentaire est créée et le commutateur est mis à jour.

Affichage des statistiques de file d'attente

Affichage des statistiques de file d'attente

La *rubrique Statistiques de file 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 *rubrique Statistiques de file d'attente* s'ouvre.

Cette page contient les champs suivants :

- **Jeu de compteurs** — Les options disponibles sont les suivantes :
  - *Jeu 1* — Affiche les statistiques du jeu 1, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) élevée.
  - *Jeu 2* — Affiche les statistiques du jeu 2, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) faible.
- **Interface** — Interface à laquelle correspondent les statistiques de file d'attente affichées.
- **File d'attente** — File d'attente d'où proviennent les paquets transférés ou éliminés, la file étant pleine (tail drop).
- **Priorité d'élimination** — Les paquets portant la priorité d'élimination la plus faible ont davantage de chances d'être conservés.
- **Nombre total de paquets** — Nombre de paquets transférés ou éliminés, la file étant pleine (tail drop).
- **Paquets éliminés** — Pourcentage de paquets éliminés, la file étant pleine (tail drop).

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter les statistiques de file d'attente* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **Jeu de compteurs** — Sélectionnez le jeu voulu :
  - *Jeu 1* — Affiche les statistiques du jeu 1, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) élevée.
  - *Jeu 2* — Affiche les statistiques du jeu 2, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) faible.
- **Interface** — Sélectionnez les ports auxquels correspondent les statistiques affichées. Les options disponibles 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 lequel 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 file d'attente est ajouté et le commutateur est mis à jour.

19

Configuration de SNMP

Ce chapitre décrit la fonctionnalité SNMP (Simple Network Management Protocol), qui fournit une méthode de gestion des unités de réseau.

Il contient les rubriques suivantes :

Versions et flux de travail SNMP

Le commutateur fonctionne comme un agent SNMP et prend en charge SNMP v1, v2 et v3. Il crée également des rapports sur les événements système pour les destinataires de trap, à l'aide des traps définis dans la base MIB qu'il prend en charge.

SNMP v1 et v2

SNMP v1 et v2

Pour contrôler l'accès au système, une liste d'entrées de communauté est définie. Chaque entrée de communauté est constituée d'une *chaîne de communauté* et de son privilège d'accès. Seuls les messages SNMP accompagnés d'une chaîne de communauté et d'une opération appropriées reçoivent une réponse du système.

Les agents SNMP maintiennent une liste de variables utilisées pour gérer le commutateur. Ces variables sont définies dans une *base d'informations de gestion* (MIB, Management Information Base). La base MIB présente les variables contrôlées par l'agent.

REMARQUE Le protocole SNMPv2 présente des vulnérabilités en matière de sécurité qui ont été identifiées. Il est recommandé d'utiliser SNMPv3.

SNMP v3

SNMP v3

En plus de la fonctionnalité fournie par SNMP v1 et v2, SNMP v3 applique un contrôle d'accès et de nouveaux mécanismes de trap aux PDU SNMPv1 et SNMPv2. SNMPv3 définit également un modèle de sécurité utilisateur (USM, User Security Model) qui inclut :

- **Authentification** : fournit une intégrité des données et une authentification de leur origine.
- **Confidentialité** : fournit une protection contre la divulgation du contenu des messages. *Cipher Block-Chaining* (CBC) est utilisé pour le cryptage. Soit l'authentification seule est activée sur un message SNMP, soit l'authentification et la confidentialité. Cependant, la confidentialité ne peut pas être activée sans authentification.
- **Actualité** : fournit une protection contre les retards de messages ou les attaques de lecture. L'agent SNMP compare l'horodatage du message entrant par rapport à l'heure d'arrivée du message.
- **Gestion de clés** : définit la génération, les mises à jour et l'utilisation des clés. Le commutateur prend en charge des filtres de notification SNMP basés sur des *ID d'objet* (OID). Les ID d'objet sont utilisés par le système pour gérer des fonctionnalités d'unité.

Flux de travail SNMP

Flux de travail SNMP

REMARQUE Par défaut, SNMP est désactivé pour le commutateur. Avant de pouvoir configurer SNMP, vous devez l'activer à l'aide de *Sécurité-> Services TCP/UDP.*

Ci-dessous figure une série d'actions recommandées pour la configuration de SNMP :

Si vous décidez d'utiliser SNMP v1 ou v2 :

Définissez une communauté à l'aide de la *rubrique Ajouter une communauté SNMP.* La communauté peut être associée à des droits d'accès et à un affichage en mode de base ou à un groupe en mode avancé. (Pour plus d'informations sur les modes de base et avancé, consultez la *rubrique Communautés*). Il existe deux méthodes pour définir des droits d'accès à une communauté :

- Mode de base : les droits d'accès d'une communauté peuvent être configurés par Lecture seule, Lecture écriture ou Admin SNMP. En outre, vous pouvez restreindre l'accès à la communauté à certains objets de la base MIB uniquement, à l'aide d'une vue. Les vues sont définies depuis la page Vues SNMP.
- Mode avancé : les droits d'accès à une communauté sont définis par un groupe. Vous pouvez configurer le groupe avec un modèle de sécurité spécifique. Les droits d'accès dans un groupe sont définis par un accès Lecture, Écriture et Notifier aux vues souhaitées. Les groupes sont définis depuis la page Groupes.

Si vous décidez d'utiliser SNMP v3 :

1. Définissez le moteur SNMP, une seule fois, à l'aide de la *rubrique ID de moteur.*
2. Si vous le souhaitez, définissez une plusieurs vues SNMP à l'aide de la *rubrique Vues SNMP.*
3. Définissez des groupes à l'aide de la *rubrique Groupes.*
4. Définissez des utilisateurs à l'aide de la *rubrique Utilisateurs SNMP,* à partir de laquelle ils peuvent être associés à un groupe.

Gestion de traps et de notifications pour SNMP v1, v2 ou v3 :

1. Activez ou désactivez des traps à l'aide de la *rubrique Paramètres d'interruption.*
2. Vous pouvez éventuellement définir un ou plusieurs filtres de notification avec la *rubrique Filtre de notification.*
3. Définissez un ou plusieurs destinataires de notification avec la *rubrique Destinataires de notification SNMPv1,2* et/ou la *rubrique Destinataires de notification SNMPv3*, respectivement.

Bases MIB activées

Les bases MIB standard suivantes sont activées :

- CISCO-CDP-MIB.mib
- CISCO-SMI.mib
- CISCO-TC.mib
- CISCO-VTP-MIB.mib
- diffserv.mib
- draft-ietf-bridge-8021x.mib
- draft-ietf-bridge-rstpmib-04.mib
- draft-ietf-entmib-sensor-mib.mib
- draft-ietf-hubmib-etherif-mib-v3-00.mib
- draft-ietf-syslog-device-mib.mib
- ianaaddrfamnumbers.mib
- ianaifty.mib
- ianaprot.mib
- inet-address-mib.mib
- ip-forward-mib.mib
- ip-mib.mib
- lldp.mib
- p-bridge-mib.mib
- q-bridge-mib.mib
- RFC-1212.mib
- rfc1213.mib
- rfc1389.mib
- rfc1493.mib
- rfc1611.mib
- rfc1612.mib

- rfc1757.mib
- rfc1850.mib
- rfc1907.mib
- rfc2011.mib
- rfc2012.mib
- rfc2013.mib
- rfc2096.mib
- rfc2233.mib
- rfc2571.mib
- rfc2572.mib
- rfc2573.mib
- rfc2574.mib
- rfc2575.mib
- rfc2576.mib
- rfc2613.mib
- rfc2618.mib
- rfc2620.mib
- rfc2665.mib
- rfc2668.mib
- rfc2674.mib
- rfc2737.mib
- rfc2851.mib
- rfc2925.mib
- rfc3621.mib
- rfc4668.mib
- rfc4670.mib
- rmon2.mib

- SNMPv2-CONF.mib
- SNMPv2-SMI.mib
- SNMPv2-TC.mib
- trunk.mib
- udp-mib.mib

ID d'objet du modèle

Ci-dessous figurent les *ID d'objet* (OID) du modèle de commutateur :

Nom du modèle	Description	Ports	ID d'objet
SG 300-10	Commutateur géré Gigabit à 10 ports	g1-g10	9.6.1.83.10.1
SG 300-10MP	Commutateur géré PoE Gigabit à 10 ports	g1-g10	9.6.1.83.10.3
SG 300-10P	Commutateur géré PoE Gigabit à 10 ports	g1-g10	9.6.1.83.10.2
SG 300-20	Commutateur géré Gigabit à 20 ports	g1-g20	9.6.1.83.20.1
SG 300-28	Commutateur géré Gigabit à 28 ports	g1-g28	9.6.1.83.28.1
SG 300-28P	Commutateur géré PoE Gigabit à 28 ports	g1-g28	9.6.1.83.28.2
SG 300-52	Commutateur géré Gigabit à 52 ports	g1-g52	9.6.1.83.52.1
SF 300-08	Commutateur géré 10/100 à huit ports	e1-e8	9.6.1.82.08.4
SF 302-08	Commutateur géré 10/100 à huit ports	e1-e8, g1-g2	9.6.1.82.08.1
SF 302-08MP	Commutateur géré PoE 10/100 à huit ports	e1-e8, g1-g2	9.6.1.82.08.3

Nom du modèle	Description	Ports	ID d'objet
SF 302-08P	Commutateur géré PoE 10/100 à huit ports	e1-e8, g1-g2	9.6.1.82.08.2
SF 300-24	Commutateur géré 10/100 à 24 ports	e1-e24, g1-g4	9.6.1.82.24.1
SF 300-24P	Commutateur géré PoE 10/100 à 24 ports	e1-e24, g1-g4	9.6.1.82.24.2
SF 300-48	Commutateur géré 10/100 à 48 ports	e1-e48, g1-g4	9.6.1.82.48.1
SF 300-48P	Commutateur géré PoE 10/100 à 48 ports	e1-e48, g1-g4	9.6.1.82.48.2

Les ID d'objet se trouvent dans : enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1).

