GUIDE D'ADMINISTRATION

Guide d'administration – Version 1.0.0.x
Commutateurs Smart Cisco série 220

OL-30971-02

Tableau des matières

1

Mise en route

Ce chapitre présente l'interface Web du Commutateur Cisco 220 et inclut les rubriques suivantes :

- **Mise en route de l'interface Web**
- **Configuration du commutateur - Démarrage rapide**
- **Conventions de nommage de l'interface**
- **Navigation dans les fenêtres**

Mise en route de l'interface Web

Deux méthodes s'offrent à vous pour accéder au Commutateur Cisco 220 et effectuer son administration : soit en utilisant l'interface Web sur votre réseau IP, soit à partir de l'interface de ligne de commande via l'interface de la console. L'utilisation de l'interface de la console nécessite des connaissances avancées. Consultez le *guide de référence d'interface de ligne de commande pour les commutateurs Smart Cisco série 220* pour plus d'informations à ce sujet.

Avant de commencer

Avant de commencer à utiliser l'interface Web, vérifiez que votre ordinateur est bien doté d'Internet Explorer 8.0 (ou version ultérieure), de Firefox 20.0 (ou version ultérieure), de Chrome 23.0 (ou version ultérieure) ou de Safari 5.7 (ou version ultérieure).

Lors de la première configuration du commutateur, les paramètres par défaut utilisés sont les suivants :

Paramètre	Valeur par défaut
Nom d'utilisateur	**cisco**

Paramètre	Valeur par défaut
Mot de passe	**cisco**
Adresse IP du commutateur	**192.168.1.254**

Connexion à l'interface Web

Afin d'accéder au commutateur depuis l'interface Web, vous devez connaître l'adresse IP utilisée par l'appareil. Par défaut, ce dernier utilise l'adresse IP par défaut (**192.168.1.254**) jusqu'à ce qu'il ait obtenu une adresse IP d'un serveur DHCP.

REMARQUE Si vous gérez le commutateur via une connexion réseau et que l'adresse IP est modifiée par un serveur DHCP ou manuellement, vous ne pouvez plus accéder au commutateur. Pour pouvoir utiliser l'interface Web, vous devez saisir la nouvelle adresse IP du commutateur dans votre navigateur. Si vous gérez le commutateur via une connexion de port de console, la liaison est maintenue.

Pour configurer le commutateur à l'aide de l'interface Web :

ÉTAPE 1 Mettez l'ordinateur et le commutateur sous tension.

ÉTAPE 2 Connectez l'ordinateur au commutateur.

Vous pouvez le connecter au même sous-réseau IP que le commutateur en les reliant directement par un câble Ethernet, ou en le connectant au même réseau local (LAN) que celui sur lequel réside le commutateur, via d'autres commutateurs. Vous pouvez également connecter votre ordinateur au commutateur à partir d'un autre sous-réseau IP, via un ou plusieurs routeurs IP.

ÉTAPE 3 Localisez l'adresse IP du commutateur.

a. Il est possible d'accéder au commutateur et de le gérer grâce aux outils et aux services réseau Cisco, y compris l'utilitaire Cisco FindIT Network Discovery Utility qui vous permet de trouver automatiquement tous les périphériques Cisco pris en charge dans le même segment du réseau local que votre ordinateur. Vous pouvez obtenir une vue instantanée de chaque périphérique ou lancer l'utilitaire de configuration du produit pour afficher et configurer les paramètres. Pour en savoir plus sur l'utilitaire FindIT, visitez www.cisco.com/go/findit.

b. Identifiez l'adresse IP attribuée par votre serveur DHCP en accédant à votre routeur ou à votre serveur DHCP. Reportez-vous aux instructions d'utilisation de votre serveur DHCP pour plus d'informations. Assurez-vous que votre serveur DHCP fonctionne et est accessible.

ÉTAPE 4 Définissez la configuration IP sur votre ordinateur.

- Si le commutateur utilise l'adresse IP statique par défaut **192.168.1.254**, vous devez choisir une adresse IP qui n'est pas encore utilisée dans la plage comprise entre 192.168.1.2 et 192.168.1.253.
- Si les adresses IP sont affectées par DHCP, assurez-vous que votre serveur DHCP est en cours d'exécution et qu'il peut être atteint depuis le commutateur et l'ordinateur. Vous devrez peut-être débrancher et rebrancher les périphériques pour qu'ils puissent détecter leur nouvelle adresse IP à partir du serveur DHCP.

REMARQUE La procédure spécifique à suivre pour modifier l'adresse IP sur votre ordinateur dépend du type d'architecture et du système d'exploitation dont vous disposez. Utilisez la fonctionnalité locale d'aide et de support de vos ordinateurs et effectuez une recherche portant sur l'« adressage IP ».

ÉTAPE 5 Ouvrez une fenêtre de votre navigateur Web. Si vous êtes invité à installer un plug-in ActiveX lors de la connexion au commutateur, suivez les invites pour accepter ce plug-in.

ÉTAPE 6 Saisissez l'adresse IP du commutateur à configurer dans la barre d'adresse du navigateur, puis appuyez sur **Entrée**. Par exemple, **http://192.168.1.254**.

ÉTAPE 7 Lorsque la page de connexion s'affiche, choisissez la langue que vous souhaitez utiliser dans l'interface Web, puis saisissez le nom d'utilisateur et le mot de passe.

Le nom d'utilisateur par défaut est **cisco** et le mot de passe par défaut est **cisco**. Ils sont tous les deux sensibles à la casse.

ÉTAPE 8 Cliquez sur **Log In**.

Lors de votre première ouverture de session avec le nom d'utilisateur et le mot de passe par défaut, vous devez saisir un nouveau mot de passe. La page Change Password s'ouvre.

HTTP/HTTPS

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

REMARQUE Vous n'avez pas besoin de saisir le nom d'utilisateur ou le mot de passe avant de cliquer sur **Secure Browsing (HTTPS)**.

Modification du mot de passe d'administration

Pour des raisons de sécurité, il est indispensable de modifier le mot de passe d'administration à la première connexion ou lorsque le mot de passe d'administration actuel arrive à expiration.

La complexité des mots de passe est activée par défaut. Les exigences en termes de complexité minimale du mot de passe sont affichées sur la page. Le nouveau mot de passe doit respecter les règles de complexité par défaut. Il peut également être temporairement désactivé en sélectionnant **Disable Password Strength Enforcement**. Consultez la section **Configuration des règles de complexité des mots de passe** pour de plus amples informations sur la complexité des mots de passe.

Pour modifier le mot de passe :

ÉTAPE 1 Renseignez les champs suivants pour définir un nouveau mot de passe d'administration :

- **Old Password** : entrez le mot de passe actuel (par défaut **cisco**).
- **Password** : entrez un nouveau mot de passe.
- **Confirm Password** : saisissez à nouveau le mot de passe pour le confirmer.
- **Password Strength Meter** : affiche le niveau de sécurité du nouveau mot de passe.
- **Disable Password Strength Enforcement** : le contrôle du niveau de sécurité des mots de passe, activé par défaut, vous oblige à respecter les paramètres par défaut suivants :
  - Le mot de passe doit être différent du nom d'utilisateur actuel.
  - Le mot de passe doit contenir au moins huit caractères.
  - Le mot de passe doit contenir des caractères appartenant au moins à trois classes de caractères (caractères majuscules, minuscules, numériques et spéciaux disponibles sur un clavier standard).

  REMARQUE Si vous ne voulez pas modifier le mot de passe, sélectionnez **Disable Password Strength Enforcement** et cliquez sur **Apply**.

ÉTAPE 2 Cliquez sur **Apply**.

La page Getting Started s'affiche. Vous pouvez désormais configurer le commutateur.

ÉTAPE 3 Sélectionnez **Do not show this page on startup** pour empêcher la page Getting Started de s'ouvrir à chaque fois que vous vous connectez au commutateur. Si vous sélectionnez cette option, la page System Summary s'ouvre à la place de la page Getting Started.

Déconnexion

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

ATTENTION Sauf si la configuration de fonctionnement est copiée dans la configuration de démarrage, toutes les modifications apportées depuis le dernier enregistrement du fichier sont perdues en cas de redémarrage du commutateur. Enregistrez la configuration de fonctionnement 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 **Save** indique que des changements apportés à la configuration de fonctionnement n'ont pas encore été enregistrés dans le fichier de configuration de démarrage. Le bouton **Disable Save Icon Blinking** de la page Copy/Save Configuration permet d'afficher une icône **X** rouge clignotante.

Lorsque le commutateur détecte automatiquement un périphérique, tel qu'un téléphone IP, il configure le port de manière adéquate pour ce périphérique. Ces commandes de configuration sont écrites dans le fichier de configuration de fonctionnement. L'icône **Save** se met alors à clignoter lorsque l'utilisateur se connecte, même s'il n'a pas modifié la configuration.
Lorsque vous cliquez sur **Save**, la page Copy/Save Configuration s'affiche. Enregistrez le fichier de configuration de fonctionnement en le copiant dans le fichier de configuration de démarrage. Une fois cet enregistrement effectué, l'icône **X** rouge et le lien d'application **Save** ne s'affichent plus.

Pour vous déconnecter, cliquez sur **Logout** 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 commutateur, un message apparaît et la page de connexion s'ouvre tout en indiquant que vous êtes déconnecté. Une fois que vous vous êtes connecté, l'application retourne à la page initiale.

La page initiale qui s'affiche est différente en fonction de l'option « **Do not show this page on startup** » de la page Getting Started. Si vous n'avez pas sélectionné cette option, la page initiale qui apparaît est la page Getting Started. Si vous avez sélectionné cette option, la page initiale qui apparaît est la page System Summary.

Configuration du commutateur - Démarrage rapide

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

Catégorie	Nom du lien (sur la page)	Page correspondante
Configuration initiale	Change Management Applications and Services	Page Security > TCP/UDP Services
	Change Device IP Address	Page Administration > Management Interface > IPv4 Interface
	Create VLAN	Page VLAN Management > Create VLAN
	Configure Port Settings	Page Port Management > Port Setting
État du périphérique	System Summary	Page Status and Statistics > System Summary
	Port Statistics	Page Status and Statistics > Interface
	RMON Statistics	Page Status and Statistics > RMON > Statistics
	View Log	Page Status and Statistics > View Log > RAM Memory

Catégorie	Nom du lien (sur la page)	Page correspondante
Accès rapide	Change Device Password	Page Administration > User Accounts
	Upgrade Device Software	Page Administration > File Management > Upgrade/ Backup Firmware/Language
	Backup Device Configuration	Page Administration > File Management > Download/ Backup Configuration/Log
	Create MAC-Based ACL	Page Access Control > MAC-Based ACL
	Create IP-Based ACL	Page Access Control > IPv4-Based ACL
	Configure QoS	Page Quality of Service > General > QoS Properties
	Configure Port Mirroring	Page Administration > Diagnostics > Port and VLAN Mirroring

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

Conventions de nommage de l'interface

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

- **Type of interface** : les types suivants d'interfaces se retrouvent dans divers types de périphériques :
  - **Fast Ethernet (10/100 bits)** : celles-ci sont désignées par **FE**.
  - **Gigabit Ethernet (10/100/1000 bits)** : celles-ci sont désignées par **GE**.
  - **LAG (PortChannel)** : celles-ci sont désignées par **LAG**.

- **VLAN** : celles-ci sont désignées par **VLAN**.
- **Tunnel** : celles-ci sont désignées par **Tunnel**.

- **Interface Number** : ID du port, du LAG, du tunnel ou du VLAN.

Navigation dans les fenêtres

Cette section décrit les fonctions de l'interface Web.

En-tête d'application

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

Nom du lien d'application	Description
Username	Affiche le nom de l'utilisateur connecté au commutateur. Le nom d'utilisateur par défaut est **cisco**. (Le mot de passe par défaut est **cisco**.)
Language Menu	Ce menu comprend les options suivantes : ▪ **Select a language :** choisissez une des langues qui apparaît dans le menu. Il s'agira de la langue utilisée par l'interface Web. ▪ **Download Language :** ajoutez une nouvelle langue au commutateur. Pour mettre à niveau un fichier de langue, accédez à la page Upgrade/ Backup Firmware/Language. ▪ **Delete Language :** supprime la deuxième langue du commutateur. La première langue (anglais) ne peut pas être supprimée.
Logout	Cliquez sur ce lien pour vous déconnecter de l'interface Web.
About	Cliquez sur ce lien pour afficher le nom du commutateur et son numéro de version.

Nom du lien d'application	Description
Help	Cliquez sur ce lien pour afficher l'aide en ligne.
Alert	L'icône d'état d'alerte SYSLOG s'affiche en cas de journalisation d'un message SYSLOG dont le niveau de gravité se situe au-dessus du niveau *critique*. Cliquez sur l'icône pour ouvrir la page RAM Memory. Une fois que vous avez accédé à cette page, l'icône d'état d'alerte SYSLOG ne s'affiche plus. Pour afficher la page en l'absence de message SYSLOG actif, cliquez sur **Status and Statistics** > **View Log** > **RAM Memory**.
Save	Une icône **X** rouge clignotante qui s'affiche à gauche du lien d'application **Save** indique que des changements apportés à la configuration de fonctionnement n'ont pas encore été enregistrés dans le fichier de configuration de démarrage. Vous pouvez désactiver le clignotement de l'icône **X** rouge sur la page Copy/Save Configuration. Cliquez sur **Save** pour afficher la page Copy/Save Configuration. Enregistrez le fichier de configuration de fonctionnement en le copiant dans 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 Save ne s'affichent plus. Au redémarrage du commutateur, la configuration de démarrage est copiée dans la configuration de fonctionnement et les paramètres du commutateur sont définis en fonction des données de la configuration de fonctionnement.

Boutons de gestion

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

Nom du bouton	Description
Add	Cliquez sur ce bouton pour afficher la page Add correspondante et ajouter une entrée à une table. Saisissez les informations requises et cliquez sur **Apply** pour les enregistrer dans la configuration de fonctionnement. Cliquez sur **Close** pour retourner à la page principale. Cliquez sur **Save** pour afficher la page Copy/Save Configuration et enregistrer la configuration de fonctionnement dans le type de fichier de configuration de démarrage sur le commutateur.
Apply	Cliquez sur ce bouton pour appliquer les modifications à la configuration de fonctionnement sur le commutateur. En cas de redémarrage du commutateur, la configuration de fonctionnement 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 **Save** pour afficher la page Copy/Save Configuration et enregistrer la configuration de fonctionnement dans le type de fichier de configuration de démarrage sur le commutateur.
Cancel	Cliquez sur ce bouton pour réinitialiser les modifications apportées à la page.
Clear All Interfaces Counters	Cliquez sur ce bouton pour effacer les compteurs de statistiques de toutes les interfaces.
Clear Interface Counters	Cliquez sur ce bouton pour effacer les compteurs de statistiques de l'interface sélectionnée.
Clear Logs	Efface les fichiers journaux.
Clear Table	Efface les entrées de la table.
Close	Permet de revenir à la page principale. Un message s'affiche si des modifications n'ont pas été appliquées à la configuration de fonctionnement.
Copper Test	Cliquez sur **Copper Test** pour effectuer un test cuivre.

Nom du bouton	Description
Copy Settings	Une table comporte généralement une ou plusieurs entrées contenant des paramètres de configuration. Au lieu de modifier chaque entrée individuellement, il est possible de modifier une entrée, puis de la copier dans plusieurs autres, comme décrit ci-dessous : 1. Sélectionnez l'entrée à copier et cliquez sur **Copy Settings**. 2. Saisissez les numéros des entrées de destination dans le champ **to**. 3. Cliquez sur **Apply** pour enregistrer les modifications et sur **Close** pour retourner à la page principale.
Delete	Après avoir sélectionné une entrée dans la table, cliquez sur **Delete** pour la supprimer.
Details	Cliquez sur ce bouton pour afficher les détails relatifs à l'entrée sélectionnée.
Edit	Sélectionnez l'entrée et cliquez sur **Edit**. La page Edit qui s'ouvre vous permet de modifier l'entrée. 1. Cliquez sur **Apply** pour enregistrer les modifications dans la configuration de fonctionnement. 2. Cliquez sur **Close** pour retourner à la page principale.
Go	Saisissez les critères de filtrage et cliquez sur **Go**. Les résultats s'affichent sur la page.
Refresh	Cliquez sur ce bouton pour actualiser manuellement les données de la page.
View All Interfaces Statistics	Cliquez sur ce bouton pour voir l'ensemble des compteurs de statistiques sur une seule et même page.
View Interface Statistics	Cliquez sur ce bouton pour voir les compteurs de statistiques de l'interface sélectionnée sur une seule page.

2

État et statistiques

Ce chapitre explique comment consulter les statistiques relatives au commutateur et inclut les rubriques suivantes :

- **Affichage de l'interface Ethernet**
- **Affichage des statistiques Etherlike**
- **Affichage de l'utilisation de la mémoire TCAM**
- **Affichage de la température et de l'état du ventilateur**
- **Gestion du contrôle à distance (RMON)**

Affichage de l'interface Ethernet

La page Interface affiche les statistiques relatives au trafic pour chaque interface. La fréquence d'actualisation des informations peut être sélectionnée. Cette page est utile pour analyser le volume de trafic envoyé et reçu, ainsi que sa dispersion (destination unique, multidestination et diffusion).

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

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

ÉTAPE 2 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port ou le LAG pour lequel les statistiques Ethernet sont affichées.
- **Refresh Rate** : sélectionnez la durée qui s'écoule avant l'actualisation des statistiques Ethernet. Les options disponibles sont les suivantes :
  - *No Refresh* : les statistiques ne sont pas actualisées.
  - *15 sec* : les statistiques sont actualisées toutes les 15 secondes.
  - *30 sec* : les statistiques sont actualisées toutes les 30 secondes.
  - *60 sec* : les statistiques sont actualisées toutes les 60 secondes.

La zone **Receive Statistics** contient les champs suivants se rapportant aux paquets entrants :

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

La zone **Transmit Statistics** contient les champs suivants se rapportant aux paquets sortants :

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

ÉTAPE 3 Cliquez sur **Clear Interface Counters** pour effacer les compteurs de l'interface sélectionnée.

ÉTAPE 4 Cliquez sur **Refresh** pour actualiser manuellement les compteurs de statistiques pour l'interface sélectionnée.

ÉTAPE 5 Cliquez sur **View All Interfaces Statistics** pour voir l'ensemble des compteurs de statistiques sur une seule et même page. La table Interface Statistics Table affiche les compteurs de statistiques de toutes les interfaces. Cette page vous permet de réaliser les actions suivantes :

- Sélectionnez la fréquence d'actualisation dans le menu déroulant **Refresh Rate**.
- Sélectionnez une interface et cliquez sur **Clear Interface Counters** pour effacer les compteurs de l'interface sélectionnée.
- Cliquez sur **Clear All Interface Counters** pour effacer les compteurs de statistiques de toutes les interfaces.
- Sélectionnez une interface et cliquez sur **View Interface Statistics** pour voir les compteurs de statistiques de l'interface sélectionnée sur une seule page.
- Cliquez sur **Refresh** pour actualiser manuellement les compteurs de statistiques pour toutes les interfaces.

Affichage des statistiques Etherlike

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

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

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

ÉTAPE 2 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port ou le LAG pour lequel les statistiques Etherlike sont affichées.
- **Refresh Rate** : sélectionnez la durée qui s'écoule avant l'actualisation des statistiques Etherlike.

Les champs suivants s'affichent pour l'interface sélectionnée :

- **Frame Check Sequence (FCS) Errors** : nombre de trames reçues ayant échoué aux contrôles de redondance cyclique (CRC).
- **Single Collision Frames** : nombre de trames impliquées dans une collision unique, mais ayant été transmises avec succès.
- **Late Collisions** : nombre de collisions ayant été détectées après les 512 premiers octets de données.
- **Excessive Collisions** : nombre de transmissions dues à des collisions excessives.
- **Oversize Packets** : nombre de paquets de plus de 1 518 octets reçus.
- **Internal MAC Receive Errors** : nombre de trames rejetées en raison d'erreurs de destination.
- **Pause Frames Received** : nombre de trames de pause de contrôle de flux reçues.
- **Pause Frames Transmitted** : nombre de trames de pause de contrôle de flux transmises à partir de l'interface sélectionnée.

ÉTAPE 3 Cliquez sur **Clear Interface Counters** pour effacer les compteurs de l'interface sélectionnée.

ÉTAPE 4 Cliquez sur **Refresh** pour actualiser manuellement les compteurs de statistiques pour l'interface sélectionnée.

ÉTAPE 5 Cliquez sur **View All Interfaces Statistics** pour voir l'ensemble des compteurs de statistiques sur une seule et même page. La table **Etherlike Statistics Table** affiche les compteurs de statistiques de toutes les interfaces. Cette page vous permet de réaliser les actions suivantes :

- Sélectionnez la fréquence d'actualisation dans le menu déroulant **Refresh Rate**.
- Sélectionnez une interface et cliquez sur **Clear Interface Counters** pour effacer les compteurs de l'interface sélectionnée.
- Cliquez sur **Clear All Interface Counters** pour effacer les compteurs de statistiques de toutes les interfaces.
- Sélectionnez une interface et cliquez sur **View Interface Statistics** pour voir les compteurs de statistiques de l'interface sélectionnée sur une seule page.
- Cliquez sur **Refresh** pour actualiser manuellement les compteurs de statistiques pour toutes les interfaces.

Affichage de l'utilisation de la mémoire TCAM

L'architecture du commutateur utilise la mémoire TCAM (Ternary Content Addressable Memory) pour prendre en charge les actions des paquets à vitesse filaire. La mémoire TCAM contient les règles produites par d'autres applications (ACL et QoS par exemple) et les règles créées par le système.

Seule une application système attribue des règles lors de sa mise en œuvre.

Pour afficher l'utilisation de la mémoire TCAM, cliquez sur **Status and Statistics** > **TCAM Utilization**.

Les champs suivants s'affichent :

- **Maximum TCAM Entries** : nombre maximum d'entrées TCAM disponibles.
- **In Use** : nombre d'entrées TCAM actuellement utilisées.

Affichage de la température et de l'état du ventilateur

La page Fan and Thermal Status présente l'état du ventilateur et de la température des commutateurs dotés de la fonctionnalité PoE.

Le tableau suivant répertorie le nombre de canaux de ventilation et de température applicables sur les différents modèles de commutateurs PoE :

Modèle	Nombre de canaux de ventilation	Nombre de canaux de température
SF220-24P	2	2
SF220-48P	4	2
SG220-26P	2	2
SG220-28MP	3	2
SG220-50P	4	2

Pour afficher l'état du ventilateur et de la température, cliquez sur **Status and Statistics** > **Fan and Thermal Status**.

Les champs suivants s'affichent :

- **FAN *x* Status** : affiche l'état de fonctionnement des ventilateurs du commutateur.
  - *Operational Status* : affiche OK si le ventilateur fonctionne normalement ou Fault s'il ne fonctionne pas correctement.
  - *Speed Value* : affiche la vitesse du ventilateur en tours par minute (tr/min).
- **Thermal *x* Status** : affiche l'état des capteurs thermiques du commutateur.
  - *Operational Status* : affiche OK si le capteur thermique fonctionne normalement ou Fault s'il ne fonctionne pas correctement.
  - *Temperature Value* : affiche la température actuelle en degrés Celsius.

- *Temperature Status* : affiche l'état de la température actuelle. Ce champ peut prendre les valeurs suivantes :

  Vert : indique que la température actuelle est inférieure au seuil jaune.

  Jaune : indique que la température actuelle est supérieure au seuil jaune, mais inférieure au seuil rouge.

  Rouge : indique que la température actuelle est supérieure au seuil rouge.

- *Yellow Threshold* : affiche la valeur du seuil jaune du capteur thermique.
- *Red Threshold* : affiche la valeur du seuil rouge du capteur thermique.

Le tableau suivant répertorie les valeurs des seuils jaune et rouge pour les deux capteurs thermiques applicables sur différents modèles de commutateurs PoE :

Modèle	Seuil jaune du capteur thermique 1	Seuil rouge du capteur thermique 1	Seuil jaune du capteur thermique 2	Seuil rouge du capteur thermique 2
SF220-24P	54° C (129° F)	59° C (138° F)	55° C (131° F)	60° C (140° F)
SF220-48P	48° C (118° F)	54° C (129° F)	49° C (120° F)	55° C (131° F)
SG220-26P	52° C (126° F)	56° C (133° F)	58° C (136° F)	62° C (144° F)
SG220-28MP	48° C (118° F)	54° C (129° F)	49° C (120° F)	55° C (131° F)
SG220-50P	51° C (124° F)	57° C (135° F)	50° C (122° F)	55° C (131° F)

Gestion du contrôle à distance (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 d'interception à un gestionnaire SNMP. L'agent SNMP local compare les compteurs en temps réel par rapport à des seuils prédéfinis et génère des alarmes, sans qu'une plate-forme de gestion SNMP centrale n'ait à générer des interrogations. Il s'agit d'un mécanisme efficace 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. RMON permet en outre au gestionnaire d'obtenir des rapports d'état en temps opportun, le commutateur signalant les événements à mesure qu'ils se produisent.

Cette fonction vous permet de réaliser les actions suivantes :

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

REMARQUE Pour une configuration RMON efficace, assurez-vous d'activer le service SNMP sur le commutateur.

Affichage des statistiques RMON

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

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

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

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

ÉTAPE 2 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port ou le LAG pour lequel les statistiques RMON sont affichées.

- **Refresh Rate** : sélectionnez la durée qui s'écoule avant l'actualisation des statistiques RMON.

Les champs suivants s'affichent pour l'interface sélectionnée :

- **RMON Received Bytes (Octets)** : nombre d'octets reçus, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **RMON Drop Events** : nombre de paquets ayant été abandonnés.
- **RMON Received Packets** : nombre de paquets reçus, y compris les paquets erronés, ainsi que les paquets de multidestination et de diffusion.
- **RMON Broadcast Packets Received** : nombre de paquets de diffusion corrects reçus. Ce nombre n'inclut pas les paquets de multidestination.
- **RMON Multicast Packets Received** : nombre de paquets de multidestination corrects reçus.
- **RMON CRC & Align Errors** : nombre d'erreurs d'alignement et CRC qui se sont produites.
- **RMON Undersize Packets** : nombre de paquets de taille insuffisante (moins de 64 octets) reçus.
- **RMON Oversize Packets** : nombre de paquets de taille excessive (plus de 1 518 octets) reçus.
- **RMON Fragments** : nombre de fragments (paquets de moins de 64 octets, à l'exception des bits de synchronisation, mais incluant les octets FCS) reçus.
- **RMON Jabbers** : nombre de paquets reçus ayant une longueur supérieure à 1 632 octets. Ce nombre exclut les bits de synchronisation, mais inclut les octets FCS qui comportaient une séquence FCS (Frame Check Sequence) erronée avec un nombre entier d'octets (erreur FCS) ou une séquence FCS erronée avec un nombre non entier d'octets (erreur d'alignement). Un paquet long est une trame Ethernet respectant les critères suivants :
  - La longueur des données du paquet est supérieure à la MRU.
  - Le paquet a un CRC non valide.
  - Un événement d'erreur Rx n'a pas été détecté.
- **RMON Collisions** : nombre de collisions reçues. Si les cadres géants sont activés, le seuil des trames longues est augmenté de façon à correspondre à la taille maximale des cadres géants.

- **Frames of 64 Bytes** : nombre de trames de 64 octets reçues.
- **Frames of 65 to 127 Bytes** : nombre de trames de 65 à 127 octets reçues.
- **Frames of 128 to 255 Bytes** : nombre de trames de 128 à 255 octets reçues.
- **Frames of 256 to 511 Bytes** : nombre de trames de 256 à 511 octets reçues.
- **Frames of 512 to 1023 Bytes** : nombre de trames de 512 à 1 023 octets reçues.
- **Frames Greater than 1024 Bytes** : nombre de trames de 1 024 à 2 000 octets et de cadres géants reçus.

ÉTAPE 3 Cliquez sur **Clear Interface Counters** pour effacer les compteurs de statistiques RMON de l'interface sélectionnée.

ÉTAPE 4 Cliquez sur **Refresh** pour actualiser manuellement les compteurs de statistiques RMON pour l'interface sélectionnée.

ÉTAPE 5 Cliquez sur **View All Interfaces Statistics** pour voir l'ensemble des compteurs de statistiques RMON sur une seule et même page. La table RMON Statistics Table affiche les compteurs de statistiques RMON de toutes les interfaces. Cette page vous permet de réaliser les actions suivantes :

- Sélectionnez la fréquence d'actualisation dans le menu déroulant **Refresh Rate**.
- Sélectionnez une interface et cliquez sur **Clear Interface Counters** pour effacer les compteurs de statistiques RMON de l'interface sélectionnée.
- Cliquez sur **Clear All Interface Counters** pour effacer les compteurs de statistiques RMON de toutes les interfaces.
- Sélectionnez une interface et cliquez sur **View Interface Statistics** pour voir les compteurs de statistiques RMON de l'interface sélectionnée sur une seule page.
- Cliquez sur **Refresh** pour actualiser manuellement les compteurs de statistiques RMON pour toutes les interfaces.

Configuration et affichage des historiques RMON

RMON vous permet de surveiller les statistiques par interface. Vous pouvez configurer la fréquence d'échantillonnage, la quantité d'échantillons à stocker, ainsi que l'interface à partir de laquelle recueillir les données via la page History Control Table. Une fois que les données ont été échantillonnées et stockées, elles apparaissent sur la page History Table que vous pouvez consulter en cliquant sur **History Table**.

Configuration des échantillons de contrôle d'historique RMON

Pour définir les échantillons de contrôle RMON :

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

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. Le champ **Current Number of Samples** représente donc le nombre d'échantillons réellement accordé à la demande, ce nombre étant inférieur ou égal à la valeur demandée.

ÉTAPE 2 Cliquez sur **Add** pour ajouter un échantillon de contrôle d'historique.

ÉTAPE 3 Saisissez les informations suivantes :

- **New History Entry** : affiche le numéro de la nouvelle entrée de l'historique.
- **Source Interface** : sélectionnez le port ou le LAG à partir duquel les échantillons d'historique doivent être recueillis.
- **Max No. of Samples to Keep** : saisissez le nombre d'échantillons à stocker.
- **Interval** : saisissez la durée (en secondes) pendant laquelle des échantillons doivent être collectés au niveau de l'interface.
- **Owner** : saisissez l'utilisateur ou la station RMON ayant demandé les informations RMON.

ÉTAPE 4 Cliquez sur **Apply**. L'échantillon de contrôle d'historique RMON est ajouté et la configuration de fonctionnement est mise à jour.

ÉTAPE 5 Cliquez sur **History Table** pour afficher les statistiques réelles.

Affichage des statistiques de l'historique RMON

La page History Table affiche les échantillonnages réseau statistiques propres à l'interface. Les échantillons sont configurés dans la table History Control Table décrite dans la section précédente.

Pour afficher les statistiques de l'historique RMON :

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

ÉTAPE 2 Cliquez sur **History Table**.

ÉTAPE 3 Sélectionnez un numéro d'entrée pour afficher les échantillons associés à cette entrée d'historique et cliquez sur **Go**.

Les champs suivants s'affichent pour l'échantillon d'historique sélectionné :

- **History Entry No.** : numéro de l'entrée dans l'historique.
- **Owner** : propriétaire de l'entrée dans l'historique.
- **Sample No.** : les statistiques ont été récupérées à partir de cet échantillon.
- **Drop Events** : nombre de paquets abandonnés en raison d'un manque de ressources réseau lors de l'intervalle d'échantillonnage. Ce champ peut ne pas correspondre au nombre exact de paquets abandonnés, mais plutôt au nombre de détections de paquets de ce type.
- **Bytes Received** : nombre d'octets reçus, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **Packets Received** : nombre de paquets reçus, y compris les paquets erronés, ainsi que les paquets de multidestination et de diffusion.
- **Broadcast Packets** : nombre de paquets de diffusion corrects reçus. Ce nombre n'inclut pas les paquets de multidestination.
- **Multicast Packets** : nombre de paquets de multidestination corrects reçus.
- **CRC & Align Errors** : nombre d'erreurs d'alignement et CRC qui se sont produites.
- **Undersize Packets** : nombre de paquets de taille insuffisante (moins de 64 octets) reçus.
- **Oversize Packets** : nombre de paquets de taille excessive (plus de 1 518 octets) reçus.
- **Fragments** : nombre de fragments (paquets de moins de 64 octets) reçus, à l'exception des bits de synchronisation, mais incluant les octets FCS.

- **Jabbers** : nombre de paquets reçus ayant une longueur supérieure à 1 632 octets. Ce nombre exclut les bits de synchronisation, mais inclut les octets FCS qui comportaient une séquence FCS 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.
- **Utilization** : pourcentage du trafic actuel de l'interface par rapport au trafic maximum pouvant être géré par cette dernière.

ÉTAPE 4 Cliquez sur **History Control Table** pour retourner à la page du même nom.

Configuration et affichage des événements RMON

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

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

Configuration des événements RMON

La page Events permet de configurer des événements qui correspondent à des actions effectuées quand une alarme est générée (les alarmes sont définies sur la page Alarms). Un événement peut être n'importe quelle combinaison de journaux et de messages d'interception. Si l'action inclut la journalisation des événements, ceux-ci s'affichent sur la page Event Log Table.

Pour configurer les événements RMON :

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

ÉTAPE 2 Cliquez sur **Add** pour ajouter un événement RMON.

ÉTAPE 3 Saisissez les informations suivantes :

- **Event Entry** : affiche le numéro de l'entrée d'événement.
- **Community** : saisissez la chaîne de communauté SNMP à inclure lors de l'envoi de messages d'interception.

- **Description** : saisissez un nom pour l'événement. Ce nom est utilisé pour joindre une alarme à un événement.
- **Notification Type** : sélectionnez le type d'action résultant de cet événement. Les options disponibles sont les suivantes :
  - *None* : aucune action ne se produit lorsque l'alarme se déclenche.
  - *Log (Event Log Table)* : ajoute une entrée de journal à la table du journal d'événements lorsque l'alarme se déclenche.
  - *Trap (SNMP Manager and Syslog Server)* : envoie un message d'interception au serveur de journalisation distante lorsque l'alarme se déclenche.
  - *Log and Trap* : ajoute une entrée de journal à la table du journal d'événements et envoie un message d'interception au serveur de journalisation distante lorsque l'alarme se déclenche.
- **Owner** : saisissez le périphérique ou l'utilisateur ayant défini l'événement.

ÉTAPE 4 Cliquez sur **Apply**. L'événement RMON est ajouté et la configuration de fonctionnement est mise à jour.

ÉTAPE 5 Cliquez sur **Event Log Table** pour afficher le journal des alarmes déclenchées et consignées.

Affichage du journal d'événements RMON

La page Event Log Table affiche le journal des événements (actions) qui se sont produits. Un événement peut être journalisé lorsqu'il est de type *Log* ou *Log and Trap*. L'action indiquée dans l'événement est mise en œuvre lorsque cet événement est lié à une alarme (voir la section **Configuration des alarmes RMON**) et que les conditions de l'alarme sont réunies.

Pour afficher le journal d'événements RMON :

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

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

Les champs suivants s'affichent :

- **Event Entry No.** : numéro d'entrée dans le journal de l'événement.
- **Log No.** : numéro du journal (au sein de l'événement).
- **Log Time** : heure à laquelle l'entrée a été enregistrée dans le journal.

- **Description** : description de l'événement qui a déclenché l'alarme.

ÉTAPE 3 Cliquez sur **Event Table** pour revenir à la page des événements.

Configuration des alarmes RMON

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

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

La page Alarms 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 définir des alarmes RMON :

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

ÉTAPE 2 Cliquez sur **Add** pour ajouter une alarme RMON.

ÉTAPE 3 Saisissez les informations suivantes :

- **Alarm Entry** : affiche le numéro d'entrée de l'alarme.
- **Interface** : sélectionnez un port ou un LAG.
- **Counter Name** : sélectionnez la variable MIB qui indique le type d'occurrence mesuré.
- **Sample Type** : sélectionnez la méthode d'échantillonnage pour générer une alarme. Les options disponibles sont les suivantes :
  - *Absolute* : si le seuil est franchi, une alarme est générée.
  - *Delta* : soustrait la valeur du dernier échantillon de la valeur actuelle. La différence obtenue est comparée au seuil. Si le seuil est franchi, une alarme est générée.

- **Rising Threshold** : saisissez la valeur de compteur supérieure qui déclenche l'alarme de seuil supérieur.
- **Rising Event** : sélectionnez un événement, parmi ceux définis sur la page des événements, à mettre en œuvre en cas de déclenchement d'un événement de hausse.
- **Falling Threshold** : saisissez la valeur de compteur inférieure qui déclenche l'alarme de seuil inférieur.
- **Falling Event** : sélectionnez un événement, parmi ceux définis sur la page des événements, à mettre en œuvre en cas de déclenchement d'un événement de baisse.
- **Startup Alarm** : sélectionnez le premier événement à partir duquel lancer la génération d'alarmes. La hausse est définie en franchissant le seuil en partant d'un seuil de faible valeur vers un seuil de valeur plus importante.
  - *Rising Alarm* : une valeur de compteur en hausse déclenche l'alarme de seuil supérieur.
  - *Falling Alarm* : une valeur de compteur en baisse déclenche l'alarme de seuil inférieur.
  - *Rising and Falling Alarm* : des valeurs de compteur en hausse et en baisse déclenchent l'alarme.
- **Interval** : saisissez l'intervalle (en secondes) entre les alarmes.
- **Owner** : saisissez le nom de l'utilisateur ou du système de gestion du réseau qui reçoit l'alarme.

ÉTAPE 4 Cliquez sur **Apply**. L'alarme RMON est ajoutée et la configuration de fonctionnement est mise à jour.

3

Administration : Journaux système

Ce chapitre décrit la fonction des journaux 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 envoyé à l'interface de la console ;
- journal enregistré dans une liste cyclique d'événements journalisés dans la mémoire RAM et effacé lors du redémarrage du commutateur ;
- journal enregistré dans un fichier journal cyclique enregistré dans la mémoire Flash et conservé d'un redémarrage à l'autre.

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

Ce chapitre aborde les points suivants :

Configurer les paramètres des journaux système

Vous pouvez activer ou désactiver la journalisation sur le commutateur et sélectionner les événements à consigner par niveau de gravité. Les niveaux de gravité des événements sont répertoriés du plus élevé au plus faible, comme suit :

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

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

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

Si vous choisissez d'enregistrer un niveau de gravité spécifique dans un journal, tous les événements de sévérité plus élevée le seront également. Les événements de gravité plus faible ne seront pas enregistrés dans le journal. Par exemple, si **Warning** est sélectionné, tous les niveaux de gravité de type **Warning** et plus élevés sont enregistrés dans le journal (Emergency, Alert, Critical, Error et Warning). Aucun événement dont le niveau de gravité est inférieur à **Warning** n'est enregistré (Notice, Informational et Debug).

Pour configurer des paramètres de journalisation globaux :

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

ÉTAPE 2 Saisissez les informations suivantes :

- **Logging** : sélectionnez l'option **Enable** pour activer la journalisation sur le commutateur ou décochez cette case pour la désactiver.
- **RAM Memory Logging** : sélectionnez l'option **Enable** pour activer la journalisation dans la mémoire RAM et vérifiez les niveaux de gravité des messages à consigner dans la mémoire RAM.
- **Flash Memory Logging** : sélectionnez l'option **Enable** pour activer la journalisation dans la mémoire Flash et vérifiez les niveaux de gravité des messages à consigner dans la mémoire Flash.

ÉTAPE 3 Cliquez sur **Apply.** Les paramètres de journalisation globaux sont définis et la configuration de fonctionnement est mise à jour.

Configurer les paramètres de journalisation distante

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

Pour configurer un serveur SYSLOG distant :

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

ÉTAPE 2 Cliquez sur **Add** pour ajouter un serveur SYSLOG distant.

ÉTAPE 3 Saisissez les informations suivantes :

- **Server Definition** : indiquez si vous souhaitez identifier le serveur de journalisation distante par son adresse IP ou par son nom.
- **IP Version** : sélectionnez **Version 4** ou **Version 6** si le serveur de journalisation distante est identifié par adresse IP.
- **Log Server IP Address/Name** : saisissez l'adresse IP ou le nom d'hôte du serveur de journalisation distante.
- **UDP Port** : saisissez le numéro du port UDP auquel les messages de journal sont envoyés.
- **Facility** : sélectionnez un équipement à partir duquel les journaux système sont envoyés au serveur distant. Un seul équipement peut être affecté à un serveur.
- **Minimum Severity** : sélectionnez le niveau minimum de gravité des messages de journalisation système à envoyer au serveur.

ÉTAPE 4 Cliquez sur **Apply.** Le serveur SYSLOG distant est ajouté et la configuration de fonctionnement est mise à jour.

Afficher les journaux de la mémoire

Le commutateur peut enregistrer des informations dans les journaux suivants :

- Journal de la RAM (effacé lors du redémarrage). Pour plus d'informations, reportez-vous à la section **Afficher les journaux de la mémoire RAM**.
- Journal de la mémoire Flash (uniquement effacé sur instruction de l'utilisateur). Pour plus d'informations, reportez-vous à la section **Afficher les journaux de la mémoire Flash**.

Vous pouvez configurer les messages consignés dans chaque journal par niveau de sévérité. Un message peut être enregistré dans plusieurs journaux, y compris dans les journaux stockés sur des serveurs SYSLOG externes.

Afficher les journaux de la mémoire RAM

La page RAM Memory affiche tous les messages enregistrés dans la mémoire RAM (cache) dans l'ordre chronologique inverse. Les entrées sont enregistrées dans le journal de la mémoire RAM en fonction de la configuration définie sur la page Log Settings.

Pour consulter les journaux de la mémoire RAM :

ÉTAPE 1 Cliquez sur **Status and Statistics** > **View Log** > **RAM Memory**.

Les champs suivants s'affichent :

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

ÉTAPE 2 Cliquez sur **Clear Logs** pour effacer les messages des journaux.

ÉTAPE 3 Par défaut, l'icône d'état d'alerte SYSLOG s'affiche et clignote en cas de journalisation d'un message SYSLOG dont le niveau de sévérité se situe au-dessus du niveau *critique*. Pour désactiver le clignotement de cette icône d'alerte, cliquez sur **Disable Alert Icon Blinking**. L'icône SYSLOG Alert Status n'est plus affichée.

Afficher les journaux de la mémoire Flash

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

Pour consulter les journaux de la mémoire Flash :

ÉTAPE 1 Cliquez sur **Status and Statistics** > **View Log** > **Flash Memory**.

Les champs suivants s'affichent :

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

ÉTAPE 2 Cliquez sur **Clear Logs** pour effacer les messages des journaux.

4

Administration : Gestion de fichiers

Ce chapitre vous présente la gestion des fichiers système : mise à niveau du microprogramme du système, redémarrage du commutateur, restauration des paramètres d'origine par défaut du commutateur, gestion des fichiers de configuration et des fichiers journaux, etc.

Il contient les rubriques suivantes :

- **Fichiers et types de fichiers**
- **Actions des fichiers**
- **Mettre à niveau/sauvegarder le microprogramme/la langue**
- **Image active**
- **Télécharger/sauvegarder la configuration ou les journaux**
- **Propriétés du fichier de configuration**
- **Copier/enregistrer les fichiers de configuration**
- **Configuration automatique DHCP**

Fichiers et types de fichiers

Les fichiers système contiennent des informations de configuration ou des images du microprogramme.

Vous pouvez effectuer diverses actions avec ces fichiers, par exemple :

- sélectionner le fichier du microprogramme à partir duquel le commutateur démarrera ;
- copier divers types de fichiers de configuration en interne sur le commutateur ;
- copier des fichiers vers ou depuis un périphérique externe, comme un serveur externe.

Les méthodes de transfert de fichiers disponibles sont les suivantes :

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

Les fichiers de configuration du commutateur sont définis en fonction de leur type et comportent les réglages et les valeurs de paramètres du commutateur. Lorsqu'une configuration est référencée sur le commutateur, cette opération s'effectue en fonction de son type de fichier de configuration (par exemple, configuration de démarrage ou configuration de fonctionnement) 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 le commutateur englobent les fichiers du microprogramme et les fichiers journaux. Ils sont couramment 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 le Bloc-notes une fois copiés sur un périphérique externe, comme un PC.

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

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

  En cas de redémarrage du commutateur, la configuration de fonctionnement est perdue. Lors du redémarrage du commutateur, ce type de fichier est copié depuis la configuration de démarrage enregistrée dans la mémoire Flash vers la configuration de fonctionnement stockée dans la RAM.

  Pour conserver toute modification apportée au commutateur, vous devez enregistrer la configuration de fonctionnement 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 de fonctionnement dans la configuration de démarrage, le commutateur recrée, lors de son redémarrage, une configuration de fonctionnement qui inclut les modifications apportées depuis le dernier enregistrement de la configuration de fonctionnement dans la configuration de démarrage.

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

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

- **Configuration de secours** : copie manuelle des définitions de paramètres servant à protéger le système en cas d'arrêt ou à maintenir un état de fonctionnement spécifique. Vous pouvez copier la configuration miroir, la configuration de démarrage ou la configuration de fonctionnement dans la configuration de secours. La configuration de secours est conservée dans la mémoire Flash et est préservée en cas de redémarrage du commutateur.

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

  - Le commutateur a fonctionné de façon continue pendant 24 heures.
  - Aucune modification n'a été apportée à la configuration de fonctionnement au cours des dernières 24 heures.
  - La configuration de démarrage est identique à la configuration de fonctionnement.

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

  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 qui sera conservée en cas de redémarrage du commutateur.

- **Microprogramme** : programme qui contrôle les opérations et les fonctions du commutateur. Plus communément appelé l'image.

- **Fichier de langue** : dictionnaire qui permet d'afficher l'interface Web dans la langue sélectionnée.

- **Journaux Flash** : messages SYSLOG stockés dans la mémoire Flash.

Actions des fichiers

Les actions suivantes peuvent être réalisées pour gérer le microprogramme, les fichiers de configuration et les journaux :

- mettre à niveau l'image du microprogramme, remplacer un fichier de seconde langue ou sauvegarder le microprogramme comme décrit dans la section **Mettre à niveau/sauvegarder le microprogramme/la langue** ;
- afficher l'image du microprogramme actuellement utilisée ou sélectionner l'image à utiliser lors du redémarrage suivant, comme décrit dans la section **Image active** ;
- enregistrer les fichiers de configuration du commutateur à un emplacement situé sur un autre périphérique, comme décrit dans la section **Télécharger/sauvegarder la configuration ou les journaux** ;
- effacer les types de fichiers de configuration de démarrage ou de configuration de secours, comme décrit dans la section **Propriétés du fichier de configuration** ;
- copier un type de fichier de configuration dans un autre type de fichier de configuration, comme décrit dans la section **Copier/enregistrer les fichiers de configuration** ;
- télécharger automatiquement un fichier de configuration depuis un serveur DHCP vers le commutateur, comme décrit dans la section **Configuration automatique DHCP**.

ATTENTION Toutes les modifications apportées depuis le dernier enregistrement du fichier seront perdues lors du redémarrage du commutateur, sauf si la configuration de fonctionnement est copiée manuellement dans la configuration de démarrage, dans la configuration de secours ou dans un fichier externe. Nous vous conseillons d'enregistrer la configuration de fonctionnement dans la configuration de démarrage avant de vous déconnecter afin de conserver toute modification effectuée au cours de cette session.

Une icône **X** rouge qui s'affiche à gauche du lien d'application **Save** 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 **Save**, la page Copy/Save Configuration s'affiche. Enregistrez le fichier de configuration de fonctionnement en le copiant dans le fichier de configuration de démarrage. Une fois cet enregistrement effectué, l'icône **X** rouge et le lien Save sont masqués.

Mettre à niveau/sauvegarder le microprogramme/la langue

La page Upgrade/Backup Firmware/Language vous permet de mettre à niveau ou de sauvegarder l'image du microprogramme et d'importer un fichier de seconde langue.

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

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

Mettre à niveau/enregistrer l'image du microprogramme

Deux images du microprogramme, 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 microprogramme, la nouvelle image remplace toujours celle identifiée comme étant inactive. Une fois le nouveau microprogramme 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 **Image active**, et que vous démarriez le commutateur en suivant le processus présenté dans la section **Redémarrage du commutateur**.

Vous pouvez également enregistrer une copie de l'image active du commutateur à un emplacement de destination, comme un serveur TFTP.

Pour mettre à niveau ou sauvegarder l'image du microprogramme :

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

ÉTAPE 2 Pour remplacer l'image du microprogramme sur le commutateur par une nouvelle version stockée sur un serveur TFTP, saisissez les informations suivantes :

- **Transfer Method** : sélectionnez **via TFTP** comme méthode de transfert.
- **Save Action** : sélectionnez **Upgrade** comme action.
- **File Type** : sélectionnez **Firmware Image** comme type de fichier.
- **TFTP Server Definition** : indiquez si vous souhaitez spécifier le serveur TFTP par son adresse IP ou par son nom de domaine.

- **IP Version** : sélectionnez **Version 4** ou **Version 6** si le serveur TFTP est identifié par adresse IP.
- **TFTP Server IP Address/Name** : saisissez l'adresse IP ou le nom de domaine du serveur TFTP.
- **Source File Name** : saisissez le nom de l'image du microprogramme stockée sur le serveur TFTP.

ÉTAPE 3 Cliquez sur **Apply**.

ÉTAPE 4 Pour remplacer l'image du microprogramme sur le commutateur par une nouvelle version stockée sur un autre périphérique tel un PC local par exemple, saisissez les informations suivantes :

- **Transfer Method** : sélectionnez **via HTTP/HTTPS** comme méthode de transfert.
- **Save Action** : sélectionnez **Upgrade** comme action.
- **File Type** : sélectionnez **Firmware Image** comme type de fichier.
- **File Name** : cliquez sur **Browse** pour sélectionner une image du microprogramme située sur un autre périphérique, comme un PC local.

ÉTAPE 5 Cliquez sur **Apply**.

ÉTAPE 6 Pour enregistrer une copie de l'image active du commutateur sur un serveur TFTP, saisissez les informations suivantes :

- **Transfer Method** : sélectionnez **via TFTP** comme méthode de transfert.
- **Save Action** : sélectionnez **Backup** comme action.
- **File Type** : sélectionnez **Firmware Image** comme type de fichier.
- **TFTP Server Definition** : indiquez si vous souhaitez spécifier le serveur TFTP par son adresse IP ou par son nom de domaine.
- **IP Version** : sélectionnez **Version 4** ou **Version 6** si le serveur TFTP est identifié par adresse IP.
- **TFTP Server IP Address/Name** : saisissez l'adresse IP ou le nom de domaine du serveur TFTP.
- **Destination File Name** : saisissez le nom de l'image du microprogramme qui sera enregistrée sur le serveur TFTP.

ÉTAPE 7 Cliquez sur **Apply**.

Mettre à niveau le fichier de langue

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

Pour charger un nouveau fichier de langue :

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

ÉTAPE 2 Pour charger un fichier de langue depuis un serveur TFTP sur le commutateur, saisissez les informations suivantes :

- **Transfer Method** : sélectionnez **via TFTP** comme méthode de transfert.
- **Save Action** : sélectionnez **Upgrade** comme action.
- **File Type** : sélectionnez **Language File** comme type de fichier.
- **TFTP Server Definition** : indiquez si vous souhaitez spécifier le serveur TFTP par son adresse IP ou par son nom de domaine.
- **IP Version** : sélectionnez **Version 4** ou **Version 6** si le serveur TFTP est identifié par adresse IP.
- **TFTP Server IP Address/Name** : saisissez l'adresse IP ou le nom de domaine du serveur TFTP.
- **Source File Name** : saisissez le nom du fichier de langue source stocké sur le serveur TFTP.

ÉTAPE 3 Cliquez sur **Apply**.

ÉTAPE 4 Pour charger un fichier de langue depuis un autre périphérique, comme un PC local, sur le commutateur, procédez comme suit :

- **Transfer Method** : sélectionnez **via HTTP/HTTPS** comme méthode de transfert.
- **Save Action** : sélectionnez **Upgrade** comme action.
- **File Type** : sélectionnez **Language File** comme type de fichier.
- **File Name** : cliquez sur **Browse** pour sélectionner un nouveau fichier de langue situé sur un autre périphérique, comme un PC local.

ÉTAPE 5 Cliquez sur **Apply**.

Image active

Deux images du microprogramme, 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 devez redémarrer le commutateur.)

Pour sélectionner l'image active :

ÉTAPE 1 Cliquez sur **Administration** > **File Management** > **Active Image**.

Les champs suivants s'affichent :

- **Active Image** : affiche le fichier image actuellement actif sur le commutateur.
- **Active Image Version Number** : affiche la version du microprogramme de l'image active.
- **Active Image Version Number After Reboot** : affiche la version du microprogramme de l'image active après le redémarrage.

ÉTAPE 2 Sélectionnez l'image dans le menu déroulant **Active Image After Reboot** pour identifier l'image du microprogramme utilisée en tant qu'image active après le redémarrage du commutateur.

ÉTAPE 3 Cliquez sur **Apply**.

ÉTAPE 4 Redémarrez le commutateur. Le commutateur démarrera avec l'image active sélectionnée.

Télécharger/sauvegarder la configuration ou les journaux

La page Download/Backup Configuration/Log permet de :

- sauvegarder des fichiers de configuration ou des journaux depuis le commutateur vers un périphérique externe ;
- restaurer des fichiers de configuration depuis un périphérique externe vers le commutateur.

Lorsque vous restaurez un fichier de configuration vers la configuration de fonctionnement, 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 vers la 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 de fonctionnement.

Charger le fichier de configuration

Pour remplacer un type de fichier par un fichier de configuration sauvegardé :

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

ÉTAPE 2 Pour remplacer un type de fichier sur le commutateur par une nouvelle version de ce type de fichier stockée sur un serveur TFTP, saisissez les informations suivantes :

- **Transfer Method** : sélectionnez **via TFTP** comme méthode de transfert.
- **Save Action** : sélectionnez **Download** comme action.
- **TFTP Server Definition** : indiquez si vous souhaitez spécifier le serveur TFTP par son adresse IP ou par son nom de domaine.
- **IP Version** : sélectionnez **Version 4** ou **Version 6** si le serveur TFTP est identifié par adresse IP.
- **TFTP Server IP Address/Name** : saisissez l'adresse IP ou le nom de domaine du serveur TFTP.
- **Source File Name** : saisissez le nom du fichier source.
- **Destination File Type** : sélectionnez le type du fichier de configuration à mettre à niveau. Le commutateur prend en charge la mise à niveau des configurations de fonctionnement, de démarrage et de secours.

ÉTAPE 3 Cliquez sur **Apply.** Le fichier est mis à niveau sur le commutateur (en fonction du type de fichier).

ÉTAPE 4 Pour remplacer un type de fichier sur le commutateur par une nouvelle version de ce type de fichier stockée sur un autre périphérique tel un PC local, saisissez les informations suivantes :

- **Transfer Method** : sélectionnez **via HTTP/HTTPS** comme méthode de transfert.
- **Save Action** : sélectionnez **Download** comme action.
- **File Name** : cliquez sur **Browse** pour sélectionner un fichier source.
- **Destination File Type** : sélectionnez le type du fichier de configuration à mettre à niveau.

ÉTAPE 5 Cliquez sur **Apply**. Le fichier est transféré de l'autre périphérique vers le commutateur.

Enregistrer le fichier de configuration ou les journaux

Pour copier les types de fichiers de configuration ou le journal Flash sur le commutateur dans un fichier d'un autre périphérique :

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

ÉTAPE 2 Pour copier un type de fichier sur le commutateur dans un fichier stocké sur un serveur TFTP, saisissez les informations suivantes :

- **Transfer Method** : sélectionnez **via TFTP** comme méthode de transfert.
- **Save Action** : sélectionnez **Backup** comme action.
- **TFTP Server Definition** : indiquez si vous souhaitez spécifier le serveur TFTP par son adresse IP ou par son nom de domaine.
- **IP Version** : sélectionnez **Version 4** ou **Version 6** si le serveur TFTP est identifié par adresse IP.
- **TFTP Server IP Address/Name** : saisissez l'adresse IP ou le nom de domaine du serveur TFTP.
- **Source File Type** : sélectionnez le type de fichier de configuration à stocker sur le serveur TFTP. Le commutateur prend en charge le stockage des configurations de fonctionnement, de démarrage, de secours, miroir, de même que celui du journal Flash.

- **Destination File Name** : sélectionnez le nom du fichier à stocker sur le serveur TFTP.

ÉTAPE 3 Cliquez sur **Apply**. Le fichier est sauvegardé sur le serveur TFTP (en fonction du type de fichier).

ÉTAPE 4 Pour copier un type de fichier sur le commutateur dans un fichier stocké sur un autre périphérique tel un PC local, saisissez les informations suivantes :

- **Transfer Method** : sélectionnez **via HTTP/HTTPS** comme méthode de transfert.
- **Save Action** : sélectionnez **Backup** comme action.
- **Source File Type** : sélectionnez le type du fichier de configuration à stocker.

ÉTAPE 5 Cliquez sur **Apply**.

ÉTAPE 6 Recherchez où stocker le fichier de configuration ou le journal Flash sélectionné, puis cliquez sur **Save**.

Propriétés du fichier de configuration

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

Pour effacer des fichiers de configuration et/ou pour connaître la date de création des fichiers de configuration :

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

Les champs suivants s'affichent :

- **Configuration File Name** : le type de fichier.
- **Creation Time** : la date et l'heure de la modification du fichier.

ÉTAPE 2 Si nécessaire, choisissez la configuration de démarrage et/ou la configuration de secours, et cliquez sur **Clear Files** pour supprimer ces fichiers.

Copier/enregistrer les fichiers de configuration

Lorsque vous cliquez sur **Apply** dans une fenêtre, les modifications que vous avez apportées aux paramètres de configuration du commutateur sont uniquement stockées dans la configuration de fonctionnement. Pour conserver les paramètres de la configuration de fonctionnement, celle-ci doit être copiée dans un autre type de configuration ou enregistrée en tant que fichier sur un autre périphérique.

La page Copy/Save Configuration permet de copier ou d'enregistrer un fichier de configuration dans un autre fichier, à des fins de sauvegarde. En bas de la page se trouve le bouton **Disable Save Icon Blinking**. Cliquez dessus pour activer ou désactiver le clignotement de l'icône d'enregistrement.

ATTENTION Sauf si la configuration de fonctionnement est copiée dans la configuration de démarrage ou dans 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 de fonctionnement vers la configuration de fonctionnement, de démarrage ou de secours ;
- de la configuration de démarrage vers la configuration de fonctionnement, de démarrage ou de secours ;
- de la configuration de secours vers la configuration de fonctionnement, de démarrage ou de secours ;
- de la configuration miroir vers la configuration de fonctionnement, de démarrage ou de secours.

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

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

ÉTAPE 2 Saisissez les informations suivantes :

- **Source File Name** : sélectionnez le type de fichier de configuration à copier.
- **Destination File Name** : sélectionnez le type de fichier de configuration qui remplacera le fichier source.

ÉTAPE 3 Cliquez sur **Apply.** Le fichier est copié et le commutateur mis à jour.

ÉTAPE 4 Le champ **Save Icon Blinking** indique si une icône clignote lorsque certaines données ne sont pas enregistrées. Pour activer ou désactiver cette fonctionnalité, cliquez sur **Disable Save Icon Blinking** ou **Enable Save Icon Blinking**.

Configuration automatique DHCP

Le processus de configuration automatique permet de transférer les informations de configuration vers les hôtes d'un réseau TCP/IP. La fonctionnalité de configuration automatique permet à un commutateur de se baser sur ce protocole pour télécharger des fichiers de configuration depuis un serveur TFTP.

Par défaut, le commutateur est activé en tant que client DHCP lorsque la configuration automatique est activée. Le commutateur peut être configuré comme client DHCPv4 auquel cas la configuration automatique depuis un serveur DHCPv4 est prise en charge et/ou comme client DHCPv6 auquel cas c'est la configuration automatique depuis un serveur DHCPv6 qui est prise en charge.

La configuration automatique DHCPv4 se déclenche dans les cas suivants :

- Après le redémarrage du commutateur, quand une adresse IP est allouée ou renouvelée dynamiquement (via DHCPv4).
- Lors d'une demande explicite de renouvellement DHCPv4 et si le commutateur et le serveur sont configurés pour agir ainsi.
- Lors du renouvellement automatique du bail DHCPv4.

La configuration automatique DHCPv6 est déclenchée dans les cas suivants :

- Lorsqu'un serveur DHCPv6 envoie des informations au commutateur. Cet envoi se produit dans les cas suivants :
  - Quand le client IPv6 sans état est activé.
  - Quand des messages DHCPv6 proviennent du serveur.
  - Lorsque des informations DHCPv6 sont actualisées par le commutateur.
  - Lorsque le client DHCPv6 sans état est activé après le redémarrage du commutateur.
- Lorsque les paquets du serveur DHCPv6 contiennent l'option de nom de fichier de configuration.

Options de serveur DHCP

Les messages DHCP peuvent éventuellement contenir le nom/l'adresse du serveur de configuration, ainsi que le nom/le chemin du fichier de configuration (facultatif). Ces options sont disponibles dans les messages d'offre provenant des serveurs DHCPv4 et dans les messages de réponse informative provenant des serveurs DHCPv6.

Les informations de secours (adresse/nom du serveur de configuration et nom/chemin du fichier de configuration) peuvent être configurées sur la page de configuration automatique DHCP. Ces informations se révèlent utiles quand le message DHCPv4 ou DHCPv6 ne les renseigne pas.

Processus de configuration automatique

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

- Le serveur DHCP est sollicité pour permettre l'acquisition du nom/de l'adresse du serveur TFTP, ainsi que du nom/du chemin du fichier de configuration (options DHCPv4 : 66,150 et 67, options DHCPv6 : 59 et 60).
- Si le serveur DHCP n'est pas en mesure de fournir des informations sur les options du fichier de configuration et du serveur, le nom du fichier de configuration de secours défini par l'utilisateur est utilisé pour DHCPv4 ou DHCPv6.
- Si le serveur DHCP n'est pas en mesure de fournir ces informations et si le paramètre d'adresse du serveur TFTP de secours n'est pas renseigné, le commutateur envoie des messages de requête TFTP à une adresse IPv4 de diffusion limitée et se sert ensuite du premier serveur TFTP dont il parvient à obtenir une réponse pour poursuivre le processus de configuration automatique.

Définir les paramètres de la configuration automatique DHCP

Pour paramétrer la configuration automatique DHCP, vous devez procéder comme suit :

- Configurez les serveurs DHCPv4 et/ou DHCPv6 de sorte qu'ils transmettent les informations requises. Ce processus n'est pas présenté dans ce guide.
- Définissez les paramètres de la configuration automatique DHCP comme décrit dans cette section.

- Définissez le type de l'adresse IP sur dynamique sur la page relative à l'interface IPv4, comme décrit dans la section **Gestion et interface IPv4**.

La page DHCP Auto Configuration permet d'effectuer les actions suivantes lorsque les informations requises sont absentes des messages DHCP :

- activer la fonctionnalité de configuration automatique DHCP ;
- configurer le commutateur pour qu'il récupère les informations de configuration dans un fichier spécifique sur un serveur donné.

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

- Un fichier de configuration placé sur le serveur TFTP doit correspondre aux exigences en termes de forme et de format du fichier de configuration pris en charge. La forme et le format du fichier sont vérifiés, mais la validité des paramètres de configuration n'est pas contrôlée avant son chargement dans la configuration de démarrage.
- Dans IPv4, des adresses IP différentes sont allouées pour chaque cycle de renouvellement DHCP. Pour s'assurer que la configuration des périphériques fonctionne comme prévu, il est conseillé de lier les adresses IP à des adresses MAC dans la table des serveurs DHCP.

REMARQUE La configuration automatique DHCP n'est applicable que lorsque l'adresse IP du commutateur est définie sur dynamique.

Pour définir la configuration automatique DHCP :

ÉTAPE 1 Cliquez sur **Administration** > **File Management** > **DHCP Auto Configuration**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Auto Configuration via DHCP** : cochez la case **Enable** pour activer la fonctionnalité de configuration automatique DHCP sur le commutateur, ou décochez-la pour la désactiver.
- **Backup Server Definition** : indiquez si vous souhaitez spécifier le serveur TFTP par son adresse IP ou par son nom de domaine.
- **IP Version** : sélectionnez **Version 4** ou **Version 6** si le serveur TFTP est identifié par adresse IP.

- **Backup TFTP Server IP Address/Name** : saisissez l'adresse IP ou le nom de domaine du serveur TFTP de secours. Si aucun nom de fichier de configuration n'a été spécifié dans le message DHCP, le commutateur téléchargera le fichier de configuration de secours sur le serveur TFTP de secours.
- **Backup Configuration File** : saisissez le chemin complet et le nom du fichier de configuration sur le serveur TFTP de secours à utiliser si aucun nom de fichier de configuration n'a été spécifié dans le message DHCP.
- **Last Auto Configuration TFTP Server IP Address** : affiche l'adresse IP ou le nom de domaine du serveur TFTP en cours d'utilisation.
- **Last Auto Configuration File Name** : affiche le nom du fichier de configuration situé sur le serveur TFTP actuellement utilisé.

ÉTAPE 3 Cliquez sur **Apply.** Les paramètres de configuration automatique DHCP sont définis et la configuration de fonctionnement est mise à jour.

5

Administration : Informations générales

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

Il contient les rubriques suivantes :

- **Modèles de périphériques**
- **Affichage du récapitulatif système**
- **Configuration des paramètres système**
- **Configuration des paramètres de console**
- **Redémarrage du commutateur**
- **Définition du délai d'expiration en cas de session inactive**
- **Envoi d'une requête Ping à un hôte**
- **Utilisation de Traceroute**

Modèles de périphériques

Tous les modèles peuvent être entièrement gérés via l'interface Web. Le tableau suivant décrit les différents modèles, le nombre et le type de ports qu'ils contiennent, leurs informations PoE et leur PID.

Nom du modèle	Ports et ports d'extension	Ports prenant en charge le PoE	PID
Ethernet rapide			
SF220-24	24 ports cuivre FE et 2 ports combinés spécifiques (GE/SFP)	N/A	SF220-24-K9-NA, SF220-24-K9-EU, SF220-24-K9-UK, SF220-24-K9-AU, SF220-24-K9-CN
SF220-24P	24 ports cuivre FE et 2 ports combinés spécifiques (GE/SFP)	1 à 24	SF220-24P-K9-NA, SF220-24P-K9-EU, SF220-24P-K9-UK, SF220-24P-K9-AU, SF220-24P-K9-CN
SF220-48	48 ports cuivre FE et 2 ports combinés spécifiques (GE/SFP)	N/A	SF220-48-K9-NA, SF220-48-K9-EU, SF220-48-K9-UK, SF220-48-K9-AU, SF220-48-K9-CN
SF220-48P	48 ports cuivre FE et 2 ports combinés spécifiques (GE/SFP)	1 à 48	SF220-48P-K9-NA, SF220-48P-K9-EU, SF220-48P-K9-UK, SF220-48P-K9-AU, SF220-48P-K9-CN
Gigabit Ethernet			
SG220-26	24 ports cuivre GE et 2 ports combinés spécifiques (GE/SFP)	N/A	SG220-26-K9-NA, SG220-26-K9-EU, SG220-26-K9-UK, SG220-26-K9-AU, SG220-26-K9-BR, SG220-26-K9-AR

Nom du modèle	Ports et ports d'extension	Ports prenant en charge le PoE	PID
SG220-26P	24 ports cuivre GE et 2 ports combinés spécifiques (GE/SFP)	1 à 24	SF220-26P-K9-NA, SF220-26P-K9-EU, SF220-26P-K9-UK, SF220-26P-K9-AU, SF220-26P-K9-BR, SF220-26P-K9-AR
SG220-50	48 ports cuivre GE et 2 ports combinés spécifiques (GE/SFP)	N/A	SG220-50-K9-NA, SG220-50-K9-EU, SG220-50-K9-UK, SG220-50-K9-AU, SG220-50-K9-BR, SG220-50-K9-AR
SG220-50P	48 ports cuivre GE et 2 ports combinés spécifiques (GE/SFP)	1 à 48	SF220-50P-K9-NA, SF220-50P-K9-EU, SF220-50P-K9-UK, SF220-50P-K9-AU, SF220-50P-K9-BR, SF220-50P-K9-AR
SG220-28	24 ports cuivre GE et 4 ports SFP	N/A	SG220-28-K9-CN
SG220-28MP	24 ports cuivre GE et 4 ports SFP	1 à 24	SG220-28MP-K9-CN
SG220-52	48 ports cuivre GE et 4 ports SFP	N/A	SG220-52-K9-CN

REMARQUE Certaines fonctions sont disponibles uniquement sur les modèles destinés à un pays spécifique. L'abréviation « -CN » indique que la fonction est applicable uniquement aux SKU relatifs à la Chine. Ces fonctions figurent dans le présent guide. Vous trouverez le PID de votre commutateur sur la page System Summary.

Affichage du récapitulatif système

La page System Summary fournit une vue graphique du commutateur et affiche des informations générales sur celui-ci, notamment des informations sur le système, le logiciel, l'alimentation PoE (le cas échéant), l'état des services TCP/UDP, etc.

Pour afficher les informations générales sur le commutateur, cliquez sur **Status and Statistics** > **System Summary**. Les champs suivants s'affichent :

System Information (informations système)

- **System Description** : description du commutateur.
- **System Location** : emplacement physique du commutateur.
- **System Contact** : nom de la personne à contacter.
- **Host Name** : nom du commutateur. Par défaut, le nom d'hôte du commutateur se compose du mot *Switch* concaténé avec les trois octets les moins significatifs de l'adresse MAC du commutateur (les six chiffres hexadécimaux les plus à droite).

  REMARQUE Cliquez sur **Edit** pour accéder à la page Administration > System Settings et modifier l'emplacement, le contact et/ou le nom d'hôte.
- **System Object ID** : identification unique du fournisseur du sous-système de gestion du réseau contenu dans l'entité SNMP.
- **System Uptime** : temps qui s'est écoulé depuis le dernier redémarrage.
- **Current Time** : heure actuelle du système.
- **Base MAC Address** : adresse MAC du commutateur.
- **Jumbo Frames** : état de prise en charge des cadres géants. Cette prise en charge peut être activée ou désactivée sur la page Port Management > Port Setting.

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

Software Information (informations sur le logiciel)

- **Firmware Version (Active Image)** : numéro de version du microprogramme de l'image active.
- **Firmware MD5 Checksum (Active Image)** : somme de contrôle MD5 du microprogramme de l'image active.
- **Firmware Version (Non-active)** : numéro de version du microprogramme de l'image non active.
- **Firmware MD5 Checksum (Non-active Image)** : somme de contrôle MD5 du microprogramme de l'image non active.
- **Boot Version** : numéro de version du chargeur de démarrage du commutateur.
- **Locale** : paramètres régionaux de la première langue. (Toujours définis sur en-US (anglais des États-Unis).)
- **Language Version** : version du module linguistique de la première langue.
- **Language MD5 Checksum** : somme de contrôle MD5 de la première langue.
- **Locale** : paramètres régionaux de la seconde langue.
- **Language Version** : version du module linguistique de la seconde langue.
- **Language MD5 Checksum** : somme de contrôle MD5 de la seconde langue.

TCP/UDP Services Status (état des services TCP/UDP)

- **HTTP Service** : indique si le service HTTP est activé ou désactivé.
- **HTTPS Service** : indique si le service HTTPS est activé ou désactivé.
- **SNMP Service** : indique si le service SNMP est activé ou désactivé.
- **Telnet Service** : indique si le service Telnet est activé ou désactivé.
- **SSH Service** : indique si le service SSH est activé ou désactivé.

  REMARQUE Cliquez sur **Edit** pour accéder à la page Security > TCP/UDP Services et activer ou désactiver ces services sur le commutateur.

PoE Power Information (informations sur l'alimentation PoE, uniquement sur les modèles PoE)

- **Maximum Available PoE Power (W)** : puissance maximale disponible pouvant être fournie par les ports PoE.
- **Total PoE Power Consumption (W)** : puissance PoE totale fournie aux périphériques PoE connectés.
- **PoE Power Mode** : limite de port (Port Limit) ou limite de classe (Class Limit).

  REMARQUE Cliquez sur **Detail** pour accéder à la page Port Management > PoE > PoE Properties et afficher davantage d'informations sur les paramètres PoE.

Other Summary Information (autres informations générales)

- **Serial Number** : numéro de série.
- **PID VID** : référence de pièce et identifiant de la version.

Configuration des paramètres système

Pour afficher ou modifier les paramètres système :

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

ÉTAPE 2 Affichez ou modifiez les paramètres système suivants :

- **System Description** : affiche une description du commutateur.
- **System Location** : indiquez l'emplacement physique du commutateur.
- **System Contact** : saisissez le nom de la personne à contacter.
- **Host Name** : sélectionnez le mode de définition du nom d'hôte du commutateur. Les options disponibles sont les suivantes :
  - *Use Default* : utiliser le nom d'hôte par défaut (le nom du système). Le nom d'hôte par défaut est *switch123456*, où 123456 représente les trois derniers octets de l'adresse MAC du commutateur au format hexadécimal.
  - *User Defined* : indiquer manuellement le nom d'hôte du commutateur. Utilisez uniquement des lettres, des chiffres et des tirets. Les noms d'hôte 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 Dans **Custom Login Screen Settings**, spécifiez les bannières système qui s'afficheront lorsque les utilisateurs accèderont au commutateur. Les bannières disponibles sont les suivantes :

- **Login Banner** : saisissez le message qui s'affichera avant l'invite de connexion demandant le nom d'utilisateur et le mot de passe (généralement sur la page de connexion). La longueur maximum du message est de 2 000 caractères. Cliquez sur **Preview** pour prévisualiser vos réglages.
- **Welcome Banner** : saisissez le message qui s'affichera lors de la création d'un processus EXEC. La longueur maximum du message est de 2 000 caractères. Cliquez sur **Preview** pour prévisualiser vos réglages.

  REMARQUE Les bannières définies sur l'interface Web peuvent également être activées sur les interfaces de ligne de commande (console, Telnet et SSH).

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres système sont modifiés et la configuration de fonctionnement est mise à jour.

Configuration des paramètres de console

La page Console Settings vous permet de configurer le débit en bauds du port de console. Les paramètres par défaut du port de console sont les suivants :

- 9 600 bits par seconde
- 8 bits de données
- aucune parité
- 1 bit d'arrêt
- aucun contrôle de flux

Pour modifier le débit en bauds du port de console :

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

ÉTAPE 2 Sélectionnez une valeur dans le menu déroulant **Console Port Baud Rate**. Les valeurs disponibles sont 2 400, 4 800, 9 600, 19 200, 38 400, 57 600 et 115 200 bits/s.

ÉTAPE 3 Cliquez sur **Apply**. Le débit en bauds du port de console est défini et la configuration de fonctionnement est mise à jour.

Redémarrage du commutateur

Certaines modifications de la configuration ne sont appliquées qu'après le redémarrage du commutateur. Cette opération supprime toutefois la configuration de fonctionnement. Il est donc indispensable de l'enregistrer dans la configuration de démarrage avant le redémarrage du commutateur. Cliquer sur **Apply** n'a pas pour effet d'enregistrer la configuration dans la configuration de démarrage.

Vous pouvez enregistrer la configuration de fonctionnement sur la page **Administration** > **Save/Copy Configuration** ou cliquer sur le bouton **Save** situé en haut de la fenêtre.

Pour redémarrer le commutateur :

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

ÉTAPE 2 Cliquez sur **Reboot** pour redémarrer le commutateur. Les informations non enregistrées de la configuration de fonctionnement étant supprimées lors du redémarrage du commutateur, vous devez cliquer sur **Save** en haut à droite de n'importe quelle fenêtre afin de conserver la configuration actuelle lors du processus de démarrage. (Si l'option **Save** ne s'affiche pas, cela signifie que la configuration de fonctionnement est identique à la configuration de démarrage et qu'aucune action n'est nécessaire.)

ÉTAPE 3 Vous pouvez également cocher la case **Enable** située en regard du champ **Reboot to Factory Defaults** et cliquer sur **Reboot** pour redémarrer le commutateur en utilisant la 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.

La configuration miroir n'est pas supprimée lorsque vous restaurez les paramètres d'origine.

Définition du délai d'expiration en cas de session inactive

La page Idle Session Timeout permet de configurer 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 :

- Session HTTP
- Session HTTPS
- Session de console
- Session Telnet
- Session SSH

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

ÉTAPE 1 Cliquez sur **Administration** > **Idle Session Timeout**.

ÉTAPE 2 Sélectionnez le délai d'expiration de la session dans le menu déroulant correspondant. La valeur par défaut est de 10 minutes.

ÉTAPE 3 Cliquez sur **Apply**. Les paramètres de délai d'expiration en cas de session inactive sont définis et la configuration de fonctionnement est mise à jour.

Envoi d'une requête Ping à un hôte

Ping est un utilitaire servant à déterminer si un hôte distant peut être atteint et à mesurer le temps de parcours du transfert de paquets entre le commutateur et un périphérique de destination.

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

Pour envoyer une requête Ping à un hôte distant :

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

ÉTAPE 2 Indiquez les informations suivantes :

- **Host Definition** : indiquez si vous souhaitez spécifier l'hôte par son adresse IP ou son nom.
- **IP Version** : sélectionnez **Version 4** ou **Version 6** si l'hôte est identifié par adresse IP.
- **Host IP Address/Name** : saisissez l'adresse IP ou le nom de l'hôte auquel la requête Ping est envoyée.
- **Number of Pings** : sélectionnez **User Defined** pour saisir le nombre de fois que l'opération Ping sera effectuée ou **Use Default** pour utiliser la valeur par défaut.

ÉTAPE 3 Cliquez sur **Active Ping** pour envoyer une requête Ping à l'hôte. Les compteurs et l'état du Ping s'affichent.

Utilisation de Traceroute

Traceroute détecte les routes IP utilisées pour le transfert des paquets en envoyant un paquet IP à l'hôte cible et en le renvoyant au commutateur. La page Traceroute affiche chaque saut entre le commutateur et un hôte cible, ainsi que le temps de parcours de chaque saut.

Pour utiliser l'utilitaire Traceroute :

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

ÉTAPE 2 Indiquez les informations suivantes :

- **Host Definition** : indiquez si vous souhaitez spécifier l'hôte par son adresse IP ou son nom.
- **Host IP Address/Name** : saisissez l'adresse IP ou le nom de l'hôte.
- **TTL** : sélectionnez **User Defined** pour saisir le nombre maximal de sauts autorisés par Traceroute. Cela permet d'éviter les situations où la trame envoyée entre dans une boucle sans fin. La commande Traceroute se termine lorsque la destination ou cette valeur est atteinte. Pour utiliser la valeur par défaut (30), sélectionnez **Use Default**.

ÉTAPE 3 Cliquez sur **Apply**.

6

Administration : Paramètres d'heure

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

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

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

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 la configuration de l'heure système, du fuseau horaire et de l'heure d'été (DST).

Il contient les rubriques suivantes :

- **Options d'heure système**
- **Configuration de l'heure système**
- **Configuration du serveur SNTP**

Options d'heure système

L'heure système peut être réglée manuellement par l'utilisateur ou dynamiquement à partir 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. Ces paramètres sont obtenus à partir du SNTP, des valeurs définies manuellement ou, en cas d'échec de ces éléments, des valeurs d'origine.

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

- **Manual** : vous devez définir l'heure manuellement.
- **SNTP** : l'heure peut être reçue du serveur de temps SNTP. Le paramètre SNTP garantit une synchronisation précise de l'heure réseau 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 impossible. Nous vous recommandons d'utiliser un serveur SNTP comme source d'horloge.

Configuration de l'heure système

La page System Time vous permet de configurer l'heure, le fuseau horaire ainsi que la source d'horloge actuels.

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 redémarre, les paramètres d'heure saisis manuellement doivent être ressaisis.

Pour définir l'heure système :

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

Le champ **Actual Time** affiche l'heure système actuelle et la source d'horloge actuellement utilisée par le commutateur.

ÉTAPE 2 Cochez la case **Enable** en regard du champ **Main Clock Source (SNTP Servers)** pour définir la source SNTP fixant l'heure système. L'heure système est obtenue d'un serveur SNTP. Pour utiliser cette fonction, vous devez également ajouter un serveur SNTP sur la page SNTP Settings, comme décrit à la section **Configuration du serveur SNTP**.

ÉTAPE 3 Dans **Manual Settings**, vous pouvez définir manuellement la date et l'heure. L'heure locale est utilisée lorsqu'aucune source d'horloge alternative, comme un serveur SNTP, n'est disponible. Vous pouvez également cliquer sur le lien sous « **here** » pour recevoir la date et l'heure à partir du PC en utilisant les informations du navigateur.

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

ÉTAPE 4 Dans **Time Zone Settings**, l'heure locale est utilisée via le décalage du fuseau horaire (Time Zone Offset).

- **Time Zone Offset** : sélectionnez la différence en heures entre le temps universel coordonné (UTC) et l'heure locale. Par exemple, le décalage de fuseau horaire pour Paris est UTC +10:00 et celui pour New York est UTC -5.
- **Time Zone Acronym** : choisissez un acronyme représentatif du fuseau horaire que vous avez configuré. L'acronyme s'affiche dans le champ **Actual Time**.

ÉTAPE 5 Dans **Daylight Saving Settings**, sélectionnez le mode de définition de l'heure d'été :

- **Daylight Saving** : cochez la case **Enable** pour activer l'heure d'été.
- **Time Set Offset** : saisissez le décalage en minutes avec l'UTC.
- **Daylight Saving Type** : cliquez sur l'un des éléments suivants :
  - *USA* : l'heure d'été est définie selon les dates utilisées aux États-Unis.
  - *European* : l'heure d'été est définie selon les dates utilisées par l'Union européenne et les autres pays qui appliquent cette norme.

- *By Dates* : l'heure d'été est définie manuellement, généralement pour les autres pays.
- *Recurring* : l'heure d'été entre en vigueur à la même date chaque année.

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

- **From** : jour et heure de début de l'heure d'été.
- **To** : jour et heure de fin de l'heure d'été.

Sélectionnez *Recurring* pour personnaliser encore davantage le début et la fin de l'heure d'été :

- **From** : date à laquelle l'heure d'été commence chaque année.
  - *Day* : jour de la semaine au cours duquel l'heure d'été débute chaque année.
  - *Week* : semaine du mois au cours de laquelle l'heure d'été débute chaque année.
  - *Month* : mois de l'année au cours duquel l'heure d'été débute chaque année.
  - *Time* : heure à laquelle l'heure d'été débute chaque année.
- **To** : date à laquelle l'heure d'été prend fin chaque année.
  - *Day* : jour de la semaine au cours duquel l'heure d'été prend fin chaque année.
  - *Week* : semaine du mois au cours de laquelle l'heure d'été prend fin chaque année.
  - *Month* : mois de l'année au cours duquel l'heure d'été prend fin chaque année.
  - *Time* : heure à laquelle l'heure d'été prend fin chaque année.

ÉTAPE 6 Cliquez sur **Apply**. L'heure système est définie et la configuration de fonctionnement est mise à jour.

Configuration du serveur SNTP

Le commutateur peut être configuré pour synchroniser son horloge système avec un serveur SNTP indiqué sur la page SNTP Settings.

Pour spécifier un serveur SNTP par son nom, vous devez d'abord configurer des serveurs DNS sur le commutateur et activer l'option Main Clock Source (SNTP Servers) sur la page System Time.

Pour ajouter un serveur SNTP :

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

ÉTAPE 2 Indiquez les informations suivantes :

- **Host Definition** : indiquez si vous souhaitez spécifier le serveur SNTP par son adresse IPv4 ou son nom.
- **SNTP Server IP Address/Name** : saisissez l'adresse IPv4 ou le nom d'hôte du serveur SNTP.
- **SNTP Server Port** : spécifiez le numéro de port UDP à indiquer dans l'en-tête des messages SNTP. Par défaut, le numéro de port correspond à la valeur IANA réservée 123.

ÉTAPE 3 Cliquez sur **Apply.** Le serveur SNTP est ajouté et la configuration de fonctionnement est mise à jour.

7

Administration : Diagnostic

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 de l'état des modules optiques et de l'utilisation du processeur.

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 du processeur**

Test des ports cuivre

La page Copper Test vous permet de réaliser des tests intégrés sur les câbles cuivre.

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

Pour tester les câbles en cuivre reliés aux ports :

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

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

ÉTAPE 3 Cliquez sur **Copper Test**.

Les champs suivants de test s'affichent :

- **Test Results** : récapitulatif des résultats du test.
- **Cable Length** : longueur estimée du câble. La longueur du câble est inconnue (Unknown) lorsque les fonctionnalités écologiques sont activées.

  REMARQUE Si les liaisons des ports sont actives ou que les câbles connectés sont inférieurs à 10 mètres, la longueur de câble estimée est utilisée à titre de référence uniquement.
- **Operational Port Status** : indique si le port est actif ou inactif.

Affichage de l'état des modules optiques

La page Optical Module Status 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.

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

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

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

- **MGBBX1** : émetteur-récepteur SFP 1000BASE-BX-20U pour la fibre monomode, longueur d'onde de 1 310 nm, jusqu'à 40 km.
- **MGBLH1** : émetteur-récepteur SFP 1000BASE-LH pour la fibre monomode, longueur d'onde de 1 310 nm, jusqu'à 40 km.
- **MGBLX1** : émetteur-récepteur SFP 1000BASE-LX pour la fibre monomode, longueur d'onde de 1 310 nm, jusqu'à 10 km.
- **MGBSX1** : émetteur-récepteur SFP 1000BASE-SX pour la fibre multimode, longueur d'onde de 850 nm, jusqu'à 550 m.

- **MGBT1 :** émetteur-récepteur SFP 1000BASE-T pour le fil cuivre de catégorie 5, jusqu'à 100 m.

Pour afficher l'état des modules optiques, cliquez sur **Administration** > **Diagnostics** > **Optical Module Status**.

Les champs suivants s'affichent :

- **Port** : numéro du port sur lequel le SFP est connecté.
- **Temperature** : température en degrés Celsius à laquelle le SFP fonctionne.
- **Voltage** : tension de fonctionnement du SFP.
- **Current** : consommation de courant du SFP.
- **Output Power** : puissance optique transmise.
- **Input Power** : puissance optique reçue.
- **Loss of Signal** : le SFP local indique une perte de signal. Les valeurs sont True (vrai) et False (faux).

Configuration de la mise en miroir des ports et de VLAN

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

Le commutateur prend en charge jusqu'à quatre sessions de mise en miroir. Chaque session peut servir à la mise en miroir locale ou à distance. La mise en miroir n'affecte pas la commutation du trafic réseau sur les ports source ou les VLAN. Le port de destination de chaque session doit être différent. À l'exception du trafic requis pour la mise en miroir, le port de destination peut aussi servir à recevoir ou à réacheminer le trafic normal.

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

La mise en miroir ne garantit pas que l'ensemble du trafic en provenance 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.

REMARQUE La fonction de VLAN RSPAN concerne uniquement les modèles de commutateurs destinés à la Chine.

Pour configurer la mise en miroir des ports et des VLAN :

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

ÉTAPE 2 Si votre commutateur prend en charge la fonction de VLAN RSPAN, indiquez les informations suivantes :

- **RSPAN VLAN** : cochez la case **Enable** pour activer la mise en miroir de VLAN RSPAN.
- **RSPAN VLAN ID** : sélectionnez le VLAN à mettre en miroir. Lors de la configuration d'une session de mise en miroir RSPAN, indiquez ce VLAN comme étant le VLAN RSPAN.

ÉTAPE 3 Cliquez sur **Add** pour ajouter une session de mise en miroir SPAN ou RSPAN.

ÉTAPE 4 Indiquez les informations suivantes :

- **Session ID** : sélectionnez l'identifiant de la session de mise en miroir.
- **Session Type** : sélectionnez l'une des options suivantes :
  - *Local Port Based* : copie le trafic sortant, entrant ou les deux, de chaque port jusqu'au port de destination.
  - *Local VLAN Based* : copie le trafic du VLAN local vers le port de destination.
  - *RSPAN Source Session* : utilise un VLAN pour copier le trafic provenant d'un port ou d'un VLAN source vers un autre périphérique.
  - *RSPAN Destination Session* : utilise un VLAN pour copier le trafic d'un port de destination vers un autre périphérique.

ÉTAPE 5 Si Local Port Based est sélectionné, indiquez les informations suivantes :

- **Destination Port** : sélectionnez le port de l'analyseur sur lequel les paquets sont copiés. Un analyseur de réseau, par exemple un PC exécutant Wireshark, est connecté à ce port. Un port identifié en tant que port de destination de l'analyseur conserve cette fonction jusqu'à ce que toutes les entrées soient supprimées.

- **Allow Ingress Packets** : cochez **Enable** pour permettre au port de destination de recevoir les paquets entrants qui ne sont pas copiés.
- **Source Port** : sélectionnez les ports source à partir desquels le trafic est mis en miroir et le type de trafic à mettre en miroir sur le port de l'analyseur. Les options sont les suivantes :
  - *Rx Only* : mise en miroir des ports sur les paquets entrants.
  - *Tx Only* : mise en miroir des ports sur les paquets sortants.
  - *Tx and Rx* : mise en miroir des ports sur les paquets entrants et sortants.
  - *N/A* : le trafic venant de ce port n'est pas mis en miroir.

ÉTAPE 6 Si Local VLAN Based est sélectionné, indiquez les informations suivantes :

- **Destination Port** : sélectionnez le port de l'analyseur sur lequel les paquets sont copiés.
- **Allow Ingress Packets** : cochez **Enable** pour permettre au port de destination de recevoir les paquets entrants qui ne sont pas copiés.
- **VLAN** : sélectionnez le VLAN source à partir duquel le trafic est mis en miroir.

ÉTAPE 7 Si RSPAN Source Session est sélectionné, indiquez les informations suivantes :

- **RSPAN VLAN** : sélectionnez le VLAN à utiliser pour copier le trafic vers un autre périphérique. Ce VLAN devrait être le même que le VLAN défini dans le champ **RSPAN VLAN ID**.
- **Reflector Port** : sélectionnez le port ou le LAG à connecter avec l'autre périphérique.
- **Source Type** : sélectionnez **Port** ou **VLAN** selon que la source soit un port ou un VLAN.

  Si Port est sélectionné, sélectionnez les ports source à partir desquels le trafic est mis en miroir et le type de trafic à mettre en miroir sur le port de l'analyseur. Les options sont les suivantes :
  - *Rx Only* : mise en miroir des ports sur les paquets entrants.
  - *Tx Only* : mise en miroir des ports sur les paquets sortants.
  - *Tx and Rx* : mise en miroir des ports sur les paquets entrants et sortants.
  - *N/A* : le trafic venant de ce port n'est pas mis en miroir.

Si VLAN est sélectionné, sélectionnez le VLAN source à partir duquel le trafic est mis en miroir.

- *VLAN* : sélectionnez le VLAN source.

ÉTAPE 8 Si RSPAN Destination Session est sélectionné, indiquez les informations suivantes :

- **RSPAN VLAN** : sélectionnez le VLAN à utiliser pour copier le trafic vers un autre périphérique. Ce VLAN devrait être le même que le VLAN défini dans le champ **RSPAN VLAN ID**.
- **Destination Port** : sélectionnez le port de l'analyseur sur lequel les paquets sont copiés.
- **Allow Ingress Packets** : cochez **Enable** pour permettre au port de destination de recevoir les paquets entrants qui ne sont pas copiés.

ÉTAPE 9 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Affichage de l'utilisation du processeur

Pour afficher l'utilisation actuelle du processeur et/ou définir la fréquence d'actualisation :

ÉTAPE 1 Cliquez sur **Administration** > **Diagnostics** > **CPU Utilization**.

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

ÉTAPE 2 Indiquez la fréquence d'actualisation dans le champ **Refresh Rate**. Il s'agit de la durée en secondes qui s'écoule avant l'actualisation des données d'utilisation du processeur.

8

Administration : Détection

Ce chapitre fournit des informations sur la configuration de la détection et contient les rubriques suivantes :

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

Configuration de 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 ou Telnet.

Le commutateur peut être détecté par un système de gestion réseau ou une autre application tierce. Par défaut, Bonjour est activé sur le VLAN de gestion. La console Bonjour détecte automatiquement le commutateur et l'affiche.

La détection Bonjour peut uniquement être activée globalement. Elle ne peut pas être activée sur certains ports ou VLAN spécifiques. Le commutateur annonce tous les services qui ont été activés par l'administrateur en fonction de la configuration définie sur la page TCP/UDP Services.

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.

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

Pour activer ou désactiver Bonjour globalement :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery Bonjour**.

ÉTAPE 2 Cochez la case **Enable** pour activer globalement la détection Bonjour sur le commutateur ou décochez-la pour désactiver cette fonction.

ÉTAPE 3 Cliquez sur **Apply**. Bonjour est activé ou désactivé sur le commutateur et la configuration de fonctionnement est mise à jour.

LLDP et CDP

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

Dans les déploiements où les périphériques prenant en charge CDP (ou LLDP) ne sont pas directement connectés et sont séparés des périphériques ne prenant pas en charge CDP (ou LLDP), les périphériques prenant en charge CDP (ou LLDP) ne peuvent recevoir l'annonce des autres périphériques que si les périphériques ne prenant pas en charge CDP (ou LLDP) transmettent les paquets CDP (ou LLDP) qu'ils reçoivent. Si les périphériques ne prenant pas en charge CDP (ou LLDP) effectuent une inondation tenant compte du VLAN, les périphériques prenant en charge CDP (ou LLDP) ne peuvent s'entendre mutuellement que s'ils se trouvent sur le même VLAN.

Veuillez noter qu'un périphérique prenant en charge CDP (ou LLDP) peut recevoir une annonce de plusieurs périphériques si les périphériques ne prenant pas en charge CDP (ou LLDP) transmettent les paquets CDP (ou LLDP).

Vous trouverez ci-dessous des informations supplémentaires sur la configuration de CDP et LLDP :

- CDP et LLDP peuvent être activés et désactivés globalement ou sur chaque port. La fonctionnalité CDP ou LLDP d'un port ne s'applique que si CDP ou LLDP est activé globalement.