La racine de la MIB (base d'informations de gestion) est 1.3.6.1.4.1.9.6.1.101.

ID de moteur SNMP

L'ID de moteur est uniquement utilisé par des entités SNMPv3 afin de les identifier de façon unique. Un agent SNMP est considéré comme un moteur SNMP faisant autorité. Cela signifie que l'agent répond aux messages entrants (Get, GetNext, GetBulk, Set) et qu'il envoie des messages Trap à un gestionnaire. Les informations locales de l'agent sont encapsulées dans des champs au sein du message.

Chaque agent SNMP conserve des informations locales utilisées dans des échanges de messages SNMPv3 (ne s'applique pas à SNMPv1 ou SNMPv2). L'ID de moteur SNMP par défaut est constitué du numéro d'entreprise et de l'adresse MAC par défaut. L'ID de moteur SNMP doit être unique pour le domaine d'administration afin que deux unités dans un réseau ne possèdent pas le même ID de moteur.

Les informations locales sont stockées dans quatre variables MIB en lecture-seule (snmpEngineId, snmpEngineBoots, snmpEngineTime et snmpEngineMaxMessageSize).

ATTENTION Lorsque l'ID de moteur est modifié, tous les utilisateurs et groupes configurés sont effacés.

Pour définir l'ID de moteur SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **ID de moteur**. La *rubrique ID de moteur* s'ouvre.

ÉTAPE 2 Sélectionnez l'**ID de moteur local**.

- **Valeurs par défaut** : sélectionnez cette option pour utiliser l'ID de moteur généré par l'unité. L'ID de moteur par défaut se base sur l'adresse MAC du commutateur et est défini de manière standard par :
  - *4 premiers octets* : premier bit = 1, le reste correspond au numéro d'entreprise IANA.
  - *Cinquième octet* : défini à l'aide de la valeur 3 pour indiquer l'adresse MAC qui suit.
  - *6 derniers octets* : adresse MAC du commutateur.
- **Aucun** : aucun ID de moteur n'est utilisé.
- **Défini par l'utilisateur** : saisissez l'ID de moteur de l'unité locale. La valeur du champ est une chaîne hexadécimale **(plage : 10 - 64)**. Chaque octet dans les chaînes de caractères hexadécimales est représenté par deux chiffres hexadécimaux. Chaque octet peut être séparé par un point ou deux points.

ÉTAPE 3 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

Configuration de vues SNMP

Une vue est une étiquette définie par l'utilisateur pour une collecte de sous-arborescences MIB. Chaque ID de sous-arborescence est défini par l'*ID d'objet* (OID) de la racine des sous-arborescences concernées. Dans des cas extrêmes, cette sous-arborescence peut être uniquement constituée d'un noeud terminal. Des noms célèbres peuvent être utilisés pour spécifier la racine de la sous-arborescence souhaitée ou un ID d'objet peut être saisi (voir *ID d'objet du modèle*).

Chaque sous-arborescence est soit incluse, soit exclue dans la vue en cours de définition.

La *rubrique Vues SNMP* active la création et la modification de vues SNMP. Les vues par défaut (Default, DefaultSuper) ne peuvent pas être modifiées.

Des vues peuvent être jointes à des groupes dans la *rubrique Groupes*.

Pour définir des vues SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Vues**. La *rubrique Vues SNMP* s'ouvre.

ÉTAPE 2 Sélectionnez les vues définies par l'utilisateur à partir de la liste **Filtre : Nom de la vue**. Les vues suivantes existent par défaut :

- **Default** : vue SNMP par défaut pour les vues en lecture et en lecture/écriture.
- **DefaultSuper** : vue SNMP par défaut pour les vues d'administrateur.

D'autres vues peuvent être ajoutées.

- **Sous-arborescence d'ID d'objet** : affiche la sous-arborescence à inclure ou exclure de la vue SNMP.
- **Vue de sous-arborescence d'ID d'objet** : indique si la sous-arborescence définie est incluse ou exclue dans la vue SNMP sélectionnée.

ÉTAPE 3 Cliquez sur **Ajouter** pour définir de nouvelles vues. La *rubrique Ajouter une vue* s'ouvre.

ÉTAPE 4 Saisissez les paramètres.

- **Nom de la vue** : saisissez un nom de vue.
- **Sous-arborescence d'ID d'objet** : sélectionnez le nœud dans l'arborescence de la base MIB qui est inclus ou exclu dans le filtre de notification sélectionné. Les options pour sélectionner l'objet se présentent comme suit :
  - *Sélectionner dans la liste* : vous permet de naviguer dans l'arborescence MIB. Appuyez sur la touche *Haut* pour accéder au niveau du père et de la fratrie du nœud sélectionné ; appuyez sur la touche *Bas* pour descendre vers le niveau des descendants du nœud sélectionné. Cliquez sur des nœuds dans la vue pour passer d'un nœud à son frère. Utilisez la barre de défilement pour faire apparaître les fratries dans une vue.
  - *Défini par l'utilisateur* : saisissez un ID d'objet qui n'est pas proposé dans l'option *Sélectionner dans la liste* (le cas échéant). Tous les descendants de ce nœud sont inclus ou exclus dans le filtre.

ÉTAPE 5 Sélectionnez ou désélectionnez **Inclure dans la vue.**

- En cas d'utilisation de *Sélectionner dans la liste*, l'**identificateur d'objet du nœud sélectionné** est inclus dans la vue ou exclus de celle-ci, selon que l'option **Inclure dans la vue** est sélectionnée ou pas.

- En cas d'utilisation de *Défini par l'utilisateur*, l'**identificateur d'objet saisi** est inclus dans la vue ou exclus de celle-ci, selon que l'option **Inclure dans la vue** est sélectionnée ou pas.

ÉTAPE 6 Cliquez sur **Appliquer**. En cas d'utilisation de *Sélectionner dans la liste*, l'identificateur d'objet du nœud sélectionné est inclus dans la vue ou exclus de celle-ci, selon que l'option **Inclure dans la vue** soit ou non sélectionnée.

En cas d'utilisation d'**ID d'objet**, l'identificateur d'objet saisi est inclus dans la vue ou exclus de celle-ci, selon que l'option **Inclure dans la vue** soit ou non sélectionnée. Cela signifie que le nœud et tous ses descendants sont inclus dans la vue ou exclus de celle-ci. Les vues SNMP sont définies et le commutateur est mis à jour.

Création de groupes SNMP

Dans SNMPv1 et SNMPv2, une chaîne de communauté est envoyée accompagnée des trames SNMP. La chaîne de communauté agit en tant que mot de passe pour accéder à un agent SNMP. Cependant, ni les trames, ni la chaîne de communauté ne sont cryptées. Par conséquent, SNMPv1 et SNMPv2 ne sont pas sécurisés. Deux mécanismes de sécurité existent dans SNMPv3. Ils peuvent tous deux être configurés.

- Authentification : le commutateur vérifie que l'utilisateur SNMP est un administrateur système autorisé. Cette opération est effectuée pour chaque trame.
- Confidentialité : les trames SNMP peuvent accueillir des données cryptées.

Ainsi, dans SNMPv3, il existe trois niveaux de sécurité :

- Aucune sécurité
- Authentification
- Authentification et confidentialité (notez que deux groupes du même nom, l'un avec l'authentification et l'autre avec la confidentialité, doivent être ajoutés).

En outre, en associant chaque utilisateur à un groupe, SNMPv3 fournit un moyen de contrôler ce que les utilisateurs - même autorisés et authentifiés - peuvent afficher et effectuer.

Un groupe est une étiquette pour une entité logique (combinaison d'attributs). Un groupe est opérationnel uniquement lorsqu'il est associé avec un utilisateur SNMP ou une communauté SNMP.

Un groupe possède également un attribut qui indique si des membres doivent disposer d'un accès en lecture, en écriture et/ou de privilèges de notification pour l'affichage.

Pour créer un groupe SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Groupes**. La *rubrique Groupes* s'ouvre.

Cette page affiche les groupes SNMP existants.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un groupe* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **Nom du groupe** : saisissez un nom de nouveau groupe pour lequel des privilèges sont définis. La plage du champ peut atteindre 30 caractères ASCII.
- **Modèle de sécurité** : sélectionnez la version SNMP jointe au groupe.
- **Niveau de sécurité** : définissez le niveau de sécurité joint au groupe. Les niveaux de sécurité s'appliquent à SNMPv3 uniquement.
  - *Aucune authentification* : les niveaux de sécurité Authentification ou Confidentialité ne sont pas affectés au groupe.
  - *Authentification* : authentifie les messages SNMP et s'assure que l'origine du message SNMP est authentifiée. Cependant, elle ne les crypte pas, ils peuvent donc être interceptés et lus.
  - *Confidentialité* : cryptage des messages SNMP.
- **Vues** : définissez des droits d'accès au groupe par groupe. Les options disponibles sont les suivantes :
  - *Lecture* : l'accès à la gestion est en lecture seule pour la vue sélectionnée. Sinon, un utilisateur ou une communauté associé à ce groupe peut lire toutes les bases MIB, à l'exception des MIB qui contrôlent le SNMP même.
  - *Ecriture* : l'accès à la gestion est en écriture pour la vue sélectionnée. Sinon, un utilisateur ou une communauté associé(e) à ce groupe peut écrire sur toutes les bases MIB, à l'exception des MIB qui contrôlent le SNMP lui-même.
  - *Notifier* : envoie uniquement des traps avec du contenu inclus dans la vue SNMP sélectionnée pour une notification. Sinon, il n'existe aucune restriction sur le contenu des traps. Cette option peut être sélectionnée pour SNMP v3 uniquement.