- Si CDP ou LLDP est activé globalement, le commutateur élimine les paquets CDP ou LLDP entrants provenant des ports où CDP ou LLDP est désactivé.
- Si CDP ou LLDP est désactivé globalement, le commutateur peut être configuré pour ignorer l'inondation (tenant compte ou non du VLAN) de tous les paquets CDP ou LLDP entrants. L'inondation tenant compte du VLAN transmet un paquet CDP ou LLDP entrant au VLAN où le paquet est reçu, mais pas au port d'entrée. L'inondation ne tenant pas compte du VLAN transmet un paquet CDP ou LLDP entrant à tous les ports, sauf au port d'entrée. Par défaut, le système ne tient pas compte du VLAN et procède à une inondation de paquets CDP ou LLDP, lorsque CDP ou LLDP est désactivé globalement. Vous pouvez configurer la suppression ou l'inondation des paquets CDP et LLDP entrants respectivement sur les pages CDP Properties et LLDP Properties.
- Les périphériques d'extrémité CDP et LLDP, tels que les téléphones IP, apprennent la configuration du VLAN voix à partir des annonces CDP et LLDP. Par défaut, le commutateur est activé pour envoyer une annonce CDP et LLDP basée sur le VLAN voix qui est configuré sur le commutateur. Pour plus d'informations, reportez-vous à la section **Configuration du VLAN voix**.

  REMARQUE CDP ou LLDP ne peut pas détecter si un port se trouve dans un LAG. Si un LAG contient plusieurs ports, CDP ou LLDP transmet les paquets sur chaque port sans tenir compte de l'appartenance des ports à un LAG.
- Le fonctionnement de CDP ou de LLDP est indépendant de l'état STP d'une interface.
- Si le contrôle d'accès au port 802.1x est activé sur une interface, le commutateur transmet les paquets CDP ou LLDP à l'interface, et les reçoit de cette dernière, uniquement si l'interface est authentifiée et autorisée.
- Si un port est la cible de la mise en miroir, il est considéré comme inactif pour CDP ou LLDP.

Configuration de LLDP

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

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

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

Le protocole LLDP possède une extension appelée LLDP Media Endpoint Discovery (LLDP MED), qui fournit et accepte des informations émanant de périphériques d'extrémité de média, tels que les téléphones VoIP et les téléphones vidéo.

Voici des exemples d'actions que vous pouvez réaliser avec la fonction LLDP, dans l'ordre suggéré :

- Activer LLDP globalement (LLDP est activé par défaut) et configurer les paramètres LLDP globaux sur la page LLDP Properties, comme décrit à la section **Configuration des propriétés LLDP**.
- Configurer LLDP sur chaque port sur la page Port Settings, comme décrit à la section **Configuration des paramètres des ports LLDP**. Cette page permet de configurer les ports pour recevoir ou transmettre des PDU LLDP et pour indiquer les TLV à annoncer.
- Créer des stratégies réseau LLDP MED sur la page LLDP MED Network Policy, comme décrit à la section **Configuration de la stratégie réseau LLDP MED**.
- Associer les stratégies réseau LLDP MED et les TLV LLDP MED facultatives aux ports souhaités sur la page LLDP MED Port Settings, comme décrit à la section **Configuration des paramètres des ports LLDP MED**.
- Afficher des informations globales sur LLDP et l'état LLDP de chaque port, comme décrit à la section **Affichage de l'état LLDP des ports**.
- Afficher des informations locales sur LLDP, comme décrit à la section **Affichage des informations LLDP locales**.
- Afficher des informations de voisinage LLDP, comme décrit à la section **Affichage des informations des voisins LLDP**.
- Afficher les statistiques LLDP de chaque port, comme décrit à la section **Affichage des statistiques LLDP**.
- Afficher les informations de surcharge LLDP, comme décrit à la section **Affichage de la surcharge LLDP**.

Configuration des propriétés LLDP

La page LLDP Properties vous permet d'activer LLDP globalement et de configurer les paramètres LLDP généraux.

Pour définir les propriétés LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery LLDP** > **Properties**.

ÉTAPE 2 Indiquez les informations suivantes :

- **LLDP Status** : cochez **Enable** pour activer LLDP sur le commutateur (activé par défaut).
- **LLDP Frames Handling** : si LLDP est désactivé, sélectionnez l'action à réaliser en cas de réception d'un paquet correspondant aux critères sélectionnés :
  - *Filtering* : supprime le paquet.
  - *Bridging* : (inondation tenant compte du VLAN) réachemine le paquet à tous les membres du VLAN.
  - *Flooding* : réachemine le paquet vers tous les ports.
- **TLV Advertise Interval** : sélectionnez **User Defined** pour indiquer la fréquence (en secondes) de mise à jour des annonces LLDP ou sélectionnez **Use Default** pour utiliser la valeur par défaut (30 secondes).
- **Hold Multiplier** : sélectionnez **User Defined** pour définir la durée de conservation des paquets LLDP avant leur élimination. La valeur doit être un multiple de l'intervalle d'annonce TLV. Par exemple, si l'intervalle d'annonce TLV est de 30 secondes et que le multiplicateur de conservation (Hold Multiplier) est 4, les paquets LLDP seront supprimés après 120 secondes. Sélectionnez **Use Default** pour utiliser la valeur par défaut (4).
- **Reinitializing Delay** : sélectionnez **User Defined** pour saisir l'intervalle (en secondes) entre la désactivation et la réinitialisation de LLDP suite à un cycle d'activation ou de désactivation de LLDP, ou sélectionnez **Use Default** pour utiliser la valeur par défaut (2 secondes).
- **Transmit Delay** : sélectionnez **User Defined** pour saisir le délai en secondes qui séparera deux transmissions de trames LLDP successives en cas de modification dans la MIB de systèmes locaux LLDP, ou sélectionnez **Use Default** pour utiliser la valeur par défaut (2 secondes).

ÉTAPE 3 Dans le champ **Fast Start Repeat Count**, saisissez le nombre d'envois de paquets LLDP lors de l'initialisation du mécanisme de démarrage rapide LLDP MED. Cela se produit lorsqu'un nouveau périphérique d'extrémité établit une liaison au commutateur. Pour plus d'informations, consultez la section **Configuration de la stratégie réseau LLDP MED**.

ÉTAPE 4 Cliquez sur **Apply**. Les propriétés LLDP sont définies et la configuration de fonctionnement est mise à jour.

Configuration des paramètres des ports LLDP

La page Port Settings vous permet d'activer LLDP sur chaque port et d'indiquer les TLV envoyées dans la PDU LLDP.

Pour définir les paramètres des ports LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery LLDP** > **Port Settings**.

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

ÉTAPE 3 Indiquez les informations suivantes :

- **Interface** : sélectionnez le port à définir.
- **Administrative Status** : sélectionnez l'option de publication LLDP pour le port. Les options disponibles sont les suivantes :
  - *Tx Only* : publication uniquement, pas de détection.
  - *Rx Only* : détection uniquement, pas de publication.
  - *Tx & Rx* : publication et détection.
  - *Disable* : désactive LLDP sur le port.
- **Available Optional TLVs** : sélectionnez les informations que le commutateur doit publier en déplaçant la TLV vers la liste **Selected Optional TLVs**. Les TLV disponibles contiennent les informations suivantes :
  - *Port Description* : informations sur le port, notamment son fabricant, son nom de produit et la version du matériel et du logiciel.
  - *System Name* : nom attribué au système, au format alphanumérique. Cette valeur est identique à l'objet sysName.

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

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres de port LLDP sont modifiés et la configuration de fonctionnement est mise à jour.

Configuration de la stratégie réseau LLDP MED

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

- Elle permet l'annonce et la détection des stratégies réseau pour les applications en temps réel telles que la voix et/ou la vidéo.
- Elle détecte l'emplacement des périphériques afin de permettre la création de bases de données d'emplacements. Dans le cas du protocole VoIP (voix sur IP), elle permet également l'accès aux services d'urgence (E-911 aux États-Unis) à l'aide des informations de géolocalisation du téléphone IP.

REMARQUE Le commutateur annonce automatiquement la stratégie en fonction de la configuration utilisateur. Toutefois, l'utilisateur doit également configurer manuellement le commutateur pour qu'il utilise cette stratégie.

Une stratégie réseau LLDP MED est un ensemble de paramètres de configuration apparentés, destinés à une application en temps réel, telle que la voix ou la vidéo. Une stratégie réseau (si elle est configurée) sera incluse dans les paquets LLDP sortants qui sont envoyés vers le périphérique d'extrémité de média LLDP associé. Le périphérique d'extrémité de média doit envoyer son trafic comme spécifié dans la stratégie réseau qu'il reçoit.

Vous pouvez associer des stratégies réseau à des ports sur la page LLDP MED Port Settings. Un administrateur peut configurer manuellement une ou plusieurs stratégies réseau, ainsi que les ports où les stratégies doivent être envoyées. Il est de la responsabilité de l'administrateur de créer manuellement les VLAN et l'appartenance des ports à ces derniers, conformément aux stratégies réseau et à leurs ports associés.

Pour définir une stratégie réseau LLDP MED :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery LLDP** > **LLDP MED Network Policy**.

ÉTAPE 2 Cochez la case **Enable** en regard de l'option **LLDP MED Network Policy for Voice Application** pour générer et annoncer automatiquement une stratégie réseau pour l'application vocale qui est basée sur le VLAN voix géré par le commutateur.

ÉTAPE 3 Cliquez sur **Apply**.

ÉTAPE 4 Cliquez sur **Add** pour ajouter une stratégie réseau LLDP MED.

ÉTAPE 5 Indiquez les informations suivantes :

- **Network Policy Number** : 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 :
  - Voice (voix)
  - Voice Signaling (signalisation vocale)
  - Guest Voice (voix d'invité)
  - Guest Voice Signaling (signalisation de voix d'invité)
  - Softphone Voice (voix de téléphone logiciel)
  - Video Conferencing (vidéoconférence)

- Streaming Video (lecture vidéo en continu)
- Video Signaling (signalisation vidéo)

- **VLAN ID** : saisissez l'ID du VLAN auquel le trafic doit être envoyé.
- **VLAN Tag** : indiquez si le trafic doit être balisé (Tagged) ou non (Untagged).
- **User Priority** : sélectionnez le niveau de priorité qui sera accordé au trafic défini par cette stratégie réseau.
- **DSCP Value** : sélectionnez la valeur DSCP à associer aux données d'application envoyées par les voisins. Cela leur indique la façon dont ils doivent marquer le trafic des applications qu'ils envoient au commutateur.

ÉTAPE 6 Cliquez sur **Apply**. La stratégie réseau LLDP MED est définie et la configuration de fonctionnement est mise à jour.

ÉTAPE 7 Associez la stratégie réseau à un port, comme décrit à la section **Configuration des paramètres des ports LLDP MED**.

Configuration des paramètres des ports LLDP MED

La page LLDP MED Port Settings vous permet de sélectionner les stratégies réseau configurées sur la page LLDP MED Network Policy pour être annoncées sur le port, et de sélectionner les TLV LLDP MED à envoyer dans la PDU LLDP.

Pour configurer LLDP MED sur chaque port :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery LLDP** > **LLDP MED Port Settings**.

ÉTAPE 2 Pour associer la stratégie réseau LLDP MED à un port, sélectionnez un port et cliquez sur **Edit**.

ÉTAPE 3 Indiquez les informations suivantes :

- **Interface** : sélectionnez le port à configurer.
- **LLDP MED Status** : activez ou désactivez LLDP MED sur ce port.
- **Available Optional TLVs** : sélectionnez les TLV que le commutateur peut publier en les déplaçant vers la liste **Selected Optional TLVs**.
- **Available Network Policies** : sélectionnez les stratégies LLDP MED que LLDP va publier en les déplaçant vers la liste **Selected Network Policies**. Ces stratégies ont été créées sur la page LLDP MED Network Policy.

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

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

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres de port LLDP MED sont modifiés et la configuration de fonctionnement est mise à jour.

ÉTAPE 5 Cliquez sur **LLDP Local Information Detail** pour consulter le détail des TLV LLDP et LLDP MED envoyées au voisin.

Affichage de l'état LLDP des ports

La page LLDP Port Status affiche des informations globales concernant LLDP, ainsi que sur l'état LLDP de chaque port.

Pour afficher l'état LLDP des ports :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery LLDP** > **LLDP Port Status**.

Les champs suivants s'affichent :

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

Les informations LLDP suivantes sont affichées pour chaque port :

- **Interface** : identificateur de port.
- **LLDP Status** : option de publication LLDP.
- **LLDP MED Status** : indique si LLDP MED est activé ou désactivé sur le port.
- **Local PoE** : (uniquement sur les modèles PoE) informations PoE locales annoncées.
- **Remote PoE** : informations PoE annoncées par les voisins (uniquement sur les modèles PoE).
- **# of neighbors** : nombre de voisins détectés.
- **Neighbor Capability of 1st Device** : affiche les principales fonctions de l'appareil activées sur le voisin. Par exemple, Bridge (pont) ou Router (routeur).

ÉTAPE 2 Cliquez sur **LLDP Local Information Detail** pour consulter le détail des TLV LLDP et LLDP MED envoyées au voisin.

ÉTAPE 3 Cliquez sur **LLDP Neighbor Information Detail** pour consulter le détail des TLV LLDP et LLDP MED reçues par le voisin.

Affichage des informations LLDP locales

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

ÉTAPE 1 Cliquez sur **Administration > Discovery LLDP > LLDP Local Information**.

ÉTAPE 2 Sélectionnez le port correspondant dans le menu déroulant **Port**.

Les champs suivants s'affichent :

Global

- **Chassis ID Subtype** : type d'ID de châssis (adresse MAC, par exemple).
- **Chassis ID** : identificateur du châssis. Si vous avez choisi l'adresse MAC comme sous-type d'ID de châssis, l'adresse MAC du commutateur est affichée.
- **System Name** : nom du commutateur.
- **System Description** : description du commutateur, au format alphanumérique.

- **Supported System Capabilities** : fonctions principales du périphérique telles que Bridge (pont), WLAN AP (point d'accès WLAN) ou Router (routeur).
- **Enabled System Capabilities** : fonctions principales activées sur le périphérique.
- **Port ID Subtype** : type d'ID de port affiché.
- **Port ID** : identificateur du port.
- **Port Description** : informations sur le port, notamment son fabricant, son nom de produit et la version du matériel et du logiciel.

Management Address (adresse de gestion)

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

- **Address Subtype** : type de l'adresse IP de gestion affichée dans le champ Management Address. Par exemple, IPv4.
- **Adress** : adresse renvoyée qui convient le mieux pour la gestion ; généralement, une adresse de couche 3.
- **Interface Subtype** : méthode de numérotation servant à définir le numéro de l'interface.
- **Interface Number** : interface spécifique associée à cette adresse de gestion.

MAC/PHY Details (informations MAC/PHY)

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

802.3 Details (informations relatives à 802.3)

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

802.3 Link Aggregation (agrégation de liaisons 802.3)

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

MED Details (informations MED)

- **Capabilities Supported** : fonctions MED prises en charge sur le port.
- **Current Capabilities** : fonctions MED activées sur le port.
- **Device Class** : classe du périphérique d'extrémité LLDP MED.
- **PoE Device Type** : (uniquement sur les modèles PoE) type PoE du port, par exemple : alimenté.
- **PoE Power Source** : (uniquement sur les modèles PoE) source d'alimentation du port.
- **PoE Power Priority** : (uniquement sur les modèles PoE) priorité d'alimentation du port.
- **PoE Power Value** : (uniquement sur les modèles PoE) valeur d'alimentation du port.
- **Hardware Revision** : version du matériel.
- **Firmware Revision** : version du microprogramme.
- **Software Revision** : version du logiciel.
- **Serial Number** : numéro de série du périphérique.
- **Manufacturer Name** : nom du fabricant du périphérique.
- **Model Name** : nom du modèle de périphérique.
- **Asset ID** : ID de la ressource.

Location Information (informations sur l'emplacement)

- **Civic** : adresse postale.
- **Coordinates** : coordonnées géographiques : latitude, longitude et altitude.

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

Network Policy Table (table des stratégies réseau)

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

ÉTAPE 3 Cliquez sur **LLDP Port Status Table** pour afficher les détails de l'état LLDP des ports dans une table.

Affichage des informations des voisins LLDP

La page LLDP Neighbor 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** > **Discovery LLDP** > **LLDP Neighbor**.

ÉTAPE 2 Sélectionnez un port local, puis cliquez sur **Go**.

Les champs suivants s'affichent :

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

- **Chassis ID** : identificateur du châssis du périphérique de voisinage réseau (LAN) 802.
- **Port ID Subtype** : type d'ID de port affiché.
- **Port ID** : identificateur du port.
- **System Name** : nom publié du commutateur.
- **Time to Live** : durée en secondes à l'issue de laquelle les informations concernant ce voisin sont supprimées.

ÉTAPE 3 Cliquez sur **Detail** pour afficher les détails de l'état LLDP des ports dans une table.

ÉTAPE 4 Cliquez sur **Refresh** pour actualiser les données dans la table des voisins LLDP.

Affichage des statistiques LLDP

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

Pour afficher les statistiques LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery LLDP** > **LLDP Statistics**.

Les champs suivants s'affichent pour chaque port :

- **Interface** : identificateur de port.
- **Tx Frames Total** : nombre total de trames transmises.
- **Rx Frames Total** : nombre de trames reçues.
- **Rx Frames Discarded** : nombre total de trames reçues qui ont été supprimées.
- **Rx Frames Errors** : nombre total de trames reçues comportant des erreurs.
- **Rx TLVs Discarded** : nombre total de TLV reçues qui ont été supprimées.
- **Rx TLVs Unrecognized** : nombre total de TLV reçues qui n'ont pas été reconnues.
- **Neighbor's Information Deletion Count** : nombre d'expirations du délai maximal du voisin sur le port.

ÉTAPE 2 Cliquez sur **Refresh** pour actualiser les statistiques LLDP.

Affichage de la surcharge LLDP

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

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

Pour afficher les informations de surcharge LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery LLDP** > **LLDP Overloading**.

Les champs suivants s'affichent :

- **Interface** : identificateur de port.
- **Total Bytes In-Use** : nombre total d'octets d'informations LLDP dans chaque paquet.
- **Available Bytes Left** : nombre total d'octets disponibles restants pour des informations LLDP supplémentaires dans chaque paquet.
- **Status** : indique si des TLV sont transmises ou si une surcharge est intervenue.

ÉTAPE 2 Sélectionnez un port, puis cliquez sur **Details**.

Les champs suivants s'affichent :

- **LLDP Mandatory TLVs** (TLV LLDP obligatoires)
  - *Size (Bytes)* : taille totale des TLV obligatoires, en octets.
  - *Status* : indique si un groupe de TLV obligatoires est transmis ou si une surcharge est intervenue.
- **LLDP MED Capabilities** (fonctionnalités LLDP MED)
  - *Size (Bytes)* : taille totale des paquets de fonctionnalités LLDP MED, en octets.
  - *Status* : indique si les paquets de fonctionnalités LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **LLDP MED Location** (emplacement LLDP MED)
  - *Size (Bytes)* : taille totale des paquets d'emplacement LLDP MED, en octets.

  - *Status* : indique si les paquets d'emplacement LLDP MED ont été envoyés ou si une surcharge est intervenue.

- **LLDP MED Network Policy** (stratégie réseau LLDP MED)
  - *Size (Bytes)* : taille totale des paquets de stratégie réseau LLDP MED, en octets.
  - *Status* : indique si les paquets de stratégie réseau LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **LLDP MED Expanded Power via MDI** (alimentation LLDP MED étendue via MDI)
  - *Size (Bytes)* : taille totale des paquets d'alimentation LLDP MED étendue via MDI, en octets.
  - *Status* : indique si les paquets d'alimentation LLDP MED étendue via MDI ont été envoyés ou si une surcharge est intervenue.
- **802.3 TLVs** (TLV 802.3)
  - *Size (Bytes)* : taille totale des paquets de TLV 802.3 LLDP, en octets.
  - *Status* : indique si les paquets de TLV 802.3 LLDP ont été envoyés ou si une surcharge est intervenue.
- **LLDP Optional TLVs** (TLV LLDP facultatives)
  - *Size (Bytes)* : taille totale des paquets de TLV LLDP facultatives, en octets.
  - *Status* : indique si les paquets de TLV LLDP facultatives ont été envoyés ou si une surcharge est intervenue.
- **LLDP MED Inventory** (inventaire LLDP MED)
  - *Size (Bytes)* : taille totale des paquets de TLV d'inventaire LLDP MED, en octets.
  - *Status* : indique si les paquets d'inventaire LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **802.1 TLVs** (TLV 802.1)
  - *Size (Bytes)* : taille totale des paquets de TLV 802.1 LLDP, en octets.
  - *Status* : indique si les paquets de TLV 802.1 LLDP ont été envoyés ou si une surcharge est intervenue.
- **Total**

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

Configuration de CDP

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

Configuration des propriétés CDP

La page CDP Properties vous permet d'activer globalement CDP sur le commutateur et de configurer les paramètres CDP généraux.

Pour définir des propriétés CDP :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery CDP** > **Properties**.

ÉTAPE 2 Indiquez les informations suivantes :

- **CDP Status** : cochez **Enable** pour activer globalement CDP sur le commutateur.
- **CDP Frames Handling** : si CDP est désactivé, sélectionnez l'action à réaliser en cas de réception d'un paquet correspondant aux critères sélectionnés :
  - *Bridging* : (inondation tenant compte du VLAN) réachemine le paquet basé sur le VLAN.
  - *Filtering* : supprime le paquet.
  - *Flooding* : (inondation ne tenant pas compte du VLAN) transmet les paquets CDP entrants à tous les ports, sauf aux ports d'entrée.
- **CDP Voice VLAN Advertisement** : cochez **Enable** pour permettre au commutateur d'annoncer le VLAN voix dans CDP sur tous les ports activés pour CDP et membres du VLAN voix.

- **CDP Mandatory TLVs Validation** : cochez **Enable** pour supprimer les paquets CDP entrants qui ne contiennent pas de TLV obligatoires et pour incrémenter le compteur d'erreurs non valides.
- **CDP Version** : sélectionnez la version du protocole CDP à utiliser.
- **CDP Hold Time** : sélectionnez **User Defined** pour saisir la durée de conservation (en secondes) des paquets CDP avant leur suppression. La valeur doit être un multiple de l'intervalle d'annonce TLV. Par exemple, si l'intervalle d'annonce TLV est de 30 secondes et que le multiplicateur de conservation (Hold Multiplier) est 4, les paquets LLDP seront supprimés après 120 secondes. Vous pouvez également sélectionner **Use Default** pour utiliser la durée par défaut (180 secondes).
- **CDP Transmission Rate** : sélectionnez **User Defined** pour indiquer la fréquence (en secondes) de mise à jour des annonces CDP ou sélectionnez **Use Default** pour utiliser la valeur par défaut (60 secondes).
- **Device ID Format** : sélectionnez le format de l'ID de périphérique (adresse MAC, numéro de série ou nom d'hôte).
- **Source Interface** : sélectionnez **User Defined** pour utiliser l'adresse IP de l'interface (définie dans le champ **Interface**) dans la TLV d'adresse, ou sélectionnez **Use Default** pour utiliser l'adresse IP de l'interface sortante.
- **Interface** : si vous avez sélectionné *User Defined* pour **Source Interface**, sélectionnez l'interface.
- **Syslog Voice VLAN Mismatch** : cochez **Enable** pour envoyer un message SYSLOG lorsqu'une non-concordance VLAN voix est détectée. Cela signifie que les informations de VLAN voix dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.
- **Syslog Native VLAN Mismatch** : cochez **Enable** pour envoyer un message SYSLOG lorsqu'une non-concordance VLAN natif est détectée. Cela signifie que les informations de VLAN natif dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.
- **Syslog Duplex Mismatch** : cochez **Enable** pour envoyer un message SYSLOG lorsque les informations duplex ne correspondent pas. Cela signifie que les informations duplex dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.

ÉTAPE 3 Cliquez sur **Apply.** Les propriétés CDP sont définies et la configuration de fonctionnement est mise à jour.

Configuration des paramètres des ports CDP

La page Port Settings vous permet d'activer ou de désactiver CDP par port. Les notifications peuvent également être déclenchées lors de l'apparition de conflits avec des voisins CDP. Le conflit peut être Voice VLAN data (données VLAN voix), Native VLAN (VLAN natif) ou Duplex.

Pour définir les paramètres des ports CDP :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery CDP** > **Port Settings**.

Les champs suivants s'affichent :

- **Interface** : identificateur de port.
- **CDP Status** : option de publication CDP pour le port.
- **Reporting Conflicts with CDP Neighbors** : affiche l'état des options de rapport (VLAN voix/VLAN natif/Duplex) qui sont activées/désactivées sur la page Edit.
- **No. of Neighbors** : nombre de voisins détectés.

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

ÉTAPE 3 Indiquez les informations suivantes :

- **Interface** : sélectionnez le port à définir.
- **CDP Status** : cochez **Enable** pour activer l'option de publication CDP pour le port.

  REMARQUE Les trois champs suivants sont opérationnels si le commutateur a été configuré pour envoyer des messages « trap » à la station de gestion.
- **Syslog Voice VLAN Mismatch** : cochez **Enable** pour envoyer un message SYSLOG lorsqu'une non-concordance VLAN voix est détectée. Cela signifie que les informations de VLAN voix dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.
- **Syslog Native VLAN Mismatch** : cochez **Enable** pour envoyer un message SYSLOG lorsqu'une non-concordance VLAN natif est détectée. Cela signifie que les informations de VLAN natif dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.

- **Syslog Duplex Mismatch** : cochez **Enable** pour envoyer un message SYSLOG lors de la détection d'informations duplex ne correspondant pas. Cela signifie que les informations duplex dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres de port CDP sont modifiés et la configuration de fonctionnement est mise à jour.

Affichage des informations locales CDP

La page CDP Local Information affiche les informations qui sont annoncées par le protocole CDP à propos du périphérique local.

Pour afficher les informations locales CDP :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery CDP** > **CDP Local Information**.

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

- **CDP State** : indique si CDP est activé ou désactivé sur le port.
- **Device ID TLV** (TLV d'ID de périphérique)
  - *Device ID Type* : type d'ID de périphérique annoncé dans la TLV d'ID de périphérique.
  - *Device ID* : ID de périphérique annoncé dans la TLV d'ID de périphérique.
- **Address TLV** (TLV de l'adresse)
  - *Address(s)* : adresses IP (annoncées dans la TLV d'adresse de périphérique).
- **Port TLV** (TLV du port)
  - *Port ID* : identificateur du port annoncé dans la TLV de port.
- **Capabilities TLV** (TLV des fonctionnalités)
  - *Capabilities* : fonctionnalités annoncées dans la TLV de port.
- **Version TLV** (TLV de la version)
  - *Version* : informations sur la version logicielle sous laquelle le périphérique fonctionne.
- **Platform TLV** (TLV de la plateforme)

  - *Platform* : identificateur de la plate-forme annoncée dans la TLV de plate-forme.

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

de demande d'alimentation est reçue avec un champ Request-ID (ID de demande) différent du dernier ensemble reçu (ou à la réception de la première valeur). L'interface passe à l'état désactivé (Down).

- *Available Power* : (uniquement sur les modèles PoE) puissance consommée par le port.
- *Management Power Level* : (uniquement sur les modèles PoE) affiche la demande du fournisseur au périphérique alimenté pour connaître sa TLV de consommation électrique. Le commutateur affiche toujours « No Preference » (aucune préférence) dans ce champ.

Affichage des informations de voisinage CDP

La page CDP Neighbor Information affiche les informations CDP reçues des périphériques voisins. Après une temporisation (basée sur la valeur reçue du paramètre de durée de vie du voisin, durée au cours de laquelle aucune PDU CDP n'a été reçue d'un voisin), les informations sont supprimées.

Pour afficher les informations de voisinage CDP :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery CDP** > **CDP Neighbor Information**.

Les champs suivants s'affichent :

- **Device ID** : ID de périphérique du voisin.
- **Local Interface** : numéro du port local auquel le voisin est connecté.
- **Advertisement Version** : version du protocole CDP.
- **Time to Live** : durée en secondes à l'issue de laquelle les informations concernant ce voisin sont supprimées.
- **Capabilities** : fonctionnalités annoncées par le voisin.
- **Platform** : informations issues de la TLV de plate-forme du voisin.
- **Neighbor Interface** : interface sortante du voisin.

ÉTAPE 2 Sélectionnez un périphérique voisin, puis cliquez sur **Detail**.

Les champs suivants sur le voisin s'affichent :

- **Device ID** : ID du périphérique de voisinage.

- **Local Interface** : numéro d'interface du port via lequel la trame a été reçue.
- **Advertisement Version** : version du protocole CDP.
- **Time to Live** : durée en secondes à l'issue de laquelle les informations concernant ce voisin sont supprimées.
- **Capabilities** : fonctions principales du périphérique. Les fonctionnalités sont indiquées par deux octets. Les bits 0 à 7 indiquent respectivement Autres, Répéteur, Pont, Point d'accès WLAN, Routeur, Téléphone, Système de câble DOCSIS et Station. Les bits 8 à 15 sont réservés.
- **Platform** : identificateur de la plate-forme du voisin.
- **Neighbor Interface** : numéro d'interface du voisin via lequel la trame a été reçue.
- **Native VLAN** : VLAN natif du voisin.
- **Duplex** : indique si l'interface de voisinage est semi-duplex ou duplex intégral.
- **Addresses** : adresses du voisin.
- **Power Drawn** : (uniquement sur les modèles PoE) puissance consommée par le voisin sur l'interface.
- **Version** : version logicielle du voisin.

ÉTAPE 3 Cliquez sur **Clear Table** pour déconnecter tous les périphériques voisins connectés du CDP.

ÉTAPE 4 Cliquez sur **Refresh** pour actualiser les informations de voisinage CDP.

Affichage des statistiques CDP

La page CDP Statistics affiche des informations sur les trames CDP qui ont été envoyées ou reçues depuis un port.

Les statistiques CDP d'un port ne s'affichent que si CDP est activé globalement et sur le port.

Pour afficher les statistiques CDP :

ÉTAPE 1 Cliquez sur **Administration** > **Discovery CDP** > **CDP Statistics**.

Les champs suivants s'affichent :

- **Packets Received** : affiche les compteurs pour différents types de paquets reçus par interface.
  - *Version 1*: nombre de paquets CDP de version 1 reçus.
  - *Version 2* : nombre de paquets CDP de version 2 reçus.
  - *Total* : nombre total de paquets CDP reçus.
- **Packets Transmitted** : affiche les compteurs pour différents types de paquets transmis par interface.
  - *Version 1*: nombre de paquets CDP de version 1 transmis.
  - *Version 2* : nombre de paquets CDP de version 2 transmis.
  - *Total* : nombre total de paquets CDP transmis.
- **CDP Error Statistics** : affiche les compteurs d'erreurs CDP.
  - *Illegal Checksum* : nombre de paquets reçus ayant une valeur de somme de contrôle incorrecte.
  - *Other Errors* : nombre de paquets reçus comportant d'autres erreurs que des sommes de contrôle incorrectes.
  - *Neighbors Over Maximum* : nombre de fois que les informations de paquet n'ont pas pu être stockées dans le cache en raison d'un manque d'espace disponible.

ÉTAPE 2 Sélectionnez une interface et cliquez sur **Clear Interface Counters** pour effacer les compteurs CDP de l'interface sélectionnée.

ÉTAPE 3 Cliquez sur **Clear All Interface Counters** pour effacer les compteurs de statistiques CDP de toutes les interfaces.

ÉTAPE 4 Cliquez sur **Refresh** pour actualiser les compteurs de statistiques CDP.

9

Gestion des ports

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

Il contient les rubriques suivantes :

- **Flux de travail de gestion des ports**
- **Configuration des paramètres de port de base**
- **Configuration des paramètres de reprise sur erreur**
- **Configuration de l'agrégation de liaisons**
- **Configuration de la fonction Energy Efficient Ethernet**

Flux de travail de gestion des ports

Pour configurer les ports, procédez comme suit :

ÉTAPE 1 Configurez les paramètres de port de base sur la page Port Settings, selon la procédure décrite dans la section **Configuration des paramètres de port de base**.

ÉTAPE 2 Activez ou désactivez les ports désactivés en raison d'une erreur en vue de la reprise à partir de causes spécifiques et activez manuellement les ports suspendus sur la page Error Recovery Settings, selon la procédure décrite dans la section **Configuration des paramètres de reprise sur erreur**.

ÉTAPE 3 Activez ou désactivez le protocole LAG (Link Aggregation Group, groupe d'agrégation de liaisons), puis configurez les ports membres potentiels sur les LAG souhaités via la page LAG Management, selon la procédure décrite dans la section **Configuration de l'agrégation de liaisons**. Par défaut, tous les LAG sont vides.

ÉTAPE 4 Configurez les paramètres Ethernet, tels que la vitesse et la négociation automatique pour les LAG, sur la page LAG Settings, selon la procédure décrite dans la section **Configuration des paramètres de LAG**.

ÉTAPE 5 Configurez les paramètres LACP des ports membres ou candidats d'un LAG dynamique sur la page LACP, selon la procédure décrite dans la section **Configuration de LACP**.

ÉTAPE 6 Configurez la fonction 802.3 Energy Efficient Ethernet pour chaque port sur la page Energy Efficient Ethernet > Port Settings, selon la procédure décrite dans la section **Configuration de la fonction Energy Efficient Ethernet**.

ÉTAPE 7 Si la fonction PoE est prise en charge pour le commutateur, configurez ce dernier en suivant les instructions du chapitre **Power over Ethernet**.

Configuration des paramètres de port de base

Utilisez la page Port Settings pour configurer les paramètres de port au niveau global ou pour chaque port.

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

Pour configurer les paramètres de port :

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

ÉTAPE 2 Cochez **Enable** en regard du champ **Jumbo Frames** pour prendre en charge les paquets dont la taille va jusqu'à 10 000 octets. Si l'option Jumbo Frames n'est pas activée (par défaut), le commutateur prend en charge les tailles de paquets jusqu'à 1 522 octets.

ÉTAPE 3 Cliquez sur **Apply**. Le paramètre de port global est défini et la configuration de fonctionnement mise à jour.

ÉTAPE 4 Pour mettre à jour les paramètres d'un port, sélectionnez le port souhaité et cliquez sur **Edit**.

ÉTAPE 5 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port à modifier.
- **Port Description** : saisissez le nom défini par l'utilisateur pour ce port ou un commentaire.

- **Port Type** : affiche le type du port.
- **Administrative Status** : indiquez si le port doit être opérationnel (Up) ou non opérationnel (Down) au redémarrage du commutateur.
- **Operational Status** : affiche l'état actuel de la connexion du port.
- **Auto Negotiation** : cochez **Enable** pour activer la négociation automatique sur le port. La négociation automatique permet à un port d'annoncer sa vitesse de transmission, son mode duplex et ses capacités de contrôle de flux à d'autres périphériques.
- **Operational Auto Negotiation** : affiche l'état actuel de la négociation automatique sur le port.
- **Administrative Port Speed** : sélectionnez la vitesse configurée pour le port. Le type de port détermine les options de définition de la vitesse disponibles. Vous pouvez choisir Administrative Port Speed uniquement si la négociation automatique est désactivée pour le port.
- **Operational Port Speed** : affiche le débit actuel du port, obtenu par négociation.
- **Administrative Duplex Mode** : 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* : l'interface prend en charge la transmission entre le commutateur et le client dans les deux directions simultanément.
  - *Half* : l'interface prend en charge la transmission entre le commutateur et le client dans une seule direction à la fois.
- **Operational Duplex Mode** : affiche le mode duplex actuel du port, obtenu par négociation.
- **Auto Advertisement Speed** : sélectionnez la capacité de débit que le port doit annoncer. Les options sont les suivantes :
  - *All Speed* : toutes les vitesses de port sont acceptées.
  - *10M* : vitesse de 10 Mbit/s.
  - *100M* : vitesse de 100 Mbit/s.
  - *10M/100M* : vitesses de 10 et 100 Mbit/s.
  - *1000M* : vitesse de 1 000 Mbit/s.

- **Auto Advertisement Duplex** : sélectionnez le mode duplex que le port doit annoncer. Les options sont les suivantes :
  - *All Duplex* : tous les modes duplex sont acceptés.
  - *Full* : l'interface prend en charge la transmission entre le commutateur et le client dans les deux directions simultanément.
  - *Half* : l'interface prend en charge la transmission entre le commutateur et le client dans une seule direction à la fois.
- **Operational Advertisement** : affiche les capacités actuellement publiées à l'attention du voisin du port pour démarrer le processus de négociation. Les options disponibles sont celles indiquées dans les champs **Auto Advertisement Speed** et **Auto Advertisement Duplex**.
- **Back Pressure** : cochez **Enable** pour activer le mode de contre-pression sur le port (utilisé en mode Semi-duplex) afin de ralentir la vitesse de réception des paquets en cas de congestion au niveau du commutateur. Cela désactive le port distant, ce qui l'empêche d'envoyer des paquets en brouillant le signal.
- **Flow Control** : activez ou désactivez le contrôle de flux 802.3X ou activez la négociation automatique du contrôle de flux sur le port (uniquement en mode Duplex intégral).
- **Current Flow Control** : affiche l'état actuel du contrôle de flux 802.3X.
- **Protected Port** : cochez **Enable** 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 Couche 2 entre les interfaces (ports Ethernet et LAG) qui partagent le même domaine de diffusion (VLAN).
  - Les paquets reçus de ports protégés peuvent uniquement être réacheminés vers des ports de sortie non protégés. Les règles de filtrage des ports protégés s'appliquent également aux paquets réacheminés par un logiciel, comme les applications de type Snooping.
  - 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.
- **Member in LAG** : indique le numéro du LAG si le port est membre d'un LAG ; sinon, ce champ reste vide.

ÉTAPE 6 Cliquez sur **Apply.** Les paramètres de port sont modifiés et la configuration de fonctionnement est mise à jour.

Configuration des paramètres de reprise sur erreur

Utilisez la page Error Recovery Settings pour définir de façon globale l'intervalle de reprise automatique, ainsi que pour activer ou désactiver le port désactivé en raison d'une erreur en vue de la reprise à partir de causes spécifiques. Vous pouvez également réactiver manuellement les ports suspendus.

Pour configurer les paramètres de reprise sur erreur :

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

ÉTAPE 2 Entrez les paramètres de port globaux suivants :

- **Automatic Recovery Interval** : saisissez le temps en secondes en vue de la reprise à partir de l'état désactivé en raison d'une erreur. Le même intervalle est appliqué à toutes les causes. L'intervalle par défaut est de 300 secondes.
- **Automatic ErrDisable Recovery** : activez ou désactivez le port désactivé en raison d'une erreur en vue de la reprise à partir de causes spécifiques. Les causes disponibles sont les suivantes :
  - *ACL* : cochez **Enable** pour activer le temporisateur en vue de la reprise à partir des causes ACL.
  - *ARP Inspection* : cochez **Enable** pour activer le temporisateur en vue de la reprise à partir des causes Inspection ARP.
  - *BPDU Guard* : cochez **Enable** pour activer le temporisateur en vue de la reprise à partir de la cause Protection BPDU.
  - *Broadcast Flood* : cochez **Enable** pour activer le temporisateur en vue de la reprise à partir de la cause Inondation de diffusion.
  - *DHCP Rate Limit* : cochez **Enable** pour activer le temporisateur en vue de la reprise à partir des causes Limite de débit DHCP.
  - *PoE* : (uniquement applicable aux modèles PoE) cochez **Enable** pour activer le temporisateur en vue de la reprise à partir des causes Power over Ethernet (PoE).

- *Port Security* : cochez **Enable** pour activer le temporisateur en vue de la reprise à partir des causes Sécurité des ports.
- *Self Loop* : cochez **Enable** pour activer le temporisateur en vue de la reprise à partir de la cause Boucle automatique.
- *Unicast Flood* : cochez **Enable** pour activer le temporisateur en vue de la reprise à partir des causes Inondation de destination unique.
- *Unknown Multicast Flood* : cochez **Enable** pour activer le temporisateur en vue de la reprise à partir des causes Inondation de multidestination inconnue.

ÉTAPE 3 Cliquez sur **Apply**. Les paramètres de reprise sur erreur sont modifiés et la configuration de fonctionnement est mise à jour.

ÉTAPE 4 La table **Suspended (errDisabled) Interface Table** affiche la liste des ports suspendus. Pour réactiver manuellement un port suspendu, sélectionnez le port souhaité et cliquez sur **Reactivate**.

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 (802.3az) qui permet de regrouper plusieurs ports physiques en une seule voie logique. L'agrégation de liaisons optimise l'utilisation des ports en reliant 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 :

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

Équilibrage de charge

Le trafic réacheminé vers un LAG fait l'objet d'un équilibrage de charge entre les ports membres actifs. Ceci permet d'obtenir une bande passante efficace proche du total cumulé des bandes passantes de tous les ports 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 destination unique et de multidestination sur la base des informations d'en-tête de paquet de Couche 2.

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

- **Selon les adresses MAC** : traitement basé sur les adresses MAC source et cible de tous les paquets.
- **Selon les adresses IP et MAC** : traitement basé sur les adresses IP source et cible et sur les adresses MAC source et cible de tous les paquets.

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. 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 en tant que port logique unique. 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.
- Les ports d'un LAG ne doivent être affectés à aucun autre LAG.
- Il est impossible d'affecter plus de 8 ports à un LAG statique. Il est également impossible de définir plus de 16 ports comme candidats pour un LAG dynamique.
- Lorsqu'un port est ajouté à un LAG, la configuration du LAG est appliquée au port. Lorsque vous retirez ce port du LAG, il reprend sa configuration d'origine.

- Les divers protocoles, tels que le protocole d'arbre recouvrant (STP, Spanning Tree Protocol), considèrent tous les ports d'un LAG comme étant un port unique.
- Tous les ports du LAG doivent avoir la même priorité 802.1p.

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

Flux de travail des LAG statiques et dynamiques

Impossible d'activer LACP pour un LAG statique ayant des membres. L'activation n'est possible qu'après avoir modifié le LAG statique et retiré tous ses membres.

Pour configurer un LAG statique, procédez comme suit :

ÉTAPE 1 Désactivez LACP sur le LAG pour le rendre statique. Attribuez jusqu'à 8 ports membres au LAG statique. Pour ce faire, sélectionnez les ports et déplacez-les de la liste **Port List** vers la liste **LAG Members** sur la page LAG Management. Pour plus d'informations, reportez-vous à la section **Configuration de la gestion des LAG**.

ÉTAPE 2 Configurez le débit et le contrôle de flux du LAG sur la page LAG Settings. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres de LAG**.

Pour configurer un LAG dynamique, procédez comme suit :

ÉTAPE 1 Activez le protocole LACP sur le LAG. Attribuez jusqu'à 16 ports candidats au LAG dynamique. Pour ce faire, sélectionnez les ports et déplacez-les de la liste **Port List** vers la liste **LAG Members** sur la page LAG Management. Pour plus d'informations, reportez-vous à la section **Configuration de la gestion des LAG**.

ÉTAPE 2 Configurez le débit et le contrôle de flux du LAG sur la page LAG Settings. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres de LAG**.

ÉTAPE 3 Configurez les paramètres LACP des ports du LAG sur la page LACP. Pour plus d'informations, reportez-vous à la section **Configuration de LACP**.

Configuration de la gestion des LAG

Utilisez la page LAG Management pour configurer les paramètres au niveau global et pour chaque LAG.

Pour définir l'algorithme d'équilibrage de charge et l'appartenance au LAG :

ÉTAPE 1 Cliquez sur **Port Management** > **Link Aggregation** > **LAG Management**.

ÉTAPE 2 Dans la zone **Load Balance Algorithm**, sélectionnez l'un des algorithmes d'équilibrage de charge suivants :

- **MAC Address** : équilibrage de charge basé sur les adresses MAC source et cible de tous les paquets.
- **IP/MAC Address** : équilibrage de charge basé sur les adresses IP source et cible ainsi que sur les adresses MAC source et cible de tous les paquets.

ÉTAPE 3 Cliquez sur **Apply**. L'algorithme d'équilibrage de charge est défini et la configuration de fonctionnement mise à jour.

ÉTAPE 4 Pour définir les ports membres ou candidats dans un LAG, sélectionnez le LAG souhaité et cliquez sur **Edit**.

ÉTAPE 5 Saisissez les informations suivantes :

- **LAG** : sélectionnez le LAG à définir.
- **LAG Name** : saisissez le nom du LAG.

- **LACP** : cochez **Enable** pour activer LACP sur le LAG sélectionné. Ceci en fait un LAG dynamique. Vous ne pouvez activer ce champ qu'après avoir déplacé au moins un port vers le LAG dans le champ suivant.
- **LAG Members** : déplacez les ports à attribuer au LAG de la liste **Port List** vers la liste **LAG Members**. Vous pouvez affecter jusqu'à huit ports par LAG statique et 16 ports à un LAG dynamique.

ÉTAPE 6 Cliquez sur **Apply**. L'appartenance au LAG est définie et la configuration de fonctionnement mise à jour.

Configuration des paramètres de LAG

Utilisez la page LAG Settings pour configurer les paramètres de LAG.

Pour configurer les paramètres de LAG :

ÉTAPE 1 Cliquez sur **Port Management** > **Link Aggregation** > **LAG Settings**.

ÉTAPE 2 Sélectionnez un LAG et cliquez sur **Edit**.

ÉTAPE 3 Saisissez les informations suivantes :

- **LAG** : sélectionnez le LAG à configurer.
- **LAG Type** : affiche le type de port inclus dans le LAG.
- **Description** : saisissez le nom du LAG.
- **Administrative Status** : indiquez si le LAG doit être opérationnel (Up) ou non opérationnel (Down).
- **Operational Status** : indique si le LAG est actuellement opérationnel.
- **Auto Negotiation** : permet d'activer ou de désactiver la négociation automatique sur le LAG. La négociation automatique est un protocole établi entre deux partenaires de liaison qui permet à un LAG d'annoncer sa vitesse de transmission et son contrôle de flux à son partenaire (le contrôle de flux est désactivé par défaut). Nous recommandons 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 vitesses de liaison sont identiques.
- **Operational Auto Negotiation** : affiche le paramètre de négociation automatique actuel.
- **Administrative Port Speed** : sélectionnez le débit du LAG.

- **Operational LAG Speed** : affiche le débit actuel de fonctionnement du LAG.
- **Auto Advertisement Speed** : sélectionnez la capacité de débit que le LAG doit annoncer. Les options sont les suivantes :
  - *All Speed* : toutes les vitesses de port sont acceptées.
  - *10M* : vitesse de 10 Mbit/s.
  - *100M* : vitesse de 100 Mbit/s.
  - *10M/100M* : vitesses de 10 et 100 Mbit/s.
  - *1000M* : vitesse de 1 000 Mbit/s.
- **Operational Advertisement** : affiche l'état de notification actuel. Le LAG annonce ses capacités à son LAG voisin pour lancer le processus de négociation. Les valeurs possibles sont celles spécifiées dans le champ **Auto Advertisement Speed**.
- **Back Pressure** : cochez **Enable** pour activer le mode de contre-pression sur le LAG (utilisé en mode Semi-duplex) afin de ralentir la vitesse de réception des paquets en cas de congestion au niveau du commutateur.
- **Flow Control** : permet d'activer ou de désactiver le contrôle de flux ou d'activer la négociation automatique du contrôle de flux sur le LAG.
- **Current Flow Control** : affiche le paramètre de contrôle de flux actuel.
- **Protected Port** : cochez **Enable** pour définir le LAG en tant que port protégé pour l'isolation Couche 2.