ÉTAPE 4 Cliquez sur **Appliquer**. Le groupe SNMP est défini et le commutateur est mis à jour.

Création d'utilisateurs SNMP

Un utilisateur SNMP est défini par les informations de connexion (nom d'utilisateur, mots de passe et méthode d'authentification), ainsi que par le contexte et l'étendue de son fonctionnement en association avec un groupe et un ID de moteur.

Une fois qu'un utilisateur a été authentifié, il hérite des attributs de ce groupe Il est ensuite en mesure d'apercevoir ou pas les vues associées à ce groupe.

La *rubrique Utilisateurs SNMP* autorise la création d'utilisateurs SNMPv3. Un utilisateur SNMPv3 constitue la combinaison entre un utilisateur et une méthode qui servent à authentifier l'utilisateur et un mot de passe. Les informations de connexion de l'utilisateur SNMP sont vérifiées à l'aide de la base de données locale.

Les groupes permettent aux gestionnaires de réseaux d'affecter des droits d'accès à des fonctionnalités spécifiques ou à des aspects de fonctionnalités à la totalité d'un groupe d'utilisateurs plutôt qu'à un utilisateur unique.

Un utilisateur peut-être uniquement membre d'un seul groupe.

Pour créer un utilisateur SNMPv3, les éléments ci-dessous doivent exister au préalable :

- Un ID de moteur doit d'abord être configuré sur le commutateur. Cette opération peut être effectuée à partir de la *rubrique ID de moteur*.
- Un groupe SNMPv3 doit être disponible. Un groupe SNMPv3 peut être défini à partir de la *rubrique Groupes*.

Les utilisateurs SNMP ne sont pas enregistrés dans le fichier de configuration pour des raisons de sécurité. En cas d'approvisionnement d'utilisateurs SNMP et d'enregistrement de la configuration, les utilisateurs SNMP ne sont pas conservés ; vous devez les saisir à nouveau manuellement.

Pour afficher des utilisateurs SNMP et en définir de nouveaux :

ÉTAPE 1 Cliquez sur **SNMP** > **Utilisateurs**. La *rubrique Utilisateurs SNMP* s'ouvre.

Cette page affiche les utilisateurs existants.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un utilisateur* s'ouvre.

Cette page fournit des informations quant à l'affectation de privilèges de contrôle d'accès SNMP à des utilisateurs SNMP.

ÉTAPE 3 Saisissez les paramètres.

- **Nom d'utilisateur** : saisissez un nom d'utilisateur.
- **ID de moteur** : sélectionnez l'entité SNMP locale ou distante à laquelle l'utilisateur est connecté. La modification ou la suppression de l'ID de moteur SNMP local supprime la base de données d'utilisateurs SNMPv3. Pour recevoir des informations et des informations de demande, vous devez définir un utilisateur local et un utilisateur distant.
  - *Local* : l'utilisateur est connecté à une entité SNMP locale. L'utilisateur peut demander des informations mais il ne reçoit aucun message d'information.
  - *Distant* : l'utilisateur est connecté à une entité SNMP distante. Si un ID de moteur distant est défini, les unités distantes reçoivent des messages d'information, mais ne peuvent effectuer de demandes d'information.

    Saisissez l'ID de moteur distant.
- **Nom du groupe** : sélectionnez les groupes SNMP auxquels appartient l'utilisateur SNMP. Les groupes SNMP sont définis depuis la *rubrique Ajouter un groupe*.
- **Méthode d'authentification** : sélectionnez la méthode d'authentification. Les options disponibles sont les suivantes :
  - *Aucune* : aucune authentification d'utilisateur n'est utilisée.
  - *Mot de passe MD5* : les utilisateurs doivent saisir un mot de passe crypté, à l'aide de la méthode d'authentification MD5.
  - *Mot de passe SHA* : les utilisateurs doivent saisir un mot de passe crypté, à l'aide de la méthode d'authentification SHA (Secure Hash Algorithm).
  - *Clé MD5* : les utilisateurs sont authentifiés à l'aide d'une clé MD5 valide.
  - *Clé SHA* : les utilisateurs sont authentifiés à l'aide d'une SHA valide.
- **Mot de passe** : si l'authentification est accomplie via un mot de passe MD5 ou SHA, saisissez le mot de passe de l'utilisateur local. Les mots de passe d'utilisateur local sont comparés à la base de données locale et peuvent contenir jusqu'à 32 caractères ASCII.

- **Clé d'authentification** : si la méthode d'authentification correspond à une clé MD5 ou SHA, saisissez la clé d'authentification MD5 ou SHA. Si la clé MD5 est sélectionnée, 16 octets sont requis. Si la clé SHA est sélectionnée, 20 octets sont requis.
- **Clé de confidentialité** : si la méthode d'authentification correspond à une clé MD5 ou SHA, saisissez la clé de confidentialité MD5 ou SHA. Si la clé MD5 est sélectionnée, 16 octets sont requis. Si la clé SHA est sélectionnée, 20 octets sont requis.

ÉTAPE 4 Cliquez sur **Appliquer**. Le commutateur est mis à jour.

Définition de communautés SNMP

Les droits d'accès dans SNMPv1 et SNMPv2 sont gérés en définissant des communautés à partir de la *rubrique Communautés*. Le nom de la communauté correspond à un type de mot de passe partagé entre la station de gestion SNMP et l'unité. Il sert à authentifier la station de gestion SNMP.

Les communautés sont définies uniquement dans SNMPv1 et v2 car SNMP v3 fonctionne avec des utilisateurs et non avec des communautés. Les utilisateurs appartiennent à des groupes qui disposent de droits d'accès qui leur sont affectés.

La *rubrique Communautés* associe des communautés à des droits d'accès, soit directement (mode de base), soit via des groupes (mode avancé) :

- Mode de base : les droits d'accès d'une communauté peuvent être configurés par Lecture seule, Lecture écriture ou Admin SNMP. En outre, vous pouvez restreindre l'accès à la communauté à uniquement certains objets de la base MIB à l'aide d'une vue. Les vues sont définies à partir de la page Vues SNMP.
- Mode avancé : les droits d'accès à une communauté sont définis par un groupe. Vous pouvez configurer le groupe avec un modèle de sécurité spécifique. Les droits d'accès à un groupe sont définis par un accès Lecture, Écriture et Notifier aux vues souhaitées. Les groupes sont définis à partir de la rubrique Vues SNMP.

Pour définir des communautés SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Communautés**. La *rubrique Communautés* s'ouvre.

Cette page affiche les tableaux de base et avancé.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter une communauté SNMP* s'ouvre.

Cette page permet aux gestionnaires de réseaux de définir et de configurer de nouvelles communautés SNMP.

ÉTAPE 3 **Station de gestion SNMP** : cliquez sur **Défini par l'utilisateur** pour saisir l'adresse IP de la station de gestion qui peut accéder à la communauté SNMP. Sinon, cliquez sur **Toutes**, afin d'indiquer que n'importe quelle unité IP peut accéder à la communauté SNMP.

- **Version IP** : sélectionnez IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 pris en charge, en cas d'utilisation d'IPv6). Les options disponibles sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière unique l'hôte situé sur une seule liaison réseau. Une adresse locale de liaison possède le préfixe **FE80**, ne peut être routée et ne peut uniquement servir qu'à la communication sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette entrée remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type IPV6 de monodiffusion globale, visible et joignable depuis d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, sélectionnez si la réception s'effectue via VLAN2 ou ISATAP.
- **Adresse IP** : saisissez l'adresse IPv4 de la station de gestion SNMP.
- **Chaîne de communauté** : saisissez le nom de la communauté (mot de passe) servant à authentifier la station de gestion auprès de l'unité.
- **De base** : sélectionnez ce mode pour une communauté spécifique. Avec ce mode, aucune connexion n'est établie avec quelque groupe que ce soit. Vous pouvez uniquement choisir le niveau d'accès de la communauté (lecture seule, lecture écriture ou administration) et, facultativement, le faire davantage correspondre à une vue. Par défaut, cela s'applique à la totalité d'une base MIB. Si cette option est sélectionnée, saisissez les champs suivants :

- *Mode d'accès* : sélectionnez les droits d'accès de la communauté. Les options disponibles sont les suivantes :

  Lecture seule — L'accès à la gestion est restreint à la lecture seule. Aucune modification ne peut être apportée à la communauté.

  Lecture/écriture — L'accès à la gestion est en lecture/écriture. Des modifications peuvent être apportées qu'à la configuration d'unité, pas à la communauté.

  Admin SNMP — L'utilisateur dispose d'un accès à toutes les options de configuration d'unité ainsi qu'aux autorisations de modification de la communauté. Admin équivaut à la lecture/écriture pour toutes les bases MIB, à l'exception des bases MIB SNMP. Admin est requis pour l'accès aux bases MIB SNMP.