ÉTAPE 4 Cliquez sur **Apply.** Les paramètres de LAG sont définis et la configuration de fonctionnement est mise à jour.

Configuration de LACP

Un LAG est dynamique si le protocole LACP est activé ; ce dernier est exécuté sur chaque port candidat défini dans le LAG.

Priorité et règles LACP

La priorité du système LACP et la priorité des ports LACP servent à déterminer les ports candidats qui deviennent des ports membres actifs d'un LAG dynamique.

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

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

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

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

- Toute liaison fonctionnant avec une vitesse différente de celle du membre actif présentant la vitesse la plus élevée ou fonctionnant en mode semi-duplex devient la liaison de réserve. Tous les ports actifs d'un LAG dynamique fonctionnent avec le même débit en bauds.
- Si la priorité LACP des ports de la liaison est inférieure à celle des membres de liaison actuellement actifs et si le nombre maximal de membres actifs a déjà été atteint, la liaison devient inactive et est placée en mode de réserve.

LACP sans partenaire de liaison

Pour que le protocole LACP puisse créer un LAG, vous devez configurer les ports situés aux deux extrémités de la liaison pour LACP, ce qui signifie que les ports envoient des PDU LACP et gèrent les PDU reçues.

Toutefois, un partenaire de liaison peut être temporairement non configuré pour LACP. C'est le cas par exemple lorsque le partenaire de liaison se trouve sur un périphérique qui est en train de recevoir sa configuration via le protocole de configuration automatique. Les ports de ce périphérique ne sont pas encore configurés pour LACP. Si la liaison LAG ne s'établit pas, le périphérique ne peut pas être configuré. Un cas similaire se produit avec les ordinateurs à amorçage réseau par double carte (PXE par exemple), qui reçoivent leur configuration LAG uniquement après leur démarrage.

Lorsque vous configurez plusieurs ports LACP et que la liaison est activée sur un ou plusieurs ports, mais que ces derniers restent sans réponse LACP de la part du partenaire de liaison, le premier port dont la liaison a été activée est ajouté au LAG LACP et devient actif (les autres ports deviennent non-candidats). Ainsi, le périphérique voisin peut par exemple obtenir son adresse IP via DHCP et obtenir sa configuration via la configuration automatique.

Configuration des paramètres LACP

Utilisez la page LACP pour configurer les ports candidats pour le LAG ainsi que définir les paramètres LACP pour chaque port.

La valeur de délai LACP est définie pour chaque port. Il s'agit de l'intervalle de temps qui s'écoule entre l'envoi et la réception de deux PDU LACP consécutives. Toutes choses égales par ailleurs, si le LAG est configuré avec davantage de ports candidats que le nombre maximal de ports actifs autorisés (8), le commutateur sélectionne des ports en tant que ports actifs à partir du LAG dynamique présentant la priorité 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 **Port Management** > **Link Aggregation** > **LACP**.

ÉTAPE 2 Dans le champ **LACP System Priority**, saisissez la valeur de priorité LACP globale pour tous les ports.

ÉTAPE 3 Cliquez sur **Apply**. La priorité du système LACP est définie et la configuration de fonctionnement mise à jour.

ÉTAPE 4 Pour modifier les paramètres LACP d'un port spécifique, sélectionnez le port souhaité et cliquez sur **Edit**.

ÉTAPE 5 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port à définir.
- **LACP Port Priority** : saisissez la valeur de priorité LACP du port sélectionné.
- **LACP Timeout** : sélectionnez des délais courts ou longs pour les PDU LACP voisines. Cela déterminera si la transmission périodique des PDU LACP voisines doit se produire à une fréquence lente (Long) ou rapide (Short).

ÉTAPE 6 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration de la fonction Energy Efficient Ethernet

La fonction Energy Efficient Ethernet (EEE) vise à économiser de l'énergie en l'absence de trafic sur la liaison. Avec Energy Efficient Ethernet, la consommation d'énergie est réduite lorsque le port est actif mais qu'il ne présente aucun trafic.

La fonction Energy Efficient Ethernet réduit la consommation énergétique globale en mode de détection d'énergie. Elle est définie pour chaque port, que ce dernier soit ou non membre d'un LAG.

Pour activer la fonction Energy Efficient Ethernet sur un port :

ÉTAPE 1 Cliquez sur **Port Management** > **Energy Efficient Ethernet** > **Port Settings**.

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

- **Interface** : sélectionnez le port à configurer.
- **Energy Efficient Ethernet** : cochez **Enable** pour activer la fonction Energy Efficient Ethernet sur le port, ou décochez la case pour désactiver la fonction.

ÉTAPE 3 Cliquez sur **Apply**. La fonction Energy Efficient Ethernet est activée ou désactivée sur le port, et la configuration de fonctionnement est mise à jour.

10

Power over Ethernet

La fonctionnalité PoE (Power over Ethernet, alimentation électrique par câble Ethernet) est disponible uniquement sur les modèles basés sur PoE. Pour connaître la liste des modèles PoE, reportez-vous à la section **Modèles de périphériques**.

Ce chapitre explique comment utiliser la fonctionnalité PoE. Il contient les rubriques suivantes :

- **Considérations relatives à la fonctionnalité PoE**
- **PoE sur le commutateur**
- **Configuration des propriétés PoE**
- **Configuration des paramètres de port PoE**

Considérations relatives à la fonctionnalité PoE

Si votre commutateur est un modèle PoE, vous devez tenir compte des points suivants :

En tant qu'appareil PSE (Power Sourcing Equipment, équipement assurant l'alimentation électrique), le commutateur pour les modèles ci-dessous peut fournir un maximum de 30 watts par port PoE sur les ports 1 à 4, et 15,4 watts par port PoE sur les autres ports à un appareil alimenté (PD, Powered Device).

Modèle	Puissance dédiée au PoE	Ports PoE	Norme PoE prise en charge
SF220-24P	180 watts	1 à 24	802.3at sur les ports 1 à 4, et 802.3af sur les ports 5 à 24

Modèle	Puissance dédiée au PoE	Ports PoE	Norme PoE prise en charge
SG220-26P	180 watts	1 à 24	802.3at sur les ports 1 à 4, et 802.3af sur les ports 5 à 24
SF220-48P	375 watts	1 à 48	802.3at sur les ports 1 à 4, et 802.3af sur les ports 5 à 48
SG220-50P	375 watts	1 à 48	802.3at sur les ports 1 à 4, et 802.3af sur les ports 5 à 48

En tant qu'appareil PSE (Power Sourcing Equipment, équipement assurant l'alimentation électrique), le commutateur pour les modèles ci-dessous avec le pays de destination (Chine) peut fournir un maximum de 30 watts par port PoE à un appareil alimenté (PD, Powered Device).

Modèle	Puissance dédiée au PoE	Ports PoE	Norme PoE prise en charge
SF220-24P	180 watts	1 à 24	802.3at
SF220-48P	375 watts	1 à 48	802.3at
SG220-28MP	375 watts	1 à 48	802.3at

ATTENTION Le commutateur doit être uniquement connecté à des réseaux PoE sans branchement sur secteur.

ATTENTION Vous devez tenir compte des points ci-dessous lorsque vous connectez des commutateurs capables de fournir une alimentation PoE :

Les commutateurs PoE sont des PSE qui peuvent assurer l'alimentation en courant continu des appareils alimentés (PD) connectés. Ces derniers englobent notamment des téléphones VoIP, des caméras IP et des points d'accès sans fil. Les commutateurs PoE peuvent détecter et alimenter des appareils alimentés PoE hérités préstandard. En raison de la prise en charge de l'alimentation PoE héritée, un commutateur PoE agissant en tant que PSE peut détecter et alimenter par erreur un PSE connecté, y compris d'autres commutateurs PoE, en tant qu'appareil alimenté hérité.

Même si les commutateurs PoE sont des PSE qui doivent par nature être alimentés en courant alternatif, ils peuvent être alimentés en tant qu'appareil alimenté hérité par un autre PSE suite à une erreur de détection. Dans cette situation, le commutateur PoE risque de ne pas fonctionner correctement et peut également ne pas alimenter convenablement ses appareils alimentés connectés.

Pour éviter toute erreur de détection, vous devez désactiver le PoE au niveau des ports des commutateurs PoE utilisés pour la connexion à des PSE. Par ailleurs, vous devez d'abord alimenter un appareil PSE avant de le connecter à un commutateur PoE. Lorsqu'un appareil est considéré à tort comme un appareil alimenté, vous devez le déconnecter du port PoE, puis l'alimenter avec du courant alternatif avant de reconnecter ses ports PoE.

PoE sur le commutateur

Un commutateur PoE est un PSE qui assure l'alimentation électrique des appareils alimentés (PD) connectés par les câbles cuivre existants sans interférence avec le trafic réseau, mise à jour du réseau physique ou modification de l'infrastructure réseau.

Caractéristiques de la fonctionnalité PoE

La fonctionnalité PoE présente les caractéristiques suivantes :

- Elle élimine le besoin d'assurer l'alimentation 110/220 V (CA) de tous les appareils connectés à un réseau local (LAN) filaire.
- Elle supprime la nécessité de placer tous les appareils réseau à proximité de sources d'alimentation.
- Elle élimine le besoin de déployer des systèmes à double câblage dans une entreprise et permet ainsi de réduire de façon significative les coûts d'installation.

La fonctionnalité PoE peut être utilisée dans tout réseau d'entreprise déployant des appareils de puissance relativement faible connectés au réseau local (LAN) Ethernet, notamment :

- les téléphones IP ;
- les points d'accès sans fil ;
- les passerelles IP ;

- les appareils de surveillance audio et vidéo à distance.

Fonctionnement du PoE

La mise en œuvre de PoE comprend les étapes suivantes :

- **Détection** : envoie des impulsions spéciales sur le câble cuivre. Lorsqu'un appareil PoE est situé à l'autre extrémité, cet appareil répond à ces impulsions.
- **Classification** : la négociation entre le PSE et l'appareil alimenté débute après l'étape de détection. Au cours de la négociation, l'appareil alimenté spécifie sa classe, qui correspond à la quantité maximale d'énergie qu'il consomme.
- **Consommation électrique** : une fois l'étape de classification terminée, le PSE assure l'alimentation de l'appareil alimenté (PD). Un appareil alimenté sans prise en charge de la classification est supposé appartenir à la classe 0 (maximum). Si un appareil alimenté essaie de consommer plus d'énergie que ne l'autorise la norme, le PSE arrête d'alimenter le port.

Le PoE prend en charge deux modes :

- **Port Limit** : (Limite du port) la puissance maximale que le commutateur accepte de fournir est limitée à la valeur configurée par l'administrateur système, indépendamment du résultat de la classification.
- **Class Limit** : (Limite de classe) la puissance maximale que le commutateur accepte de fournir est déterminée par les résultats de l'étape de classification. Cela signifie qu'elle est définie conformément à la demande du client.

Considérations relatives à la configuration du PoE

Deux facteurs sont à prendre en considération dans la fonctionnalité PoE :

- la quantité d'énergie que le PSE peut fournir ;
- la quantité d'énergie que l'appareil alimenté essaie vraiment de consommer.

Vous pouvez décider :

- De passer du mode Class Limit au mode Port Limit et inversement alors que l'appareil est en fonctionnement. Les valeurs de puissance par port qui ont été configurées pour le mode Port Limit sont conservées.

REMARQUE Le passage du mode Class Limit au mode Port Limit et inversement alors que le commutateur est opérationnel impose une reconnexion de l'appareil alimenté.

- De la limite de port maximale autorisée en tant que limite numérique par port en mW (mode Port Limit).
- De générer un filtre lorsqu'un appareil alimenté essaie de consommer trop d'énergie et à quel pourcentage de la puissance maximale ce filtre est généré.

En mode Class Limit, le matériel PoE spécifique détecte automatiquement la classe de l'appareil alimenté et sa limite de puissance en fonction de la classe de l'appareil connecté à chaque port spécifique.

Si, à un moment quelconque au cours de la connexion, un appareil alimenté connecté nécessite plus de puissance de la part du commutateur que ce que permet l'affectation configurée (que le commutateur soit en mode Class Limit ou Port Limit), le commutateur :

- maintient l'état actif/inactif de la liaison du port PoE ;
- désactive l'alimentation du port PoE ;
- maintient l'alimentation des autres ports PoE ;
- consigne le motif de l'arrêt de l'alimentation ;
- génère un filtre SNMP.

Configuration des propriétés PoE

La page des propriétés permet de sélectionner le mode de fonctionnement PoE (Port Limit ou Class Limit) et de spécifier les filtres PoE à générer.

Ces paramètres sont saisis à l'avance. Lorsque l'appareil alimenté se connecte et consomme de l'énergie, il peut consommer beaucoup moins que la puissance maximale autorisée.

L'alimentation est désactivée lors du redémarrage, de l'initialisation et de la configuration système pour éviter toute détérioration des appareils alimentés.

Pour configurer la fonctionnalité PoE et surveiller la consommation électrique actuelle :

ÉTAPE 1 Cliquez sur **Port Management** > **PoE** > **PoE Properties**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Power Mode** : sélectionnez l'une des options suivantes :
  - *Port Limit* : la limite maximale de puissance par port est configurée par l'utilisateur.
  - *Class Limit* : la limite maximale de puissance par port est déterminée par la classe de l'appareil, qui résulte de l'étape de classification.

  REMARQUE Lorsque vous passez de Port Limit à Class Limit ou inversement, les ports sont reconnectés.
- **Legacy** : active ou désactive les appareils alimentés hérités sous-jacents. Cette fonctionnalité fonctionne uniquement lors de l'établissement de la négociation automatique de connexion. Pour les appareils alimentés hérités déjà connectés, la désactivation de cette fonctionnalité prend seulement effet une fois les câbles correspondants débranchés.
- **Traps** : active ou désactive les filtres. Si les filtres sont activés, vous devez également activer le service SNMP et configurer au moins un destinataire de notification SNMP (voir **Configuration des destinataires de notifications SNMP**).
- **Power Trap Threshold** : saisissez le seuil d'utilisation sous la forme d'un pourcentage de la puissance système. Une alarme se déclenche si la puissance dépasse cette valeur.

Les compteurs suivants sont affichés pour chaque appareil :

- **Operational Status** : affiche l'état opérationnel (Normal ou Fault) du commutateur PoE.
- **Nominal Power** : affiche la quantité totale d'énergie que le commutateur peut fournir à l'ensemble des appareils alimentés connectés.
- **Consumed Power** : affiche la quantité d'énergie actuellement consommée par les ports PoE.
- **Allocated Power** : affiche la quantité d'énergie affectée aux ports PoE.
- **Available Power** : puissance nominale moins la quantité d'énergie affectée.

ÉTAPE 3 Cliquez sur **Apply**. Les propriétés PoE sont définies et la configuration de fonctionnement mise à jour.

Configuration des paramètres de port PoE

Utilisez la page des paramètres de port PoE pour activer PoE sur les ports et surveiller la consommation électrique actuelle ainsi que la limite maximale de puissance par port.

Cette page permet de limiter la puissance par port de deux façons différentes, en fonction du mode d'alimentation :

- **Port Limit** : la puissance est limitée à une consommation en watts spécifique. Pour que ces paramètres soient actifs, le commutateur doit être en mode Port Limit. Vous pouvez configurer ce mode sur la page PoE Properties. Lorsque l'énergie consommée sur le port dépasse la limite du port, l'alimentation du port est désactivée.
- **Class Limit** : la puissance est limitée en fonction de la classe de l'appareil alimenté connecté. Pour que ces paramètres soient actifs, le commutateur doit être en mode Class Limit. Vous pouvez configurer ce mode sur la page PoE Properties. Lorsque l'énergie consommée sur le port dépasse la limite de classe, l'alimentation du port est désactivée.

Pour configurer les paramètres de port PoE :

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

ÉTAPE 2 Pour modifier la limite de puissance par port, sélectionnez un port et cliquez sur **Edit.**

ÉTAPE 3 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port à configurer.
- **PoE Administrative Status** : activez ou désactivez PoE sur le port.
- **Power Priority Level** : sélectionnez la priorité des ports pour la gestion de l'alimentation lorsque l'alimentation du commutateur est insuffisante. Par exemple, lorsque la puissance système est insuffisante et que l'appareil alimenté est inséré dans le port 1, qui présente une priorité élevée, l'alimentation des ports de faible priorité peut être désactivée.
- **Administrative Power Allocation** : si le mode d'alimentation est Power Limit, entrez la puissance maximale (en milliwatts) affectée au port. La valeur par défaut est 30 000 mW pour les ports 802.3at ou 15 400 mW pour les ports 802.3af.

Les compteurs suivants sont affichés pour chaque appareil :

- **Max Power Allocation** : affiche la puissance maximale (en milliwatts) affectée à l'appareil alimenté connecté au port sélectionné. En mode Class Limit, cette valeur est déterminée au moment de la détection de la classe de l'appareil alimenté connecté, 15,4 W (802.3af, classes 0 à 3) et 30 W (802.3at, classe 4). En mode Power Limit, cette valeur est déterminée par la norme PoE du port, 15,4 W (802.3af) et 30 W (802.3at).
- **Power Consumption** : affiche la puissance (en milliwatts) affectée à l'appareil alimenté connecté au port sélectionné.
- **Class** : affiche les informations sur la classe de l'appareil alimenté connecté si le mode d'alimentation est Class Limit.

Classe	Puissance maximale fournie par le port du commutateur
Classe 0	15,4 W
Classe 1	4,0 W
Classe 2	7,0 W
Classe 3	15,4 W
Classe 4	30,0 W

- **Overload Counter** : affiche le nombre total d'occurrences de surcharges de courant.
- **Short Counter** : affiche le nombre total d'occurrences de coupures de courant.
- **Denied Counter** : affiche le nombre de fois où l'alimentation a été refusée à l'appareil alimenté.
- **Absent Counter** : affiche le nombre de fois où l'alimentation de l'appareil alimenté a été arrêtée parce que ce dernier n'était plus détecté.
- **Invalid Signature Counter** : 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 **Apply**. Les propriétés de port PoE sont définies et la configuration de fonctionnement mise à jour.

11

Gestion des VLAN

Ce chapitre explique comment définir les paramètres de VLAN. Il contient les rubriques suivantes :

- VLAN
- Configuration du VLAN par défaut
- Création d'un VLAN
- Configuration des paramètres VLAN d'interface
- Configuration des ports d'un VLAN
- Affichage de l'appartenance VLAN
- Configuration de GVRP
- Configuration du VLAN voix

VLAN

Un VLAN (Virtual LAN, réseau local virtuel) est un groupe logique de ports qui permet aux périphériques qui lui sont associés de communiquer entre eux sur une couche MAC Ethernet, quel que soit le segment LAN physique du réseau ponté auquel ils sont connectés.

Description du VLAN

Chaque VLAN est configuré avec un VID unique (ID VLAN) dont la valeur est comprise entre 1 et 4094. Un port sur un périphérique dans un réseau ponté est membre d'un VLAN s'il peut échanger (envoyer/recevoir) des données avec le VLAN. Un port est un membre non balisé d'un VLAN si aucun des paquets qui lui sont destinés ne dispose d'une balise VLAN. Un port est un membre balisé d'un VLAN si tous les paquets qui lui sont destinés disposent d'une balise VLAN. Un port peut être membre d'un ou de plusieurs VLAN.

Un port en mode Accès VLAN ne peut faire partie que d'un seul VLAN. S'il est en mode General (Général) ou Trunk (Liaison), le port peut faire partie d'un ou de plusieurs VLAN.

Les VLAN permettent de faire face aux problèmes de sécurité et d'évolutivité. Le trafic d'un VLAN reste à l'intérieur du VLAN et se termine au niveau de ses périphériques. Le VLAN facilite également la configuration réseau en connectant logiquement les périphériques sans les transférer physiquement.

Si une trame est balisée VLAN, une balise VLAN à quatre octets est ajoutée à chaque trame Ethernet. La balise contient un ID VLAN compris entre 1 et 4094 et une balise de priorité VLAN (VPT, VLAN Priority Tag) comprise entre 0 et 7.

Lorsqu'une trame entre dans un périphérique tenant compte du VLAN, elle est classée comme appartenant à un VLAN, en vertu de la balise VLAN à quatre octets qu'elle contient.

S'il n'existe aucune balise VLAN dans la trame ou si la trame comporte une balise de priorité seulement, elle est classée dans le VLAN sur la base du PVID (Port VLAN Identifier, identificateur de port VLAN) configuré au niveau du port d'entrée de la trame.

La trame est désactivée au niveau du port d'entrée si le filtrage d'entrée est activé et si le port d'entrée n'est pas membre du VLAN auquel appartient le paquet. Une trame est considérée comme balisée d'une priorité uniquement si le VID présent dans sa balise VLAN est 0.

Les trames appartenant à un VLAN restent dans le VLAN. Ce principe est appliqué par l'envoi ou le réacheminement d'une trame uniquement aux ports de sortie membres du VLAN cible. Un port de sortie peut être un membre balisé ou non balisé d'un VLAN.

Le port de sortie :

- Ajoute une balise VLAN à la trame si le port de sortie est un membre balisé du VLAN cible et si la trame d'origine n'a pas de balise VLAN.
- Supprime la balise VLAN de la trame si le port de sortie est un membre non balisé du VLAN cible et si la trame d'origine a une balise VLAN.

Rôles du VLAN

Les VLAN fonctionnent au niveau de la Couche 2. L'ensemble du trafic VLAN (destination unique, diffusion et multidestination) demeure au sein du VLAN correspondant. Les périphériques reliés à différents VLAN n'ont pas de connectivité directe entre eux sur la couche MAC Ethernet.

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 ponté. Les VLAN sur un périphérique peuvent être créés de façon statique ou dynamique en fonction 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 **Configuration de GVRP**.

Certains VLAN peuvent avoir des rôles supplémentaires, notamment :

- **VLAN voix** : reportez-vous à la section **Configuration du VLAN voix** pour en savoir plus.
- **VLAN invité** : à configurer sur la page Edit VLAN Authentication.
- **VLAN par défaut** : reportez-vous à la section **Configuration du VLAN par défaut** pour en savoir plus.
- **VLAN de gestion** (dans les systèmes en mode système Couche 2) : reportez-vous à la section **Adressage IP** pour en savoir plus.

Flux de travail de configuration des VLAN

Pour configurer des VLAN :

- Le cas échéant, modifiez le VLAN par défaut en suivant les instructions de la section **Configuration du VLAN par défaut**.
- Créez les VLAN requis en suivant les instructions de la section **Création d'un VLAN**.
- Définissez la configuration VLAN souhaitée pour chaque port en suivant les instructions de la section **Configuration des paramètres VLAN d'interface**.
- Affectez des interfaces aux VLAN en suivant les instructions de la section **Configuration des ports d'un VLAN**.
- Affichez l'appartenance actuelle des ports aux VLAN pour toutes les interfaces en suivant les instructions de la section **Affichage de l'appartenance VLAN**.
- Activez GVRP au niveau global ainsi que sur chaque port en suivant les instructions de la section **Configuration de GVRP**.
- Configurez les paramètres du VLAN voix en suivant les instructions de la section **Configuration du VLAN voix**.

Configuration du VLAN par défaut

Si les paramètres d'usine (par défaut) sont utilisés, le commutateur crée automatiquement un VLAN 1 en tant que VLAN par défaut. L'état de l'interface par défaut de tous les ports est défini sur Trunk (Liaison) et tous les ports sont configurés en tant que membres non balisés du VLAN par défaut.

Le VLAN par défaut présente les caractéristiques suivantes :

- Il est distinct, non statique et non dynamique ; tous les ports sont des membres non balisés par défaut.
- Il ne peut pas être supprimé.
- Il ne peut pas recevoir d'étiquette.
- Il ne peut pas être utilisé pour un rôle spécial tel qu'un VLAN non authentifié ou un VLAN voix. Cette option ne concerne que les VLAN voix avec le mode OUI activé.
- Si un port n'est plus membre d'un VLAN, le 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 si le port est supprimé du VLAN.

Lorsque le VID du VLAN par défaut est modifié, le commutateur exécute les opérations suivantes sur tous les ports du VLAN :

- Il supprime l'appartenance VLAN des ports du VLAN par défaut d'origine.
- Il remplace le PVID des ports par le VID du nouveau VLAN par défaut.
- Il ajoute les ports en tant que membres VLAN non balisés du nouveau VLAN par défaut.

Pour changer le VLAN par défaut :

ÉTAPE 1 Cliquez sur **VLAN Management** > **Default VLAN Settings**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Current Default VLAN ID** : affiche l'ID de VLAN par défaut actuel.
- **Default VLAN ID** : saisissez un nouvel ID de VLAN pour remplacer l'ID de VLAN par défaut.

ÉTAPE 3 Cliquez sur **Apply.** Le VLAN par défaut est modifié et la configuration de fonctionnement mise à jour.

Création d'un VLAN

Vous pouvez créer un VLAN, mais cela n'a aucun effet tant que le VLAN n'est pas manuellement ou dynamiquement lié à un port au moins. Les ports doivent toujours appartenir à un ou plusieurs VLAN.

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 dans le VLAN d'abandon sont abandonnés à l'entrée et ne sont jamais réacheminés vers un port.

Pour créer un VLAN :

ÉTAPE 1 Cliquez sur **VLAN Management** > **Create VLAN**.

Les champs suivants s'affichent :

- **VLAN ID** : identifiant du VLAN.
- **VLAN Name** : nom du VLAN.
- **Type** : type de VLAN. Les options sont les suivantes :
  - *GVRP* : le VLAN a été dynamiquement créé via le protocole GVRP (Generic VLAN Registration Protocol).
  - *Static* : le VLAN a été défini par l'utilisateur.
  - *Default* : il s'agit du VLAN par défaut.

ÉTAPE 2 Cliquez sur **Add** pour ajouter un nouveau VLAN, ou sélectionnez un VLAN existant et cliquez sur **Edit** pour modifier ses paramètres.

ÉTAPE 3 Pour créer un seul VLAN, sélectionnez la case d'option **VLAN**, saisissez l'**ID de VLAN (VID)** et éventuellement le **nom du VLAN**.

ÉTAPE 4 Pour créer une plage de VLAN, sélectionnez la case d'option **Range** et indiquez la plage de VLAN à créer dans les champs **VLAN Range**.

ÉTAPE 5 Cliquez sur **Apply**. Les VLAN sont créés et la configuration de fonctionnement est mise à jour.

Configuration des paramètres VLAN d'interface

Utilisez la page Interface Settings pour configurer les paramètres VLAN de toutes les interfaces. Le commutateur prend en charge 4 094 VLAN, y compris le VLAN par défaut.

Pour configurer les paramètres VLAN d'interface :

ÉTAPE 1 Cliquez sur **VLAN Management** > **Interface Settings**.

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

ÉTAPE 3 Sélectionnez un port ou un LAG et cliquez sur **Edit**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Interface** : sélectionnez un port ou un LAG à configurer.
- **Interface VLAN Mode** : sélectionnez le mode VLAN. Les options sont les suivantes :
  - *General* : l'interface peut prendre en charge toutes les fonctions telles qu'elles sont définies dans la spécification IEEE 802.1q. Elle peut être un membre balisé ou non balisé d'un ou de plusieurs VLAN.
  - *Access* : l'interface est un membre non balisé d'un VLAN unique. Un port configuré dans ce mode est appelé un port d'accès.
  - *Trunk* : l'interface est un membre non balisé d'un VLAN au maximum ainsi qu'un membre balisé de zéro ou plusieurs VLAN. Un port configuré dans ce mode est appelé un port de liaison.

- *Dot1p-Tunnel* : sélectionnez cette option pour mettre l'interface en mode QinQ. L'utilisateur peut ainsi appliquer son propre agencement VLAN (PVID) sur le réseau du fournisseur. Le commutateur est en mode QinQ lorsqu'il comporte un ou plusieurs ports dot1p-tunnel.

- **Administrative PVID** : (disponible dans les modes General et Trunk) saisissez l'ID VLAN de port (PVID) du VLAN dans lequel les trames non balisées entrantes et les trames balisées de priorité sont classées.
- **Frame Type** : (disponible en mode General) sélectionnez le type de trame que l'interface peut recevoir. Les trames qui ne sont pas du type configuré sont abandonnées à l'entrée. Ces types de trames sont uniquement disponibles en mode General. Les valeurs possibles sont les suivantes :
  - *Admit All* : l'interface accepte tous les types de trames : trames non balisées, trames balisées et trames balisées de priorité.
  - *Admit Tagged Only* : l'interface accepte uniquement les trames balisées.
  - *Admit Untagged Only* : l'interface accepte uniquement les trames de priorité et non balisées.
- **Ingress Filtering** : (disponible en mode General) cochez **Enable** pour activer le filtrage d'entrée. Lorsqu'une interface est en mode de filtrage d'entrée, elle abandonne toutes les trames entrantes classées comme appartenant aux VLAN dont elle n'est pas membre. Le filtrage d'entrée peut être désactivé ou activé sur les ports généraux. Il est toujours activé sur les ports d'accès et les ports de liaison.
- **Uplink** : (disponible en mode Trunk) cochez **Enable** pour définir l'interface en tant que port de liaison montante.
- **TPID** : (disponible en mode Trunk) Si l'option Unlink est activée, sélectionnez la valeur TPID (Tag Protocol Identifier, identifiant du protocole de la balise) modifiée pour l'interface.

ÉTAPE 5 Cliquez sur **Apply**. Les paramètres VLAN d'interface sont définis et la configuration de fonctionnement est mise à jour.

Configuration des ports d'un VLAN

Utilisez la page Port to VLAN pour configurer les ports membres d'un VLAN.

Pour mapper des ports ou des LAG à un VLAN :

ÉTAPE 1 Cliquez sur **VLAN Management** > **Port to VLAN**.

ÉTAPE 2 Sélectionnez un VLAN et le type d'interface (Port ou LAG), puis cliquez sur **Go**.

Le mode de chaque port ou LAG s'affiche dans son état actuel (Access, Trunk, General ou Dot1q-Tunnel), défini sur la page Interface Settings.

ÉTAPE 3 Pour modifier l'enregistrement d'une interface auprès du VLAN, sélectionnez l'option souhaitée dans la liste suivante :

- **Forbidden** : 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).
- **Excluded** : 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.
- **Tagged** : l'interface est un membre balisé du VLAN.
- **Untagged** : 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 propre à chaque port.

ÉTAPE 4 Cliquez sur **Apply.** Les interfaces sont affectées au VLAN et la configuration de fonctionnement est mise à jour.

Affichage de l'appartenance VLAN

La page Port VLAN Membership affiche la liste des VLAN auxquels chaque port appartient.

Lorsque l'appartenance au VLAN par défaut est interdite pour un port, celui-ci ne peut appartenir à aucun autre VLAN. Le VID interne 4095 est affecté au port.

Pour un réacheminement correct des 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 et leurs appartenances de ports via le protocole GVRP.

Les ports non balisés entre deux périphériques tenant compte du VLAN sans aucune intervention des périphériques doivent appartenir au même VLAN. En d'autres termes, le PVID sur les ports entre les deux périphériques doit être le même si les ports doivent échanger (envoyer/recevoir) des paquets non balisés avec le VLAN. Dans le cas contraire, le trafic peut fuir d'un VLAN vers un autre.

Les trames balisées VLAN peuvent traverser d'autres périphériques réseau tenant compte ou non du VLAN. Si un nœud d'extrémité de destination ne tient pas compte du VLAN, mais doit recevoir du trafic d'un VLAN, alors le dernier périphérique tenant compte du VLAN (s'il en existe un) doit envoyer les trames du VLAN de destination au nœud d'extrémité sous forme non balisée.

Pour afficher l'appartenance VLAN :

ÉTAPE 1 Cliquez sur **VLAN Management** > **Port VLAN Membership**.

ÉTAPE 2 Sélectionnez le type d'interface (port ou LAG), puis cliquez sur **Go**.

Les champs suivants s'affichent :

- **Interface** : ID du port ou du LAG.
- **Mode** : mode VLAN d'interface qui a été sélectionné sur la page Interface Settings.
- **Administrative VLANs** : affiche tous les VLAN dont l'interface peut être membre.
- **Operational VLANs** : affiche tous les VLAN dont l'interface est actuellement membre.
- **LAG** : si l'interface sélectionnée est Port, ce champ affiche le LAG dont elle est membre.

ÉTAPE 3 Sélectionnez un port et cliquez sur **Join VLAN**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port ou LAG à définir.
- **Mode** : affiche le mode VLAN de port qui a été sélectionné sur la page Interface Settings.

- **Select VLAN** : pour associer un port aux VLAN, déplacez les ID VLAN de la liste de gauche vers la liste de droite à l'aide des flèches. Le VLAN par défaut peut apparaître dans la liste de droite s'il est balisé. Il ne peut cependant pas être sélectionné.
- **Tagging** : sélectionnez l'une des options de balisage ou PVID suivantes :
  - *Forbidden* : 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).
  - *Excluded* : 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.
  - *Tagged* : permet d'indiquer si le port est balisé. Cette option ne concerne pas les ports d'accès.
  - *Untagged* : permet d'indiquer si le port est 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 Access ou Trunk, le commutateur fait automatiquement de l'interface un membre non balisé du VLAN. Si l'interface est en mode General, vous devez configurer manuellement l'appartenance VLAN.

ÉTAPE 5 Cliquez sur **Apply**. Les paramètres sont modifiés et la configuration de fonctionnement est mise à jour.

ÉTAPE 6 Pour afficher les VLAN administratifs et opérationnels sur une interface, cliquez sur **Details**.

Configuration de GVRP

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

Étant donné que le protocole GVRP nécessite une prise en charge du balisage et doit assurer la liaison du VLAN autorisé, vous devez configurer le port en mode Trunk.

Lorsqu'un port rejoint un VLAN via GVRP, il est ajouté au VLAN en tant que membre dynamique, sauf si cette action a été expressément interdite sur la page Port VLAN Membership. Si le VLAN n'existe pas, il est dynamiquement créé lorsque l'option de création de VLAN dynamiques est activée pour ce port (sur la page GVRP Settings).

Le protocole GVRP doit être activé au niveau global 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 pouvoir être propagé, un VLAN doit être actif sur un port au moins.

Pour définir les paramètres GVRP :

ÉTAPE 1 Cliquez sur **VLAN Management** > **GVRP Settings**.

ÉTAPE 2 Cochez **Enable** en regard du champ **GVRP Global Status** pour activer globalement GVRP sur le commutateur.

ÉTAPE 3 Cliquez sur **Apply**.

ÉTAPE 4 Sélectionnez le type d'interface (port ou LAG), puis cliquez sur **Go**.

Les champs suivants s'affichent :

- **Interface** : numéro d'interface.
- **GVRP State** : indique si le protocole GVRP est activé ou désactivé sur l'interface.
- **Dynamic VLAN Creation** : indique si la création de VLAN dynamiques est activée ou désactivée sur l'interface. Si elle est désactivée, GVRP peut fonctionner mais aucun VLAN n'est créé.
- **GVRP Registration** : indique le mode d'enregistrement VLAN sur l'interface.

ÉTAPE 5 Pour définir les paramètres GVRP d'une interface, sélectionnez l'interface souhaitée et cliquez sur **Edit**.

ÉTAPE 6 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port ou LAG à définir.
- **GVRP State** : cochez **Enable** pour activer GVRP sur cette interface.
- **Dynamic VLAN Creation** : cochez **Enable** pour activer la création de VLAN dynamiques sur cette interface.
- **GVRP Registration** : sélectionnez le mode d'enregistrement VLAN via GVRP sur cette interface.

ÉTAPE 7 Cliquez sur **Apply.** Les paramètres GVRP sont modifiés et la configuration de fonctionnement est mise à jour.

Configuration du VLAN voix

Dans un LAN, les périphériques vocaux tels que les téléphones IP, les points d'extrémité VoIP et les systèmes vocaux sont placés dans le même VLAN. On appelle ce VLAN un VLAN voix. Le VLAN voix est utilisé lorsque le trafic provenant de téléphones ou d'équipements VoIP est affecté à un VLAN spécifique. Le commutateur peut automatiquement détecter et ajouter des ports membres au VLAN voix, et affecter la qualité de service (QoS) configurée aux paquets depuis le VLAN voix.

Modes VLAN voix dynamiques

Le commutateur prend en charge deux modes VLAN voix dynamiques : le mode OUI de téléphonie (OUI = Organization Unique Identifier) et le mode VLAN voix automatique. Les deux modes influencent la façon dont le VLAN voix et/ou les appartenances de ports du VLAN voix sont configurés. Les deux modes s'excluent mutuellement.

- **OUI de téléphonie** : dans ce mode, le VLAN voix doit être un VLAN configuré manuellement et ne peut pas être le VLAN par défaut.

  Lorsque le commutateur est en mode OUI de téléphonie et qu'un port est configuré manuellement comme candidat au VLAN voix, le commutateur ajoute dynamiquement le port au VLAN voix s'il reçoit un paquet dont l'adresse MAC source correspond à l'un des OUI de téléphonie configurés. Un OUI correspond aux trois premiers octets d'une adresse MAC Ethernet. Pour plus d'informations sur le mode OUI de téléphonie, reportez-vous à la section **Configuration du OUI de téléphonie**.

- **VLAN voix automatique** : dans ce mode, le VLAN voix peut être soit le VLAN voix par défaut soit être configuré manuellement.

Contrairement au mode OUI de téléphonie qui détecte les périphériques vocaux sur la base du OUI de téléphonie, le mode VLAN voix automatique ajoute dynamiquement les ports au VLAN voix en fonction des fonctionnalités CDP et/ou LLDP MED si elles sont activées. Il ajoute un port au VLAN voix s'il détecte sur le port un périphérique en cours de connexion qui s'annonce en tant que téléphone ou que point d'extrémité de supports par l'intermédiaire de CDP et/ou LLDP MED.

Contraintes du VLAN voix

Les contraintes suivantes existent :

- Un seul VLAN voix est pris en charge.
- Un VLAN défini en tant que VLAN voix ne peut pas être supprimé.

En outre, les contraintes suivantes s'appliquent au OUI de téléphonie :

- Le VLAN voix ne peut pas être le VLAN1 (VLAN par défaut).
- 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 pas être le VLAN invité si le mode VLAN voix est défini sur OUI de téléphonie.
- Le VLAN d'interface d'un port candidat peut être en mode General ou Trunk.
- À 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 ports statiques ainsi qu'aux ports candidats qui ont rejoint le VLAN voix.

Options de VLAN voix

Vous pouvez effectuer les opérations suivantes avec cette fonctionnalité :

- Définissez les paramètres de VLAN voix globaux et le mode de VLAN voix dynamique en suivant les instructions de la section **Configuration des propriétés du VLAN voix**.
- Configurez et mettez à jour la table des OUI de téléphonie avec un maximum de 16 entrées (chaque entrée est un numéro à trois octets) conformément aux instructions de la section **Configuration du OUI de téléphonie**. Le

commutateur utilise la table pour déterminer si l'appartenance VLAN voix automatique d'un port est activée et si le port va rejoindre le VLAN voix.

- Ajoutez une interface au VLAN voix sur la base de l'identifiant OUI et configurez le mode QoS OUI du VLAN voix selon la procédure décrite dans la section **Ajout d'interfaces au VLAN voix sur la base des OUI**.

Configuration des propriétés du VLAN voix

Utilisez la page des propriétés pour configurer les paramètres de VLAN voix au niveau global.

Pour configurer les propriétés du VLAN voix :

ÉTAPE 1 Cliquez sur **VLAN Management** > **Voice VLAN** > **Properties**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Voice VLAN ID** : sélectionnez le VLAN en tant que VLAN voix.
- **CoS/802.1p** : sélectionnez la valeur CoS/802.1p qui sera utilisée par LLDP MED en tant que stratégie de réseau téléphonique. Les valeurs possibles sont comprises entre 0 et 7, 7 correspondant à la priorité la plus élevée. La valeur 0 est utilisée dans le cadre d'une stratégie de « meilleur effort » (best effort) et est automatiquement appliquée lorsqu'aucune autre valeur n'a été définie (par défaut).
- **DSCP** : sélectionnez la valeur DSCP qui sera utilisée par LLDP MED en tant que stratégie de réseau téléphonique.
- **Dynamic Voice VLAN** : sélectionnez l'un des modes VLAN voix suivants :
  - *Enable Auto Voice VLAN*: cette option permet d'activer le mode VLAN voix automatique.
  - *Enable Telephony OUI*: cette option permet d'activer le mode OUI de téléphonie.
  - *Disable* : cette option permet de désactiver le VLAN voix.

ÉTAPE 3 Cliquez sur **Apply**. Les propriétés VLAN sont définies et la configuration de fonctionnement est mise à jour.

Configuration du OUI de téléphonie

Les OUI (Organizationally Unique Identifiers, identifiants uniques organisationnels) sont attribués par l'autorité d'enregistrement intégrée IEEE (Institute of Electrical and Electronics Engineers). Le nombre de fabricants de téléphones IP étant limité et bien connu, les valeurs OUI connues entraînent l'affectation automatique des trames concernées, et du port sur lequel elles sont détectées, à un VLAN voix.

La table globale des OUI peut contenir jusqu'à 16 entrées.

Utilisez la page Telephony OUI pour configurer les propriétés des OUI de téléphonie. Si le délai indiqué dans le champ Auto Membership Aging Time expire sans aucune activité téléphonique, le port est supprimé du VLAN voix.

Pour configurer le OUI de téléphonie :

ÉTAPE 1 Cliquez sur **VLAN Management** > **Voice VLAN** > **Telephony OUI**.

La table des OUI de téléphonie contient les informations suivantes :

- **Telephony OUI** : six premiers chiffres de l'adresse MAC réservés aux OUI.
- **Description** : description du OUI affecté par l'utilisateur.

ÉTAPE 2 Définissez les paramètres de OUI de téléphonie généraux ci-dessous :

- **Telephony OUI Operational Status** : indique si des OUI sont utilisés pour identifier le trafic vocal.
- **CoS/802.1p** : sélectionnez la file d'attente CoS à affecter au trafic vocal.
- **Remark CoS/802.1p** : cochez cette case pour remarquer le trafic de sortie.
- **Auto Membership Aging Time** : entrez le délai à l'issue duquel un port doit être supprimé du VLAN voix une fois que toutes les adresses MAC des téléphones détectés sur les ports ont expiré.

ÉTAPE 3 Cliquez sur **Apply**.

ÉTAPE 4 Cliquez sur **Add** pour ajouter un OUI.

ÉTAPE 5 Saisissez les informations suivantes :

- **Telephony OUI** : saisissez un nouvel identifiant OUI.
- **Description** : saisissez un nom d'identifiant OUI.

ÉTAPE 6 Cliquez sur **Apply.** L'identifiant OUI est ajouté et la configuration de fonctionnement mise à jour.

ÉTAPE 7 Cliquez sur **Restore Default OUI** pour supprimer tous les OUI créés par l'utilisateur et conserver uniquement les OUI par défaut dans la table.

Ajout d'interfaces au VLAN voix sur la base des OUI

Les attributs QoS peuvent être affectés aux paquets voix pour chaque port dans l'un des deux modes suivants :

- **All** : les valeurs QoS configurées sur le VLAN voix sont appliquées à toutes les trames entrantes reçues sur l'interface et classées dans le VLAN voix.
- **Telephony Source MAC Address (SRC)** : les valeurs QoS configurées pour le VLAN voix sont appliquées à toute trame entrante classée dans le VLAN voix et contenant un OUI dans l'adresse MAC source qui correspond à un OUI de téléphonie configuré.

Utilisez la page Telephony OUI Interface pour ajouter une interface au VLAN voix sur la base de l'identifiant OUI et configurer le mode QoS OUI du VLAN voix.

Pour configurer le mode OUI de téléphonie sur une interface :

ÉTAPE 1 Cliquez sur **VLAN Management** > **Voice VLAN** > **Telephony OUI Interface**.

ÉTAPE 2 Pour configurer une interface en tant que port candidat du VLAN voix basé sur les OUI de téléphonie, sélectionnez l'interface souhaitée et cliquez sur **Edit**.

ÉTAPE 3 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port ou LAG à configurer.
- **Telephone OUI VLAN Membership** : cochez **Enable** pour définir l'interface en tant que port candidat du VLAN voix basé sur les OUI de téléphonie. Lorsque des paquets correspondant à l'un des OUI de téléphonie configurés sont reçus, l'interface est ajoutée au VLAN voix.
- **Telephone OUI Mode** : sélectionnez **Auto** ou **Manual** comme mode de port.
  - *Auto* : le port est identifié comme candidat au VLAN voix. Lorsqu'un paquet doté d'une adresse MAC OUI source, qui identifie l'équipement distant en tant qu'équipement voix, est détecté sur le port, ce dernier rejoint le VLAN

voix en tant que port balisé. Si le délai d'expiration de la dernière adresse MAC de téléphonie dans la table des adresses MAC dépasse le délai d'expiration du VLAN voix, le port est supprimé du VLAN voix.

- *Manual* : affectation manuelle au VLAN voix.

- **Telephony OUI QoS Mode** : sélectionnez l'une des options suivantes :
  - *Telephony Source MAC Address* : les attributs QoS sont uniquement appliqués aux paquets provenant de téléphones IP.
  - *All* : les attributs QoS sont uniquement appliqués aux paquets classés dans le VLAN voix.

ÉTAPE 4 Cliquez sur **Apply.** Les paramètres d'interface des OUI de téléphonie sont définis et la configuration de fonctionnement est mise à jour.

12

Protocole STP (Spanning Tree Protocol)

Le protocole STP (Spanning Tree Protocol - IEEE802.1D et IEEE802.1Q) est activé par défaut avec le mode STP classique.

Ce chapitre indique la marche à suivre pour configurer le protocole STP et il aborde les sujets suivants :

- **Modes STP**
- **Configuration de l'état STP et des paramètres globaux**
- **Configuration des paramètres d'interface STP**
- **Configuration des paramètres d'interface RSTP**
- **Configuration MSTP**

Modes STP

Le protocole STP protège un domaine de diffusion de couche 2 (Layer 2) contre les avalanches de messages diffusés en paramétrant certains liens sur le mode de réserve pour empêcher les boucles. En mode de réserve, ces liens cessent temporairement de transférer des données d'utilisateur. Les liens sont automatiquement réactivés lorsque la topologie permet à nouveau le transfert de données.

Des boucles se produisent lorsque des chemins alternatifs existent entre les hôtes. Les boucles d'un réseau étendu peuvent utiliser des commutateurs pour acheminer indéfiniment le trafic, ce qui augmente celui-ci et nuit à l'efficacité du réseau.

Le protocole STP fournit une topologie en arborescence pour l'agencement des commutateurs et des liens d'interconnexion afin de créer un chemin d'accès unique entre les stations d'arrivée sur un réseau et d'éliminer les boucles.