- *Nom de la vue* : sélectionnez une vue SNMP (collecte de sous-arborescences de bases MIB auxquelles un accès est accordé).

▪ **Avancé** : sélectionnez ce mode pour une communauté spécifique.

- *Nom du groupe* : sélectionnez un groupe SNMP qui détermine les droits d'accès.

ÉTAPE 4 Cliquez sur **Appliquer**. La communauté SNMP est définie et le commutateur mis à jour.

Définition de paramètres de messages « trap »

La *rubrique Paramètres d'interruption* permet de configurer si des notifications SNMP sont envoyées à partir du commutateur et à quelles conditions. Les destinataires des notifications SNMP peuvent être configurés à partir de la *rubrique Destinataires de notification SNMPv1,2* ou de la *rubrique Destinataires de notification SNMPv3*.

Pour définir des paramètres de messages « trap » :

ÉTAPE 1 Cliquez sur **SNMP** > **Paramètres de messages « trap »**. La *rubrique Paramètres d'interruption* s'ouvre.

ÉTAPE 2 Sélectionnez **Activer** pour **Notifications SNMP** pour spécifier que le commutateur peut envoyer des notifications SNMP.

ÉTAPE 3 Sélectionnez **Activer** pour **Notifications d'authentification** pour activer la notification d'échec d'authentification SNMP.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres des messages « trap » SNMP sont définis et le commutateur est mis à jour.

Destinataires de notifications

Des messages « trap » sont générés pour signaler des événements système, tels que définis dans la RFC 1215. Le système peut générer des messages « trap » définis dans la base MIB qu'il prend en charge.

Les destinations du trap (connus sous le nom de destinataires de notification) sont des nœuds réseau où des messages « trap » sont envoyés par le commutateur. Plusieurs destinations du trap sont définies dans une liste en tant que cibles de messages « trap ».

Une entrée de destination du trap contient l'adresse IP du nœud et les informations SNMP qui correspondent à la version qui doit être incluse dans le message du trap. Lorsqu'un événement se présente et nécessite l'envoi d'un message du trap, il est envoyé vers chaque nœud répertorié dans la liste de destinations du trap.

La *rubrique Destinataires de notification SNMPv1,2* et la *rubrique Destinataires de notification SNMPv3* permettent la configuration de la destination d'envoi de notifications SNMP ainsi que les types des notifications SNMP qui sont envoyés vers chaque destination (traps ou informations). Les messages contextuels *Ajouter/Modifier* permettent la configuration des attributs des notifications.

Une notification SNMP est un message envoyé depuis le commutateur vers la station de gestion SNMP qui indique qu'un événement spécifique s'est produit, tel que l'activation/la désactivation d'une liaison.

Vous pouvez également filtrer certaines notifications. Pour cela, vous pouvez créer un filtre dans la *rubrique Filtre de notification* et le joindre à un destinataire de notification SNMP. Le filtre de notification permet le filtrage du type des notifications SNMP envoyées à la station de gestion, en fonction de l'ID d'objet de la notification sur le point d'être envoyée.

Définition de destinataires de notifications SNMPv1.2

Pour définir un destinataire dans SNMPv1.2 :

ÉTAPE 1 Cliquez sur **SNMP** > **Destinataires de notification SNMPv1.2**. La *rubrique Destinataires de notification SNMPv1,2* s'ouvre.

Cette page affiche les destinataires pour SNMPv1.2.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un destinataire de notification SNMP* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **Version IP** : sélectionnez IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez soit *Liaison locale*, soit *Global*.
  - *Liaison locale* : l'adresse IPv6 identifie de manière unique l'hôte situé sur une seule liaison réseau. Une adresse locale de liaison possède le préfixe **FE80**, ne peut être routée et ne peut uniquement servir qu'à la communication sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette entrée remplace l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type IPV6 de monodiffusion globale, visible et joignable depuis d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, sélectionnez si la réception s'effectue via VLAN2 ou ISATAP.
- **Adresse IP du destinataire** : saisissez l'adresse IP vers laquelle les traps sont envoyées.
- **Port UDP** : saisissez le port UDP utilisé pour les notifications sur l'unité du destinataire.
- **Chaîne de communauté** : saisissez la chaîne de communauté du gestionnaire des traps.
- **Type de notification** : indiquez le type de données à envoyer (Traps ou Informations). Si les deux sont nécessaires, deux destinataires doivent être créés.
- **Version de notification** : sélectionnez la version SNMP du trap.

  SNMPv1 ou SNMPv2 peut être utilisé en tant que version des traps une seule version ne pouvant être activée à la fois.

- **Filtre de notification** : sélectionnez si activer le filtrage du type des notifications SNMP transmises à la station de gestion. Les filtres sont créés à partir de la *rubrique Filtre de notification*.
- **Nom du filtre** : sélectionnez le filtre SNMP qui définit les informations contenues dans des traps (définies dans la *rubrique Filtre de notification*).
- **Délai d'expiration (informations)** : saisissez le nombre de secondes d'attente de l'unité avant de renvoyer des informations. Période : 1-300, par défaut : 15.
- **Tentatives d'envoi (informations)** : saisissez le nombre de fois où l'unité renvoie une demande d'information. Plage de nouvelles tentatives : 1 à 255, par défaut: 3

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres de destinataire de notification SNMP sont définis et le commutateur est mis à jour.

Définition de destinataires de notifications SNMPv3

Pour définir un destinataire dans SNMPv3 :

ÉTAPE 1 Cliquez sur **SNMP** > **Destinataires de notification SNMPv3**. La *rubrique Destinataires de notification SNMPv3* s'ouvre.

Cette page affiche les destinataires pour SNMPv3.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un destinataire de notification SNMP* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **Version IP** : sélectionnez IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options disponibles sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière unique l'hôte situé sur une seule liaison réseau. 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 entrée remplace l'adresse dans la configuration.

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

- **Interface de liaison locale** : sélectionnez dans la liste de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée).
- **Adresse IP du destinataire** : saisissez l'adresse IP vers laquelle les traps sont envoyées.
- **Port UDP** : saisissez le port UDP utilisé pour les notifications sur l'unité du destinataire.
- **Nom d'utilisateur** : saisissez l'utilisateur vers lequel sont envoyées les notifications SNMP.
- **Niveau de sécurité** : sélectionnez le niveau d'authentification appliqué au paquet. Les options disponibles sont les suivantes :
  - *Aucune authentification* : indique que le paquet n'est jamais authentifié ni crypté.
  - *Authentification* : indique que le paquet est authentifié mais pas crypté.
  - *Confidentialité* : indique que le paquet est à la fois authentifié et crypté.
- **Type de notification** : indiquez le type de données à envoyer (Traps ou Informations). Si les deux sont nécessaires, deux destinataires doivent être créés.
- **Filtre de notification** : sélectionnez si activer le filtrage du type des notifications SNMP transmises à la station de gestion. Les filtres sont créés à partir de la *rubrique Filtre de notification*.
- **Nom du filtre** : sélectionnez le filtre SNMP qui définit les informations contenues dans des traps (définies dans la *rubrique Filtre de notification*).
- **Délai d'expiration (informations)** : saisissez la durée (en secondes) d'attente de l'unité avant de renvoyer des informations/traps. Expiration : plage de 1 à 300, par défaut :
- **Tentatives d'envoi (informations)** : saisissez le nombre de fois où l'unité renvoie une demande d'information. Tentatives : plage de 1 à 255, 3 par défaut

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres de destinataire de notification SNMP sont définis et le commutateur est mis à jour.

Filtres de notification SNMP

La *rubrique Filtre de notification* permet la configuration de filtres de notification SNMP et d'ID d'objets qui ont été vérifiés. Après la création d'un filtre de notification, il est possible de le joindre à un destinataire de notification depuis la *rubrique Destinataires de notification SNMPv1,2* et la rubrique *Destinataires de notifications SNMPv3*.

Le filtre de notification permet le filtrage du type des notifications SNMP envoyées à la station de gestion, en fonction de l'ID d'objet de la notification à envoyer.

Pour définir un filtre de notification :

ÉTAPE 1 Cliquez sur **SNMP** > **Filtre de notification**. La *rubrique Filtre de notification* s'ouvre.

La *rubrique Filtre de notification* affiche les informations de notification pour chaque filtre. Ce tableau peut filtrer des entrées de notification par nom de filtre.

ÉTAPE 2 Cliquez sur **Ajouter**. La *rubrique Ajouter un filtre de notification* s'ouvre.

ÉTAPE 3 Saisissez les paramètres.

- **Nom du filtre** : saisissez un nom.
- **Sous-arborescence d'ID d'objet** : sélectionnez le nœud dans l'arborescence de la base MIB qui est inclus ou exclus dans la vue SNMP sélectionnée. Les options disponibles sont les suivantes :
  - *Sélectionner dans la liste* : vous permet de naviguer dans l'arborescence MIB. Cliquez sur *Haut* pour accéder au niveau du père et de la fratrie du nœud sélectionné. Cliquez sur *Bas* pour accéder au niveau des descendants du nœud sélectionné. Cliquez sur les nœuds dans la vue pour passer d'un nœud à son frère. Utilisez la barre de défilement pour faire apparaître les fratries dans une vue.
  - *ID d'objet* : saisissez un ID d'objet qui n'est pas proposé dans l'option *Sélectionner dans la liste* (le cas échéant). Tous les descendants de ce nœud sont inclus ou exclus dans la vue.
  - En cas d'utilisation de *Sélectionner dans la liste*, l'**identificateur d'objet du nœud sélectionné** est inclus dans le filtre de notification ou exclu de celui-ci, selon que l'option **Inclure dans le filtre** est sélectionnée ou non.
  - En cas d'utilisation d'*ID d'objet*, l'**identificateur d'objet saisi** est inclus dans la vue ou exclus de celle-ci, selon que l'option **Inclure dans le filtre** est sélectionnée ou non.

- **Inclure dans le filtre** : en cas d'utilisation de *Sélectionner dans la liste*, l'identificateur d'objet du nœud sélectionné est inclus dans le filtre de notification ou exclus de celui-ci, selon que l'option **Inclure dans le filtre** est sélectionnée ou non. En cas d'utilisation d'**ID d'objet**, l'identificateur d'objet saisi est inclus dans le filtre de notification ou exclus de celui-ci, selon que l'option **Inclure dans le filtre** est sélectionnée ou non. Cela signifie que le nœud est tous ses descendants sont inclus dans le filtre de notification ou exclus de celui-ci.

ÉTAPE 4 Cliquez sur **Appliquer**. Les filtres de notification SNMP sont définis et le commutateur est mis à jour.

20

Interface de la console

Le commutateur fournit une interface console basée sur des menus pour la configuration de base du commutateur. Cette interface console est utile pour la configuration du commutateur lorsque :

- le commutateur ne dispose pas d'une adresse IP définie, l'adresse IP est inconnue ou seule une connexion directe via un câble série peut être utilisée pour communiquer avec le commutateur ;
- vous devez configurer des fonctions - comme le certificat SSL/SSH - qui ne peuvent pas être gérées via l'utilitaire Web de configuration du commutateur.

Vous pouvez établir une connexion entre le commutateur et votre PC à l'aide d'un câble série, en établissant une session Telnet ou en utilisant une application d'émulation de terminal.

Ce chapitre englobe les rubriques suivantes :

- **Connexion à l'aide d'une application d'émulation de terminal**
- **Connexion via Telnet**
- **Navigation dans le menu de configuration de la console**
- **Menu principal de l'interface de console**

Connexion à l'aide d'une application d'émulation de terminal

Pour établir une connexion avec l'interface console en utilisant une application d'émulation de terminal (Microsoft HyperTerminal sous Windows XP est utilisé ici à titre d'exemple), configurez l'application comme suit :

ÉTAPE 1 Sur le bureau du PC, cliquez sur le bouton **Démarrer**.

ÉTAPE 2 Sélectionnez **Programmes** > **Accessoires** > **Communications** > **HyperTerminal**. La fenêtre HyperTerminal - Connection Description s'affiche.

ÉTAPE 3 Saisissez un nom pour cette connexion et sélectionnez si vous le souhaitez une icône pour le raccourci d'application créé.

ÉTAPE 4 Cliquez sur **OK**. La fenêtre Connexion s'affiche.

ÉTAPE 5 Si vous avez connecté le commutateur à l'aide d'un câble série, sélectionnez le port COM qui relie votre PC au commutateur dans la liste déroulante Se connecter en utilisant. Sinon, sélectionnez **TCP/IP**.

ÉTAPE 6 Passez à la section **« Communication via une connexion avec câble série »** ou **« Communication via une connexion TCP/IP »**.

Communication via une connexion avec câble série

Dans cette procédure, Com 1 est utilisé comme exemple. Le paramètre utilisé sur votre système peut être différent.

Pour afficher le menu de la console :

ÉTAPE 1 Configurez les **Propriétés de COM1** > **Paramètres du port** en indiquant les paramètres de connexion suivants :

- Bits par seconde = 115200
- Bits de données = 8
- Parité = Aucun
- Bits d'arrêt = 1
- Contrôle de flux = Aucun

ÉTAPE 2 Cliquez sur **OK**. La fenêtre HyperTerminal s'affiche.

ÉTAPE 3 Dans la fenêtre HyperTerminal, appuyez une ou deux fois sur **Entrée** jusqu'à ce que le menu de connexion s'affiche. Appuyez sur **Ctrl-R** pour actualiser l'écran CLI Login (connexion de l'interface de ligne de commande) ou accédez à cet écran à partir d'une autre fenêtre .

ÉTAPE 4 Saisissez **cisco** (par défaut) en tant que User Name (nom d'utilisateur).

ÉTAPE 5 Saisissez le mot de passe **cisco** (par défaut).

ÉTAPE 6 Appuyez sur **Enter** (Entrée).

REMARQUE S'il s'agit de votre première ouverture de session ou si les paramètres par défaut du commutateur ont été réinitialisés, vous êtes invité(e) à modifier votre mot de passe. (Consultez la section **Paramètres de nom d'utilisateur et de mot de passe** afin d'apprendre comment créer et enregistrer un nouveau mot de passe.)

ÉTAPE 7 Sélectionnez **Execute** (Exécuter) ou appuyez sur Entrée. L'écran *Switch Main Menu* (Menu principal du commutateur) s'affiche.

ÉTAPE 8 Passez à la section **Menu principal de l'interface de console**.

Communication via une connexion TCP/IP

On suppose que vous avez sélectionné TCP/IP dans l'application d'émulation de terminal.

REMARQUE Telnet doit être activé sur le commutateur.

Pour afficher le menu de la console :

ÉTAPE 1 Saisissez l'adresse IP du commutateur dans le champ Host Address (Adresse de l'hôte).

ÉTAPE 2 Cliquez sur **OK**. L'émulation de terminal s'affiche.

ÉTAPE 3 Appuyez une ou deux fois sur **Entrée** jusqu'à ce que le menu de connexion (Login) s'affiche. Appuyez sur **Ctrl-R** pour actualiser l'écran CLI Login (connexion de l'interface de ligne de commande) ou accédez à cet écran à partir d'une autre fenêtre.

ÉTAPE 4 Sélectionnez Edit (Modifier) afin de rendre une modification des paramètres possible .

ÉTAPE 5 Saisissez **cisco** (par défaut) en tant que User Name (nom d'utilisateur) .

ÉTAPE 6 Saisissez le username (mot de passe) cisco (par défaut).

ÉTAPE 7 Appuyez sur **Enter** (Entrée).

REMARQUE S'il s'agit de votre première ouverture de session ou si les paramètres par défaut du commutateur ont été réinitialisés, vous êtes invité(e) à modifier votre mot de passe. L'écran Modification du mot de passe utilisateur s'affiche. Utilisez ces options pour créer et enregistrer un nouveau mot de passe. Consultez **« Modification du mot de passe utilisateur »** à la **page 321**.

L'écran *Menu principal du commutateur* s'affiche.

ÉTAPE 8 Passez à la section **Menu principal de l'interface de console**.

Connexion via Telnet

Telnet est désactivé par défaut Vous devez l'activer en utilisant l'utilitaire Web de configuration du commutateur ou l'interface console et une connexion via un câble série. La procédure d'activation de Telnet via l'interface console est décrite dans la section **Configuration Telnet**.

Pour ouvrir l'interface console en exécutant Telnet dans la ligne de commande de Windows :

ÉTAPE 1 Sélectionnez **Démarrer** > **Exécuter**.

ÉTAPE 2 Saisissez **CMD** dans le champ Ouvrir et appuyez sur **Entrée**.

ÉTAPE 3 Saisissez **telnet**, un espace et l'adresse IP du commutateur. Par exemple :

c : \ >**telnet** *192.168.1.114*

ÉTAPE 4 Appuyez sur **Entrée**. L'écran **Login** (Connexion) s'affiche. Appuyez sur **Ctrl-R** pour actualiser l'écran CLI Login (connexion de l'interface de ligne de commande) ou accédez à cet écran à partir d'une autre fenêtre .

ÉTAPE 5 Saisissez **cisco** (par défaut) en tant que User Name (nom d'utilisateur).

ÉTAPE 6 Saisissez le username (mot de passe) **cisco** (par défaut).

ÉTAPE 7 Appuyez sur **Entrée**.

REMARQUE S'il s'agit de votre première ouverture de session ou si les paramètres par défaut du commutateur ont été réinitialisés, vous êtes invité(e) à modifier votre mot de passe. L'écran Change User Password (Modifier un mot de passe d'un utilisateur) s'affiche. Utilisez ces options pour créer et enregistrer un nouveau mot de passe.

Sinon, *l'écran Switch Main Menu* (Menu principal du commutateur) s'affiche.

ÉTAPE 8 Passez à la section **Menu principal de l'interface de console**.

Navigation dans le menu de configuration de la console

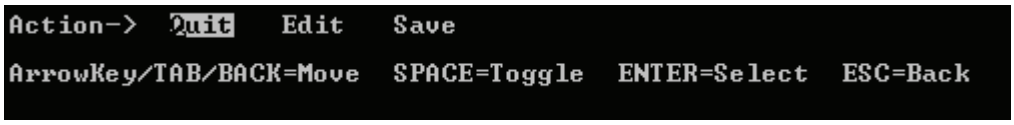
L'interface console se compose de deux parties : la *options list* (liste des options) et la *action list* (liste des actions). Naviguez dans les paramètres de configuration en utilisant la options list (liste des options). Gérez la configuration d'exécution en utilisant la action list (liste des actions). Par exemple, pour changer une valeur de paramètre, procédez comme suit :

1. Accédez à la options list (liste des options) appropriée.
2. Sélectionnez **Edit** (Modifier)en utilisant les touches fléchées pour accéder à l'action et la mettre en surbrillance puis appuyez sur **Enter** (Entrée). (Si aucun paramètre ne peut être modifié par l'administrateur système, la action list (liste des actions) ne s'affiche pas.)
3. Utilisez les touches fléchées pour accéder au champ approprié.
4. Saisissez les valeurs des paramètres ou utilisez la **barre d'espacement** pour passer d'une valeur à l'autre.
5. Appuyez sur Esc / Échap pour retourner à la action list (liste des actions).
6. Sélectionnez **Save** (Enregistrer) en utilisant les touches fléchées pour accéder à l'action et la mettre en surbrillance.
7. Appuyez sur **Entrée**. Les valeurs de vos paramètres sont enregistrées dans la configuration d'exécution.