Le commutateur prend en charge les modes STP suivants :

- **Classic STP** : fournit un chemin d'accès unique entre deux stations d'arrivée afin d'empêcher et d'éliminer les boucles.
- **Rapid STP (RSTP)** : détecte les topologies de réseau afin d'accélérer la convergence de l'arbre recouvrant. 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.
- **Multiple STP (MSTP)** : le protocole MSTP est basé sur le protocole RSTP. Il 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 (Layer 2), il peut arriver qu'une boucle se crée dans le VLAN A, mais pas dans le VLAN B. Si les deux VLAN sont définis sur un port X alors que le protocole STP souhaite réduire la boucle, le protocole stoppe le trafic sur tout le port, y compris le trafic du VLAN B.

  MSTP résout ce problème en activant plusieurs instances STP afin de détecter et de réduire séparément les boucles pour chaque instance. En associant les instances aux VLAN, chacune d'entre elles est associée au domaine de couche 2 (Layer 2) sur lequel elle détecte et réduit les boucles. Cela permet d'arrêter un port d'une instance. Par exemple, pour 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.

Configuration de l'état STP et des paramètres globaux

Utilisez la page des états STP et des paramètres globaux pour activer STP, RSTP ou MSTP sur le commutateur.

Utilisez respectivement la page des paramètres d'interface STP, la page des paramètres d'interface RSTP et la page des propriétés MSTP pour configurer chaque mode.

Pour définir l'état et les paramètres globaux du protocole STP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **STP Status and Global Settings**.

ÉTAPE 2 Dans la zone **Global Settings**, saisissez les informations suivantes :

- **Spanning Tree State** : activez ou désactivez STP sur le commutateur.
- **STP Operation Mode** : sélectionnez le mode STP.

- **BPDU Handling** : sélectionnez la manière dont les paquets BPDU (Bridge Protocol Data Unit) sont gérés lorsque STP est désactivé sur le commutateur. Les BPDU servent à transmettre des informations du protocole STP. Les options sont les suivantes :
  - *Filtering* : filtre les paquets BPDU lorsque le protocole STP est désactivé.
  - *Flooding* : inonde les paquets BPDU lorsque le protocole STP est désactivé.
- **Path Cost Default Values** : sélectionnez la méthode utilisée pour assigner les coûts d'acheminement par défaut aux ports STP. Les coûts d'acheminement par défaut affectés aux ports varient en fonction de la méthode sélectionnée.
  - *Short* : spécifie la plage de 1 à 65 535 pour les coûts d'acheminement des ports.
  - *Long* : spécifie la plage de 1 à 200 000 000 pour les coûts d'acheminement des ports.

ÉTAPE 3 Dans la zone **Bridge Settings**, saisissez les informations suivantes :

- **Priority** : indiquez la valeur de priorité du pont. Après l'échange de BPDU, le périphérique de priorité moindre devient le pont racine. Si tous les ponts utilisent la même priorité, leurs adresses MAC sont alors utilisées pour déterminer le pont racine. La valeur de priorité du pont est fournie par paliers de 4 096. Par exemple 4 096, 8 192, 12 288, etc.
- **Hello Time** : indiquez le temps d'attente en secondes d'un pont racine entre deux messages de configuration. Ce délai peut être de 1 à 10 secondes. La valeur par défaut est 2 secondes.
- **Max Age** : indiquez le temps d'attente en secondes du commutateur pour redéfinir sa propre configuration lorsqu'il ne reçoit pas de message de configuration. Ce délai peut être de 6 à 40 secondes. La valeur par défaut est 20 secondes.
- **Forward Time** : indiquez la durée en secondes durant laquelle le pont reste en état d'apprentissage (learning) avant de réacheminer des paquets. Ce délai peut être de 4 à 30 secondes. La valeur par défaut est 15 secondes.

La zone **Designated Root** comporte les champs suivants :

- **Bridge ID** : priorité du pont concaténée avec l'adresse MAC du commutateur.
- **Root Bridge ID** : priorité du pont racine concaténée avec l'adresse MAC du pont racine.

- **Port racine** : port offrant le chemin de moindre coût entre ce pont et le pont racine. (Cette information est importante lorsque le pont n'est pas le pont racine.)
- **Root Path Cost** : coût du chemin entre ce pont et le pont racine.
- **Topology Changes Counts** : nombre total des changements de topologie STP effectués.
- **Last Topology Change** : durée écoulée depuis le dernier changement de topologie. Cette durée s'affiche au format jours/heures/minutes/secondes.

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres globaux du protocole STP sont définis et la configuration de fonctionnement est mise à jour.

Configuration des paramètres d'interface STP

Utilisez la page des paramètres d'interface STP pour configurer STP par interface et pour prendre connaissance des informations apprises par le protocole, par exemple, pour connaître le pont désigné.

La configuration indiquée sur cette page est active pour tous les modes STP.

Pour configurer STP sur une interface :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **STP Interface Settings**.

ÉTAPE 2 Sélectionnez le type d'interface (Port ou LAG) et cliquez sur **Go**.

ÉTAPE 3 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port ou le LAG à définir.
- **Edge Port** : activez ou désactivez Fast Link sur l'interface. Si le mode Fast Link est activé pour une interface, celle-ci passe automatiquement en état de réacheminement (Forwarding) lorsque sa liaison est active. Fast Link optimise la convergence du protocole STP.
- **BPDU Guard** : si cette option est activée, l'interface se ferme lorsqu'un message BPDU se présente.

- **BPDU Filter** : si cette option est activée, l'interface n'envoie ni ne reçoit de messages BPDU.
- **Path Cost** : sélectionnez **User Defined** pour indiquer la contribution du port au coût d'acheminement vers le pont racine ou sélectionnez **Use Default** pour utiliser le coût par défaut généré par le système.
- **Priority** : sélectionnez la valeur de priorité de l'interface. La valeur de priorité influence le choix de l'interface lorsqu'un pont dispose de deux ports connectés au sein d'une boucle. La priorité est une valeur comprise entre 0 et 240, définie par incréments de 16.
- **Port State** : indique l'état STP de l'interface.
  - *Disabled* : le protocole STP est désactivé sur l'interface. L'interface réachemine le trafic tout en apprenant les adresses MAC.
  - *Blocking* : l'interface est bloquée et ne peut pas réacheminer le trafic (à l'exception des données BPDU) ni apprendre des adresses MAC.
  - *Learning* : l'interface est en mode d'apprentissage et ne peut pas réacheminer le trafic, mais elle peut appendre de nouvelles adresses MAC.
  - *Forwarding* : l'interface est en mode de réacheminement ; elle peut réacheminer le trafic et apprendre de nouvelles adresses MAC.
- **Designated Bridge ID** : affiche la priorité du pont et les adresses MAC du pont désigné.
- **Designated Port ID** : affiche la priorité et l'ID de l'interface sélectionnée.
- **Designated Cost** : affiche le coût de l'interface participant à la topologie STP. Les interfaces avec un coût moindre sont peu susceptibles d'être bloquées si STP détecte des boucles.

ÉTAPE 5 Cliquez sur **Apply.** Les paramètres de l'interface STP sont modifiés et la configuration de fonctionnement est mise à jour.

Configuration des paramètres d'interface RSTP

Le protocole RSTP (Rapid Spanning Tree Protocol) permet une convergence STP plus rapide sans création de boucles de réacheminement.

Utilisez la page des paramètres d'interface RSTP pour configurer le protocole RSTP par port. Toute configuration effectuée sur cette page est active lorsque le mode STP global est défini sur RSTP ou MSTP.

Pour définir les paramètres d'interface RSTP :

ÉTAPE 1 Définissez le mode de fonctionnement STP sur RSTP comme il est indiqué dans la section **Configuration de l'état STP et des paramètres globaux**.

ÉTAPE 2 Cliquez sur **Spanning Tree** > **RSTP Interface Settings**.

ÉTAPE 3 Sélectionnez le type d'interface (Port ou LAG) et cliquez sur **Go**.

ÉTAPE 4 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 5 Saisissez les informations suivantes :

- **Interface** : indiquez le port ou le LAG à configurer.
- **Point-to-Point Administrative Status** : définissez l'état de la liaison. Les options disponibles sont les suivantes :
  - *Enable* : le type de liaison du port est **point-to-point**.
  - *Disable* : le type de liaison du port est **share**.
  - *Auto* : détermine automatiquement le statut du type de liaison du port à l'aide de son mode duplex (**point-to-point** pour un mode duplex intégral et **share** pour un mode semi-duplex).
- **Point-to-Point Operational Status** : affiche l'état de fonctionnement du lien.
- **Role** : affiche le rôle de l'interface assigné par STP pour fournir les chemins STP. Les rôles possibles sont :
  - *Root* : chemin de moindre coût pour réacheminer des paquets vers le pont racine.
  - *Designated* : port par lequel le pont est relié au LAN et qui fournit le chemin de moindre coût entre le LAN et le pont racine.
  - *Alternate* : fournit un chemin alternatif entre l'interface racine et le pont racine.

- *Backup* : fournit un chemin de sauvegarde pour le chemin de port désigné vers les nœuds terminaux STP. 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 au moins deux connexions reliées à un segment partagé.
- *Disabled* : le port ne participe pas à l'arbre recouvrant.

▪ **Fast Link Operational Status** : indique si Fast Link (port de bordure) est activé ou désactivé sur l'interface.

▪ **Port Status** : indique l'état RSTP de l'interface. Les valeurs disponibles sont les suivantes :

- *Disabled* : RSTP est désactivé sur l'interface.
- *Blocking* : l'interface est bloquée et ne peut pas réacheminer le trafic ni apprendre des adresses MAC.
- *Learning* : l'interface est en mode d'apprentissage (learning) et ne peut pas réacheminer le trafic, mais elle peut appendre de nouvelles adresses MAC.
- *Forwarding* : l'interface est en mode de réacheminement ; elle peut réacheminer le trafic et apprendre de nouvelles adresses MAC.

ÉTAPE 6 Cliquez sur **Apply.** Les paramètres de l'interface RSTP sont modifiés et la configuration de fonctionnement est mise à jour.

ÉTAPE 7 Si l'interface sélectionnée est connectée au pont associé en cours de test, la migration de protocole est activée. Lorsqu'un partenaire de lien est détecté via STP, cliquez sur **Activate Protocol Migration** pour effectuer un test de migration des protocoles. Le test 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.

Configuration MSTP

Le protocole MSTP (Multiple Spanning Tree Protocol) est utilisé pour séparer l'état du port STP entre divers domaines (sur différents VLAN). Par exemple, si un port A est bloqué dans une instance STP en raison d'une boucle sur le VLAN A, le même port peut être placé en mode de réacheminement dans une autre instance STP.

Pour configurer MSTP :

ÉTAPE 1 Définissez le mode de fonctionnement STP sur MSTP comme il est indiqué dans la section **Configuration de l'état STP et des paramètres globaux**.

ÉTAPE 2 Définissez les paramètres MSTP globaux comme il est indiqué dans la section **Configuration des propriétés MSTP**.

ÉTAPE 3 Définissez les instances MSTP comme il est indiqué dans la section **Configuration des paramètres d'instance MSTP**. Chaque instance MSTP calcule et établit une topologie sans boucles pour transmettre les paquets à partir des VLAN qui se connectent à l'instance.

ÉTAPE 4 Définissez les instances MSTP à activer, dans quels VLAN, et associez ces instances MSTP aux VLAN, comme il convient, tel qu'il est indiqué dans la section **Mappage de VLAN à des instances MST**.

Configuration des propriétés MSTP

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

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 avoir le même mappage VLAN-instances MSTP, le même numéro de révision de la configuration ainsi que le même nom de région. Ce mappage peut être effectué sur la page VLAN vers instance MST.

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.

Pour définir les propriétés MSTP globales :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **MSTP Properties**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Region Name** : définissez un nom de région MSTP.
- **Revision** : définissez un numéro à 16 bits non affecté qui identifie la révision de la configuration MST actuelle. La valeur de ce champ est comprise entre 0 et 65535.
- **Max Hops** : 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. La valeur de ce champ est comprise entre 1 et 40. La valeur par défaut est 20.

ÉTAPE 3 Cliquez sur **Apply**. Les propriétés MSTP sont définies et le fichier de la configuration de fonctionnement est mis à jour.

Mappage de VLAN à des instances MST

Utilisez la page de mappage de VLAN à des instances MSTP pour mapper des VLAN à des instances MSTP. Pour que les périphériques soient dans la même région, leur mappage de VLAN à des instances MSTP doit être identique.

REMARQUE La même instance MSTP peut être mappée à plusieurs VLAN, mais chaque VLAN ne peut être lié qu'à une seule instance MSTP.

Il est possible de définir jusqu'à 16 instances MSTP sur le commutateur.
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 MSTP. L'instance CIST est l'instance MSTP 0.

Pour mapper des VLAN à des instances MSTP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **VLAN to MSTP Instance**.

ÉTAPE 2 Pour ajouter des VLAN à une instance MSTP, sélectionnez l'instance MSTP voulue et cliquez sur **Edit**.

ÉTAPE 3 Saisissez les informations suivantes :

- **MSTP Instance ID** : sélectionnez l'instance MSTP.
- **VLANs** : indiquez les VLAN à mapper à cette instance MSTP.
- **Action** : sélectionnez **Add** pour mapper les VLAN à l'instance MSTP ou **Remove** pour supprimer des VLAN de celle-ci.

ÉTAPE 4 Cliquez sur **Apply**. Le mappage VLAN à instances MSTP est défini et le fichier de la configuration de fonctionnement est mis à jour.

Configuration des paramètres d'instance MSTP

Utilisez la page des paramètres d'instance MSTP pour configurer les paramètres d'une instance MSTP.

Pour définir les paramètres d'une instance MSTP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **MSTP Instance Settings**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Instance ID** : sélectionnez l'instance MSTP à configurer.
- **Included VLAN** : affiche les VLAN mappés à l'instance MSTP sélectionnée. Par défaut, tous les VLAN sont mappés à l'instance CIST (instance 0).
- **Priority** : définissez la priorité de ce pont pour l'instance MSTP sélectionnée.
- **Designated Root Bridge ID** : affiche la priorité et l'adresse MAC du pont racine pour l'instance MSTP sélectionnée.
- **Root Port** : affiche le port racine de l'instance MSTP sélectionnée.
- **Root Path Cost** : affiche le coût du chemin vers le pont racine de l'instance MSTP sélectionnée.

- **Bridge ID** : affiche la priorité du pont et l'adresse MAC de ce commutateur pour l'instance MSTP sélectionnée.
- **Remaining Hops** : affiche le nombre de sauts restant jusqu'à la prochaine destination.

ÉTAPE 3 Cliquez sur **Apply.** Les paramètres de l'interface MSTP sont modifiés et la configuration de fonctionnement est mise à jour.

Configuration des paramètres d'interface MSTP

Utilisez la page des paramètres d'interface MSTP pour configurer les paramètres de chaque instance MSTP et pour visualiser les informations 'apprises' par le protocole, comme le pont désigné par instance MSTP.

Pour configurer les paramètres d'une interface MSTP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **MSTP Interface Settings**.

ÉTAPE 2 Sélectionnez une instance MSTP et le type d'interface (Port ou LAG) et cliquez sur **Go**.

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

ÉTAPE 3 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Instance ID** : sélectionnez l'instance MSTP à configurer.
- **Interface** : sélectionnez le port ou le LAG à configurer.
- **Path Cost** : sélectionnez **User Defined** pour indiquer la contribution du port au coût d'acheminement vers le pont racine ou sélectionnez **Use Default** pour utiliser la valeur par défaut. Le coût d'acheminement vers le pont racine est le coût d'acheminement entre le commutateur et le pont racine de l'instance MSTP spécifiée.
- **Priority** : indiquez la priorité pour le port et l'instance MSTP sélectionnés.
- **Port State** : affiche l'état MSTP du port. Les valeurs disponibles sont les suivantes :
  - *Disabled* : MSTP est actuellement désactivé.

- *Blocking* : le port sur cette instance est actuellement bloqué et ne peut ni réacheminer le trafic (à l'exception des données BPDU) ni apprendre des adresses MAC.
- *Learning* : le port sur cette instance est en mode d'apprentissage, par conséquent il ne peut pas réacheminer le trafic. En revanche, il peut apprendre de nouvelles adresses MAC.
- *Forwarding* : le port est en mode de réacheminement, il peut réacheminer le trafic et apprendre de nouvelles adresses MAC.

- **Port Role** : affiche le rôle de port par instance. Le rôle est assigné par l'algorithme MSTP pour fournir des chemins STP :
  - *Master* : un port maître (Master) fournit la connectivité entre une région MSTP et la racine CIST éloignée.
  - *Root* : le réacheminement des paquets vers ce port fournit le chemin de moindre coût pour réacheminer les paquets vers le périphérique racine.
  - *Designated* : port par lequel le pont est relié au LAN et qui fournit le chemin de moindre coût entre le LAN et le pont racine pour l'instance MST.
  - *Alternate* : le port fournit un chemin alternatif entre l'interface racine et le périphérique racine.
  - *Backup* : fournit un chemin de secours pour le chemin de port désigné vers les nœuds terminaux STP. 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 au moins deux connexions reliées à un segment partagé.
  - *Disabled* : l'interface ne participe pas à l'arbre recouvrant.
- **Mode** : affiche le mode STP actuel.
  - *STP* : le STP classique est activé sur le port.
  - *Rapid STP* : RSTP est activé sur le port.
  - *MSTP* : MSTP est activé sur le port.
- **Type** : affiche le type MSTP du port.
  - *Boundary* : un port de limite relie les ponts MSTP 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.
  - *Internal* : le port est un port interne.

- **Designated Bridge ID** : affiche le numéro d'ID de pont qui connecte le lien ou le LAN partagé à la racine.
- **Designated Port ID** : affiche la priorité et le numéro d'ID du port sur le pont désigné qui connecte le lien ou le LAN partagé à la racine.
- **Designated Cost** : 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.
- **Remaining Hops** : affiche les sauts restant jusqu'à la prochaine destination.

ÉTAPE 5 Cliquez sur **Apply.** La configuration de fonctionnement est mise à jour.

13

Tables d'adresses MAC

Ce chapitre indique la marche à suivre pour ajouter des adresses MAC au commutateur. Il aborde les sujets suivants :

- **Types d'adresses MAC**
- **Configuration d'adresses MAC statiques**
- **Configuration du filtre d'adresses MAC statiques**
- **Configuration du délai d'expiration d'adresses MAC dynamiques**
- **Interrogation de la table des adresses MAC dynamiques**
- **Configuration des adresses MAC réservées**

Types d'adresses MAC

Il existe deux types d'adresses MAC : les adresses statiques et les adresses dynamiques. Selon leur type, les adresses MAC sont stockées dans la table des adresses statiques ou dans la table des adresses dynamiques avec les informations relatives aux VLAN et aux ports.

Les adresses statiques sont configurées par l'utilisateur, par conséquent elles n'expirent jamais. Une nouvelle adresse MAC source qui apparaît dans une trame reçue par le commutateur est ajoutée à la table des adresses dynamiques. Cette adresse MAC est conservée pendant une période que vous pouvez configurer. Si aucune autre trame avec la même adresse MAC source ne se présente sur le commutateur avant l'expiration de ce délai, l'entrée MAC est supprimée de la table, car elle est arrivée à expiration.

Lorsqu'une trame se présente sur le commutateur, celui-ci recherche une adresse MAC de destination correspondante dans la table des adresses statiques ou la table des adresses dynamiques. Si le commutateur trouve une adresse correspondante, la trame est marquée comme étant en sortie sur le port spécifié dans la table. Si des trames sont envoyées à une adresse MAC qui n'existe pas dans les tables, elles sont transmises à tous les ports sur le VLAN approprié. Ces trames sont appelées trames de destination unique inconnue.

Configuration d'adresses MAC statiques

Les adresses MAC statiques sont affectées à une interface physique et à un VLAN spécifiques sur le commutateur. Si une adresse MAC est détectée sur une autre interface, elle est ignorée et n'est pas consignée dans la table des adresses. Il est possible de configurer jusqu'à 256 adresses MAC statiques sur le commutateur.

Pour définir une adresse MAC statique :

ÉTAPE 1 Cliquez sur **MAC Address Tables** > **Static Address**.

ÉTAPE 2 Pour ajouter une adresse MAC statique, cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **VLAN ID** : sélectionnez un ID de VLAN.
- **MAC Address** : saisissez l'adresse MAC.
- **Interface** : sélectionnez un port ou un LAG pour l'adresse MAC.
- **Status** : sélectionnez le mode de traitement de l'adresse MAC. Les options sont les suivantes :
  - *Permanent* : le commutateur ne supprime jamais cette adresse MAC. Si l'adresse MAC statique est enregistrée dans la configuration de démarrage, elle est conservée après le redémarrage.
  - *Delete on Reset* : l'adresse MAC statique est supprimée lorsque le commutateur est réinitialisé.
  - *Delete on Timeout* : l'adresse MAC est supprimée lorsqu'elle a expiré.
  - *Secure* : l'adresse MAC est sécurisée lorsque le port est en mode verrouillé classique.

ÉTAPE 4 Cliquez sur **Apply**. L'adresse MAC statique est ajoutée et la configuration de fonctionnement est mise à jour.

Configuration du filtre d'adresses MAC statiques

Utilisez la page du filtre d'adresses statiques pour configurer les profils du filtre d'adresses MAC statiques afin que des adresses MAC spécifiques ne soient pas affectées aux VLAN spécifiés sur le commutateur.

Pour définir un profil de filtre d'adresses MAC statiques :

ÉTAPE 1 Cliquez sur **MAC Address Tables** > **Static Address Filtering**.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **MAC Address** : saisissez l'adresse MAC.
- **VLAN ID** : sélectionnez un ID de VLAN. L'adresse MAC spécifiée ne sera pas affectée à ce VLAN.

ÉTAPE 4 Cliquez sur **Apply**. Le profil du filtre d'adresses MAC statiques est ajouté et la configuration de fonctionnement est mise à jour.

Configuration du délai d'expiration d'adresses MAC dynamiques

La table des adresses dynamiques contient les adresses MAC obtenues en surveillant les adresses source du trafic entrant dans le commutateur. Pour éviter le débordement de cette table et libérer de l'espace pour de nouvelles adresses MAC, une adresse est supprimée si aucun trafic n'est reçu pendant une période donnée. Ce délai correspond au délai d'expiration.

Pour définir le délai d'expiration des adresses MAC dynamiques :

ÉTAPE 1 Cliquez sur **MAC Address Tables** > **Dynamic Address Settings**.

ÉTAPE 2 Saisissez la valeur dans le champ **Aging Time**. Le délai d'expiration est une valeur comprise entre la valeur configurée par l'utilisateur et deux fois cette valeur moins 1. Par exemple, si vous avez saisi 300 secondes, le délai d'expiration sera compris entre 300 et 599 secondes.

ÉTAPE 3 Cliquez sur **Apply**. Le délai d'expiration est défini et la configuration de fonctionnement est mise à jour.

Interrogation de la table des adresses MAC dynamiques

Utilisez la page des adresses dynamiques pour interroger la table des adresses MAC dynamiques selon les critères suivants :

- ID de VLAN
- Interface
- Adresse MAC

Cette page présente les adresses MAC dynamiquement apprises. Vous pouvez effacer les adresses dynamiques de la table et spécifier des critères d'interrogation afin d'afficher un sous-ensemble de la table, comme les adresses MAC apprises via une interface spécifique. Vous pouvez également spécifier le mode de tri des résultats de l'interrogation. Si aucun critère de filtre n'est spécifié, la table entière s'affiche.

Pour interroger la table des adresses dynamiques :

ÉTAPE 1 Cliquez sur **MAC Address Tables** > **Dynamic Address**.

ÉTAPE 2 Saisissez les critères d'interrogation :

- **VLAN ID equals to** : cochez l'option et indiquez l'ID du VLAN pour lequel vous interrogez la table.
- **MAC Address equals to** : cochez l'option et indiquez l'adresse MAC pour laquelle vous interrogez la table.
- **Interface equals to** : cochez l'option et sélectionnez l'interface pour laquelle vous interrogez la table. Il peut s'agir d'un port ou d'un LAG spécifique.

ÉTAPE 3 Cliquez sur **Go**. Les résultats de l'interrogation de la table des adresses dynamiques s'affichent.

ÉTAPE 4 Le cas échéant, sélectionnez la clé de tri de la table dans le menu déroulant **Dynamic Address Table Sort Key** et cliquez sur **Go**. Les adresses de la table peuvent être triées par ID de VLAN, adresse MAC ou interface.

ÉTAPE 5 Cliquez sur **Clear Table** pour supprimer toutes les adresses MAC dynamiques.

Configuration des 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.

Utilisez la page des adresses MAC réservées pour définir les adresses MAC à réserver et les actions de traitement de la trame.

Pour réserver une adresse MAC :

ÉTAPE 1 Cliquez sur **MAC Address Tables** > **Reserved MAC Address**.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **MAC Address** : sélectionnez l'adresse MAC à réserver.
- **Action** : sélectionnez l'une des actions suivantes qui sera appliquée au paquet entrant correspondant aux critères sélectionnés.
  - *Bridge* : réacheminez le paquet vers tous les membres du VLAN.
  - *Discard* : supprime le paquet.
  - *Peer* : ignore ou traite le paquet en fonction du protocole.

ÉTAPE 4 Cliquez sur **Apply**. L'adresse MAC est réservée et la configuration de fonctionnement est mise à jour.

14

Réacheminement multidestination

Ce chapitre décrit la fonction de réacheminement multidestination. Il aborde les sujets suivants :

- **Réacheminement multidestination**
- **Configuration des propriétés multidestination**
- **Configuration d'adresses IP de groupe de multidestination**
- **Configuration d'IGMP Snooping**
- **Configuration de MLD Snooping**
- **Recherche d'adresses IP de groupes multidestination IGMP/MLD**
- **Configuration des ports des routeurs multidestination**
- **Configuration de la multidestination Forward All (Tout réacheminer)**
- **Configuration du nombre maximal de groupes IGMP et MLD**
- **Configuration du filtrage multidestination**

Réacheminement multidestination

Le réacheminement multidestination permet la transmission d'informations en mode 1-à-n. Les applications multidestination sont particulièrement utiles pour transmettre des informations à plusieurs clients lorsque ces clients n'ont pas besoin de l'intégralité du contenu. Ceci est par exemple le cas dans le cadre d'un service de TV par câble, où les clients peuvent rejoindre et quitter une chaîne au cours de la transmission d'un programme.

Les données sont uniquement envoyées aux ports pertinents. Le fait de ne réacheminer les données que vers les ports pertinents permet d'économiser de la bande passante et des ressources d'hôte sur les liaisons.

Pour que le réacheminement multidestination fonctionne sur des sous-réseaux IP, les nœuds et les routeurs doivent être compatibles avec la multidestination. Un nœud compatible avec la multidestination doit pouvoir :

- envoyer et recevoir des paquets multidestination ;
- enregistrer les adresses multidestination qu'il écoute auprès des routeurs locaux afin que les routeurs locaux et distants puissent acheminer les paquets vers les nœuds.

Configuration de multidestination type

Tandis que les routeurs multidestination acheminent les paquets d'un sous-réseau IP à un autre, les commutateurs couche 2 multidestination réacheminent les paquets aux nœuds enregistrés d'un LAN ou d'un VLAN.

La configuration type inclut un routeur qui transfère les flux multidestination entre des réseaux IP privés et/ou publics, un périphérique doté de fonctions de traçage (Snooping) IGMP (Internet Group Membership Protocol, protocole d'adhésion aux groupes Internet) ou MLD (Multicast Listener Discovery, détection des services d'écoute multidestination) et un client qui souhaite recevoir un flux multidestination. Dans cette configuration, le routeur envoie des requêtes IGMP à intervalle régulier.

REMARQUE MLD pour IPv6 est dérivé d'IGMP v2 pour IPv4. Même si cette section décrit principalement IGMP, elle décrit également l'utilisation de MLD lorsque ce protocole est requis. Ces requêtes se présentent sur le commutateur, qui les transmet au VLAN et reconnaît également le port où réside un routeur multidestination (Mrouter). Lorsqu'un hôte reçoit le message de requête IGMP, il répond en envoyant un message d'adhésion IGMP indiquant qu'il souhaite recevoir un flux multidestination spécifique en provenance, le cas échéant, d'un port spécifique. Le commutateur avec fonction de traçage IGMP Snooping analyse les messages d'adhésion et apprend que le flux multidestination demandé par l'hôte doit être réacheminé vers ce port spécifique. Il transfère alors les messages d'adhésion IGMP, uniquement vers le routeur Mrouter. De même, lorsque le routeur Mrouter reçoit un message d'adhésion IGMP, il apprend que l'interface de laquelle il a reçu ce message souhaite recevoir un flux multidestination spécifique. Le routeur Mrouter transfère le flux multidestination demandé à l'interface.

Dans un service multidestination couche 2, un commutateur couche 2 reçoit une seule trame, adressée à une adresse multidestination 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 multidestination, il la transfère à tous les ports qui se sont enregistrés pour recevoir le flux multidestination en question à l'aide de messages d'adhésion IGMP.

Le commutateur transfère les flux multidestination selon l'adresse MAC des groupes multidestination. Cela peut être configuré par VLAN.

Le commutateur gère des listes de groupes multidestination pour chaque VLAN, ce qui permet de gérer les informations multidestination que chaque port doit recevoir. Les groupes multidestination 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.

L'enregistrement multidestination est le processus qui consiste à écouter les protocoles d'enregistrement multidestination et à y répondre. Les protocoles disponibles sont IGMP pour IPv4 et MLD pour IPv6. Lorsque le traçage IGMP/MLD Snooping est activé sur un périphérique d'un VLAN, il analyse les paquets IGMP/MLD que le périphérique reçoit du VLAN et de tous les routeurs multidestination du réseau.

Lorsqu'un périphérique apprend qu'un hôte demande de recevoir un flux multidestination à l'aide de messages IGMP/MLD, éventuellement à partir d'une source spécifique, ce périphérique ajoute cet hôte à sa base MFDB (Multicast Forwarding Data Base, base de données de réacheminement multidestination).

Le traçage IGMP/MLD Snooping peut considérablement réduire le trafic multidestination en provenance d'applications IP grosses consommatrices de bande passante de flux. Un périphérique qui utilise le traçage IGMP/MLD Snooping transfère le trafic multidestination uniquement aux hôtes intéressés par ce trafic. Cette réduction du trafic multidestination diminue la charge de traitement des paquets sur le périphérique et réduit la charge de travail des hôtes puisqu'ils n'ont pas besoin de recevoir tout le trafic multidestination généré sur le réseau et de le filtrer.

Les versions suivantes sont prises en charge :

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

Un émetteur de requêtes IGMP est nécessaire pour gérer le protocole IGMP sur un sous-réseau particulier. En général, un routeur multidestination est également un émetteur de requêtes IGMP. Lorsqu'un sous-réseau inclut plusieurs émetteurs de requêtes IGMP, ces émetteurs élisent l'un des leurs comme 'requérant' principal.

Vous pouvez configurer le commutateur en tant qu'émetteur de requêtes IGMP de secours lorsqu'il n'existe aucun émetteur de requêtes IGMP standard. Le commutateur 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 si aucun trafic (requêtes) IGMP n'est détecté depuis un routeur multidestination, après que le quart du délai de requête défini s'est écoulé. En présence d'autres émetteurs de requêtes IGMP, le périphérique peut cesser d'envoyer des requêtes (ou non), ceci en fonction des résultats du processus de sélection de l'émetteur de requêtes standard.

Propriétés des adresses multidestination

Les adresses multidestination possèdent les propriétés suivantes :

- Chaque adresse multidestination IPv4 se trouve dans la plage d'adresses 224.0.0.0 à 239.255.255.255.
- L'adresse multidestination IPv6 est FF00:/8.
- Pour mapper une adresse IP de groupe de multidestination sur une adresse multidestination couche 2 :
  - Pour IPv4, le mappage s'effectue en prenant les 23 bits de droite de l'adresse IPv4 et en les ajoutant au préfixe 01:00:5e. Normalement, les neuf bits de gauche de l'adresse IP sont ignorés et toutes les adresses IP qui diffèrent uniquement par ces bits de gauche sont mappées sur la même adresse couche 2 puisque les 23 bits de droite sont identiques. Par exemple, l'adresse 234.129.2.3 est mappée sur l'adresse MAC de groupe de multidestination 01:00:5e:01:02:03. Il est possible de mapper jusqu'à 32 adresses IP de groupe de multidestination sur une même adresse couche 2.
  - Pour IPv6, le processus de mappage utilise les 32 bits de droite de l'adresse multidestination et ajoute le préfixe 33:33. Par exemple, l'adresse multidestination IPv6 FF00:1122:3344 est mappée sur l'adresse multidestination couche 2 : 33:33:11:22:33:44.

Configuration des propriétés multidestination

Utilisez la page des propriétés pour activer globalement le traçage IGMP Snooping et/ou le traçage MLD Snooping IPv6 sur le commutateur et définir l'action par défaut pour le trafic multidestination inconnu. Par défaut, toutes les trames multidestination sont envoyées à tous les ports du VLAN.

Pour configurer les propriétés multidestination :

ÉTAPE 1 Cliquez sur **Multicast** > **Properties**.

ÉTAPE 2 Saisissez les informations suivantes :

- **IGMP Snooping** : activez ou désactivez globalement le traçage IGMP Snooping sur le commutateur (le traçage est activé par défaut). Lorsque vous activez le traçage IGMP Snooping, les périphériques qui surveillent le flux réseau déterminent quels hôtes ont demandé de recevoir le trafic multidestination et le commutateur exécute uniquement le traçage IGMP Snooping.
- **MLD Snooping** : activez ou désactivez globalement le traçage MLD Snooping sur le commutateur (le traçage est désactivé par défaut).
- **Unknown Multicast Action** : choisissez la manière de traiter les trames multidestination inconnues. Les options possibles sont les suivantes :
  - *Drop* : ignore les trames multidestination inconnues.
  - *Flood* : transmet les trames multidestination inconnues.
  - *Forward to Router Port* : transmet les trames multidestination inconnues au port Mrouter.

ÉTAPE 3 Cliquez sur **Apply**. Les propriétés multidestination sont définies et la configuration de fonctionnement est mise à jour.

Configuration d'adresses IP de groupe de multidestination

Utilisez la page des adresses IP de groupe de multidestination pour rechercher et ajouter des adresses IP de groupe de multidestination.

Pour définir et afficher des adresses IP de groupe de multidestination :

ÉTAPE 1 Cliquez sur **Multicast** > **IP Multicast Group Address**.

ÉTAPE 2 Saisissez les critères d'interrogation :

- **VLAN ID equals to** : définissez le VLAN du groupe à afficher.
- **IP Version equals to** : sélectionnez **Version 4** ou **Version 6**.
- **IP Multicast Group Address equals to** : définissez l'adresse IP du groupe de multidestination à afficher.

ÉTAPE 3 Cliquez sur **Go**. Les adresses IP de groupe de multidestination qui correspondent aux critères s'affichent.

ÉTAPE 4 Pour ajouter une adresse IP statique de groupe de multidestination, cliquez sur **Add**.

ÉTAPE 5 Saisissez les informations suivantes :

- **VLAN ID** : sélectionnez le VLAN du groupe à ajouter.
- **IP Version** : sélectionnez **Version 4** ou **Version 6**.
- **IP Multicast Group Address** : saisissez l'adresse IP du nouveau groupe de multidestination.

ÉTAPE 6 Pour chaque port, sélectionnez le type d'association. Les options sont les suivantes :

- **Static** : rattache le port au groupe de multidestination en tant que membre statique.
- **None** : indique que le port n'est actuellement pas membre de ce groupe de multidestination sur ce VLAN.

ÉTAPE 7 Cliquez sur **Apply**. L'adresse IP du groupe de multidestination est ajoutée et la configuration de fonctionnement est mise à jour.

Configuration d'IGMP Snooping

Pour prendre en charge le réacheminement multidestination sélectif (IPv4), le traçage IGMP Snooping doit être activé globalement et pour chaque VLAN concerné.

Par défaut, le commutateur transfère les trames multidestination à tous les ports du VLAN concerné, traitant en fait les trames comme dans le cadre d'une diffusion (Broadcast). Avec le traçage IGMP Snooping, le commutateur transfère les trames multidestination aux ports des clients enregistrés dans le groupe de multidestination.

REMARQUE Le commutateur prend en charge le traçage IGMP Snooping sur les VLAN statiques et dynamiques.

Lorsque vous activez le traçage IGMP Snooping, globalement ou sur un VLAN, tous les paquets IGMP sont réacheminés vers le CPU. Le CPU analyse les paquets entrants et détermine ce qui suit :

- les ports qui demandent à rejoindre tel ou tel groupe de multidestination sur un VLAN spécifique ;
- les ports connectés aux routeurs multidestination (Mrouters) qui génèrent des requêtes IGMP ;
- les ports qui reçoivent les protocoles de requête PIM, OSFP, DVMRP ou IGMP.

Les ports demandant à rejoindre un groupe de multidestination spécifique envoient un rapport IGMP qui spécifie le groupe que l'hôte concerné souhaite rejoindre. Cela entraîne la création d'une entrée de réacheminement dans la base de données de réacheminement multidestination.

L'émetteur de requêtes IGMP Snooping permet de prendre en charge un domaine multidestination couche 2 de commutateurs de traçage, en l'absence d'un routeur multidestination. Par exemple, lorsqu'un serveur local fournit un contenu multidestination et que le routeur (s'il en existe un) de ce réseau ne prend pas en charge la multidestination.

Il ne doit exister qu'un seul émetteur de requêtes IGMP dans chaque domaine multidestination couche 2. Le commutateur prend en charge l'élection de l'émetteur de requêtes IGMP selon des normes lorsqu'il existe plusieurs émetteurs de requêtes IGMP dans le domaine.

Pour configurer les paramètres IGMP Snooping et activer le traçage IGMP Snooping sur un VLAN :

ÉTAPE 1 Cliquez sur **Multicast** > **IGMP Snooping**.

ÉTAPE 2 Saisissez les informations suivantes :

- **IGMP Snooping Version** : sélectionnez IGMPv2 ou IGMPv3.
- **Report Suppression** : activez ou désactivez la suppression de rapports IGMP. Lorsque cette option est désactivée, tous les rapports IGMP sont transmis aux routeurs multidestination.

  REMARQUE La suppression de rapports IGMP est uniquement possible lorsque la requête multidestination comporte des rapports IGMPv1 et IGMPv2. Elle n'est pas possible lorsque la requête comporte des rapports IGMPv3.

  Le commutateur utilise la suppression de rapports IGMP pour transmettre uniquement un rapport IGMP par requête de routeur multidestination aux périphériques. Lorsque la suppression de rapports IGMP est activée, le commutateur envoie le premier rapport IGMP provenant des hôtes d'un groupe à tous les routeurs multidestination. Il n'envoie pas les rapports IGMP restants aux routeurs multidestination. Cela évite que des rapports en double soient envoyés aux périphériques.

  Le commutateur transmet toujours uniquement le premier rapport IGMPv1 ou IGMPv2 des hôtes d'un groupe à tous les routeurs multidestination, même si les requêtes émises par les routeurs multidestination comportent des demandes de rapports IGMPv3.

ÉTAPE 3 Sélectionnez un VLAN et cliquez sur **Edit**.

ÉTAPE 4 Saisissez les informations suivantes :

- **VLAN ID** : sélectionnez l'ID du VLAN sur lequel le traçage IGMP Snooping est défini.
- **IGMP Snooping Status** : activez ou désactivez la surveillance du trafic réseau pour déterminer les hôtes qui ont demandé à recevoir le trafic multidestination.
- **MRouter Ports Auto Learn** : activez ou désactivez l'apprentissage automatique des ports auxquels le routeur multidestination (Mrouter) est connecté.
- **Query Robustness** : saisissez la valeur de la variable de robustesse à utiliser si ce commutateur est élu en tant qu'émetteur de requêtes.

- **Query Interval** : saisissez l'intervalle à appliquer entre deux requêtes générales si ce commutateur est élu en tant qu'émetteur de requêtes.
- **Query Max Response Interval** : saisissez la durée utilisée pour calculer le code de réponse maximal inséré dans les requêtes générales périodiques.
- **Last Member Query Counter** : 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, si ce commutateur a été élu en tant qu'émetteur de requêtes.
- **Last Member Query Interval** : 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 élu.
- **Immediate Leave** : activez la sortie immédiate pour réduire la durée nécessaire au blocage d'un flux multidestination envoyé à un port membre lorsque ce dernier reçoit un message de sortie d'un groupe IGMP.
- **IGMP Querier Status** : activez ou désactivez l'émetteur de requêtes IGMP.

  Il ne doit exister qu'un seul émetteur de requêtes IGMP par réseau. Le commutateur prend en charge l'élection de l'émetteur de requêtes IGMP selon des normes. Certaines des valeurs des paramètres de fonctionnement de cette table sont envoyées par l'émetteur de requêtes élu. Les autres valeurs sont dérivées du commutateur.
- **IGMP Querier Version** : sélectionnez la version IGMP utilisée si le commutateur devient l'émetteur de requêtes élu. Sélectionnez IGMPv3 s'il existe des commutateurs et/ou des routeurs multidestination dans le VLAN qui réalise le réacheminement multidestination IP propre à la source.

ÉTAPE 5 Cliquez sur **Apply.** Les paramètres du traçage IGMP Snooping sont définis et la configuration de fonctionnement est mise à jour.

Configuration de MLD Snooping

Pour prendre en charge le réacheminement multidestination sélectif (IPv6), le traçage MLD Snooping doit être activé globalement et pour chaque VLAN concerné. Le commutateur prend en charge le traçage MLD Snooping sur les VLAN statiques et dynamiques.

Les hôtes emploient le protocole MLD pour signaler leur participation aux sessions multidestination tandis que le commutateur utilise le traçage MLD Snooping pour générer des listes de membres multidestination. Ces listes servent à transmettre les paquets multidestination uniquement aux ports du commutateur où existent des nœuds hôtes membres de groupes multidestination. Le commutateur ne prend pas en charge l'émetteur de requêtes MLD.

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 selon les adresses de multidestination IPv6.
- Le MLDv2 Snooping utilise les paquets de contrôle MLDv2 pour réacheminer le trafic uniquement en fonction de l'adresse multidestination IPv6. Il prend en charge la capacité à résoudre les paquets de contrôle MLDv2.

La version MLD réelle est sélectionnée par le routeur multidestination sur le réseau.

De même qu'avec le traçage IGMP Snooping, les trames MLD font l'objet d'un traçage lorsqu'elles sont réacheminées par le commutateur des stations de travail vers un routeur multidestination en amont et inversement. Un commutateur peut ainsi déterminer :

- les ports sur lesquels il existe des stations de travail intéressées par l'adhésion à un groupe de multidestination particulier ;
- les ports sur lesquels résident les routeurs multidestination qui envoient des trames multidestination.

Ces informations servent à exclure les ports non pertinents (ceux sur lesquels aucune station de travail n'est enregistrée pour recevoir un groupe de multidestination spécifique) du réacheminement d'une trame multidestination entrante.

Si vous activez le traçage MLD Snooping en plus des groupes multidestination configurés manuellement, une union entre les membres des groupes et des ports multidestination, dérivés de la configuration manuelle et de la détection dynamique par traçage MLD Snooping, est créée. Toutefois, seules les définitions statiques sont conservées si vous redémarrez le commutateur.

Pour activer le traçage MLD Snooping :

ÉTAPE 1 Cliquez sur **Multicast** > **MLD Snooping**.

ÉTAPE 2 Saisissez les informations suivantes :

- **MLD Snooping Version** : sélectionnez MLDv1 ou MLDv2.
- **Report Suppression** : activez ou désactivez la suppression de rapports MLD Snooping. Lorsque cette option est désactivée, tous les rapports MLDv1 sont transmis aux routeurs multidestination.

ÉTAPE 3 Cliquez sur **Apply**.

ÉTAPE 4 Sélectionnez un VLAN et cliquez sur **Edit**.

ÉTAPE 5 Saisissez les informations suivantes :

- **ID VLAN** : sélectionnez l'ID du VLAN.
- **MLD Snooping Status** : activez ou désactivez le traçage MLD Snooping sur le VLAN. Le commutateur surveille le trafic réseau pour déterminer les hôtes qui ont demandé à recevoir du trafic multidestination. Le commutateur effectue le traçage MLD Snooping uniquement lorsque celui-ci est activé globalement et sur le VLAN.
- **MRouter Ports Auto Learn** : activez ou désactivez l'apprentissage automatique pour le routeur multidestination.
- **Query Robustness** : 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 élu.
- **Query Interval** : saisissez la valeur d'intervalle de requête que le commutateur doit appliquer s'il ne peut pas dériver cette valeur des messages envoyés par l'émetteur de requêtes élu.
- **Query Max Response Interval** : saisissez le délai maximal de réponse aux requêtes à appliquer si le commutateur ne peut pas lire cette valeur dans les requêtes générales envoyées par l'émetteur de requêtes élu.
- **Last Member Query Counter** : 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 élu.
- **Last Member Query Interval** : 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 élu.

- **Immediate Leave** : activez cette option pour réduire la durée nécessaire au blocage du trafic MLD inutile envoyé à un port du commutateur.

ÉTAPE 6 Cliquez sur **Apply.** La configuration de fonctionnement est mise à jour.

Recherche d'adresses IP de groupes multidestination IGMP/MLD

La page relative aux adresses IP des groupes multidestination IGMP/MLD affiche les adresses IPv4 et IPv6 des groupes que le commutateur a appris à partir des messages IGMP/MLD qu'il trace (Snooping).

Pour rechercher l'adresse IP d'un groupe de multidestination :

ÉTAPE 1 Cliquez sur **Multicast** > **IGMP/MLD IP Multicast Group**.

ÉTAPE 2 Saisissez les critères d'interrogation :

- **VLAN ID equals to** : indiquez l'ID du VLAN à interroger.
- **IP Version equals to** : sélectionnez **Version 4** ou **Version 6**.
- **IP Multicast Group Address equals to** : saisissez l'adresse IP du groupe de multidestination à rechercher.

ÉTAPE 3 Cliquez sur **Go.** Les champs suivants s'affichent pour chaque groupe de multidestination :

- **VLAN ID** : ID du VLAN.
- **IP Multicast Group Address** : adresse IP du groupe de multidestination.
- **Member Ports** : liste des ports vers lesquels le flux multidestination correspondant est réacheminé.
- **Type** : le type du groupe est statique ou dynamique.
- **Life (sec)** : durée de vie du groupe dynamique.

Configuration des ports des routeurs multidestination

Un port de routeur multidestination (Mrouter) est un port qui se connecte à un routeur multidestination. Le commutateur inclut le ou les ports de routeur multidestination (Mrouter) lorsqu'il transfère les flux multidestination et les messages d'enregistrement IGMP/MLD. Cela est indispensable pour que tous les routeurs multidestination puissent, à leur tour, réacheminer les flux multidestination et propager les messages d'enregistrement vers d'autres sous-réseaux.

Utilisez la page relative aux ports de routeurs multidestination pour configurer de manière statique ou voir les ports connectés aux routeurs multidestination, détectés de manière dynamique.

Pour définir des ports de routeur multidestination :

ÉTAPE 1 Cliquez sur **Multicast** > **Multicast Router Port**.

ÉTAPE 2 Saisissez les critères d'interrogation :

- **VLAN ID equals to** : sélectionnez l'ID de VLAN pour les ports de routeur qui sont décrits.
- **IP Version equals to** : sélectionnez **Version 4** ou **Version 6** pour la version prise en charge par le routeur multidestination.
- **Interface Type equals to** : sélectionnez le type de l'interface (port ou LAG).