Pour naviguer dans les listes :

- Utilisez la flèche haut ou bas pour vous déplacer vers le haut ou le bas de la liste. Vous pouvez également saisir le numéro correspondant à l'option souhaitée pour la sélectionner.
- Utilisez la flèche gauche ou droite pour vous déplacer vers la gauche ou la droite de la liste.
- Appuyez sur **Entrée** pour sélectionner une option de menu.
- Appuyez sur **Esc / Échap** pour passer de la options list (liste des options) à la action list (liste des actions).

Les actions disponibles s'affichent en bas de chaque écran.



Si vous quittez (**Quit**) sans enregistrer les changements, les modifications apportées aux valeurs de paramètres au cours de cette session seront ignorées.

Menu principal de l'interface de console

Chaque menu de l'interface console affiche les options dans une liste numérotée.

L'écran *Switch Main Menu* (Menu principal du commutateur) fournit les options suivantes :

- System Configuration Menu (Menu de configuration du système)
- Port Status (État des ports)
- Port Configuration (Configuration des ports)
- System Mode (Mode du système)
- Help (Aide)
- Logout (Se déconnecter)

Menu de configuration du système

Utilisez l'écran System Configuration Menu (Menu de configuration du système) pour sélectionner l'une des options suivantes :

- System Information (Informations système)
- Management Settings (Paramètres de gestion)
- Username & Password Settings (Paramètres de nom d'utilisateur et de mot de passe)
- Security Settings (Paramètres de sécurité)
- VLAN Management (Gestion des VLAN)
- IP Configuration (Configuration IP)

- File Management (Gestion de fichiers)
- Delete Startup Configuration (Supprimer la configuration de démarrage)
- Reboot to Factory Defaults (Redémarrer avec les paramètres d'origine)
- Reboot System (Redémarrer le système)

Informations système

Chemin d'accès : **Switch Main Menu** > **System Configuration Menu** > **System Information** (Menu principal du commutateur > Menu de configuration du système > Informations système)

Utilisez le menu *System Information* (Informations système) pour afficher les versions du micrologiciel du commutateur ainsi que les informations générales se rapportant au système. Vous pouvez également modifier le nom d'hôte ou la description de l'emplacement.

- Versions
- Informations système générales

Versions

Chemin d'accès : **Switch Main Menu > System Configuration Menu > System Information > Versions** (Menu principal du commutateur > Menu de configuration du système > Informations système > Versions)

Versions (Versions) affiche les versions du logiciel, de démarrage et du micrologiciel du matériel.

Informations système générales

Chemin d'accès : **Switch Main Menu** > **System Configuration Menu** > **System Information** > **General System Information** (Menu principal du commutateur > Menu de configuration du système > Informations système > Informations système générales)

General System Information (Informations système générales) affiche des informations générales se rapportant au commutateur. Vous pouvez modifier les informations de contact du système, le nom d'hôte et les informations d'emplacement du système.

Paramètres de gestion

Chemin d'accès : **Switch Main Menu** > **System Configuration Menu** > **Management Settings** (Menu principal du commutateur > Menu de configuration du système > Paramètres de gestion)

Le menu Management Settings (Paramètres de gestion) fournit les options suivantes :

- Serial Port Configuration (Configuration du port série)
- Telnet Configuration (Configuration Telnet)
- SSH Configuration (Configuration SSH)
- SNMP Configuration (Configuration SNMP)

Configuration du port série

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Management Settings** (Menu principal du commutateur > Menu de configuration du système > Paramètres de gestion)

Utilisez *Serial Port Configuration* (Configuration du port série) pour afficher ou modifier le débit en bauds du port de configuration. Si vous utilisez l'application HyperTerminal de Windows et que vous modifiez la valeur du paramètre de débit en bauds, vous devez vous déconnecter de l'application et réinitialiser la session pour faire correspondre les valeurs.

Configuration Telnet

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Management Settings** (Menu principal du commutateur > Menu de configuration du système > Paramètres de gestion)

Telnet Configuration (Configuration Telnet) affiche la valeur d'expiration de connexion Telnet et l'état du service Telnet. Vous pouvez activer ou désactiver le service Telnet et définir la valeur d'expiration en minutes. Si vous ne souhaitez pas que la session Telnet expire, saisissez une valeur de 0 minute.

Configuration SSH

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Management Settings** (Menu principal du commutateur > Menu de configuration du système > Paramètres de gestion)

Utilisez le menu *SSH Configuration* (Configuration SSH) pour afficher ou configurer les options suivantes :

- SSH Server Configuration (Configuration du serveur SSH)
- SSH Server Status (État du serveur SSH)
- SSH Crypto Key Generation (Génération de clé de cryptage SSH)
- SSH Keys Fingerprints (Empreintes de clés SSH)

Configuration du serveur SSH

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Management Settings > SSH Configuration** (Menu principal du commutateur > Menu de configuration du système > Paramètres de gestion > Configuration SSH)

Utilisez *SSH Server Configuration* (Configuration du serveur SSH) pour activer ou désactiver le serveur SSH. Le port du serveur SSH peut être modifié en entrant une valeur de port.

État du serveur SSH

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Management Settings > SSH Server Status** (Menu principal du commutateur > Menu de configuration du système > Paramètres de gestion > État du serveur SSH)

Utilisez *SSH Server Status* (État du serveur SSH) pour afficher l'état du serveur SSH, l'état des clés RSA et DSA ainsi que toute session SSH ouverte.

Sélectionnez **Refresh** (Actualiser) pour mettre l'écran à jour.

Génération de clé de cryptage SSH

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Management Settings > SSH Configuration > SSH Crypto Key Generation** (Menu principal du commutateur > Menu de configuration du système > Paramètres de gestion > Configuration SSH > Génération de clé de cryptage SSH)

Utilisez *SSH Crypto Key Generation* (Génération de clé de cryptage SSH) pour afficher la longueur de la clé publique SSH ou pour générer une clé de cryptage SSH.

Pour générer une clé de cryptage SSH :

ÉTAPE 1 Sélectionnez **Edit** (Modifier).

ÉTAPE 2 Utilisez la **barre d'espacement** pour basculer entre les options RSA et DSA.

ÉTAPE 3 Appuyez sur **Esc / Échap** pour retourner à la action list (liste des actions).

ÉTAPE 4 Sélectionnez **Execute** (Exécuter) et appuyez sur **Enter** (Entrée). Un message *operation complete* (Opération terminée) s'affichera une fois la génération de clé terminée.

ÉTAPE 5 Utilisez la flèche vers le haut pour accéder à la action list (liste des actions).

Empreintes de clés SSH

Chemin d'accès : **Menu principal du commutateur** > **Menu de configuration du système** > **Paramètres de gestion** > **Configuration SSH** > **Empreintes de clés SSH**

SSH Keys Fingerprints (Empreintes de clés SSH) affiche les clés RSA et DSA (si ces clés ont été générées).

Sélectionnez **Refresh** (Actualiser) pour mettre l'écran à jour.

Configuration SNMP

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Management Settings** (Menu principal du commutateur > Menu de configuration du système > Paramètres de gestion)

Utilisez *SNMP Configuration* (Configuration SNMP) pour activer ou désactiver SNMP sur le commutateur.

Paramètres de nom d'utilisateur et de mot de passe

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Username & Password Settings** (Menu principal du commutateur > Menu de configuration du système > Paramètres de nom d'utilisateur et de mot de passe)

Utilisez *Username & Password Settings* (Paramètres de nom d'utilisateur et de mot de passe) pour configurer les noms d'utilisateur et les mots de passe des personnes accédant au commutateur. Vous pouvez ajouter jusqu'à cinq utilisateurs. Le nom d'utilisateur d'origine par défaut est **cisco**. Le mot de passe d'origine par défaut est **cisco**.

Paramètres de sécurité

Chemin d'accès : **Switch Main Menu > System Configuration Menu** (Menu principal du commutateur > Menu de configuration du système)

Utilisez *Security Settings* (Paramètres de sécurité) pour configurer la sécurité sur le commutateur ainsi que pour générer et afficher le certificat SSL.

Génération de certificat SSL

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Security Settings** (Menu principal du commutateur > Menu de configuration du système > Paramètres de sécurité)

Utilisez *Certificate Generation* (Génération de certificat) pour créer un certificat SSL généré par l'appareil.

- Public Key Length (Longueur de la clé publique) : indique la longueur de la clé RSA SSL. (Plage : 512–2048)
- Organization Name (Nom de l'organisation) : indique le nom de l'organisation. (1 à 64 caractères)
- Locality or City Name (Nom de la localité ou de la ville) : indique le nom du lieu ou de la ville. (1 à 64 caractères)
- State or Province Name (Nom du département, de la région ou de la province) : indique le nom du département, de la région ou de la province. (1 à 64 caractères)

- Country Name (Nom du pays) : indique le nom du pays. (Utilisez un code à deux caractères.)
- Validity Term (Durée de validité) : indique le nombre de jours de validité de la certification. (Plage : 30–3650)

Afficher le certificat

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Security Settings** (Menu principal du commutateur > Menu de configuration du système > Paramètres de sécurité)

Utilisez Show Certificate (Afficher le certificat) pour afficher le certificat SSL interne.

Désactiver le profil d'accès de gestion actif

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Security Settings** (Menu principal du commutateur > Menu de configuration du système > Paramètres de sécurité)

Utilisez cette option pour désactiver les profils d'accès de gestion.

Si vous choisissez cette option, vous serez invité à la confirmer. Saisissez **O** pour confirmer.

Gestion des VLAN

Chemin d'accès : **Switch Main Menu > System Configuration Menu** (Menu principal du commutateur > Menu de configuration du système)

Utilisez le menu VLAN Management (Gestion des VLAN) pour définir le VLAN par défaut. Les modifications apportées au VLAN par défaut ne sont effectives qu'une fois le commutateur redémarré.

Sélectionnez **Default VLAN Setup** (Configuration du VLAN par défaut) pour afficher la *configuration du VLAN par défaut*.

Configuration IP

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration** (Menu principal du commutateur > Menu de configuration du système > Configuration IP)

Utilisez le menu *IP Configuration* (Configuration IP) pour configurer les options suivantes :

- IPv4 Address Configuration (Configuration d'adresse IPv4)
- IPv6 Address Configuration (Configuration d'adresse IPv6)
- HTTP Configuration (Configuration HTTP)
- HTTPS Configuration (Configuration HTTPS)
- Network configuration (Configuration réseau)
- IPv4 Default Route (Layer 3 devices only) (Route par défaut IPv4 (appareils de Niveau 3 uniquement))

Configuration d'adresse IPv4

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration** (Menu principal du commutateur > Menu de configuration du système) > Configuration IP)

Utilisez *IPv4 Address Configuration Menu* (Menu de configuration d'adresse IPv4) pour configurer l'adresse IPv4 du commutateur.

Paramètres d'adresse IPv4

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration** (Menu principal du commutateur > Menu de configuration du système > Configuration IP)

Utilisez *IP Address - Add/IP Address Settings* (Adresse IP - Ajouter/Paramètres d'adresse IP) pour ajouter ou modifier l'adresse IPv4 du commutateur.

- IPv4 Address (Adresse IPv4) : saisissez l'adresse IPv4 que vous souhaitez affecter au commutateur si ce dernier est désactivé en tant que client DHCP. Assurez-vous que l'adresse IP n'est pas en conflit avec un autre appareil présent sur le réseau.
- Subnet Mask (Masque de sous-réseau) : saisissez le masque de sous-réseau que vous souhaitez affecter au commutateur.

- Default Gateway (Passerelle par défaut) : saisissez l'adresse de la passerelle par défaut du commutateur (**Paramètres d'adresse IPv4**).
- Management VLAN (VLAN de gestion) : saisissez l'ID du VLAN de gestion (**Paramètres d'adresse IPv4**).
- Client DHCP (Client DHCP) : utilisez la **barre d'espacement** pour activer ou désactiver le client DHCP.
- Interface Type (Type d'interface) : sélectionnez le type d'interface : LAG, VLAN ou GE (ajout d'adresse IPv4).
- Interface Number (Numéro d'interface) : saisissez le numéro d'interface (ajout d'adresse IPv4).

Table des adresses IPv4

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration** (Menu principal du commutateur > Menu de configuration du système > Configuration IP)

La IP Address Table (Table des adresses IP) affiche les adresses IPv4 du Niveau 3.

- Delete/Keep (Supprimer/Conserver) : utilisez la barre d'espacement pour basculer entre **Delete** (Supprimer) et **Keep** (Conserver). Lorsque l'action est exécutée, cette entrée est appliquée en fonction de votre sélection.

Configuration d'adresse IPv6

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > IPv6 Address Configuration** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration d'adresse IPv6)

Utilisez le menu *IPv6 Address Configuration* (Configuration d'adresse IPv6) pour configurer l'adresse IPv6 du commutateur.

Activer l'interface IPv6

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > IPv6 Address Configuration > IPv6 Interface Enable** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration d'adresse IPv6 > Activer l'interface IPv6)

Utilisez *IPv6 Interface Enable* (Activer l'interface IPv6) pour sélectionner l'interface IPv6.

Paramètres d'adresse IPv6

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > IPv6 Address Configuration** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration d'adresse IPv6)

Utilisez l'option *IPv6 Address Settings* (Paramètres d'adresse IPv6) afin de configurer l'adresse IPv6 pour chaque interface du commutateur.

- **IPv6 Address** (Adresse IPv6) : l'appareil prend en charge une interface IPv6. Outre les adresses link-local et de multidiffusion par défaut, le commutateur ajoute automatiquement des adresses globales à l'interface, en se basant sur les 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.
- **Prefix Length** (Longueur du préfixe) : la longueur du préfixe IPv6 global en tant que valeur décimale de 0 à 128, indiquant le nombre de bits contigus les plus significatifs de l'adresse dont se compose le préfixe (la partie réseau de l'adresse).
- **Interface Type** (Type d'interface) : adresse IPv6, type d'interface (LAG, VLAN, FE, GE).

Table des adresses IPv6

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > IPv6 Address Configuration > IPv6 Address Table** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration d'adresse IPv6 > Table des adresses IPv6)

La IPv6 Address Table (Table des adresses IPv6) affiche les adresses IPv6 de chaque interface.

Tunnel ISATAP IPv6

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > IPv6 Address Configuration > IPv6 ISATAP Enable** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration d'adresse IPv6 > Activer ISATAP IPv6)

Utilisez l'option *ISATAP Tunnel* (Tunnel ISATAP) pour activer et configurer les paramètres de tunnel ISATAP IPv6. Pour plus d'informations, consultez la section **Définition d'une interface IPv6** du chapitre **Configuration des informations IP**.

Afficher l'interface ISATAP IPv6

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > IPv6 Address Configuration > IPv6 Default Gateway** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration d'adresse IPv6 > Afficher l'interface ISATAP IPv6)

L'option *ISATAP Interface Show* (Afficher l'interface ISATAP) affiche les informations de tunnel ISATAP actives.

Passerelle IPv6 par défaut

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > IPv6 Address Configuration > IPv6 Default Gateway** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration d'adresse IPv6 > Passerelle IPv6 par défaut)

Utilisez l'option *IPv6 Default Gateway* (Passerelle IPv6 par défaut) pour activer ou désactiver et spécifier l'interface qui fera office de passerelle IPv6 par défaut.

Configuration HTTP

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > HTTP Configuration** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration HTTP)

Utilisez l'option *HTTP Configuration* (Configuration HTTP) pour activer ou désactiver le serveur HTTP et définir le numéro de port du serveur HTTP.

Configuration HTTPS

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > HTTPS Configuration** (Menu principal du commutateur> Menu de configuration du système > Configuration IP > Configuration HTTPS)

Utilisez l'option *Configuration HTTPS* (HTTPS Configuration) pour activer ou désactiver le serveur HTTPS, définir le numéro de port du serveur HTTPS ou vérifier l'état du certificat HTTPS.

Configuration réseau

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Network Configuration** (Menu principal du commutateur > Menu de configuration du système > Configuration réseau)

Utilisez *le menu Network Configuration* (Configuration réseau) pour configurer les options suivantes :

- Ping <IPv4> (Ping <IPv4>)
- Ping <IPv6> (Ping <IPv6>)
- TraceRoute IPv4 (TraceRoute IPv4)
- TraceRoute IPv6 (TraceRoute IPv6)
- Telnet Session (Session Telnet)

Ping IPv4

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > Network Configuration > TraceRoute IPv4** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration réseau > Ping IPv4)

Utilisez l'option *Ping IPv4* (Ping IPv4) pour entrer l'adresse IPv4 que vous souhaitez tester.

Sélectionnez Execute (Exécuter) pour lancer le test. Les résultats de la commande ping s'affichent dans les champs Status (État) et Statistics (Statistiques).

Ping IPv6

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > Network Configuration > Ping IPv6** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration réseau > Ping IPv6)

Utilisez l'option *Ping IPv6* pour entrer l'adresse IPv6, le type d'interface (VLAN, LAG, FE, GE) et l'ID d'interface que vous souhaitez tester.

Sélectionnez Execute (Exécuter) pour lancer le test. Les résultats de la commande ping s'affichent dans les champs Status (État) et Statistics (Statistiques).

TraceRoute IPv4

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > Network Configuration > TraceRoute IPv4** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration réseau > TraceRoute IPv4)

Utilisez l'option *TraceRoute IPv4* pour entrer l'adresse IPv4 de la route réseau dont vous souhaitez suivre le cheminement.

Sélectionnez **Execute** (Exécuter) pour lancer le test. Les résultats s'affichent dans le champ Status (État).

Une fois le test traceroute terminé, il affiche l'adresse IP, l'état et les statistiques du test.

TraceRoute IPv6

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > Network Configuration > TraceRoute IPv6** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration réseau > TraceRoute IPv6)

Utilisez l'option *TraceRoute IPv6* pour entrer l'adresse IPv6 de la route réseau dont vous souhaitez suivre le cheminement.

Sélectionnez **Execute** (Exécuter) pour lancer le test. TraceRoute affiche l'adresse IP, l'état et les statistiques du test traceroute dans les champs État et Résultats.

Session Telnet

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > Network Configuration > Telnet Session** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Configuration réseau > Session Telnet)

Utilisez *Telnet Session Configuration* (Configuration de la session Telnet) pour entrer l'adresse IP de l'emplacement que vous souhaitez atteindre en utilisant une connexion Telnet.