ÉTAPE 3 Cliquez sur **Go**. Les interfaces répondant aux critères de requête s'affichent.

ÉTAPE 4 Sélectionnez le type d'association de chaque interface. Les options sont les suivantes :

- **Static** : le port est configuré de manière statique en tant que port de routeur multidestination.
- **Dynamic** : le port est configuré de manière dynamique en tant que port de routeur multidestination à l'aide d'une requête MLD/IGMP. Pour activer l'apprentissage dynamique des ports de routeurs multidestination, accédez aux pages **IGMP Snooping** et **MLD Snooping**.
- **Forbidden** : ce port ne doit pas être configuré en tant que port de routeur multidestination, même s'il reçoit des requêtes IGMP ou MLD.
- **None** : le port n'est actuellement pas un port de routeur multidestination.

ÉTAPE 5 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration de la multidestination Forward All (Tout réacheminer)

Utilisez la page Forward All pour configurer les ports ou les LAG devant recevoir des flux multidestination d'un VLAN spécifique.

Vous pouvez configurer un port en mode Forward All (Tout réacheminer) de manière statique si les périphériques qui se connectent à ce port ne prennent pas en charge IGMP ou MLD.

REMARQUE Cette configuration concerne uniquement les ports membres du VLAN sélectionné.

Pour définir la multidestination Forward All (Tout réacheminer) :

ÉTAPE 1 Cliquez sur **Multicast** > **Forward All**.

ÉTAPE 2 Définissez l'ID du VLAN, la version IP et le type du port devant recevoir le trafic multidestination et cliquez sur **Go**.

ÉTAPE 3 Sélectionnez l'interface à définir en mode Forward All (Tout réacheminer) à l'aide des méthodes suivantes :

- **Static** : le port reçoit tous les flux multidestination enregistrés.
- **Forbidden** : le port ne peut recevoir aucun flux multidestination enregistré, même si le traçage IGMP/MLD Snooping a déterminé que ce port doit rejoindre un groupe de multidestination.
- **None** : le port n'est actuellement pas un port Forward All (Tout réacheminer).

ÉTAPE 4 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration du nombre maximal de groupes IGMP et MLD

Utilisez la page permettant de définir le nombre maximal de groupes multidestination autorisés sur chaque interface et l'action à effectuer lorsque la limite est atteinte.

Pour définir le nombre maximal de groupes IGMP et MLD sur une interface :

ÉTAPE 1 Cliquez sur **Multicast** > **Maximum Multicast Groups**.

ÉTAPE 2 Sélectionnez le type d'interface (port ou LAG), puis cliquez sur **Go**.

ÉTAPE 3 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port ou le LAG à définir.
- **IGMP Maximum Multicast Group** : saisissez le nombre maximal de groupes IGMP autorisés sur l'interface.
- **IGMP Exceed Action** : refuse le groupe existant ou le remplace par le nouveau groupe pour lequel le rapport IGMP a été reçu lorsque la limite est atteinte.
- **MLD Maximum Multicast Group** : saisissez le nombre maximal de groupes MLD autorisés sur l'interface.
- **MLD Exceed Action** : refuse le groupe existant ou le remplace par le nouveau groupe pour lequel le rapport IGMP a été reçu lorsque la limite est atteinte.

ÉTAPE 5 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration du filtrage multidestination

Vous pouvez ajouter un profil de filtre multidestination pour autoriser ou refuser l'apprentissage de groupes multidestination par rapport à une plage d'adresses IP de groupes définie. Il ne vous reste plus ensuite qu'à affecter le profil à une interface. Les paramètres du filtre multidestination sont appliqués à l'interface sélectionnée.

Configuration de profils de filtre multidestination

Un profil de filtre multidestination permet d'autoriser ou de refuser l'apprentissage de groupes multidestination par rapport à une plage d'adresses IP de groupes définie.

Pour créer un profil de filtre multidestination :

ÉTAPE 1 Cliquez sur **Multicast** > **Multicast Filtering** > **Profiles**.

ÉTAPE 2 Sélectionnez **Version 4** ou **Version 6** en fonction du trafic multidestination, IPv4 ou IPv6, auquel le profil sera appliqué et cliquez sur **Go**.

ÉTAPE 3 Cliquez sur **Add**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Profile Index** : saisissez le numéro de séquence du profil.
- **IP Version** : sélectionnez **Version** 4 ou **Version 6** en fonction du trafic multidestination, IPv4 ou IPv6, auquel appliquer le profil de filtre.
- **Start Multicast Address** : saisissez l'adresse du groupe de multidestination de début.
- **End Multicast Address** : saisissez l'adresse du groupe de multidestination de fin.
- **Action** : refuse ou autorise les trames multidestination par rapport à une plage d'adresses IP de groupes définie.

ÉTAPE 5 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration des paramètres de filtre d'interface

Pour affecter un profil de filtre multidestination à une interface afin de refuser ou d'autoriser un groupe sur celle-ci par rapport à ce profil de filtre :

ÉTAPE 1 Cliquez sur **Multicast** > **Multicast Filtering** > **Filter Settings**.

ÉTAPE 2 Sélectionnez la version IP et le type d'interface (port ou LAG), puis cliquez sur **Go**.

ÉTAPE 3 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port ou le LAG à définir.
- **Filter** : activez ou désactivez le filtrage du trafic multidestination sur cette interface.
- **Filter Profile Index** : si cette option est activée, sélectionnez le profil du filtre multidestination à appliquer. Les paramètres du filtre multidestination définis dans le profil sont appliqués à l'interface.

ÉTAPE 5 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

15

Configuration 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, soit manuellement soit en faisant du commutateur un client DHCP.

Il contient les sections suivantes :

- **Adressage IP**
- **Gestion et interface IPv4**
- **Interface et gestion IPv6**
- **Configuration du système de noms de domaine**

Adressage IP

Le commutateur dispose d'une adresse IPv4 et d'une interface IPv6 dans le VLAN de gestion. Cette adresse IP et la passerelle par défaut peuvent être configurées manuellement ou par DHCP. Vous pouvez configurer l'adresse IP statique et la passerelle par défaut sur les pages Interface IPv4 et Interface IPv6. 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. Le commutateur n'est accessible à l'adresse IP configurée que via son VLAN de gestion.

Le paramètre d'usine par défaut de la configuration de l'adresse IPv4 est DHCPv4. Cela signifie que le commutateur joue le rôle de client DHCPv4 et envoie une demande DHCPv4 lors de l'amorçage.

Si le commutateur reçoit une réponse DHCPv4 du serveur DHCPv4 (contenant une adresse IPv4), il envoie des paquets ARP (Address Resolution Protocol, protocole de résolution d'adresse) pour vérifier que cette adresse IP est unique. Si la réponse ARP indique que l'adresse IPv4 est déjà utilisée, le commutateur envoie le message DHCPDECLINE (Refus DHCP) au serveur DHCP qui a répondu. Il envoie ensuite un nouveau paquet DHCPDISCOVER (Détection DHCP) pour relancer le processus.

Si le commutateur n'a reçu aucune réponse DHCPv4 au bout de 60 secondes, il continue à lancer des requêtes DHCPDISCOVER et utilise l'adresse IPv4 : 192.168.1.254/24.

Des collisions d'adresse IP se produisent lorsqu'une même adresse IP est utilisée par plusieurs périphériques sur un même sous-réseau IP. Les collisions d'adresse nécessitent une action de la part de l'administrateur sur le serveur DHCP et/ou sur le périphérique en conflit avec le commutateur.

Lorsqu'un VLAN est configuré pour utiliser des adresses IPv4 dynamiques, le commutateur envoie des demandes DHCPv4 jusqu'à ce qu'un serveur DHCPv4 lui attribue une adresse IPv4. Vous pouvez configurer le VLAN de gestion uniquement avec une adresse IP statique ou dynamique.

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

- Si le commutateur n'est pas configuré avec une adresse IP statique, il émet des requêtes DHCPv4 jusqu'à ce qu'il reçoive une réponse d'un serveur DHCP.
- La DEL d'état du système située sur le panneau avant du commutateur 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).
- Avec les paramètres d'usine, si aucune adresse IP n'est disponible (qu'elle soit définie de manière statique ou acquise via DHCP), le système utilise l'adresse IP par défaut. Lorsque d'autres adresses IP deviennent disponibles, elles sont automatiquement utilisées. L'adresse IP par défaut se trouve toujours sur le VLAN de gestion.

Pour que vous puissiez accéder au commutateur et le gérer à l'aide de l'interface Web, vous devez définir et connaître l'adresse IP de gestion du commutateur. La configuration par défaut du commutateur utilise l'adresse IP par défaut définie en usine, à savoir : **192.168.1.254**. Vous pouvez configurer manuellement l'adresse IP du commutateur.

Gestion et interface IPv4

Pour que vous puissiez gérer le commutateur à l'aide de l'interface Web, 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 de gestion IPv4 :

ÉTAPE 1 Cliquez sur **Administration** > **Management Interface** > **IPv4 Interface**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Management VLAN** : sélectionnez le VLAN de gestion utilisé pour accéder au commutateur via telnet ou l'interface Web. VLAN1 est le VLAN de gestion par défaut.
- **IP Adresse Type** : sélectionnez l'une des options suivantes :
  - *Dynamic* : détectez l'adresse IP via DHCP sur le VLAN de gestion.
  - *Static* : définissez manuellement une adresse IP statique.

Si vous utilisez une adresse IP statique, renseignez les champs suivants :

- **IP Address** : saisissez l'adresse IP du commutateur. L'adresse par défaut est 192.168.1.254.
- **Mask** : saisissez le masque ou la longueur de préfixe de l'adresse IP.
  - *Network Mask* : sélectionnez et saisissez le masque d'adresse IP.
  - *Prefix Length* : sélectionnez et saisissez la longueur du préfixe d'adresse IPv4.
- **Administrative Default Gateway** : sélectionnez **User Defined** pour saisir manuellement l'adresse IP de la passerelle par défaut. Vous pouvez aussi sélectionner **None** pour supprimer de l'interface l'adresse IP de passerelle par défaut sélectionnée.
- **Operational Default Gateway** : indique l'adresse IP actuelle de la passerelle par défaut.

  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 :

- **DHCP Force Auto Configuration** : cochez l'option **Enable** pour forcer le commutateur à effectuer une configuration automatique qui permettra de renouveler l'adresse IP à partir d'un serveur DHCP. L'adresse IP dynamique du commutateur peut être renouvelée à tout moment après son affectation par le serveur DHCP. Notez que, selon la configuration de votre serveur DHCP, le commutateur peut recevoir une nouvelle adresse IP après le renouvellement, ce qui nécessite le paramétrage de l'interface Web à la nouvelle adresse IP.
- **Auto Configuration via DHCP** : indique si la fonctionnalité DHCP Auto Configuration est activée ou désactivée. Vous pouvez configurer cette fonctionnalité sur la page Administration > File Management > DHCP Auto Configuration.

ÉTAPE 3 Cliquez sur **Apply**. Les paramètres d'interface IPv4 sont définis et la configuration de fonctionnement est mise à jour.

Interface et gestion IPv6

Le commutateur prend en charge une interface IPv6. Outre les adresses de liaison locale et de multidestination par défaut, le commutateur ajoute aussi automatiquement des adresses globales à l'interface sur la base des annonces de routeur qu'il reçoit. 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.

Pour affecter une adresse IPv6 à l'interface IPv6 :

ÉTAPE 1 Cliquez sur **Administration** > **Management Interface** > **IPv6 Interface**.

ÉTAPE 2 Cochez l'option **Enable** en regard du champ **IPv6 Address Auto Configuration** pour que les adresses IPv6 soient automatiquement assignées par le serveur DHCPv6, ou décochez cette option pour désactiver la fonctionnalité.

ÉTAPE 3 Cochez l'option **Enable** en regard du champ **DHCPv6** pour activer le serveur DHCPv6, ou décochez-la pour désactiver la fonctionnalité.

ÉTAPE 4 Si vous désactivez la configuration automatique d'adresses IPv6 et DHCPv6, veuillez renseigner manuellement les champs suivants :

- **IPv6 Address** : saisissez l'adresse IPv6 du commutateur.
- **Prefix_Length** : saisissez la longueur du préfixe IPv6 global du commutateur.
- **IPv6 Gateway** : saisissez l'adresse IPv6 du lien local vers le routeur par défaut.
- **Link Local Address** : affiche l'adresse IPv6 du lien local.
- **IPv6 Address Inuse** : affiche l'adresse IPv6 actuellement utilisée par le commutateur.
- **IPv6 Gateway Inuse** : affiche la passerelle IPv6 actuellement utilisée par le commutateur.

ÉTAPE 5 Pour configurer l'interface en tant que client DHCPv6 de manière qu'elle puisse recevoir des informations du serveur DHCPv6 pour la fonctionnalité de configuration automatique DHCPv6, accédez aux champs **DHCPv6 Client** :

- **Stateless** : cochez l'option **Enable** pour activer l'interface comme client DHCPv6 sans état.
- **Minimum Information Refresh Time** : sélectionnez **Infinite** (no refresh unless the server sends this option) ou **User Defined** pour définir manuellement une valeur. Cette valeur est utilisée pour mettre une limite sur la valeur de l'intervalle d'actualisation. Lorsque le serveur envoie une option d'intervalle d'actualisation inférieure à cette valeur, cette valeur est utilisée en substitution.
- **Information Refresh Time** : sélectionnez **Infinite** (no refresh unless the server sends this option) ou **User Defined** pour définir manuellement une valeur. Cette valeur indique à quelle fréquence le commutateur actualise les informations reçues par le serveur DHCPv6. Si cette option n'est pas reçue du serveur, la valeur entrée ici est utilisée.

ÉTAPE 6 Cliquez sur **Apply.** Les paramètres d'interface IPv6 sont définis et la configuration de fonctionnement est mise à jour.

Configuration du système de noms de domaine

Le DNS (Domain Name System, système de noms de domaine) convertit les noms de domaine en adresses IP en vue de localiser et de gérer des hôtes. En tant que client DNS, le commutateur convertit les noms de domaine en adresses IP via un ou plusieurs serveurs DNS configurés.

Configuration des paramètres DNS généraux

Utilisez la page Paramètres DNS pour activer la fonction DNS, configurer les serveurs DNS et définir le domaine par défaut utilisé par le commutateur.

Pour configurer les paramètres DNS généraux :

ÉTAPE 1 Cliquez sur **IP Configuration** > **Domain Name System** > **DNS Settings**.

ÉTAPE 2 Cochez la case **Enable** en regard du champ **DNS** pour désigner le commutateur comme client DNS et lui permettre de convertir les noms DNS en adresses IP via un ou plusieurs serveurs DNS configurés.

ÉTAPE 3 Si l'option DNS est activée, saisissez le nom de domaine DNS utilisé pour compléter les noms d'hôtes non qualifiés dans le champ **Default Domain Name**. Le commutateur ajoute ces informations à tous les noms de domaine incomplets, afin de les convertir en noms de domaine complets (FQDN).

REMARQUE N'incluez pas le point initial qui sépare un nom incomplet du nom de domaine (comme cisco.com).

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres DNS sont définis et la configuration de fonctionnement est mise à jour.

ÉTAPE 5 Cliquez sur **Details** en regard du champ **DHCP Domain Search List** pour afficher la liste des serveurs DNS configurés sur le commutateur, y compris le serveur DNS statique ajouté par l'utilisateur et tous les serveurs DNS dynamiques reçus des serveurs DHCPv4 et DHCPv6.

ÉTAPE 6 Pour ajouter un serveur DNS, cliquez sur **Add**.

ÉTAPE 7 Saisissez les informations suivantes :

- **IP Version** : sélectionnez **Version 6** ou **Version 4**.
- **DNS Server IP Address** : saisissez l'adresse IP du serveur DNS.

- **Preference** : sélectionnez la valeur de préférence du serveur DNS. Chaque serveur dispose d'une valeur de préférence ; une valeur plus petite signifie une plus grande probabilité d'être utilisée.

ÉTAPE 8 Cliquez sur **Apply.** Le serveur DNS est défini et la configuration de fonctionnement est mise à jour.

Affichage des serveurs DNS statiques et dynamiques

La liste de recherche contient un nom de domaine statique défini par l'utilisateur et des noms de domaine dynamiques reçus des serveurs DHCPv4 et DHCPv6.

Pour afficher les noms de domaine configurés sur le commutateur, cliquez sur **IP Configuration** > **Domain Name System** > **Search List**.

Les champs suivants s'affichent :

- **Source** : source de l'adresse IP du serveur (statique ou DHCPv4 ou DHCPv6) pour ce domaine.
- **Preference** : ordre dans lequel les domaines sont utilisés (du bas vers le haut). Cette option détermine efficacement l'ordre dans lequel les noms incomplets sont complétés au cours des requêtes DNS.
- **Domain Name** : nom de domaine qui peut être utilisé sur le commutateur.

Configuration du mappage d'hôtes

Les mappages des noms d'hôte et des adresses IP sont enregistrés dans la zone Table de mappage d'hôtes (cache DNS).

Ce cache contient les entrées statiques (paires de mappage) ajoutées manuellement au cache.

La résolution des noms commence toujours par une vérification des entrées statiques, puis est suivie de l'envoi de requêtes au serveur DNS externe.

Il est possible de mapper jusqu'à huit adresses IP à un hôte, mais pour l'instant, seul le mappage de la première adresse IP à l'hôte s'applique.

Pour ajouter un mappage d'hôte :

ÉTAPE 1 Cliquez sur **IP Configuration** > **Domain Name System** > **Host Mapping**.

Les champs suivants s'affichent :

- **Host Name** : nom d'hôte défini par l'utilisateur ou nom complet.
- **IP Address** : adresse IP d'hôte.
- **IP Version** : version IP de l'adresse IP de l'hôte.
- **Type** : entrée statique du cache.
- **Status** : affiche les résultats des tentatives d'accès à l'hôte (indique toujours OK pour les entrées statiques).

ÉTAPE 2 Pour ajouter un mappage d'hôtes, cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **IP Version** : sélectionnez **Version 6** ou **Version 4**.
- **Host Name** : saisissez un nom d'hôte défini par l'utilisateur ou un nom complet. Les noms d'hôte sont limités aux lettres ASCII de A à Z (avec distinction majuscules/minuscules), les chiffres de 0 à 9, le caractère souligné et le tiret. Le point (.) est utilisé pour séparer les étiquettes.
- **IP Address (es)** : saisissez une seule adresse ou jusqu'à huit adresses IP associées (IPv4 ou IPv6).

ÉTAPE 4 Cliquez sur **Apply.** Le mappage d'hôte est ajouté et la configuration de fonctionnement est mise à jour.

16

Configuration de la sécurité

Le Commutateur Cisco 220 gère différents types de sécurité, comme les autorisations d'administrer le commutateur, la protection contre les attaques dirigées vers le processeur du commutateur, le contrôle de l'accès des utilisateurs au réseau via le commutateur et la protection contre les autres utilisateurs du réseau (empêche les attaques qui transitent via le commutateur mais qui ne sont pas dirigées vers lui).

Ce chapitre décrit les différents aspects de la sécurité et du contrôle d'accès et il inclut les sujets suivants :

- **Configuration des utilisateurs**
- **Configuration des serveurs TACACS+**
- **Configuration des serveurs RADIUS**
- **Configuration des méthodes d'accès de gestion**
- **Configuration des règles de complexité des mots de passe**
- **Configuration de l'Authentification de l'accès de gestion**
- **Configuration des services TCP/UDP**
- **Configuration du contrôle des tempêtes**
- **Configuration de la sécurité des ports**
- **Configuration de 802.1X**
- **Configuration de la protection contre les DoS**
- **Configuration du DHCP Snooping**
- **Configuration de la protection de la source IP**
- **Configuration de l'inspection ARP dynamique**

Configuration des utilisateurs

Le nom d'utilisateur/mot de passe par défaut est **cisco/cisco**. Lors de votre première ouverture de session avec le nom d'utilisateur et le mot de passe par défaut ou à l'expiration du mot de passe, vous devez saisir un nouveau mot de passe. La complexité des mots de passe est activée par défaut.

Utilisez la page User Accounts pour ajouter des utilisateurs supplémentaires autorisés à gérer le commutateur ou à modifier les mots de passe d'utilisateurs existants.

REMARQUE Vous ne pouvez pas supprimer l'utilisateur par défaut (**cisco**).

Pour ajouter un nouvel utilisateur :

ÉTAPE 1 Cliquez sur **Administration** > **User Accounts**.

Le tableau User Account Table affiche tous les utilisateurs définis sur le commutateur ainsi que leur niveau de privilèges.

ÉTAPE 2 Cliquez sur **Add** pour ajouter un nouvel utilisateur ou sur **Edit** pour en modifier un.

ÉTAPE 3 Saisissez les informations suivantes :

- **User Name** : saisissez un nouveau nom d'utilisateur comportant 32 caractères maximum.
- **Password** : saisissez un mot de passe. Le mot de passe doit être conforme à la stratégie de sécurité et de complexité indiquée sur la page.
- **Confirm Password** : saisissez à nouveau le mot de passe.
- **Password Strength Meter** : affiche le niveau de sécurité du mot de passe. Vous pouvez définir la stratégie de sécurité et de complexité du mot de passe sur la page Password Strength. Pour plus d'informations, reportez-vous à la section **Configuration des règles de complexité des mots de passe**.
- **User Level** : sélectionnez le niveau de privilèges de l'utilisateur.
  - *Read-Only CLI Access (1)* : l'utilisateur peut accéder uniquement à l'interface de ligne de commande (CLI) et il ne peut effectuer que les opérations qui ne modifient pas la configuration du commutateur. L'utilisateur ne peut pas accéder à l'interface Web.
  - *Read/Write Management Access (15)* : l'utilisateur peut accéder à l'interface Web et il peut configurer le commutateur.

ÉTAPE 4 Cliquez sur **Apply**. L'utilisateur est ajouté ou modifié et la configuration de fonctionnement est mise à jour.

Configuration des serveurs TACACS+

Une entreprise peut établir un serveur Système de contrôle d'accès au contrôleur d'accès des terminaux (TACACS+) pour fournir une sécurité centralisée à tous les périphériques. Ainsi, les stratégies d'authentification et d'autorisation peuvent être traitées sur un seul serveur pour tous les périphériques de l'entreprise.

Le commutateur peut servir de client TACACS+ utilisant le serveur TACACS+ pour 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.

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.

Utilisez la page TACACS+ pour configurer les serveurs TACACS+ et définir les paramètres par défaut utilisés pour la communication avec les autres serveurs 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 les paramètres TACACS+ par défaut et ajouter un serveur TACACS+ :

ÉTAPE 1 Cliquez sur **Security** > **TACACS+**.

ÉTAPE 2 Dans la zone **Use Default Parameters**, précisez les paramètres TACACS+ par défaut :

- **Key String** : entrez la chaîne de clé par défaut pour les communications avec tous les serveurs TACACS+ en format crypté ou en texte en clair. Si vous n'entrez pas de chaîne de clé ici, la clé entrée sur la page Add doit correspondre à la clé de cryptage utilisée par le serveur TACACS+. Si vous entrez ici la chaîne de clé par défaut et une chaîne de clé pour un seul serveur TACACS+, la chaîne de clé configurée pour le serveur TACACS+ est prioritaire.

- **Timeout for Reply** : saisissez la durée en secondes qui s'écoule avant l'expiration de la connexion entre le commutateur et le serveur TACACS+. Si aucune valeur n'est indiquée pour un serveur individuel, la valeur de ce champ sera utilisée.

ÉTAPE 3 Cliquez sur **Apply**. Les paramètres TACACS+ par défaut sont définis et la configuration de fonctionnement est mise à jour

ÉTAPE 4 Pour ajouter un serveur TACACS+, cliquez sur **Add**.

ÉTAPE 5 Saisissez les informations suivantes :

- **Server Definition** : indiquez si vous souhaitez spécifier le serveur TACACS+ par son adresse IP ou son nom.
- **IP Version** : indiquez la **version 4** ou la **version 6** si le serveur TACACS+ est identifié par son adresse IP.
- **Server IP Address/Name** : saisissez l'adresse IP ou le nom d'hôte du serveur TACACS+.
- **Priority** : 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.
- **Key String** : une chaîne de clé est utilisée pour crypter les communications à l'aide de MD5. Vous pouvez sélectionner **Use Default** pour utiliser la clé par défaut (définie dans les paramètres TACACS+ par défaut) ou vous pouvez sélectionner **User Defined (Encrypted)** ou **User Defined (Plaintext)** pour entrer la clé en format crypté ou en texte en clair. La clé doit correspondre à la clé de cryptage configurée sur le serveur TACACS+. Si vous ne disposez pas de chaîne de clé cryptée (à partir d'un autre périphérique), saisissez la chaîne de clé en texte en clair et cliquez sur **Apply**. La chaîne de clé cryptée est générée et affichée.
- **Timeout for Reply** : sélectionnez **User Defined** pour entrer le délai qui doit s'écouler avant que la connexion entre le commutateur et le serveur TACACS+ n'expire ou sélectionnez **Use Default** pour utiliser la valeur par défaut.
- **Authentication IP Port** : saisissez le numéro de port via lequel s'opère la session TACACS+. La valeur par défaut est 49.

ÉTAPE 6 Cliquez sur **Apply**. Le serveur TACACS+ est ajouté et la configuration de fonctionnement est mise à jour.

Configuration des serveurs RADIUS

Une société peut établir un serveur RADIUS (Remote Authorization Dial-In User Service, service d'authentification à distance des utilisateurs) pour fournir un contrôle d'accès réseau basé MAC ou 802.1X centralisé à tous ses périphériques. Le commutateur peut agir comme un client RADIUS qui utilise le serveur RADIUS pour fournir des fonctionnalités centralisées de sécurité, d'autorisation et d'authentification utilisateur.

Pour utiliser un serveur RADIUS, ouvrez un compte pour le commutateur sur le serveur RADIUS et configurez ce serveur RADIUS en même temps que les autres paramètres sur la page RADIUS.

REMARQUE Si plusieurs serveurs RADIUS ont été configurés, le commutateur utilise les priorités configurées des serveurs RADIUS disponibles pour sélectionner le serveur RADIUS à utiliser par le commutateur.

Pour définir les paramètres RADIUS par défaut et ajouter un serveur RADIUS :

ÉTAPE 1 Cliquez sur **Security** > **RADIUS**.

ÉTAPE 2 Dans la zone **Use Default Parameters**, entrez les paramètres RADIUS par défaut appliqués à tous les serveurs RADIUS. Si aucune valeur n'est entrée pour un serveur spécifique, le commutateur utilise les valeurs indiquées dans ces champs.

- **Retries** : saisissez le nombre de demandes transmises qui sont envoyées au serveur RADIUS avant que le système considère qu'une défaillance s'est produite.
- **Timeout for Reply** : saisissez le nombre de secondes pendant lesquelles le commutateur attend une réponse du serveur RADIUS avant de relancer la requête ou de passer au serveur suivant.
- **Key String** : la chaîne de clé permet de crypter les communications entre le commutateur et le serveur RADIUS à l'aide de MD5. Saisissez la chaîne de clé par défaut en format crypté ou en texte en clair. Cette clé doit correspondre à la clé configurée sur le serveur RADIUS. Si vous ne possédez pas de chaîne de clé cryptée (à partir d'un autre périphérique), saisissez la chaîne de clé en texte en clair.

ÉTAPE 3 Cliquez sur **Apply**. Les paramètres RADIUS par défaut sont définis et la configuration de fonctionnement est mise à jour.

ÉTAPE 4 Pour ajouter un serveur RADIUS, cliquez sur **Add**.

ÉTAPE 5 Saisissez les informations suivantes :

- **Server Definition** : indiquez si vous souhaitez spécifier le serveur RADIUS par son adresse IP ou son nom.
- **IP Version** : indiquez la **version 4** ou la **version 6** si le serveur RADIUS est identifié par son adresse IP.
- **Server IP Address/Name** : saisissez l'adresse IP ou le nom d'hôte du serveur RADIUS.
- **Priority** : saisissez la priorité du serveur. La priorité détermine l'ordre dans lequel le commutateur essaie de contacter les serveurs pour authentifier les utilisateurs. Le commutateur commence par le serveur ayant la priorité la plus élevée (priorité zéro).
- **Key String** : sélectionnez **User Defined (Encrypted)** ou **User Defined (Plaintext)** pour saisir la chaîne de clé en format crypté ou en texte en clair utilisée pour l'authentification et le cryptage des communications entre le commutateur et le serveur RADIUS. Cette clé doit correspondre à la clé configurée sur le serveur RADIUS. Vous pouvez également sélectionner **Use Default** pour utiliser la chaîne de clé par défaut.
- **Timeout for Reply** : sélectionnez **User Defined** pour entrer 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, ou sélectionnez **Use Default** pour utiliser la valeur par défaut.
- **Authentication IP Port** : saisissez le numéro de port UDP du serveur RADIUS pour les demandes d'authentification.
- **Retries** : sélectionnez **User Defined** pour saisir le nombre de requêtes envoyées au serveur RADIUS avant que le système ne considère qu'une défaillance s'est produite, ou sélectionnez **Use Default** pour utiliser la valeur par défaut.
- **Usage Type** : saisissez le type d'authentification du serveur RADIUS. Les options sont les suivantes :
  - *Login* : 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.
  - *All* : 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 6 Cliquez sur **Apply**. Le serveur RADIUS est ajouté et la configuration de fonctionnement est mise à jour.

Configuration des méthodes d'accès de gestion

L'authentification de l'accès de gestion configure les méthodes d'authentification à utiliser pour authentifier et autoriser les utilisateurs depuis les différentes méthodes d'accès de gestion (voir **Configuration de l'Authentification de l'accès de gestion** pour de plus amples informations). Les profils d'accès de gestion permettent de limiter les accès de gestion depuis certaines sources.

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 fonction de leur priorité dans le profil d'accès (de haut en bas).

Les règles sont composées de filtres qui incluent les éléments suivants :

- **Access Methods** : méthodes permettant l'accès au commutateur et sa gestion :
  - Telnet
  - Secure Telnet (SSH)
  - Hypertext Transfer Protocol (HTTP)
  - Secure HTTP (HTTPS)
  - Simple Network Management Protocol (SNMP)
  - Tous les éléments ci-dessus
- **Action** : permet d'autoriser ou de refuser l'accès à une interface ou à une adresse source.
- **Interface** : les ports, LAG ou VLAN autorisés ou non à accéder à l'interface Web.
- **Source IP Address** : 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 page Access Profiles affiche les profils d'accès définis et permet de sélectionner un profil d'accès en tant que profil actif. Un seul profil d'accès peut être actif sur le commutateur. Toute tentative d'accès à ce dernier doit respecter les règles du profil d'accès actif.

Lorsqu'un utilisateur tente d'accéder au commutateur par le biais d'une méthode d'accès, le commutateur vérifie si le profil d'accès actif autorise explicitement l'accès de gestion au commutateur via cette méthode. Si aucune correspondance n'est trouvée, l'accès est refusé.

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, vous pouvez ajouter des règles ou en modifier sur la page Profiles Rules. Pour plus d'informations, reportez-vous à la section **Configuration des règles de profils**.

Configuration des profils d'accès

Utilisez la page Access Profiles pour créer un profil d'accès et ajouter sa première règle. Si le profil d'accès ne contient qu'une seule règle, vous avez terminé. Pour ajouter des règles supplémentaires au profil, utilisez la page Profile Rules.

Pour ajouter ou sélectionner un autre profil d'accès actif :

ÉTAPE 1 Cliquez sur **Security** > **Management Access Method** > **Access Profiles**.

La page Access Profiles Table 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 **Active Access Profile** et cliquez sur **Apply**. Le profil sélectionné devient alors le profil d'accès actif.

REMARQUE Un message d'avertissement s'affiche si vous avez sélectionné Console Only. Si vous poursuivez, vous serez immédiatement déconnecté de l'interface Web et ne pourrez plus accéder au commutateur que via le port console.

REMARQUE 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'interface Web.

ÉTAPE 3 Pour ajouter un nouveau profil d'accès et une règle, cliquez sur **Add**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Access Profile Name** : saisissez un nom pour votre profil d'accès.
- **Rule Priority** : saisissez la priorité des règles. Lorsque le paquet est mis en correspondance avec une règle, les groupes d'utilisateurs se voient accorder ou refuser l'accès au 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.
- **Management Method** : 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 sont les suivantes :
  - *All* : 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 sont les suivantes :
  - *Permit* : autorise l'accès au commutateur dans la mesure où l'utilisateur correspond aux paramètres du profil.
  - *Deny* : refuse l'accès au commutateur dans la mesure où l'utilisateur correspond aux paramètres du profil.
- **Applies to Interface** : sélectionnez l'interface rattachée à la règle. Les options sont les suivantes :
  - *All* : s'applique à tous les ports, VLAN et LAG.

- *User Defined* : s'applique à l'interface sélectionnée. Vous devez sélectionner un port ou LAG dans le menu déroulant **Interface**.

- **Applies to Source IP Address** : sélectionnez le type d'adresse IP source auquel le profil d'accès s'applique. Les options sont les suivantes :
  - *All* : s'applique à toutes les adresses IP.
  - *User Defined* : s'applique uniquement aux types d'adresses IP définis dans les champs.
- **IP Version** : sélectionnez **Version 4** ou **Version 6** pour définir l'adresse IP source.
- **IP Address** : saisissez l'adresse IP source.
- **Mask** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs suivants :
  - *Network Mask* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Prefix Length* : sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l'adresse IP source.

ÉTAPE 5 Cliquez sur **Apply**. Le profil d'accès est créé et la configuration de fonctionnement est mise à jour.

Configuration des règles de profils

Les profils d'accès peuvent comporter de nombreuses règles afin de déterminer qui est autorisé à gérer le commutateur ainsi qu'à y accéder et les méthodes d'accès pouvant être utilisées.

Chaque règle d'un profil d'accès comporte une action et des critères (un ou plusieurs paramètres) à faire correspondre. Une priorité est affectée à chaque règle. Les règles ayant la priorité la plus basse sont vérifiées en premier. Si le paquet entrant correspond à une règle, l'action associée à cette dernière est appliquée. Si aucune règle correspondante n'est trouvée dans le profil d'accès actif, le paquet est abandonné.

Par exemple, vous pouvez limiter l'accès au commutateur depuis toutes les adresses IP à l'exception de celles qui sont attribuées au centre de gestion informatique. Le commutateur peut ainsi continuer à être géré tout en bénéficiant d'un autre niveau de sécurité.

Pour ajouter des règles à un profil d'accès :

ÉTAPE 1 Cliquez sur **Security** > **Management Access Method** > **Profile Rules**.

ÉTAPE 2 Sélectionnez un profil d'accès et cliquez sur **Go**.

ÉTAPE 3 Pour ajouter une règle au profil d'accès sélectionné, cliquez sur **Add**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Access Profile Name** : sélectionnez un profil d'accès à configurer.
- **Rule Priority** : saisissez la priorité des règles. Lorsque le paquet est mis en correspondance avec une règle, les groupes d'utilisateurs se voient accorder ou refuser l'accès au 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.
- **Management Method** : sélectionnez la méthode de gestion pour laquelle la règle est définie. Les options sont les suivantes :
  - *All* : affecte toutes les méthodes de gestion à la règle.
  - *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 **Permit** 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 **Deny** pour leur interdire l'accès.
- **Applies to Interface** : sélectionnez l'interface rattachée à la règle. Les options sont les suivantes :

- *All* : s'applique à toutes les interfaces.
- *User Defined* : s'applique uniquement à un port ou LAG spécifiques. Vous devez sélectionner un port ou LAG dans le menu déroulant **Interface**.

- **Applies to Source IP Address** : sélectionnez le type d'adresse IP source auquel le profil d'accès s'applique. Les options sont les suivantes :
  - *All* : s'applique à toutes les adresses IP.
  - *User Defined* : s'applique uniquement aux types d'adresses IP définis dans les champs.
- **IP Version** *:* sélectionnez **Version 4** ou **Version 6** pour définir l'adresse IP source.
- **IP Address** *:* saisissez l'adresse IP source.
- **Mask** *:* sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs :
  - *Network Mask :* sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Prefix Length :* sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l'adresse IP source.

ÉTAPE 5 Cliquez sur **Apply**. La règle de profil est ajoutée au profil d'accès et la configuration de fonctionnement est mise à jour.

Configuration des règles de complexité des mots de passe

Les mots de passe sont utilisés pour authentifier les utilisateurs accédant au commutateur. Les mots de passe simples constituent des risques de sécurité potentiels. Par conséquent, les exigences de complexité du mot de passe sont appliquées par défaut et peuvent être configurées si nécessaire.

Utilisez la page Password Strength pour modifier les exigences minimales de complexité de mot de passe et définir le délai d'expiration du mot de passe.

Pour définir les exigences minimales de complexité de mot de passe :

ÉTAPE 1 Cliquez sur **Security** > **Password Strength**.

ÉTAPE 2 Saisissez les paramètres d'expiration du mot de passe :

- **Password Aging** : cochez la case **Enable** pour inviter l'utilisateur à modifier le mot de passe une fois le délai d'expiration du mot de passe atteint.
- **Password Aging Time** : saisissez la durée en jours à l'issue de laquelle le système invite l'utilisateur à changer de mot de passe.

  REMARQUE L'expiration du mot de passe s'applique aussi aux mots de passe de longueur nulle (pas de mot de passe).
- **Password Complexity Settings** : cochez la case **Enable** pour activer les règles de complexité pour les mots de passe. Si la complexité du mot de passe est activée, les mots de passe doivent être conformes aux paramètres par défaut suivants :
  - Être différents du mot de passe actuel.
  - Être différents du nom d'utilisateur actuel.
  - Contenir des caractères appartenant à au moins trois classes de caractères (caractères majuscules, minuscules, numériques et spéciaux disponibles sur un clavier standard).
  - Ne pas contenir de caractère répété plus de trois fois consécutivement.
  - Avoir une longueur minimale de huit caractères.

ÉTAPE 3 Vous pouvez modifier les paramètres par défaut de mot de passe dans les champs suivants :

- **Minimal Password Length** : saisissez le nombre minimum de caractères requis pour les mots de passe.

  REMARQUE Un mot de passe de longueur nulle (pas de mot de passe) est autorisé, et un délai d'expiration du mot de passe peut lui être attribué.
- **Allowed Character Repetition** : saisissez le nombre de fois qu'un caractère peut être répété.
- **Minimal Number of Character Classes** : saisissez le nombre de classes de caractères qui doivent être présentes dans un mot de passe. Les classes de caractères sont minuscules, majuscules, chiffres et symboles ou caractères spéciaux.
- **The New Password Must Be Different than the Current One** : si cette option est sélectionnée, lors de la modification du mot de passe, le nouveau mot de passe ne peut pas être identique au mot de passe actuel.
- **The New Password Must Be Different than the User Name** : si cette option est sélectionnée, lors de la modification du mot de passe, le nouveau mot de passe ne peut pas être identique au nom d'utilisateur actuel.

ÉTAPE 4 Cliquez sur **Apply.** Les paramètres de complexité de mot de passe sont définis et la configuration de fonctionnement est mise à jour.

Configuration de l'Authentification de l'accès de gestion

Vous pouvez attribuer des méthodes d'authentification aux différentes méthodes d'accès de gestion, telles que 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.

Pour que le serveur RADIUS accorde l'accès à l'interface Web, le serveur RADIUS doit renvoyer cisco-avpair = shell:priv-lvl=15.

L'authentification de l'utilisateur s'effectue en fonction de l'ordre de sélection des méthodes d'authentification. Si la première méthode d'authentification n'est pas disponible, la méthode suivante sera utilisée. Par exemple, si les méthodes d'authentification sélectionnées sont RADIUS et Local, et que tous les serveurs RADIUS configurés sont interrogés en vertu de leur ordre de priorité et qu'ils ne répondent pas, l'utilisateur sera authentifié au niveau local.

Si une méthode d'authentification échoue ou si le niveau de privilège d'un utilisateur est insuffisant, ce dernier se voit refuser l'accès au commutateur. En d'autres termes, si l'authentification échoue au niveau d'une méthode d'authentification, le commutateur n'essaie pas d'utiliser la méthode d'authentification suivante et s'arrête.

Pour définir les méthodes d'authentification d'une méthode d'accès :

ÉTAPE 1 Cliquez sur **Security** > **Management Access Authentication**.

ÉTAPE 2 Sélectionnez une méthode d'accès dans le menu déroulant **Application**.

ÉTAPE 3 Déplacez la méthode d'authentification entre la colonne **Optional Methods** et la colonne **Selected Methods**. La première méthode sélectionnée correspond à celle qui sera utilisée en premier. Les méthodes d'authentification applicables sont les suivantes :

- **RADIUS** : l'utilisateur est authentifié sur un serveur RADIUS. Vous devez avoir configuré un ou plusieurs serveurs RADIUS.
- **TACACS+** : l'utilisateur est authentifié sur un serveur TACACS+. Vous devez avoir configuré un ou plusieurs serveurs TACACS+.
- **None** : 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 de nom d'utilisateur et mot de passe sont définies sur la page User Accounts.

REMARQUE La méthode d'authentification **Local** ou **None** doit toujours être sélectionnée en dernier. Toutes les méthodes d'authentification sélectionnées après **Local** ou **None** sont ignorées.

ÉTAPE 4 Cliquez sur **Apply**. Les méthodes d'authentification sélectionnées sont associées à la méthode d'accès et la configuration de fonctionnement est mise à jour.

Configuration des services TCP/UDP

Utilisez la page TCP/UDP Services pour activer ou désactiver les services TCP ou UDP sur le commutateur, généralement pour des raisons de sécurité. Les connexions TCP et UDP actives sont également affichées sur cette page.

Pour configurer les services TCP/UDP :

ÉTAPE 1 Cliquez sur **Security** > **TCP/UDP Services**.

Le tableau **TCP Service Table** affiche les informations suivantes pour toutes les connexions TCP actives :

- **Service Name** : méthode d'adressage utilisée par le commutateur pour fournir le service TCP.
- **Type** : protocole IP utilisé par le service.
- **Local IP Address** : adresse IP locale via laquelle le commutateur propose le service.
- **Local Port** : port TCP local via lequel le commutateur propose le service.
- **Remote IP Address** : adresse IP de l'appareil distant qui demande le service.
- **Remote Port** : port TCP de l'appareil distant qui demande le service.
- **State** : affiche l'état du service. Les valeurs facultatives sont les suivantes :
  - *ESTABLISHED* : le connecteur présente une connexion établie.
  - *SYN_SENT* : le connecteur tente d'établir une connexion.
  - *SYN_RECV* : une demande de connexion a été reçue du réseau.

- *FIN_WAIT1*: le connecteur est fermé et la connexion est en cours de fermeture.
- *FIN_WAIT2*: la connexion est fermée et le connecteur attend la fermeture du point d'extrémité distant.
- *TIME_WAIT*: le connecteur attend la fermeture pour gérer les paquets toujours présents dans le réseau.
- *CLOSED* : le connecteur n'est pas utilisé.
- *CLOSE_WAIT*: le point d'extrémité distant est éteint, en attente de la fermeture du connecteur.
- *LAST_ACK* : le point d'extrémité distant est fermé et le connecteur est fermé. En attente de validation.
- *LISTEN*: le connecteur est à l'écoute des demandes de connexion.
- *CLOSING* : les deux connecteurs sont fermés mais nos données n'ont pas encore toutes été envoyées.
- *UNKNOWN*: l'état du connecteur est inconnu.

Le tableau **UDP Service Table** affiche les informations suivantes pour toutes les connexions UDP actives :

- **Service Name** : méthode d'accès utilisée par le commutateur pour fournir le service UDP.
- **Type** : protocole IP utilisé par le service.
- **Local IP Address** : adresse IP locale via laquelle le commutateur propose le service.
- **Local Port** : port UDP local via lequel le commutateur propose le service.

ÉTAPE 2 Selon les besoins, activez ou désactivez les services TCP/UDP suivants sur le commutateur :

- **HTTP Service** : cochez la case **Enable** pour activer le service HTTP ou décochez-la pour le désactiver. La valeur par défaut est Enabled.
- **HTTPS Service** : cochez la case **Enable** pour activer le service HTTPS ou décochez-la pour le désactiver. La valeur par défaut est Enabled.
- **SNMP Service** : cochez la case **Enable** pour activer le service SNMP ou décochez-la pour le désactiver. Elle est désactivée par défaut.
- **Telnet Service** : cochez la case **Enable** pour activer le service Telnet ou décochez-la pour le désactiver. Elle est désactivée par défaut.

- **SSH Service** : cochez la case **Enable** pour activer le service SSH ou décochez-la pour le désactiver. Elle est désactivée par défaut.

ÉTAPE 3 Cliquez sur **Apply.** Les services sont activés ou désactivés et la configuration de fonctionnement est mise à jour.

Configuration du contrôle des tempêtes

Lorsque des trames de diffusion, de multidestination inconnue ou de destination unique inconnue 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.

Lorsque la fréquence de trames de diffusion, de multidestination inconnue ou de destination unique inconnue est supérieure au seuil défini par l'utilisateur, les trames reçues au-delà du seuil sont supprimées ou l'interface s'arrête.

Pour définir le contrôle des tempêtes :

ÉTAPE 1 Cliquez sur **Security** > **Storm Control**.

ÉTAPE 2 Configurez les paramètres suivants :

- **Frame Configuration** : sélectionnez **Included** (préambule et IFG de 20 octets inclus) pour compter les trames de diffusion, de multidestination inconnue ou de destination unique inconnue, ou sélectionnez **Excluded** (préambule et IFG de 20 octets exclus) pour ne pas les compter.
- **Storm Control Rate Threshold Mode** : sélectionnez le mode du seuil de débit : Paquets par seconde ou kbit/s.

ÉTAPE 3 Cliquez sur **Apply.** Les paramètres de contrôle des tempêtes sont définis et la configuration de fonctionnement est mise à jour.

ÉTAPE 4 Pour modifier les paramètres de contrôle des tempêtes pour un port, sélectionnez le port souhaité et cliquez sur **Edit**.

ÉTAPE 5 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port à définir.
- **Storm Control** : activez ou désactivez le contrôle des tempêtes sur le port.
- **Unknown Unicast** : activez ou désactivez le contrôle des tempêtes pour le trafic de destination unique inconnue. Le trafic de destination unique inconnue sera compté dans le seuil de bande passante.
- **Storm Control Rate Threshold** : saisissez le débit maximum auquel les paquets de destination unique inconnue peuvent être réacheminés. La valeur par défaut de ce seuil est de 10 000.
- **Unknown Multicast** : activez ou désactivez le contrôle des tempêtes pour le trafic de multidestination inconnue. Le trafic de multidestination inconnue sera compté dans le seuil de bande passante.
- **Storm Control Rate Threshold** : saisissez le débit maximum auquel les paquets de multidestination inconnue peuvent être réacheminés. La valeur par défaut de ce seuil est de 10 000.
- **Broadcast** : active ou désactive le contrôle des tempêtes pour le trafic de diffusion. Le trafic de diffusion sera compté dans le seuil de bande passante.
- **Storm Control Rate Threshold** : saisissez le débit maximum auquel les paquets de diffusion peuvent être réacheminés. La valeur par défaut de ce seuil est de 10 000.
- **Action** : sélectionnez l'action à effectuer si le débit des trames de diffusion, de multidestination inconnue ou de destination unique inconnue est supérieur au seuil défini par l'utilisateur. Les options sont les suivantes :
  - *Drop* : supprime les trames reçues au-dessus de ce seuil.
  - *Shutdown* : ferme le port.