Route par défaut IPv4 (uniquement pour appareils de Niveau 3)

Chemin d'accès : **Switch Main Menu > System Configuration Menu > IP Configuration > IPv4 Default Route** (Menu principal du commutateur > Menu de configuration du système > Configuration IP > Route par défaut IPv4)

Utilisez *IPv4 Default Route* (Route par défaut IPv4) afin de définir l'adresse IP du saut suivant pour le commutateur.

Gestion de fichiers

Chemin d'accès : **Switch Main Menu > System Configuration Menu > File Management** (Menu principal du commutateur > Menu de configuration du système > Gestion de fichiers)

Utilisez le *menu File Management* (Gestion de fichiers) pour télécharger des fichiers ou modifier l'image active.

- Upgrade/Backup <IPv4> (Mettre à niveau/sauvegarder <IPv4>)
- Upgrade/Backup <IPv6> (Mettre à niveau/sauvegarder <IPv6>)
- Active Image (Image active)

Deux images de micrologiciel, Image1 et Image2, sont stockées sur le commutateur. Une des images est identifiée en tant qu'*image active* et l'autre en tant qu'**image inactive**. Le commutateur démarre à partir de l'image que vous avez définie en tant qu'image active.

Lors de la mise à niveau du micrologiciel, la nouvelle image remplace toujours celle identifiée comme étant l'image inactive. Une fois le nouveau micrologiciel téléchargé sur le commutateur, celui-ci continue de démarrer en utilisant l'image active (l'ancienne version) jusqu'à ce que vous changiez l'état de la nouvelle image en image active. Vous pouvez changer en image active l'image identifiée en tant qu'image inactive en suivant la procédure décrite dans la section **Image active**.

Mettre à niveau/sauvegarder <IPv4>

Chemin d'accès : **Switch Main Menu > System Configuration Menu > File Management > Upgrade/Backup <IPv4>** (Menu principal du commutateur > Menu de configuration du système > Gestion de fichiers > Mettre à niveau/sauvegarder <IPv4>)

Utilisez *Upgrade/Backup <IPv4>* (Mettre à niveau/sauvegarder <IPv4>) pour télécharger des fichiers, tels que le fichier de configuration de démarrage, le fichier de démarrage (boot) ou un fichier image, via un serveur TFTP.

Mettre à niveau/sauvegarder <IPv6>

Chemin d'accès : **Switch Main Menu > System Configuration Menu > File Management > Upgrade/Backup <IPv6>** (Menu principal du commutateur > Menu de configuration du système > Gestion de fichiers > Mettre à niveau/sauvegarder <IPv6>)

Utilisez *Upgrade/Backup <IPv6>* (Mettre à niveau/sauvegarder <IPv6>) pour télécharger des fichiers, tels que le fichier de configuration de démarrage, le fichier de démarrage (boot) ou un fichier image, via un serveur TFTP.

Pour télécharger un nouveau fichier de démarrage et image, procédez comme suit :

ÉTAPE 1 Si nécessaire, téléchargez le nouveau code de démarrage. NE REDÉMARREZ PAS L'APPAREIL. Définissez le fichier source sur TFTP et le fichier de destination sur **boot** (démarrage) en utilisant la barre d'espacement pour passer d'une valeur à l'autre. Nom du fichier correspond au nom du fichier de démarrage à télécharger. Adresse IP correspond à l'adresse IP du serveur TFTP.

ÉTAPE 2 Si nécessaire, téléchargez la nouvelle image du micrologiciel. Définissez le fichier source sur TFTP et le fichier de destination sur **image** en utilisant la barre d'espacement pour passer d'une valeur à l'autre. Nom du fichier correspond au nom du fichier image à télécharger. Adresse IP correspond à l'adresse IP du serveur TFTP.

ÉTAPE 3 Changez l'image active en utilisant le menu *Active Image* (Image active).

ÉTAPE 4 Redémarrez le commutateur.

Image active

Chemin d'accès : **Switch Main Menu > System Configuration Menu > File Management > Active Image** (Menu principal du commutateur > Menu de configuration du système > Gestion de fichiers > Image active)

L'écran *Active Image* (Image active) affiche et indique si Image 1 ou Image 2 est active, ainsi que la version de micrologiciel associée à l'image.

Supprimer la configuration de démarrage

Permet de supprimer la configuration de démarrage.

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Delete Startup Configuration** (Menu principal du commutateur > Menu de configuration du système > Supprimer la configuration de démarrage)

En cas de redémarrage du commutateur, ses paramètres d'origine par défaut sont restaurés. Saisissez **O** pour supprimer la configuration ou **N** pour annuler.

Redémarrer avec les paramètres d'origine

Redémarrer avec les paramètres d'origine supprimera la configuration de démarrage et redémarrera le commutateur. Lorsque cette action est sélectionnée, tout paramètre non enregistré dans un fichier est perdu.

Si une configuration est disponible sur un serveur TFTP, le commutateur la télécharge.

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Reset to Factory Defaults** (Menu principal du commutateur > Menu de configuration du système > Réinitialiser les paramètres par défaut)

Pour restaurer les paramètres par défaut du commutateur, sélectionnez **Reset to Factory Defaults** (Réinitialiser les paramètres par défaut) et appuyez sur **Enter** (Entrée). Le programme vous demande si vous souhaitez poursuivre cette opération. Saisissez **O** pour restaurer les paramètres par défaut du commutateur ou **N** pour annuler.

Redémarrer le système

Chemin d'accès : **Switch Main Menu > System Configuration Menu > Reboot System** (Menu principal du commutateur > Menu de configuration du système > Redémarrer le système)

Sélectionnez **Reboot System** (Redémarrer le système) et appuyez sur **Enter** (Entrée) si vous souhaitez redémarrer le commutateur. Le programme vous demande si vous souhaitez poursuivre cette opération. Saisissez **O** pour redémarrer le commutateur ou **N** pour annuler.

État des ports

Chemin d'accès : **Switch Main Menu > Port Status** (Menu principal du commutateur > État des ports)

L'option Port Status (État des ports) du Switch Main Menu (Menu principal du commutateur) affiche l'état des ports pour les commutateurs sur lesquels PoE n'est pas activé. L'option État des ports du Menu principal du commutateur affiche, pour les commutateurs sur lesquels PoE est activé, le menu Menu d'état des ports, qui comprend les options Port Status (État des ports) et PoE Status (État PoE) . Utilisez *Port Configuration* (Configuration des ports) et *Port Configuration* (Configuration PoE) pour modifier la configuration des ports.

État des ports

Chemin d'accès : **Switch Main Menu > Port Status > Port Status Menu > Port Status** (Menu principal du commutateur > État des ports > Menu d'état des ports > État des ports)

Port Status (Etat des ports) affiche le numéro des ports, l'état d'activation, l'état des liaisons, la vitesse et l'état de contrôle de flux (le flux de transmissions de paquets) des ports non-PoE. Douze ports s'affichent simultanément. Utilisez les flèches pour vous déplacer vers le haut ou le bas de la liste.

État PoE

Chemin d'accès : **Switch Main Menu > Port Status > PoE Status** (Menu principal du commutateur > État des ports > État PoE)

PoE Status (État PoE) affiche l'état des ports PoE.

Configuration des ports

Chemin d'accès : **Switch Main Menu > Port Configuration** (Menu principal du commutateur > Configuration des ports)

Utilisez *le menu Port Configuration* (Configuration des ports) pour modifier la configuration des ports et de PoE.

Configuration des ports

Chemin d'accès : **Switch Main Menu > Port Configuration Menu > Port Configuration** (Menu principal du commutateur > Menu de configuration des ports > Configuration des ports)

Utilisez l'option *Port Configuration* (Configuration des ports) pour modifier les paramètres des ports non-PoE. Vous pouvez activer ou désactiver les ports, activer ou désactiver la négociation automatique (Auto Negociation) , définir la vitesse (speed) et le mode duplex (Auto, 10H, 100H, 10F, 100F, 1000F) et définir le contrôle de flux (Flow Control sur On, Off, Auto, respectivement Activé, Désactivé, Auto). Douze ports s'affichent simultanément. Utilisez les flèches pour vous déplacer vers le haut ou le bas de la liste.

Configuration PoE

Chemin d'accès : **Switch Main Menu > Port Configuration Menu > PoE Configuration** (Menu principal du commutateur > Menu de configuration des ports > Configuration PoE)

Utilisez *Poe Configuration* (Configuration PoE) pour modifier les paramètres PoE des ports PoE. Vous pouvez définir la priorité des ports (faible, élevée ou critique via respectivement Low, High et Critical), activer (enable) ou désactiver (disable) PoE et définir l'affectation de puissance (en mW) via Power Allocation (in mW) .

Mode du système

Chemin d'accès : **Switch Main Menu > System Mode** (Menu principal du commutateur > Mode du système)

Utilisez *System Mode* (Mode du système) pour établir le commutateur sur le niveau 2 ou sur le niveau 3 (respectivement Layer 2 ou Layer 3).

Aide

Chemin d'accès : **Switch Main Menu > Help** (Menu principal du commutateur > Aide)

Sélectionnez Help (Aide) pour afficher des informations se rapportant à la navigation dans les options de l'interface console.

Se déconnecter

Chemin d'accès : **Switch Main Menu > Logout** (Menu principal du commutateur > Se déconnecter)

Sélectionnez Logout (Se déconnecter) pour mettre fin à la session de console en cours.

78-19308-01