ÉTAPE 6 Cliquez sur **Apply**. Les paramètres de contrôle des tempêtes sont modifiés et la configuration de fonctionnement est mise 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 :

- **Classic Lock** : toutes les adresses MAC apprises sur le port sont verrouillées et le commutateur apprend jusqu'au nombre maximum d'adresses autorisées sur le port (défini par l'option Max No. of Addresses Allowed). Les adresses apprises ne sont pas soumises à un délai d'expiration ni à un réapprentissage.
- **Limited Dynamic Lock** : le commutateur apprend des adresses MAC jusqu'à la limite configurée des adresses autorisées. Une fois la limite atteinte, le commutateur n'apprend pas d'adresses supplémentaires. Dans ce mode, les adresses sont soumises à un délai d'expiration ainsi qu'à un réapprentissage.

Lorsqu'une trame ayant une nouvelle adresse MAC est détectée sur un port sur lequel elle n'est pas autorisée (le port est verrouillé de façon classique et la nouvelle adresse MAC de cette trame est apprise sur un autre port verrouillé de façon classique ou bien le port est verrouillé de façon dynamique et le nombre maximal des adresses autorisées a été dépassé), il est fait appel à la fonction de protection et l'une des actions suivantes peut s'appliquer :

- La trame est supprimée.
- La trame est réacheminée.
- La trame est supprimée et un message SYSLOG est généré.
- Le port est fermé.

Lorsque l'adresse MAC sécurisée est détectée sur un autre port, la trame est traitée avec l'action de violation spécifiée et l'adresse MAC n'est pas apprise sur ce port.

Utilisez la page Port Security pour configurer les paramètres de sécurité pour tous les ports et pour activer leur modification.

Pour configurer la sécurité des ports :

ÉTAPE 1 Cliquez sur **Security** > **Port Security**.

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

ÉTAPE 3 Saisissez les informations suivantes :

- **Interface Status** : cochez la case **Lock** pour verrouiller le port.
- **Learning Mode** : sélectionnez le type de verrouillage du port. Ce champ est uniquement activé si le champ Interface Status est verrouillé. Pour modifier le mode d'apprentissage, l'état de l'interface doit être désactivé. Une fois ce mode modifié, vous pouvez rétablir l'état de l'interface. Les options sont les suivantes :
  - *Classic Lock* : verrouille l'interface immédiatement. Mais si le nombre d'adresses déjà apprises dépasse le nombre maximum d'adresses autorisées, toutes les adresses apprises sont supprimées.
  - *Limited Dynamic Lock* : verrouille l'interface en supprimant les adresses MAC dynamiques actuellement associées à l'interface. L'interface apprend au maximum le nombre d'adresses autorisées sur l'interface. Le réapprentissage et le délai d'expiration des adresses MAC sont activés.
- **Max No. of Addresses Allowed** : saisissez le nombre maximum d'adresses MAC pouvant être apprises sur l'interface dans la mesure où le mode d'apprentissage Limited Dynamic Lock est sélectionné. La plage est comprise entre 1 et 256. La valeur par défaut est 1.
- **Action on Violation** : si l'état de l'interface est verrouillé, sélectionnez l'action à appliquer aux paquets qui arrivent sur une interface verrouillée. Les options sont les suivantes :
  - *Discard*: supprime les paquets en provenance d'une source non apprise.
  - *Forward* : réachemine les paquets en provenance d'une source inconnue sans apprendre l'adresse MAC.
  - *Discard and Log* : supprime les paquets en provenance de sources non apprises, ferme l'interface, enregistre les événements dans le journal et envoie des filtres aux destinataires des filtres spécifiés.
  - *Shutdow* : supprime les paquets en provenance de sources non apprises, ferme l'interface, enregistre les événements dans le journal et envoie des filtres aux destinataires des filtres spécifiés. L'interface reste fermée jusqu'à sa réactivation ou jusqu'au redémarrage du commutateur.

- **Trap Frequency** : saisissez la durée minimale qui s'écoulera entre deux filtres. Le commutateur active les filtres lorsqu'un paquet est reçu sur une interface verrouillée. Ceci est approprié pour les violations de verrouillage.

ÉTAPE 4 Cliquez sur **Apply.** La sécurité des ports est modifiée et la configuration de fonctionnement est mise à jour.

Configuration de 802.1X

Le contrôle d'accès basé sur les ports a pour effet de créer deux types d'accès sur les ports du commutateur. Un point d'accès active la communication non contrôlée, ceci indépendamment de l'état d'autorisation (port non contrôlé). Le second point d'accès autorise la communication entre l'hôte et le commutateur.

802.1X est une norme IEEE pour le contrôle d'accès réseau basé sur les ports. Le cadre 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 le demandeur 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.

VLAN invité

Le VLAN invité fournit 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.

Le VLAN invité 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 balisé du VLAN invité lorsque le port n'est pas autorisé et il supprime le port du VLAN invité lorsque le premier demandeur du port est autorisé.
- Le VLAN invité ne peut pas être utilisé en tant que VLAN voix.

Flux de travail de configuration de la fonction 802.1X

Pour configurer la fonction 802.1X, procédez comme suit :

- Activez l'authentification basée sur les ports globalement au niveau du commutateur. Si besoin, activez le VLAN invité et spécifiez le VLAN comme le VLAN invité. Pour plus d'informations, reportez-vous à la section **Configuration des propriétés 802.1X**.
- Configurez l'authentification basée sur les ports 802.1X sur chaque port. Pour plus d'informations, reportez-vous à la section **Configuration de l'authentification des ports 802.1X**.
- Affichez les informations complètes des hôtes authentifiés. Pour plus d'informations, reportez-vous à la section **Affichage des hôtes authentifiés**.

Configuration des propriétés 802.1X

Utilisez la page 802.1X Properties pour activer globalement la fonction 802.1X sur le commutateur. La fonction 802.1X doit être activée à la fois globalement et sur chaque port individuel.

Pour définir l'authentification basée sur les ports :

ÉTAPE 1 Cliquez sur **Security** > **802.1X** > **Properties**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Port-Based Authentication** : cochez la case **Enable** pour activer l'authentification 802.1X basée sur les ports.
- **Guest VLAN** : cochez la case **Enable** pour permettre l'utilisation d'un VLAN invité pour les ports non autorisés. Si la fonction Guest VLAN est activée, tous les ports non autorisés se connectent automatiquement au VLAN sélectionné dans le champ **Guest VLAN ID**. Si un port est par la suite autorisé, il est supprimé du VLAN invité.

- **Guest VLAN ID** : si la fonction Guest VLAN est activée, sélectionnez le VLAN invité dans la liste des VLAN.

ÉTAPE 3 Cliquez sur **Apply.** Les propriétés 802.1X sont modifiées et la configuration de fonctionnement est mise à jour.

Configuration de l'authentification des ports 802.1X

Utilisez la page Port Authentication pour configurer les paramètres 802.1X pour chaque port. Puisque certaines modifications de la configuration ne sont possibles que si le port a l'état Force Authorized (par exemple, l'authentification des hôtes), il est recommandé de changer le contrôle du port en Force Authorized 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 **Security** > **802.1X** > **Port Authentication**.

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

ÉTAPE 3 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port à configurer.
- **User Name** : affiche le nom de l'utilisateur.
- **Administrative Port Control** : sélectionnez l'état d'autorisation du port administratif. Les options sont les suivantes :
  - *Disabled* : n'authentifie pas les utilisateurs.
  - *Force Unauthorized* : refuse l'accès au port en passant ce dernier en mode non autorisé. Le commutateur ne fournit pas de services d'authentification au client via le port.
  - *Auto* : active l'authentification et l'autorisation basées sur les ports sur le commutateur. Le port bascule entre un état autorisé ou non autorisé en fonction de l'échange d'authentification entre le commutateur et le client.
  - *Force Authorized* : autorise le port sans authentification.

- **Guest VLAN** : cochez la case **Enable** pour activer le VLAN invité sur ce port ou décochez cette case pour désactiver le VLAN invité sur ce port. Si le VLAN invité est activé, le port non autorisé rejoint automatiquement le VLAN invité.

  Après un échec d'authentification et si le VLAN invité est activé globalement sur un port donné, le VLAN invité est automatiquement attribué aux ports non autorisés en tant que VLAN non balisé.

- **Periodic Reauthentication** : cochez la case **Enable** pour autoriser les tentatives de réauthentification du port une fois la période de réauthentification spécifiée expirée.

- **Reauthentication Period** : saisissez le délai (en secondes) au bout duquel le port sélectionné est réauthentifié.

- **Authenticator State** : affiche l'état défini de l'autorisation du port. Les options sont les suivantes :

  - *Initialize* : processus de démarrage.
  - *Force-Authorized* : l'état du port contrôlé est défini sur Force-Authorized (le trafic est réacheminé).
  - *Force-Unauthorized* : l'état du port contrôlé est défini sur Force-Unauthorized (le trafic est abandonné).

  REMARQUE Si l'état est du port n'est pas Force-Authorized ou Force-Unauthorized forcée, il est en Auto Mode et l'authentificateur affiche l'état de l'authentification en cours. Une fois le port authentifié, l'état indique Authenticated.

- **Quiet Period** : saisissez le délai (en secondes) pendant lequel le commutateur reste en état silencieux après l'échec d'un échange d'authentification.

- **Max EAP Requests** : saisissez le nombre maximum de demandes EAP pouvant être envoyées. Si aucune réponse n'est reçue après la période définie (délai pour demandeur), le processus d'authentification est relancé.

- **Supplicant Timeout** : saisissez le nombre de secondes qui s'écoulent avant que les demandes EAP soient renvoyées au demandeur.

ÉTAPE 4 Cliquez sur **Apply.** Les paramètres de port sont définis et la configuration de fonctionnement est mise à jour.

Affichage des hôtes authentifiés

La page Authenticated Hosts affiche des informations sur les utilisateurs qui ont 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 connexion de l'utilisateur.

Pour consulter les informations sur les utilisateurs authentifiés, cliquez sur **Security** > **802.1X** > **Authenticated Hosts**.

La page Authenticated Hosts affiche les champs suivants :

- **User Name** : nom des demandeurs authentifiés sur chaque port.
- **Port** : identificateur du port.
- **Session Time (DD:HH:MM:SS)** : durée pendant laquelle le demandeur a été connecté au port.
- **Authentication Method** : affiche la méthode utilisée pour authentifier la dernière session.
- **MAC Address** : affiche l'adresse MAC du demandeur.

Configuration de la protection contre les DoS

Le déni de service (DoS) est une tentative de piratage visant à rendre le périphérique indisponible pour les utilisateurs. Les attaques DoS saturent le périphérique avec des demandes de communication externes, de telle manière que le périphérique ne peut pas répondre au trafic légitime. Ces attaques provoquent souvent la surcharge du processeur du périphérique.

La fonctionnalité de protection DoS est un ensemble de règles prédéfinies qui protègent le réseau contre les attaques malveillantes. Les paramètres de la suite de sécurité DoS permettent d'activer la suite de sécurité.

Secure Core Technology (SCT)

Une méthode pour contrer les dénis de service (DoS) employée par le commutateur est la fonction SCT. La fonction SCT est activée par défaut sur le commutateur et ne peut pas être désactivée.

Le périphérique Cisco est un périphérique avancé qui gère le trafic de gestion, de protocole et de surveillance, outre le trafic de l'utilisateur final (TCP). La fonction SCT garantit que le commutateur reçoit et traite le trafic de gestion et de protocole, quel que soit le volume de trafic reçu. Ceci est possible en limitant le débit du trafic TCP sur le processeur.

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

La fonction SCT peut être contrôlée sur la page Security > Denial of Service > Security Suite Settings (bouton **Details**).

Configuration par défaut

La fonctionnalité de protection DoS est configurée par défaut comme suit :

- La fonction de protection DoS est désactivée par défaut sur tous les ports.
- La fonction de protection DoS est activée par défaut dans la suite de sécurité.
- Les protections SYN-FIN et SYN-RST sont activées par défaut.
- Le mode par défaut de la protection SYN est Block and Report. Le seuil par défaut est 60 paquets SYN par seconde. Le délai de reprise du port par défaut est de 60 secondes.

Configuration des paramètres de la suite de sécurité DoS

Utilisez la page Security Suite Settings pour activer le filtrage du trafic. Vous pouvez ainsi protéger le réseau contre les attaques DoS et DDoS.

REMARQUE Avant d'activer la protection DoS, vous devez supprimer toutes les listes de contrôle d'accès ou 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 DoS est activée sur un port.

Pour configurer les paramètres globaux de protection DoS et contrôler la fonction SCT :

ÉTAPE 1 Cliquez sur **Security** > **Denial of Service** > **Security Suite Settings**.

Le champ **CPU Protection Mechanism** affiche **Enabled**, ce qui indique que le SCT est activé.

ÉTAPE 2 Cliquez sur **Details** en regard du champ **CPU Utilization** pour accéder à la page CPU Utilization et afficher les informations d'utilisation des ressources du processeur.

ÉTAPE 3 Cliquez sur **Edit** en regard de **TCP SYN Protection** pour accéder à la page SYN Protection et activer cette fonctionnalité. Pour plus d'informations, reportez-vous à la section **Configuration de la protection SYN**.

ÉTAPE 4 Dans la zone **Denial of Service Protection**, activez une ou plusieurs des options suivantes de protection DoS et indiquez un seuil si nécessaire :

- DA Equals SA
- ICMP Frag Packets
- ICMP Ping Maximum Length
- IPv6 Minimum Frag Length
- Land
- Null Scan
- POD
- Smurf Netmask
- TCP Source Port Less 1024
- TCP Blat
- TCP Frag-Off Minimum check
- TCP Herder Minimum Length
- UDP Blat
- XMA

ÉTAPE 5 Cliquez sur **Apply**. Les paramètres de la suite de sécurité de protection DoS sont définis et la configuration de fonctionnement est mise à jour.

Configuration des paramètres de l'interface DoS

Utilisez les paramètres d'interface pour activer la protection DoS et la protection ARP gratuite d'IP sur des ports spécifiques. La fonction de protection DoS activée dans la suite de sécurité prend effet sur les ports concernés.

Pour activer la protection DoS et la protection ARP gratuite d'IP sur un port :

ÉTAPE 1 Cliquez sur **Security** > **Denial of Service** > **Interface Settings**.

Le tableau Interface Settings contient les informations suivantes :

- **Interface** : affiche l'ID du port.
- **Denial of Service Protection** : indique si la fonction de protection DoS est activée ou non sur le port.

- **IP Gratuitous ARPs Protection** : indique si la fonction de protection ARP gratuite d'IP est activée ou non sur le port.

ÉTAPE 2 Pour modifier les paramètres DoS pour un port, sélectionnez le port souhaité et cliquez sur **Edit**.

ÉTAPE 3 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port à configurer.
- **Denial of Service Protection** : cochez la case **Enable** pour activer la fonction de protection DoS sur le port, ou décochez-la pour désactiver cette fonction sur le port.
- **IP Gratuitous ARPs Protection** : cochez la case **Enable** pour activer la fonction de protection ARP gratuite d'IP sur le port, ou décochez-la pour désactiver cette fonction sur le port.

ÉTAPE 4 Cliquez sur **Apply**. La protection DoS et la protection ARP gratuite d'IP sont activées ou désactivées sur le port et la configuration de fonctionnement est mise à jour.

Configuration de la protection SYN

Les ports du réseau risquent d'être utilisés par les pirates pour attaquer le commutateur lors d'une attaque SYN, ce qui utilise des ressources TCP (tampons) et de l'énergie du processeur.

Étant donné que le processeur est protégé à l'aide de la fonction SCT, le trafic TCP vers le CPU est limité. Cependant, si un ou plusieurs ports sont attaqués par un grand nombre de paquets SYN, le processeur reçoit uniquement les paquets du pirate, ce qui crée un déni de service (DoS).

Lors de l'utilisation de la fonctionnalité de protection SYN, le processeur compte les paquets SYN entrants par seconde par chaque port de réseau vers le processeur.

Si le nombre est supérieur au nombre spécifique, le seuil défini par l'utilisateur, un SYN de déni avec une règle MAC-to-me est appliqué sur le port. Cette règle est supprimée de l'intervalle défini par l'utilisateur du port (période de protection SYN).

Pour configurer les paramètres de protection SYN :

ÉTAPE 1 Cliquez sur **Security** > **Denial of Service** > **SYN Protection**.

Le tableau SYN Protection Interface contient les informations suivantes :

- **Interface** : affiche l'ID du port.

- **Current State** : indique si la fonction de protection SYN est activée ou non sur le port.
- **Last Attack** : indique l'heure de la dernière attaque d'inondation SYN détectée sur le port.

ÉTAPE 2 Configurez les paramètres globaux de protection SYN :

- **Block SYN-RST Packets** : cochez la case **Enable** pour activer cette fonction. Tous les paquets TCP ayant à la fois des indicateurs SYN et RST sont envoyés sur les ports ayant activé la protection DoS.
- **Block SYN-FIN Packets** : cochez la case **Enable** pour activer cette fonction. Tous les paquets TCP ayant à la fois des indicateurs SYN et FIN sont envoyés sur les ports ayant activé la protection DoS.
- **SYN Protection Mode** : sélectionnez l'un des modes de protection suivants :
  - *Disable* : la fonctionnalité est désactivée sur le port.
  - *Report* : génère un message SYSLOG. L'état du port passe à Attacked lorsque le seuil est dépassé.
  - *Block and Report* : lorsqu'une attaque TCP SYN est identifiée, les paquets TCP SYN destinés au système sont rejetés et l'état du port bascule vers **Blocked**.
- **SYN Protection Threshold** : saisissez le nombre de paquets SYN par seconde avant de bloquer les paquets SYN (un SYN de déni avec une règle MAC-to-me sera appliqué sur le port).
- **SYN Protection Period** : saisissez le délai en secondes avant de débloquer les paquets SYN (le SYN de déni avec la règle MAC-to-me est supprimé du port).

ÉTAPE 3 Cliquez sur **Apply**. Les paramètres globaux de protection SYN sont définis et la configuration de fonctionnement est mise à jour.

Configuration du DHCP Snooping

Le DHCP Snooping permet de sécuriser le réseau en filtrant les messages DHCP non validés et en créant et en maintenant une base de données de liaison de DHCP Snooping (tableau). Le DHCP Snooping agit comme un pare-feu entre les hôtes non validés et les serveurs DHCP. Il différencie les interfaces non validées connectées à l'utilisateur et les interfaces validées connectées au serveur DHCP ou un autre commutateur.

REMARQUE Le DHCP Snooping ne s'applique qu'aux modèles de commutateur avec le pays de destination (-CN).

Configuration des propriétés du DHCP Snooping

Utilisez la page Properties pour activer le DHCP Snooping sur le commutateur et pour en définir les paramètres généraux.

Pour définir les propriétés générales de DHCP Snooping :

ÉTAPE 1 Cliquez sur **Security** > **DHCP Snooping** > **Properties**.

ÉTAPE 2 Saisissez les informations suivantes :

- **DHCP Snooping Status** : cochez la case **Enable** pour activer le DHCP Snooping sur le commutateur ou décochez-la pour désactiver cette fonction. Le DHCP Snooping est désactivé par défaut.
- **Verify MAC Address** : cochez la case **Enable** pour vérifier (sur un port non validé) que l'adresse MAC source de l'en-tête de couche 2 correspond à l'adresse de matériel client telle qu'elle apparaît dans l'en-tête DHCP (partie de la capacité utile). Décochez cette case pour désactiver la fonction. Elle est désactivée par défaut.
- **Option 82 Status** : cochez la case **Enable** pour activer l'insertion globale de l'option 82 sur le commutateur ou décochez-la pour désactiver cette fonction.
- **Remote ID** : si l'option 82 est activée, sélectionnez **User Defined** pour saisir manuellement l'ID distant ou sélectionnez **Use Default** pour utiliser la valeur par défaut.
- **Backup Database Type** : configurez le type d'agent de base de données de secours de DHCP Snooping. Les options sont les suivantes :
  - *None* : désactive l'agent de base de donnée de DHCP Snooping.
  - *Flash* : enregistre la base de données de liaison de DHCP Snooping dans la NVRAM du commutateur.
  - *TFTP* : enregistre la base de données de liaison de DHCP Snooping sur un serveur TFTP.
- **File Name** : lorsque TFTP est sélectionné, entrez le nom du fichier dans lequel les paramètres de DHCP Snooping seront enregistrés sur le serveur TFTP.
- **Server IP Address** : lorsque TFTP est sélectionné, saisissez l'adresse IP ou le nom d'hôte du serveur TFTP distant.

- **Write Delay** : entrez la durée en secondes pendant laquelle le transfert doit être retardé après toute modification de la base de données de liaison de DHCP Snooping. La valeur par défaut est 300 secondes. La plage valide va de 15 à 86400 secondes.
- **Timeout** : entrez la valeur en secondes à laquelle le processus de transfert de base de données doit s'arrêter après la modification de la base de données de liaison de DHCP Snooping. La valeur par défaut est 300 secondes. La plage est comprise entre 0 et 86400. Utilisez la valeur 0 pour une durée infinie.

ÉTAPE 3 Cliquez sur **Apply**. Les propriétés de DHCP Snooping sont définies et la configuration de fonctionnement est mise à jour.

Configuration du DHCP Snooping sur les VLAN

Utilisez la page VLAN Settings pour activer le DHCP Snooping sur les VLAN. Pour activer le DHCP Snooping sur un VLAN, assurez-vous qu'il est activé globalement sur le commutateur.

Pour définir le DHCP Snooping sur les VLAN :

ÉTAPE 1 Cliquez sur **Security** > **DHCP Snooping** > **VLAN Settings**.

ÉTAPE 2 Sélectionnez les VLAN depuis la colonne **Available VLANs** et ajoutez-les à la colonne **Enabled VLANs**.

ÉTAPE 3 Cliquez sur **Apply**. Le DHCP Snooping est activé sur les VLAN sélectionnés et la configuration de fonctionnement est mise à jour.

Configuration des interfaces validées de DHCP Snooping

Utilisez la page Interface Settings pour définir les interfaces validées de DHCP Snooping. Le commutateur transfère toutes les requêtes DHCP aux interfaces validées.

Pour définir des interfaces validées de DHCP Snooping :

ÉTAPE 1 Cliquez sur **Security** > **DHCP Snooping** > **Interface Settings**.

ÉTAPE 2 Sélectionnez le type d'interface (Port ou LAG), puis cliquez sur **Go**.

ÉTAPE 3 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Trusted Interface** : indiquez si l'interface sélectionnée est validée ou non.

  REMARQUE Configurez les ports qui sont connectés à un serveur DHCP ou à d'autres commutateurs ou routeurs en tant que ports validés. Configurez les ports qui sont connectés à des clients DHCP en tant que ports validés.

- **Rate Limit (pps)** : cochez la case **Enable** pour limiter le débit sur l'interface. Si la limite de débit est activée, entrez le débit maximum autorisé sur l'interface.

ÉTAPE 5 Cliquez sur **Apply**. Les propriétés d'interface validée de DHCP Snooping sont définies et la configuration de fonctionnement est mise à jour.

Interrogation de la base de données de liaison de DHCP Snooping

Utilisez la page Binding Database pour interroger la base de données de liaison de DHCP Snooping.

Pour interroger des adresses liées à la base de données de DHCP Snooping :

ÉTAPE 1 Cliquez sur **Security** > **DHCP Snooping** > **Binding Database**.

ÉTAPE 2 Définissez un des champs suivants comme un filtre de requête :

- **VLAN ID** : indique les VLAN enregistrés dans la base de données DHCP. La base de données peut être interrogée par VLAN.
- **MAC Address** : indique les adresses MAC enregistrées dans la base de données DHCP. La base de données peut être interrogée par adresse MAC.
- **IP Address** : indique les adresses IP enregistrées dans la base de données DHCP. La base de données peut être interrogée par adresse IP.
- **Interface** : contient l'interface par laquelle la base de données DHCP peut être interrogée.

ÉTAPE 3 Cliquez sur **Go**. Les options suivantes apparaissent dans le tableau Binding Database :

- **VLAN ID** : l'ID de VLAN auquel l'adresse IP est liée dans la base de données de DHCP Snooping.
- **MAC Address** : adresse MAC trouvée lors de l'interrogation.

- **IP Address** : adresse IP trouvée lors de l'interrogation.
- **Interface** : interface liée à l'adresse trouvée lors de l'interrogation.
- **Type** : type de liaison de l'adresse IP. Ce champ peut prendre les valeurs suivantes :
  - *Static* : indique que l'adresse IP est statique.
  - *Dynamic* : indique que l'adresse IP est définie par une adresse dynamique dans la base de données DHCP.
- **Lease Time** : la durée pendant laquelle l'entrée de DHCP Snooping est active. Les adresses dont la durée de bail est arrivée à expiration sont supprimées de la base de données.

Affichage des statistiques de l'option 82

Pour afficher les statistiques de l'option 82 du DHCP Snooping :

ÉTAPE 1 Cliquez sur **Security** > **DHCP Snooping**> **Statistics**.

ÉTAPE 2 Sélectionnez le type d'interface (Port ou LAG) et cliquez sur **Go**.

Les statistiques suivantes relatives à l'option 82 de DHCP Snooping sont affichées :

- **Interface** : identificateur de port ou LAG.
- **Forward** : nombre total des paquets réacheminés.
- **Chaddr Check Dropped** : nombre total des paquets rejetés par la vérification Chaddr.
- **Untrust Port Dropped** : nombre total des paquets rejetés par les ports non validés.
- **Untrust Port with Option 82 Dropped** : nombre total des paquets rejetés par les ports non validés sur lesquels l'option 82 est activée.
- **Invalid Drop** : nombre total de paquets rejetés car non valides.

ÉTAPE 3 Cliquez sur **Refresh** pour actualiser les données du tableau ou sur **Clear** pour effacer toutes les données du tableau.

Configuration des paramètres d'interface de l'option 82

Utilisez la page Option82 Port Settings pour accepter les paquets DHCP avec des informations de l'option 82 qui sont reçues d'interfaces non validées.

Pour définir l'action à effectuer pour les paquets reçus sur une interface non validée :

ÉTAPE 1 Cliquez sur **Security** > **DHCP Snooping** > **Option82 Port Settings**.

ÉTAPE 2 Sélectionnez le type d'interface (Port ou LAG) et cliquez sur **Go**.

ÉTAPE 3 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port ou LAG à définir.
- **Allow Untrusted** : parmi les actions suivantes, sélectionnez celle qui doit être effectuée lorsque le port non validé reçoit des paquets DHCP :
  - *Drop* : rejette les paquets DHCP avec des informations de l'option 82.
  - *Keep* : conserve les paquets DHCP avec des informations de l'option 82.
  - *Replace* : remplace les paquets DHCP avec des informations de l'option 82.

ÉTAPE 5 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration des paramètres CID de port de l'option 82

Utilisez la page Option82 Port CID Settings pour configurer la sous-option d'ID de circuit (CID) de l'option 82.

Pour configurer la sous-option de CID de l'option 82 :

ÉTAPE 1 Cliquez sur **Security** > **DHCP Snooping** > **Option82 Port CID Settings**.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **Interface** : sélectionnez un port ou un LAG.
- **VLAN Status** cochez la case **Enable** pour utiliser l'ID de circuit sur un VLAN spécifique ou décochez-la pour utiliser l'ID de circuit sur tous les VLAN.
- **ID VLAN** : sélectionnez l'ID du VLAN.

- **Circuit ID** : entrez l'ID de circuit qui compte entre 1 et 64 caractères ASCII (pas d'espace). Lorsque la fonction Option 82 est activée, la sous-option d'ID de circuit par défaut est le VLAN de commutateur et l'identifiant du port, au format vlan-mod-port.

ÉTAPE 4 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration de la protection de la source IP

La protection de la source IP restreint le trafic IP client aux adresses IP sources configurées dans la base de données de liaison de source IP. Par exemple, la protection de source IP peut aider à la prévention des attaques de trafic lorsqu'un hôte essaie d'utiliser l'adresse IP de son voisin.

REMARQUE La protection de source IP ne s'applique qu'aux modèles de commutateur avec le pays de destination (-CN).

Configuration des paramètres d'interface de la protection de la source IP

Utilisez la page Interface Settings pour activer la protection de source IP sur les interfaces.

Pour activer la protection de source IP sur une interface :

ÉTAPE 1 Cliquez sur **Security** > **IP Source Guard** > **Interface Settings**.

ÉTAPE 2 Sélectionnez le type d'interface (Port ou LAG) et cliquez sur **Go**.

ÉTAPE 3 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Interface** : sélectionnez un port ou LAG.
- **IP Source Guard** : cochez la case **Enable** pour activer la protection de source IP sur l'interface ou décochez-la pour désactiver cette option.
- **Verify Source** : sélectionnez le type de trafic source à valider. Il peut être IP uniquement ou MAC et IP.
- **Maximum Entry** : saisissez le nombre maximum de règles de liaison source IP. La plage est comprise entre 0 et 50, où 0 signifie aucune limite.

ÉTAPE 5 Cliquez sur **Apply.** Les paramètres d'interface de protection de source IP sont définis et la configuration de fonctionnement est mise à jour.

Interrogation de la base de données de liaison de source IP

Utilisez la page Binding Database pour interroger et afficher des informations sur les adresses inactives enregistrées dans la base de données de protection de source IP.

Pour interroger la base de données de protection de source IP et/ou définir une règle de liaison de source IP :

ÉTAPE 1 Cliquez sur **Security** > **IP Source Guard** > **Binding Database.**

ÉTAPE 2 Définissez le filtre souhaité pour faire des recherches dans la base de données de protection de source IP :

- **VLAN ID** : interroge la base de données par ID VLAN.
- **MAC Address** : interroge la base de données par adresse MAC.
- **IP Address** : interroge la base de données par adresse IP.
- **Interface** : interroge la base de données par numéro d'interface.

ÉTAPE 3 Cliquez sur **Go.** Les options suivantes apparaissent dans le tableau Binding Database :

- **VLAN ID** : VLAN avec lequel l'adresse IP est associée.
- **MAC Address** : adresse MAC de l'interface.
- **IP Address** : adresse IP de l'interface.
- **Interface** : numéro d'interface.
- **Type** : type d'adresse IP. Ce champ peut prendre les valeurs suivantes :
  - *Dynamic* : indique que l'adresse IP est apprise dynamiquement.
  - *Static* : indique que l'adresse IP est statique.
- **Lease Time** : la durée pendant laquelle l'adresse IP est active. Les adresses IP dont la durée de bail est arrivée à expiration sont supprimées de la base de données.

ÉTAPE 4 Cliquez sur **Add** pour ajouter une règle de liaison de source IP.

ÉTAPE 5 Saisissez les informations suivantes :

- **Interface** : sélectionnez une interface.
- **VLAN ID** : sélectionnez un VLAN avec lequel l'adresse est associée.
- **MAC Address** : entrez l'adresse MAC du trafic source.
- **IP Address** : entrez l'adresse IP du trafic source.

ÉTAPE 6 Cliquez sur **Apply.** La règle de liaison de source IP est définie et la configuration de fonctionnement est mise à jour.

Configuration de l'inspection ARP dynamique

Le protocole Dynamic Address Resolution Protocol (ARP) est un protocole TCP/IP de traduction des adresses IP en adresses MAC.

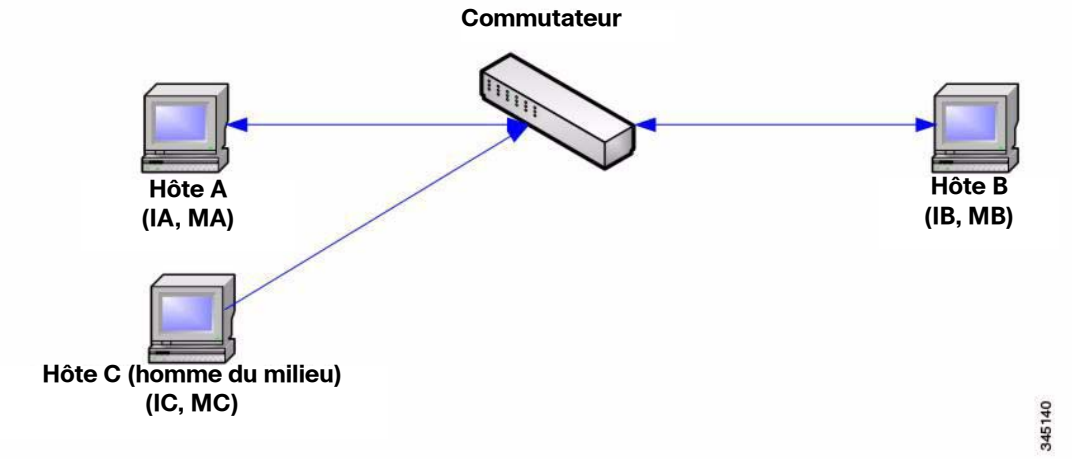
REMARQUE L'inspection ARP dynamique ne s'applique qu'aux modèles de commutateur avec le pays de destination (-CN).

Empoisonnement de cache ARP

Un utilisateur malveillant peut attaquer les hôtes, les commutateurs et les routeurs connectés à un réseau en mode de couche 2 en empoisonnant les caches ARP des systèmes connectés au sous-réseau et en interceptant le trafic destiné aux autres hôtes du sous-réseau. Cette situation s'avère possible parce qu'ARP permet une réponse gratuite à partir d'un hôte, même si aucune requête ARP n'a été reçue. Après l'attaque, tout le trafic issu du périphérique attaqué se dirige vers l'ordinateur de la personne malveillante, puis vers le routeur, le commutateur ou l'hôte.

Vous trouverez ci-dessous un exemple d'empoisonnement de cache ARP :

Figure 1 Empoisonnement de cache ARP



Les hôtes A, B et C sont connectés à un commutateur sur les interfaces A, B et C, toutes se trouvant sur le même sous-réseau. Leurs adresses IP et MAC sont indiquées entre parenthèses ; par exemple, l'hôte A utilise l'adresse IP IA et l'adresse MAC MA. Lorsque l'hôte A a besoin de communiquer avec l'hôte B au niveau de la couche IP, il diffuse une requête ARP relative à l'adresse MAC associée à l'adresse IP IB. L'hôte B répond ensuite à l'aide d'une réponse ARP. Le commutateur et l'hôte A mettent à jour leur cache ARP avec les adresses MAC et IP de l'hôte B.

L'hôte C peut empoisonner les caches ARP du commutateur, de l'hôte A et de l'hôte B en diffusant des réponses ARP falsifiées avec des liaisons vers un hôte possédant une adresse IP égale à IA (ou IB) et une adresse MAC égale à MC. Les hôtes dont les caches ARP ont été empoisonnés utilisent alors l'adresse MAC MC en tant qu'adresse MAC de destination pour le trafic destiné à IA ou IB, permettant ainsi à l'hôte C d'intercepter ce trafic. L'hôte C connaissant les véritables adresses MAC associées à IA et IB, il peut réacheminer le trafic intercepté vers ces hôtes en utilisant l'adresse MAC correcte en guise de destination. L'hôte C s'est par conséquent inséré dans le flux de trafic situé entre l'hôte A et l'hôte B, exécutant ainsi une attaque classique dite de l'homme du milieu.

Comment ARP peut empêcher l'empoisonnement de cache

La fonction d'inspection ARP s'applique aux interfaces validées ou non (reportez-vous à la page Security > ARP Inspection > Interface Settings).

Les interfaces sont classées par l'utilisateur comme suit :

- **Trusted** : les paquets ne sont pas inspectés.
- **Untrusted** : les paquets sont inspectés comme décrit ci-dessus.

L'inspection ARP est effectuée uniquement sur les interfaces non validées. Les paquets ARP qui sont reçus sur une interface validée sont simplement réacheminés.

La logique suivante est appliquée lors de l'arrivée de paquets sur des interfaces non validées :

- Le système recherche les règles de contrôle d'accès ARP relatives aux adresses IP/MAC du paquet. Si l'adresse IP est trouvée et si l'adresse MAC figurant dans la liste correspond à l'adresse MAC du paquet, alors le paquet est valide.
- Si l'adresse IP du paquet est introuvable et si le DHCP Snooping est activé pour le VLAN du paquet, le système recherche la paire <VLAN - adresse IP> du paquet dans la base de données de liaison de DHCP Snooping. Si la paire <VLAN - adresse IP> a été trouvée et si l'adresse MAC ainsi que l'interface dans la base de données correspondent à l'adresse MAC et à l'interface d'entrée du paquet, alors le paquet est valide.
- Si l'adresse IP du paquet est introuvable dans les règles de contrôle d'accès ARP ou dans la base de données de liaison de DHCP Snooping, le paquet n'est pas valide et il est supprimé. Un message SYSLOG est alors généré.
- Lorsqu'un paquet est valide, il est réacheminé et le cache ARP est mis à jour.

Si l'option ARP Packet Validation est sélectionnée (sur la page Properties), les vérifications de validation supplémentaires suivantes sont effectuées :

- **Source MAC Address** : compare l'adresse MAC source du paquet figurant dans l'en-tête Ethernet à l'adresse MAC de l'expéditeur présente dans la requête ARP. Cette vérification est effectuée à la fois sur les requêtes et les réponses ARP.
- **Destination MAC Address** : compare l'adresse MAC de destination du paquet figurant dans l'en-tête Ethernet à l'adresse MAC de l'interface de destination. Cette vérification est effectuée sur les réponses ARP.
- **IP Address** : recherche les adresses IP non valides et inattendues dans le corps ARP. Ces adresses incluent 0.0.0.0, 255.255.255.255 ainsi que toutes les adresses de multidestination IP.

Les paquets contenant des liaisons d'inspection ARP non valides sont enregistrés dans le journal et supprimés.

Interaction entre l'inspection ARP et le DHCP Snooping

Si le DHCP Snooping est activé, l'inspection ARP utilise la base de données de liaison de DHCP Snooping en plus des règles de contrôle d'accès ARP. Si le DHCP Snooping n'est pas activé, seules les règles de contrôle d'accès ARP sont utilisées.

Tableau 1 Valeur ARP par défaut

Option	État par défaut
Inspection ARP dynamique	Désactivé.
Validation de paquet ARP	Désactivé.
Inspection ARP activée sur VLAN	Désactivé.
Intervalle du tampon du journal	La génération d'un message SYSLOG pour les paquets supprimés est activée avec un intervalle de 5 secondes.

Flux de travail de configuration de l'inspection ARP

Pour configurer l'inspection ARP :

ÉTAPE 1 Activez l'inspection ARP et configurez diverses options à la page Security > ARP Inspection > Properties. Pour plus d'informations, reportez-vous à la section **Configuration des propriétés d'inspection ARP**.

ÉTAPE 2 Configurez les interfaces en tant qu'interfaces ARP validées ou non à la page Security > ARP Inspection > Interface Settings. Pour plus d'informations, reportez-vous à la section **Configuration des interfaces validées d'inspection ARP**.

ÉTAPE 3 Définissez les VLAN sur lesquels l'inspection ARP est activée sur la page Security > ARP Inspection > VLAN Settings. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres VLAN d'inspection ARP**.

ÉTAPE 4 Affichez les statistiques de l'inspection ARP sur la page Security > ARP Inspection > Statistics. Pour plus d'informations, reportez-vous à la section **Affichage des statistiques d'inspection ARP**.

Configuration des propriétés d'inspection ARP

Utilisez la page Properties pour activer l'inspection ARP dynamique sur le commutateur et pour configurer les paramètres de validation des paquets ARP.

Pour définir les propriétés d'inspection ARP :

ÉTAPE 1 Cliquez sur **Security** > **ARP Inspection** > **Properties**.

ÉTAPE 2 Saisissez les informations suivantes :

- **ARP Inspection Status** : cochez la case **Enable** pour activer l'inspection ARP sur le commutateur ou décochez-la pour désactiver cette fonction. L'inspection ARP est désactivée par défaut.
- **ARP Packet Validation** : définit les propriétés suivantes de validation d'inspection ARP :
  - *Source MAC Address* : cochez la case **Enable** pour valider les adresses MAC source dans les requêtes et les réponses ARP.
  - *Destination MAC Address* : cochez la case **Enable** pour valider les adresses MAC de destination dans les réponses ARP.
  - *IP Address* : cochez la case **Enable** pour valider les adresses IP dans les requêtes et les réponses ARP.
  - *Allow all-zeros IP* : si la validation d'adresse IP est activée, cochez la case **Enable** pour autoriser l'adresse IP 0.0.0.0.

ÉTAPE 3 Cliquez sur **Apply**. Les propriétés d'inspection ARP sont définies et la configuration de fonctionnement est mise à jour.

Configuration des interfaces validées d'inspection ARP

Utilisez la page Interface Settings pour définir les interfaces validées et non validées. Ces paramètres sont indépendants des paramètres d'interface validée définis pour le DHCP Snooping. L'inspection ARP est activée uniquement sur les interfaces non validées.

Pour modifier l'état validé ARP d'une interface :

ÉTAPE 1 Cliquez sur **Security** > **ARP Inspection** > **Interface Settings**.

ÉTAPE 2 Sélectionnez le type d'interface (Port ou LAG), puis cliquez sur **Go**.

ÉTAPE 3 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Interface :** sélectionnez un port ou un LAG sur lequel le mode de validation d'inspection ARP peut être activé.
- **Trusted Interface** : cliquez sur **Yes** pour activer le mode de validation d'inspection ARP sur l'interface, ou cliquez sur **No** pour le désactiver.
  - S'il est activé, le port ou le LAG est une interface validée et l'inspection ARP n'est pas réalisée sur les requêtes ou réponses ARP envoyées vers et depuis l'interface.
  - S'il est désactivé, le port ou le LAG n'est pas une interface validée et l'inspection ARP est réalisée sur les requêtes ou réponses ARP envoyées vers et depuis l'interface. Elle est désactivée par défaut.
- **Rate Limit (pps)** : saisissez la quantité maximale de bande passante autorisée sur l'interface. La plage est comprise entre 1 et 300 pps. La valeur par défaut est 15.

ÉTAPE 5 Cliquez sur **Apply**. Les interfaces validées d'inspection ARP sont définies et la configuration de fonctionnement est mise à jour.

Affichage des statistiques d'inspection ARP

La page Statistics affiche les statistiques de l'inspection ARP.

Pour afficher les statistiques d'inspection ARP :

ÉTAPE 1 Cliquez sur **Security** > **ARP Inspection** > **Statistics**.

Les informations suivantes sont indiquées :

- **VLAN ID** : identifiant du réseau VLAN.
- **Forward** : nombre total de paquets ARP réacheminés par le VLAN.
- **Source MAC Failures** : nombre total de paquets ARP qui comprennent de mauvaises adresses MAC source.
- **Destination MAC Failures** : nombre total de paquets ARP qui comprennent de mauvaises adresses MAC de destination.

- **Source IP Address Valication Failures** : nombre total de paquets ARP qui échouent à la validation d'adresse IP source.
- **Destination IP Address Valication Failures** : nombre total de paquets ARP qui échouent à la validation d'adresse IP de destination.
- **IP-MAC Mismatch Failures** : nombre total de paquets ARP pour lesquels l'adresse IP ne correspond pas à l'adresse MAC.

ÉTAPE 2 Cliquez sur **Refresh** pour actualiser les données du tableau ou sur **Clear** pour effacer toutes les statistiques d'inspection ARP.

Configuration des paramètres VLAN d'inspection ARP

Utilisez la page VLAN Settings pour activer l'inspection ARP sur les VLAN. Dans le tableau Enabled VLAN, les utilisateurs assignent des listes d'inspection ARP statique à des VLAN activés. Lorsqu'un paquet passe par une interface non validée qui est activée pour l'inspection ARP, le commutateur effectue les vérifications suivantes dans l'ordre :

- Détermine si l'adresse IP et l'adresse MAC du paquet existent dans la liste d'inspection ARP statique. Si les adresses correspondent, le paquet passe par l'interface.
- Si le commutateur ne trouve pas d'adresse IP correspondant, mais que le DHCP Snooping est activé sur le VLAN, il recherche une correspondance adresse IP-VLAN dans la base de données de DHCP Snooping. Si l'entrée existe dans la base de données de DHCP Snooping, le paquet passe par l'interface.
- Si l'adresse IP du paquet n'apparaît pas dans la liste d'inspection ARP ni dans la base de données de DHCP Snooping, le commutateur rejette le paquet.

Pour définir l'inspection ARP sur les VLAN :

ÉTAPE 1 Cliquez sur **Security** > **ARP Inspection** > **VLAN Settings**.

ÉTAPE 2 Sélectionnez les VLAN depuis la colonne **Available VLANs** et ajoutez-les à la colonne **Enabled VLANs**.

ÉTAPE 3 Cliquez sur **Apply**. Les paramètres d'inspection ARP sont appliqués sur les VLAN sélectionnés et la configuration de fonctionnement est mise à jour.

17

Contrôle d'accès

La fonction de liste de contrôle d'accès (ACL, Access Control List) fait partie intégrante des fonctions de sécurité. Les définitions ACL permettent, entre autres, de définir les flux de trafic auxquels sont attribués une qualité de service (QoS) spécifique. Pour plus d'informations, reportez-vous au chapitre **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 inclut les rubriques suivantes :

- **Listes de contrôle d'accès**
- **Configuration d'ACL basées sur MAC**
- **Configuration d'ACE basés sur MAC**
- **Configuration d'ACL basées sur IPv4**
- **Configuration d'ACE basés sur IPv4**
- **Configuration d'ACL basées sur IPv6**
- **Configuration d'ACE basés sur IPv6**
- **Configuration 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 constitué de filtres qui distinguent 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 128 ACE par ACL.

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.

REMARQUE 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. Par exemple, si vous ne souhaitez pas supprimer tous les paquets qui ne remplissent pas les conditions dans une ACL, vous devez explicitement ajouter un ACE ayant la priorité la plus basse dans l'ACL autorisant l'ensemble du trafic.

Si IGMP/MLD Snooping est activé sur un port lié à une ACL, ajoutez dans cette dernière des filtres ACE pour réacheminer 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 en même temps.

Il ne peut y avoir qu'une seule ACL par port, à une exception près : il est possible d'associer à la fois une ACL basée sur IPv4 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) (reportez-vous au paragraphe **Configuration des stratégies QoS** de la section **Configuration du mode QoS avancé**).

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 la couche 2 uniquement, comme décrit dans la section **Configuration d'ACL basées sur MAC**.
- **ACL IP** : examine la couche 3 des trames IP, comme décrit dans la section **Configuration d'ACL basées sur IPv4**.
- **ACL IPv6** : examine la couche 3 des trames IPv4, comme décrit dans la section **Configuration 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 **Configuration du mode QoS avancé**).

Création d'un flux de travail d'ACL

Pour créer des ACL et les associer à une interface, procédez comme suit :

ÉTAPE 1 Créez un ou plusieurs des types d'ACL suivants :

- ACL basée sur MAC via les pages MAC-Based ACL et MAC-Based ACE. Pour plus d'informations, reportez-vous aux sections **Configuration d'ACL basées sur MAC** et **Configuration d'ACE basés sur MAC**.
- ACL basée sur IPv4 via la page IPv4-Based ACL et la page IPv4-Based ACE. Pour plus d'informations, reportez-vous aux sections **Configuration d'ACL basées sur IPv4** et **Configuration d'ACE basés sur IPv4**.
- ACL basée sur IPv6 via la page IPv6-Based ACL et la page IPv6-Based ACE. Pour plus d'informations, reportez-vous aux sections **Configuration d'ACL basées sur IPv6** et **Configuration d'ACE basés sur IPv6**.

ÉTAPE 2 Associez l'ACL aux interfaces via la page ACL Binding. Pour plus d'informations, reportez-vous à la section **Configuration d'une 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 un mappage de classe en mode avancé de QoS, mais qu'elle a été associée à une interface, supprimez la liaison avec cette interface via la page ACL Binding. Pour plus d'informations, reportez-vous à la section **Configuration d'une 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 de la stratégie contenant le plan de classe avec l'interface sur la page Policy Binding. Pour plus d'informations, reportez-vous à la section **Configuration des associations de stratégies**.
  - Supprimez de la stratégie la « class-map » contenant l'ACL. Pour plus d'informations, reportez-vous à la section **Configuration des stratégies QoS**.
  - Supprimez la « class-map » contenant l'ACL. Pour plus d'informations, reportez-vous à la section **Configuration d'un mappage de classe**.

Configuration d'ACL basées sur MAC

Les ACL basées sur MAC sont utilisées pour filtrer le trafic basé sur les champs de la couche 2. Ces ACL vérifient toutes les trames à la recherche d'une correspondance.

Vous pouvez définir les ACL basées sur MAC sur la page MAC-Based ACL. Vous pouvez définir les règles sur la page MAC-Based ACE.

Pour définir une ACL basée sur MAC :

ÉTAPE 1 Cliquez sur **Access Control** > **MAC-Based ACL**.

La table MAC-Based ACL Table affiche toutes les ACL basées sur MAC actuellement définies.

ÉTAPE 2 Pour ajouter une nouvelle ACL basée sur MAC, cliquez sur **Add**.

ÉTAPE 3 Saisissez le nom de la nouvelle ACL dans le champ **ACL Name**. Les noms d'ACL respectent la casse.

ÉTAPE 4 Cliquez sur **Apply**. L'ACL basée sur MAC est ajoutée et le fichier de configuration de fonctionnement est mis à jour.

ÉTAPE 5 Cliquez sur **MAC-Based ACE Table**.

La page MAC-Based ACE s'ouvre. Vous pouvez afficher et/ou ajouter des règles à cette ACL basée sur MAC. Pour plus d'informations, reportez-vous à la section **Configuration d'ACE basés sur MAC**.

Configuration d'ACE basés sur MAC

Pour ajouter des règles (ACE) à une ACL basée sur MAC :

ÉTAPE 1 Cliquez sur **Access Control** > **MAC-Based ACE**.

ÉTAPE 2 Sélectionnez une ACL basée sur MAC et cliquez sur **Go**. Tous les ACE basés sur MAC actuellement définis dans l'ACL sont répertoriés.

ÉTAPE 3 Pour ajouter une règle (ACE) pour l'ACL sélectionnée, cliquez sur **Add**.

ÉTAPE 4 Saisissez les informations suivantes :

- **ACL Name** : affiche le nom de l'ACL à laquelle un ACE est ajouté.
- **Priority** : 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 sont les suivantes :
  - *Permit* : transfère les paquets qui répondent aux critères de l'ACE.
  - *Deny* : abandonne les paquets qui répondent aux critères de l'ACE.
  - *Shutdown* : 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 sur la page Port Management > Error Recovery Settings.
- **Destination MAC Address** : sélectionnez **Any** si toutes les adresses de destination sont possibles ou **User Defined** pour entrer une adresse de destination ou une plage d'adresses de destination.
  - *Destination MAC Address Value* : saisissez l'adresse MAC avec laquelle l'adresse MAC de destination sera mise en correspondance et saisissez également, le cas échéant, son masque.
  - *Destination MAC Wildcard Mask* : saisissez le masque pour définir une plage d'adresses MAC. Ce masque est différent de ceux employés à d'autres fins, comme les masques de sous-réseau. Ici, un bit égal à **1** indique d'ignorer la valeur et **0** indique de la masquer. Par exemple, FFFFFF000000 indique que seuls les trois premiers octets de l'adresse MAC de destination seront utilisés.

  REMARQUE Si le masque est 0000 0000 0000 0000 0000 0000 1111 1111 1111 1111 1111 1111 1111 1111, les bits correspondant aux 0 sont utilisés et ceux correspondant aux 1 sont ignorés. Pour écrire le masque, les 1 doivent être transformés en un entier décimal et chaque série de quatre zéros s'écrit sous la forme 0. Dans cet exemple, étant donné que 1111 1111 = FF, le masque serait donc 000000FFFFFF.
- **Source MAC Address** : sélectionnez **Any** si toutes les adresses source sont possibles ou **User Defined** pour entrer une adresse source ou une plage d'adresses source.
  - *Source MAC Address Value* : saisissez l'adresse MAC avec laquelle l'adresse MAC source sera mise en correspondance et saisissez également, le cas échéant, son masque.
  - *Source MAC Wildcard Mask* : saisissez le masque afin de définir une plage d'adresses MAC.
- **VLAN ID** : saisissez l'ID VLAN de la balise VLAN à mettre en correspondance.

- **802.1p** : sélectionnez **Include** pour utiliser 802.1p. et renseignez comme suit les champs suivants :
  - *802.1p Value* : saisissez la valeur 802.1p à ajouter à la balise VPT.
  - *802.1p Mask* : saisissez le masque générique à appliquer à la balise VPT.
- **Ethertype** : saisissez l'Ethertype de trame à mettre en correspondance.

ÉTAPE 5 Cliquez sur **Apply**. L'ACE basé sur MAC est défini et la configuration de fonctionnement est mise à jour.

Configuration d'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)
- Adresses IP source/de destination (y compris les caractères génériques)
- Ports source/de destination pour le trafic TCP/UDP
- Valeurs des balises pour les trames TCP
- Valeur de priorité DSCP/IP
- Type et code ICMP et IGMP

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 **Configuration du mode QoS avancé**).

Vous pouvez définir les ACL basés sur IPv4 sur la page IPv4-Based ACL. Vous pouvez définir les règles sur la page IPv4-Based ACE.

Vous pouvez définir les ACL basés sur IPv6 sur la page IPv6-Based ACL.

Pour définir une ACL basée sur IPv4 :

ÉTAPE 1 Cliquez sur **Access Control** > **IPv4-Based ACL**.

La table IPv4-Based ACL Table affiche toutes les ACL basées sur IPv4 actuellement définies.

ÉTAPE 2 Pour ajouter une nouvelle ACL basée sur IPv4, cliquez sur **Add**.

ÉTAPE 3 Saisissez le nom de la nouvelle ACL dans le champ **ACL Name**. Les noms respectent la casse.

ÉTAPE 4 Cliquez sur **Apply**. L'ACL basée sur IPv4 est définie et la configuration de fonctionnement est mise à jour.

ÉTAPE 5 Cliquez sur **IPv4-Based ACE Table**.

La page IPv4-Based ACE s'ouvre. Vous pouvez afficher et/ou ajouter des règles à cette ACL basée sur IPv4. Pour plus d'informations, reportez-vous à la section **Configuration d'ACE basés sur IPv4**.

Configuration d'ACE basés sur IPv4

Pour ajouter des règles (ACE) à une ACL basée sur IPv4 :

ÉTAPE 1 Cliquez sur **Access Control** > **IPv4-Based ACE**.

ÉTAPE 2 Sélectionnez une ACL et cliquez sur **Go**. Tous les ACE basés sur IPv4 actuellement définis pour l'ACL sélectionnée s'affichent.

ÉTAPE 3 Pour ajouter une règle (ACE) pour l'ACL sélectionnée, cliquez sur **Add**.

ÉTAPE 4 Saisissez les informations suivantes :

- **ACL Name** : affiche le nom de l'ACL.
- **Priority** : permet d'entrer la priorité. Les ACE disposant d'une priorité plus élevée sont traités en premier.
- **Action** : sélectionnez l'action affectée au paquet correspondant à l'ACE. Les options sont les suivantes :
  - *Permit* : transfère les paquets qui répondent aux critères de l'ACE.
  - *Deny* : abandonne les paquets qui répondent aux critères de l'ACE.
  - *Shutdown* : abandonne le paquet qui répond aux critères de l'ACE et désactive le port auquel le paquet était adressé. Vous pouvez réactiver ces ports sur la page Port Management > Error Recovery Settings.

- **Protocol** : crée un ACE basé sur un protocole ou un ID de protocole spécifique.
  - **Any (IP)** : sélectionnez cette option pour accepter tous les protocoles IP.
  - **Select from list** : sélectionnez l'un des protocoles suivants dans le menu déroulant :

    ICMP : Internet Control Message 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

    IPV6 : tunneling IPv6 sur IPv4

    IPV6:ROUT : fait correspondre les paquets appartenant à la route IPv6 sur IPv4 par le biais d'une passerelle.

    IPV6:FRAG : fait correspondre les paquets appartenant à l'en-tête de fragment IPv6 sur IPv4.

    RSVP : ReSerVation Protocol

    IPV6:ICMP : Internet Control Message Protocol

    OSPF : Open Shortest Path First

    PIM : Protocol Independent Multicast

    L2TP : Layer2 Tunneling Protocol
  - **Protocol ID to match** : au lieu de sélectionner le nom, saisissez l'ID du protocole.

- **Source IP Address** : sélectionnez **Any** si toutes les adresses source sont possibles ou **User Defined** pour entrer une adresse source ou une plage d'adresses source.
  - *Source IP Address Value* : saisissez l'adresse IP avec laquelle l'adresse IP source sera mise en correspondance.
  - *Source IP Wildcard Mask* : saisissez le masque pour définir une plage d'adresses IP. Ce masque est différent de ceux employés à d'autres fins, comme les masques de sous-réseau. Ici, un bit égal à **1** indique d'ignorer la valeur et **0** indique de la masquer.
- **Destination IP Address** : sélectionnez **Any**, si toutes les adresses de destination sont acceptables, ou **User Defined** pour entrer une adresse de destination ou une plage d'adresses de destination.
  - *Destination IP Address Value* : entrez l'adresse IP à laquelle l'adresse IP de destination sera associée.
  - *Destination IP Wildcard Mask* : saisissez le masque pour définir une plage d'adresses IP.
- **Source Port** : sélectionnez une des options suivantes :
  - *Any* : correspond à tous les ports source.
  - *Single* : 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 **Select from list**.
  - *Range* : 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.
- **Destination Port** : sélectionnez l'une des valeurs disponibles. (Elles sont identiques à celles du champ **Source Port** décrit ci-dessus.)

REMARQUE Vous devez sélectionner un protocole IP pour l'ACE avant de saisir les ports source et de destination.

- **TCP Flags** : sélectionnez un ou plusieurs indicateurs TCP avec lesquels vous souhaitez 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.
  - *Set* : filtre les paquets pour lesquels l'indicateur est sur SET.
  - *Unset* : filtre les paquets pour lesquels l'indicateur n'est pas sur SET.
  - *Don't care* : ignore l'indicateur TCP.
- **Type of Service** : sélectionnez le type de service des paquets IP. Les options sont les suivantes :
  - *Any* : tout type de service.
  - *DSCP to match* : DSCP (Differentiated Serves Code Point) à faire correspondre.
  - *IP Precedence to match* : la priorité IP est un modèle de TOS (type de service) utilisé par le réseau pour fournir les engagements QoS appropriés. Ce modèle utilise les 3 bits les plus significatifs de l'octet du type de service dans l'en-tête IP, comme décrit dans RFC 791 et RFC 1349.
- **ICMP** : si le protocole IP de l'ACL est ICMP, sélectionnez le type de message ICMP utilisé afin de filtrer. Les options sont les suivantes :
  - *Any (IP)* : tous les types de message sont acceptés.
  - *Select from list* : permet de sélectionner le type de message en fonction de son nom.
  - *ICMP Type to match* : numéro du type de message à utiliser pour filtrer.
- **ICMP Code** : les messages ICMP peuvent disposer d'un champ de code indiquant comment gérer le message. Sélectionnez **Any** pour accepter tous les codes, ou sélectionnez **User Defined** pour entrer un code ICMP afin de filtrer.

ÉTAPE 5 Cliquez sur **Apply**. L'ACE basé sur IPv4 est défini et la configuration de fonctionnement est mise à jour.

Configuration d'ACL basées sur IPv6

Utilisez la page IPv6-Based ACL pour créer des ACL basées sur IPv6 qui contrôlent le trafic purement basé sur IPv6. Les ACL basées sur 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 **Configuration du mode QoS avancé**).

Pour définir une ACL basée sur IPv6 :

ÉTAPE 1 Cliquez sur **Access Control** > **IPv6-Based ACL**.

ÉTAPE 2 Pour ajouter une nouvelle ACL basée sur IPv6, cliquez sur **Add**.

ÉTAPE 3 Saisissez le nom de la nouvelle ACL dans le champ **ACL Name**. Les noms respectent la casse.

ÉTAPE 4 Cliquez sur **Apply**. L'ACL basée sur IPv6 est définie et la configuration de fonctionnement est mise à jour.

ÉTAPE 5 Cliquez sur **IPv6-Based ACE Table**.

La page IPv6-Based ACE s'ouvre. Vous pouvez afficher et/ou ajouter des règles à cette ACL basée sur IPv6. Pour plus d'informations, reportez-vous à la section **Configuration d'ACE basés sur IPv6**.

Configuration d'ACE basés sur IPv6

Pour ajouter des règles (ACE) à une ACL basée sur IPv6 :

ÉTAPE 1 Cliquez sur **Access Control** > **IPv6-Based ACE**.

ÉTAPE 2 Sélectionnez une ACL basée sur IPv6 et cliquez sur **Go**. Tous les ACE basés sur IPv6 actuellement définis pour l'ACL sélectionnée s'affichent.

ÉTAPE 3 Pour ajouter une règle (ACE) pour l'ACL sélectionnée, cliquez sur **Add**.

ÉTAPE 4 Saisissez les informations suivantes :

- **ACL Name** : affiche le nom de l'ACL à laquelle un ACE est ajouté.
- **Priority** : permet d'entrer la priorité. Les ACE disposant d'une priorité plus élevée sont traités en premier.
- **Action** : sélectionnez l'action affectée au paquet correspondant à l'ACE. Les options sont les suivantes :
  - *Permit* : transfère les paquets qui répondent aux critères de l'ACE.
  - *Deny* : abandonne les paquets qui répondent aux critères de l'ACE.
  - *Shutdown* : abandonne les paquets qui répondent aux critères de l'ACE et désactive le port auquel les paquets étaient adressés. Vous pouvez réactiver ces ports sur la page Port Management > Error Recovery Settings.
- **Protocol** : crée cet ACE basé sur un protocole ou un ID de protocole spécifique.
  - **Any (IP)** : sélectionnez cette option pour accepter tous les protocoles IP.
  - **Select from List** : sélectionnez l'un des types de protocole 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).
  - **Protocol ID to match** : saisissez l'ID du protocole avec lequel établir la correspondance.
- **Source IP Address** : sélectionnez **Any** si toutes les adresses source sont possibles ou **User Defined** pour entrer une adresse source ou une plage d'adresses source.
  - *Source IP Address Value* : saisissez l'adresse IP avec laquelle l'adresse IP source sera mise en correspondance et saisissez également, le cas échéant, son masque.
  - *Source IP Prefix Length* : saisissez la longueur du préfixe de l'adresse IP source.

- **Destination IP Address** : sélectionnez **Any**, si toutes les adresses de destination sont acceptables, ou **User Defined** pour entrer une adresse de destination ou une plage d'adresses de destination.
  - *Destination IP Address Value* : saisissez l'adresse IP avec laquelle l'adresse IP de destination sera mise en correspondance et saisissez également, le cas échéant, son masque.
  - *Destination IP Prefix Length* : saisissez la longueur du préfixe de l'adresse IP.
- **Source Port** : sélectionnez une des options suivantes :
  - *Any* : correspond à tous les ports source.
  - *Single* : 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 **Select from list**.
  - *Range* : sélectionnez une plage de ports source TCP/UDP avec lesquels le paquet est mis en correspondance.
- **Destination Port** : sélectionnez l'une des valeurs disponibles. (Elles sont identiques à celles du champ **Source Port** décrit ci-dessus.)

  REMARQUE Vous devez sélectionner un protocole IPv6 pour l'ACE avant de configurer les ports source et de destination.
- **TCP Flags** : 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.
  - *Set* : filtre les paquets pour lesquels l'indicateur est sur SET.
  - *Unset* : filtre les paquets pour lesquels l'indicateur n'est pas sur SET.
  - *Don't care* : ignore l'indicateur TCP.
- **Type of Service** : sélectionnez le type de service des paquets IP. Les options sont les suivantes :
  - *Any* : tout type de service.
  - *DSCP to match* : DSCP (Differentiated Serves Code Point) à faire correspondre.

- *IP Precedence to match* : la priorité IP est un modèle de TOS (type de service) utilisé par le réseau pour fournir les engagements QoS appropriés. Ce modèle utilise les 3 bits les plus significatifs de l'octet du type de service dans l'en-tête IP, comme décrit dans RFC 791 et RFC 1349.

ICMP : si l'ACL est basée sur ICMP, sélectionnez le type de message ICMP à utiliser afin de filtrer. Les options sont les suivantes :

- *Any (IP)* : tous les types de message sont acceptés.
- *Select from list* : permet de sélectionner le type de message en fonction de son nom dans la liste déroulante.
- *ICMP Type to match* : numéro du type de message à utiliser pour filtrer.

- **Code ICMP** : les messages ICMP peuvent disposer d'un champ de code indiquant comment gérer le message. Sélectionnez **Any** pour accepter tous les codes, ou sélectionnez **User Defined** pour entrer un code ICMP afin de filtrer.

ÉTAPE 5 Cliquez sur **Apply**. L'ACE basé sur IPv6 est défini et la configuration de fonctionnement est mise à jour.

Configuration 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 toutes les interfaces auxquelles elle est liée ou sur lesquelles elle est utilisée.

REMARQUE Il est possible de lier une interface à une stratégie ou à une ACL, mais il est impossible de lier les deux.

Pour lier une ACL à une interface :

ÉTAPE 1 Cliquez sur **Access Control** > **ACL Binding**.

ÉTAPE 2 Sélectionnez le type d'interface (Port ou LAG), puis cliquez sur **Go**.

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.
- **MAC ACL** : les ACL basées sur MAC qui sont liées à l'interface (le cas échéant).
- **IPv4 ACL** : les ACL de type IPv4 qui sont liées à l'interface (le cas échéant).
- **IPv6 ACL** : les ACL de type IPv6 qui sont liées à l'interface (le cas échéant).

ÉTAPE 3 Pour supprimer la liaison de toutes les ACL au niveau d'une interface, sélectionnez cette dernière puis cliquez sur **Clear**.

ÉTAPE 4 Pour lier les ACL à une interface, sélectionnez l'interface souhaitée et cliquez sur **Edit**.

ÉTAPE 5 Sélectionnez l'une des options suivantes :

- **Select MAC-Based ACL** : sélectionnez une ACL basée sur MAC à lier à l'interface.
- **Select IPv4-Based ACL** : sélectionnez une ACL basée sur IPv4 à lier à l'interface.
- **Select IPv6-Based ACL** : sélectionnez une ACL basée sur IPv6 à lier à l'interface.

ÉTAPE 6 Cliquez sur **Apply**. Le paramètre de liaison ACL est modifié et la configuration de fonctionnement est mise à jour.

REMARQUE Si aucune ACL n'est sélectionnée, la ou les ACL précédemment liées à l'interface sont supprimées.

18

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 inclut les rubriques suivantes :

- **Fonctions et composants QoS**
- **Flux de travail de configuration des paramètres QoS**
- **Configuration du mode QoS de base**
- **Configuration du mode QoS avancé**

Fonctions et composants QoS

La fonction QoS permet d'optimiser les performances du réseau. Elle classifie le trafic entrant selon des classes de trafic basées sur les attributs suivants :

- Configuration du périphérique
- Interface d'entrée
- Contenu des paquets
- Combinaison de ces attributs

La QoS inclut :

- **Traffic Classification** : permet de marquer chaque paquet entrant comme appartenant à un flux de trafic spécifique, sur la base du contenu de ce paquet et/ou du port. Cette classification est réalisée à l'aide d'une ACL. Seul le trafic répondant aux critères de l'ACL est soumis à la classification CoS (Class of Service) ou QoS.

- **Assignment to Hardware Queues** : affecte les paquets entrants à des files d'attente de réacheminement. Les paquets sont envoyés à une file d'attente particulière pour gestion en tant que fonction de la classe de trafic à laquelle ils appartiennent. Reportez-vous à la section **Configuration de files d'attente de QoS**.
- **Other Traffic Class-Handling Attribute** : applique des mécanismes QoS à diverses classes, y compris la gestion de bande passante.

Le mode QoS sélectionné s'applique à toutes les interfaces du commutateur. Le commutateur prend en charge les modes QoS suivants :

- **Basic Mode** : CoS (Class of 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. Lorsqu'il fonctionne en mode QoS de base, le commutateur considère cette valeur QoS affectée en externe comme validée. La valeur de QoS affectée en externe à un paquet détermine sa classe de trafic et la QoS.

- **Advanced Mode** : QoS (Quality of Service, qualité de service) pour chaque flux.

  En mode QoS avancé, une QoS pour chaque flux est constituée 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 configurée à un flux. La configuration de QoS d'un flux peut regrouper une file d'attente de sortie, la valeur DSCP ou CoS/802.1p et les actions à appliquer au trafic hors profil (excédent).

- **Disable Mode** : tout le trafic est mappé sur une seule file d'attente de type « meilleur effort » et aucun type de trafic n'est prioritaire sur les autres.

REMARQUE Vous ne pouvez activer qu'un seul mode à la fois. Lorsque le commutateur est configuré pour fonctionner en mode QoS avancé, les paramètres du mode QoS de base sont inactifs, et inversement.

Lorsque vous changez de mode QoS, les événements suivants se produisent :

- Lorsque vous passez du mode 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 QoS de base au mode avancé, la configuration du mode QoS validé dans le mode de base n'est pas conservée.
- Lorsque vous désactivez la QoS, les paramètres de mise en forme 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 configuration des paramètres QoS

Pour configurer les paramètres de QoS, procédez comme suit :

ÉTAPE 1 Sélectionnez le mode QoS (de base, avancé ou désactivé) pour le commutateur et affectez à chaque interface une priorité CoS par défaut, comme indiqué dans la section **Configuration des propriétés de QoS**.

ÉTAPE 2 Attribuez la méthode de planification (priorité stricte ou WRR) et la valeur d'affectation de bande passante WRR aux files d'attente de sortie, comme indiqué dans la section **Configuration de files d'attente de QoS**.

ÉTAPE 3 Associez une file d'attente de sortie à chaque priorité CoS/802.1p, comme indiqué dans la section **Mappage de CoS/802.1p vers une file d'attente**. Si le commutateur fonctionne en mode CoS/802.1 validé, tous les paquets entrants sont placés dans les files d'attente de sortie prévues en fonction de la priorité CoS/802.1 des paquets.

ÉTAPE 4 Associez une file d'attente de sortie à chaque priorité IP, comme indiqué dans la section **Mappage de la priorité IP aux files d'attente**.

ÉTAPE 5 Associez une file d'attente de sortie pour chaque valeur IP DSCP/TC sur la page DSCP to Queue, comme indiqué dans la section **Mappage DSCP vers file d'attente**. Si le commutateur fonctionne en mode DSCP validé, les paquets entrants sont placés dans les files d'attente de sortie en fonction de leur valeur DSCP/TC.

ÉTAPE 6 Remarquez la priorité CoS/802.1p, la priorité IP et/ou la valeur DSCP pour le trafic de sortie sur un port. Les priorités CoS/802.1p et IP, ou la priorité CoS/802.1p et la valeur DSCP, peuvent être remarquées simultanément, mais pas la priorité IP et les valeurs DSCP.

- Remarquez la priorité CoS/802.1p pour le trafic de sortie pour chaque file d'attente, comme indiqué dans la section **Mappage des files d'attente vers CoS/802.1p**.
- Remarquez la priorité IP pour le trafic de sortie pour chaque file d'attente, comme indiqué dans la section **Mappage des files d'attente aux priorités IP**.
- Remarquez la valeur DSCP pour le trafic de sortie pour chaque file d'attente, comme indiqué dans la section **Mappage d'une file d'attente à une valeur DSCP**.

ÉTAPE 7 Entrez les limites de bande passante et de débit :

- Définissez la limite de débit d'entrée et le taux de mise en forme en sortie pour chaque port, comme indiqué dans la section **Configuration de la bande passante**.
- Configurez la mise en forme de sortie par file d'attente, comme indiqué dans la section **Configuration de la mise en forme en sortie par file d'attente**.
- Définissez la limite de débit d'entrée du VLAN, comme indiqué dans la section **Configuration de la limite de débit VLAN**.

ÉTAPE 8 Configurez le mode sélectionné en réalisant l'une des opérations suivantes :

- Configurez le mode QoS de base comme indiqué dans la section **Configuration du mode QoS de base**.
- Configurez le mode QoS avancé, comme indiqué dans la section **Configuration du mode QoS avancé**.

ÉTAPE 9 Activez l'algorithme d'évitement des congestions TCP, comme indiqué dans la section **Configuration de l'évitement des congestions TCP**.

Configuration des propriétés de QoS

Utilisez la page QoS Properties pour configurer le mode QoS pour le commutateur et pour définir la priorité CoS par défaut pour chaque interface.

Pour sélectionner le mode QoS et définir la priorité CoS par défaut pour chaque interface :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **QoS Properties**.

ÉTAPE 2 Sélectionnez le mode QoS (de base, avancé ou désactivé) qui sera actif sur le commutateur.

ÉTAPE 3 Cliquez sur **Apply**. Le mode QoS est défini et la configuration de fonctionnement est mise à jour.

ÉTAPE 4 Le tableau **Interface CoS Configuration Table** affiche la valeur de CoS par défaut pour chaque interface. Pour modifier la valeur de CoS par défaut d'une interface, sélectionnez l'interface souhaitée et cliquez sur **Edit**.

ÉTAPE 5 Saisissez les informations suivantes :

- **Interface** : sélectionnez l'interface à configurer.
- **Default CoS** : sélectionnez la valeur de CoS par défaut à affecter aux paquets entrants (qui ne possèdent pas de balise VLAN). Cette plage est comprise entre 0 et 7.

  La valeur de CoS par défaut n'est applicable que si le commutateur est en mode QoS de base et que CoS/802.1p est le mode validé.

ÉTAPE 6 Cliquez sur **Apply**. La valeur de CoS par défaut de l'interface est modifiée et la configuration de fonctionnement est mise à jour.

ÉTAPE 7 Pour restaurer les valeurs de CoS par défaut, cochez les interfaces et cliquez sur **Restore Defaults**.

Configuration de files d'attente de QoS

Le commutateur prend en charge huit files d'attente pour chaque interface. La file d'attente numéro 8 est celle qui dispose de la priorité la plus élevée. La file d'attente numéro 1 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 (SP) et WRR (Weighted Round Robin, technique du tourniquet pondéré).

- **Strict Priority (SP)** : 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 plus faible n'est traité qu'après transmission des files d'attente de priorité supérieure, 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).

Vous pouvez sélectionner les modes de mise en file d'attente sur la page Queue. 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 8 (celle dont la priorité est la plus élevée), puis en passant à la file d'attente de niveau immédiatement inférieur à la fin du traitement de chaque file.

Lorsque la mise en file d'attente est de type WRR (Weighted Round Robin), chaque file d'attente est traitée jusqu'à ce que son quota soit atteint. Le système passe ensuite à une autre file d'attente.

Il est également possible d'affecter une WRR à certaines des files d'attente de priorité plus faible tout en maintenant le traitement de priorité stricte pour des files d'attente de niveau plus élevé. Dans ce cas, le trafic des files d'attente à priorité stricte est toujours envoyé avant celui des files d'attente WRR. Une fois que les files d'attente à priorité stricte sont vides, le trafic des files d'attente WRR est réacheminé. (La portion relative en provenance de chaque file d'attente WRR dépend de sa pondération.)

Pour sélectionner la méthode de priorité et entrer les données WRR :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **Queue**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Queue** : affiche le numéro de la file d'attente.
- **Scheduling Method** : sélectionnez l'une des options suivantes :
  - *Strict Priority* : la planification du trafic de la file d'attente sélectionnée et de toutes les files d'attente supérieures est strictement basée sur la priorité de chaque file d'attente.
  - *WRR* : la planification du trafic de la file d'attente sélectionnée se base sur une WRR. Chaque période est divisée entre les files d'attente WRR qui ne sont pas vides (celles qui ont des descripteurs de sortie). Ceci ne s'applique que lorsque les files d'attente à priorité stricte sont vides.
- **WRR Weight** : si vous choisissez WRR, saisissez la pondération WRR attribuée à la file d'attente.
- **% of WRR Bandwidth** : affiche la quantité de bande passante affectée à la file d'attente. Ces valeurs représentent un pourcentage de la pondération WRR.

ÉTAPE 3 Cliquez sur **Apply**. Les files d'attente sont configurées et la configuration de fonctionnement est mise à jour.

Mappage de CoS/802.1p vers une file d'attente

Utilisez la page CoS/802.1p to Queue pour mapper des priorités 802.1p vers des files d'attente de sortie. La table CoS/802.1p to Queue détermine les files d'attente de sortie des paquets entrants sur la base de la priorité 802.1p figurant dans leurs balises VLAN. Pour les paquets entrants non balisés, la priorité 802.1p utilisée est la priorité CoS/802.1p par défaut affectée aux ports d'entrée.

Valeurs 802.1p (0 à 7, 7 étant la valeur la plus élevée)	File d'attente (8 files d'attente, la numéro 8 ayant la priorité la plus élevée)	Notes
0	2	Arrière-plan
1	1	Meilleur effort (Best effort)

Valeurs 802.1p (0 à 7, 7 étant la valeur la plus élevée)	File d'attente (8 files d'attente, la numéro 8 ayant la priorité la plus élevée)	Notes
2	3	Excellent effort
3	4	Application critique - SIP pour téléphone LVS
4	5	Vidéo
5	6	Voix - Valeur par défaut de téléphone IP Cisco
6	7	Contrôle de l'interfonctionnement - RTP pour téléphone LVS
7	8	Contrôle du réseau

En modifiant le mappage CoS/802.1p to Queue, la méthode de planification des files d'attente ainsi que l'affectation de bande passante, il est possible d'obtenir la qualité de QoS 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 QoS de base et en mode validé CoS/802.1p.
- Le commutateur est en mode QoS avancé et les paquets appartiennent à des flux en mode validé CoS/802.1p.

Pour mapper des valeurs de CoS sur des files d'attente de sortie :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **CoS/802.1p to Queue**.

ÉTAPE 2 Saisissez les informations suivantes :

- **802.1p** : affiche les valeurs de balise de priorité 802.1p à affecter à une file d'attente de sortie, où 0 est la priorité la plus faible et 7 la plus élevée.
- **Output Queue** : sélectionnez la file d'attente de sortie sur laquelle la priorité 802.1p est mappée. Le système prend en charge huit files d'attente de sortie, parmi lesquelles la file d'attente 8 dispose de la priorité la plus élevée et la file d'attente 1 de la priorité la plus faible.

Pour chaque priorité 802.1p, sélectionnez la file d'attente de sortie sur laquelle elle est mappée.

ÉTAPE 3 Cliquez sur **Apply**. Les valeurs de priorité 802.1p vers les files d'attente sont mappées et la configuration de fonctionnement est mise à jour.

ÉTAPE 4 Cliquez sur **Restore Defaults** pour restaurer la configuration par défaut des mappages CoS/802.1p to Queue.

Mappage de la priorité IP aux files d'attente

Pour mapper des priorités IP aux files d'attente de sortie :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **IP Precedence to Queue**.

ÉTAPE 2 Sélectionnez la file d'attente de sortie à laquelle la priorité IP est mappée. Le système prend en charge huit files d'attente de sortie, parmi lesquelles la file d'attente 8 dispose de la priorité la plus élevée et la file d'attente 1 de la priorité la plus faible.

ÉTAPE 3 Cliquez sur **Apply**. Les valeurs de priorité IP vers les files d'attente sont mappées et la configuration de fonctionnement est mise à jour.

ÉTAPE 4 Cliquez sur **Restore Defaults** pour restaurer la configuration par défaut des mappages IP Precedence to Queue.

Mappage DSCP vers file d'attente

Utilisez la page DSCP to Queue pour mapper les valeurs IP DSCP aux files d'attente de sortie. La table DSCP to Queue 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.

Il est possible d'obtenir la QoS souhaitée sur un réseau en modifiant simplement le mappage DSCP vers file d'attente, la méthode de planification de file d'attente et l'affectation de bande passante.

Le mappage DSCP vers file d'attente s'applique aux paquets IP si :

- Le commutateur est en mode QoS de base et DSCP est le mode validé.
- Le commutateur est en mode QoS avancé et les paquets appartiennent à des flux en mode de validation DSCP.

Les paquets non IP sont toujours classés comme appartenant à la file d'attente de meilleur effort.

Pour mapper des valeurs DSCP aux files d'attente :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **DSCP to Queue**.

La colonne **Ingress DSCP** affiche la valeur DSCP dans le paquet entrant et la classe qui lui est associée.

ÉTAPE 2 Sélectionnez la file d'attente de réacheminement de trafic dans le menu déroulant **Output Queue** vers laquelle la valeur DSCP est mappée.

ÉTAPE 3 Cliquez sur **Apply**. Les valeurs DSCP vers les files d'attente sont mappées et la configuration de fonctionnement est mise à jour.

ÉTAPE 4 Cliquez sur **Restore Defaults** pour restaurer la configuration par défaut des mappages DSCP to Queue.

Mappage des files d'attente vers CoS/802.1p

Utilisez la page Queues to CoS/802.1p pour remarquer la priorité CoS/802.1p pour le trafic sortant pour chaque file d'attente.

Pour mapper des files d'attente aux valeurs de CoS :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **Queues to CoS/802.1p**.

ÉTAPE 2 Pour chaque file d'attente de sortie, sélectionnez la priorité CoS/802.1p sur laquelle le trafic sortant de la file d'attente est remarquée.

ÉTAPE 3 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

ÉTAPE 4 Cliquez sur **Restore Defaults** pour restaurer la configuration par défaut des mappages Queue to CoS/802.1p.

Mappage des files d'attente aux priorités IP

Pour mapper une file d'attente de sortie à une priorité IP :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **Queues to IP Precedence**.

ÉTAPE 2 Pour chaque file d'attente de sortie, sélectionnez la priorité IP sur laquelle le trafic sortant de la file d'attente est remarquée.

ÉTAPE 3 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

ÉTAPE 4 Cliquez sur **Restore Defaults** pour restaurer la configuration par défaut des mappages Queue to IP precedence.

Mappage d'une file d'attente à une valeur DSCP

Utilisez la page Queues to DSCP pour remarquer la valeur DSCP pour un trafic sortant pour chaque file d'attente.

Pour mapper des files d'attente aux valeurs DSCP :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **Queues to DSCP**.

ÉTAPE 2 Pour chaque file d'attente de sortie, sélectionnez la valeur DSCP sur laquelle le trafic sortant de la file d'attente est remarqué.

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

ÉTAPE 4 Cliquez sur **Restore Defaults** pour restaurer la configuration par défaut des mappages Queue to DSCP.

Configuration du remarquage d'interface

Utilisez la page Remark Interface Settings pour remarquer la priorité CoS/802.1p, la priorité IP et la valeur DSCP pour le trafic sortant sur un port. La priorité CoS/802.1p et la priorité IP ou la priorité CoS/802.1p et la valeur DSCP peuvent être remarquées simultanément, mais la valeur DSCP et la valeur IP ne peuvent pas être remarquées simultanément.

Pour remarquer le trafic sortant sur une interface :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **Remark Interface Settings**.

ÉTAPE 2 Sélectionnez le type d'interface (Port ou LAG), puis cliquez sur **Go**.

ÉTAPE 3 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port ou LAG à définir.
- **Remark CoS** : cochez la case **Enable** pour remarquer la priorité CoS/802.1p pour le trafic sortant sur ce port ou ce LAG.
- **Remark IP Precedence** : cochez la case **Enable** pour remarquer la priorité IP pour le trafic sortant sur ce port ou ce LAG.
- **Remark DSCP** : cochez la case **Enable** pour remarquer la valeur DSCP pour le trafic sortant sur ce port ou ce LAG.

ÉTAPE 5 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration de la bande passante

Utilisez la page Bandwidth pour définir deux ensembles de valeurs, qui déterminent la quantité de trafic que le commutateur peut recevoir et envoyer.

La limite de débit d'entrée indique le nombre de bits par seconde que l'interface d'entrée peut recevoir. La bande passante dépassant cette limite est éliminée.

Pour indiquer la limite de bande passante :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **Bandwidth**.

ÉTAPE 2 Pour limiter la bande passante sur un port, sélectionnez le port et cliquez sur **Edit**.

ÉTAPE 3 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port à configurer.
- **Ingress Rate Limit** : cochez la case **Enable** pour activer la limite de débit entrant et saisissez le montant maximum de bande passante autorisé sur le port dans le champ **Ingress Rate Limit**.
- **Egress Shaping Rates** : cochez la case **Enable** pour activer la mise en forme en sortie sur le port et entrez la bande passante maximum pour l'interface de sortie dans le champ **Committed Information Rate (CIR)**.

ÉTAPE 4 Cliquez sur **Apply**. Les paramètres de bande passante sont modifiés et la configuration de fonctionnement est mise à jour.

Configuration de la mise en forme en sortie par file d'attente

Outre la limitation de la vitesse de transmission de chaque port, que vous configurez sur la page Bandwidth, le commutateur peut limiter la vitesse de transmission des trames en sortie sélectionnées pour chaque file d'attente et pour chaque port. La limitation du débit en sortie est réalisée par mise en forme de la charge de sortie.

Le 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 la mise en forme du débit en sortie pour chaque file d'attente.

Cette fonctionnalité requiert que le commutateur soit en mode QoS de base ou en mode QoS avancé.

Pour définir la mise en forme en sortie pour chaque file d'attente :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **Egress Shaping Per Queue**.

ÉTAPE 2 Pour mettre en forme en sortie jusqu'à huit files d'attente sur chaque interface, sélectionnez l'interface et cliquez sur **Edit**.

ÉTAPE 3 Saisissez les informations suivantes :

- **Queue *x***: cochez la case **Enable** pour activer la mise en forme en sortie sur les files d'attente.
- **Committed Information Rate (CIR)** : saisissez le débit maximal (CIR) en kilobits par seconde (kbit/s). Le CIR est la quantité maximale moyenne de données pouvant être envoyée.

ÉTAPE 4 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration de la limite de débit VLAN

La limitation du débit pour chaque VLAN, que vous réalisez sur la page VLAN Ingress Rate Limit, permet de limiter le trafic sur les VLAN. La limitation de débit QoS (configurée sur la page Policy Table) est prioritaire sur 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 compte plusieurs périphériques, les valeurs de limites de débit VLAN sont appliquées indépendamment sur chacun des périphériques.

Cette fonctionnalité requiert que le commutateur soit en mode QoS de base ou en mode QoS avancé.

Pour définir la limite de débit d'entrée VLAN :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **VLAN Ingress Rate Limits**.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **VLAN ID** : sélectionnez un VLAN.
- **Committed Information Rate (CIR)** : saisissez la quantité moyenne maximale de données qui peut être acceptée sur le VLAN, en kilo-octets par seconde.

ÉTAPE 4 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration de la limite de débit de port VLAN

La limitation du débit par port VLAN, réalisée sur la page VLAN Port Ingress Rate Limit, permet de limiter le trafic sur les ports associés à un VLAN spécifique.

Lorsque vous configurez des limites de débit d'entrée VLAN, cela limite le trafic agrégé de tous les ports spécifiés du commutateur.

Cette fonctionnalité requiert que le commutateur soit en mode QoS de base ou en mode QoS avancé.

Si la limitation de bande passante et la limitation de débit d'entrée de port VLAN sont toutes les deux activées, le paramètre le plus faible a priorité.

Pour définir la limite de débit d'entrée de port VLAN :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **VLAN Port Ingress Rate Limits**.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **VLAN ID** : sélectionnez un VLAN.
- **Committed Information Rate (CIR)** : saisissez la quantité moyenne maximale de données qui peut être acceptée sur les interfaces spécifiées, en kilo-octets par seconde.
- **Interface** : entrez une interface ou une plage d'interfaces. Les interfaces doivent être associées au VLAN sélectionné.

ÉTAPE 4 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration de l'évitement des congestions TCP

Utilisez la page TCP Congestion Avoidance pour activer un algorithme d'évitement des congestions TCP. Cet algorithme casse ou évite la synchronisation TCP globale sur un nœud encombré lorsque la congestion est due au fait que plusieurs sources envoient des paquets munis de mêmes nombres d'octets.

Pour configurer l'évitement des congestions TCP :

ÉTAPE 1 Cliquez sur **Quality of Service** > **General** > **TCP Congestion Avoidance**.

ÉTAPE 2 Activez ou désactivez l'évitement des congestions TCP.

ÉTAPE 3 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration du mode QoS de base

En mode QoS de base, vous pouvez définir un domaine spécifique du réseau en qualité de domaine validé. 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 validé.

Pour configurer le mode QoS de base, procédez comme suit :

ÉTAPE 1 Sélectionnez le mode QoS de base pour le commutateur, comme indiqué dans la section **Configuration des propriétés de QoS**.

ÉTAPE 2 Sélectionnez le comportement validé, comme indiqué dans la section **Configuration du mode QoS de base validé**. Le commutateur prend en charge les quatre modes validés suivants : CoS/802.1p, DSCP, priorité IP et CoS/802.1p-DSCP. Le mode validé CoS/802.1p utilise la priorité 802.1p figurant dans la balise VLAN. Le mode validé DSCP utilise la valeur DSCP figurant dans l'en-tête IP.

ÉTAPE 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 sur la page Interface Settings, comme indiqué dans la section **Configuration des paramètres d'interface de QoS de base**.

Activez ou désactivez le mode validé sélectionné au niveau global sur les divers ports via la page Interface Settings. Si un port est désactivé sans mode validé, tous ses paquets d'entrée sont réacheminés en mode Meilleur effort (Best effort). Il est recommandé de désactiver le mode validé 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 du mode QoS de base validé

Utilisez la page Global Settings pour configurer le comportement validé pour le mode QoS de base. Cette configuration est active lorsque le commutateur est en mode QoS de base. Les paquets entrant dans un domaine QoS sont classifiés à la bordure du domaine QoS.

Pour définir le mode validé pour le mode QoS de base :

ÉTAPE 1 Cliquez sur **Quality of Service** > **QoS Basic Mode** > **Global Settings**.

ÉTAPE 2 Sélectionnez le mode validé lorsque le commutateur est en mode QoS de base. Si le niveau de CoS et la balise DSCP d'un paquet sont mappés sur des files d'attente distinctes, le mode validé 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 de la 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 pouvez configurer le mappage VPT vers la file d'attente réelle sur la page CoS/802.1p to Queue.
- **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 vers file d'attente sur la page DSCP to Queue. Si le trafic n'est pas de type IP, il est mappé sur la file d'attente de meilleur effort.
- **IP Precedence** : le trafic est mappé sur les files d'attente en fonction de la priorité IP. Vous pouvez configurer le mappage effectif de la priorité IP vers file d'attente sur la page IP Precedence to Queue.
- **CoS/802.1p-DSCP** : utilise le mode validé de CoS pour le trafic non IP et le mode validé DSCP pour le trafic IP.

ÉTAPE 3 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration des paramètres d'interface de QoS de base

Utilisez la page Interface Settings pour configuration la QoS sur chaque port, comme indiqué ci-dessous :

- **QoS State Disabled** : tout le trafic entrant sur le port est mappé sur la file d'attente de meilleur effort et aucune classification/attribution de priorité n'est effectuée.
- **QoS State Enabled** : le trafic d'entrée sur le port reçoit un ordre de priorité qui dépend du mode validé configuré à l'échelle du système, à savoir CoS/802.1p ou DSCP.

Pour activer ou désactiver la QoS sur une interface :

ÉTAPE 1 Cliquez sur **Quality of Service** > **QoS Basic Mode** > **Interface Settings**.

ÉTAPE 2 Sélectionnez le type d'interface (Port ou LAG) et cliquez sur **Go**.

ÉTAPE 3 Pour activer ou désactiver la QoS sur une interface, sélectionnez l'interface souhaitée et cliquez sur **Edit**.

ÉTAPE 4 Saisissez les informations suivantes :

- **Interface** : sélectionnez le port ou LAG à définir.
- **QoS State** : cochez la case **Enable** pour activer la QoS sur cette interface ou décochez cette case pour la désactiver.

ÉTAPE 5 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration du mode 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 mode QoS avancé à ces flux.

En mode 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 Permit (forward) 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 : gestionnaire de stratégie individuelle et 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.

Lors de la configuration du mode QoS avancé, veuillez prendre note des points suivants :

- 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 ses flux, de façon agrégée, ceci sans tenir compte ni des stratégies ni des ports.

Les paramètres de QoS avancé se composent de trois parties :

- Définitions 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.

Pour configurer le mode QoS avancé, procédez comme suit :

ÉTAPE 1 Sélectionnez le mode QoS avancé pour le système sur la page QoS Properties, comme indiqué dans la section **Configuration des propriétés de QoS**.

ÉTAPE 2 Sélectionnez le mode QoS avancé validé sur la page Global Settings, comme indiqué dans la section **Configuration des paramètres globaux de QoS avancé**.

ÉTAPE 3 Créez des ACL comme décrit dans la section **Création d'un flux de travail d'ACL**.

ÉTAPE 4 Si des ACL ont été définies, créez des mappages de classes et associez-leur ces ACL via la page Class Mapping, comme indiqué dans la section **Configuration d'un mappage de classe**.

ÉTAPE 5 Créez une stratégie sur la page Policy Table, comme indiqué dans la section **Configuration des stratégies QoS**.

ÉTAPE 6 Associez la stratégie à un ou plusieurs mappages de classes sur la page Policy Class Maps, comme indiqué dans la section **Configuration des mappages de classe de stratégies**.

ÉTAPE 7 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.

- **Single Policer** : créez une stratégie qui associe un mappage de classe à un gestionnaire de stratégie individuelle, sur la page Policy Class Maps et la page Class Mapping. Dans la stratégie, définissez le gestionnaire de stratégie individuelle.
- **Aggregate Policer** : créez une action de QoS pour chaque flux pour envoyer toutes les trames concordantes au même gestionnaire de stratégie (d'agrégats), via la page Aggregate Policer (voir section **Configuration de gestionnaires de stratégie d'agrégats**). Créez une stratégie pour associer un mappage de classe à ce gestionnaire de stratégie d'agrégats, via la page Policy Class Maps.

ÉTAPE 8 Associez la stratégie aux interfaces sur la page *Policy Binding*, comme décrit dans la section **Configuration des associations de stratégies**.

Configuration des paramètres globaux de QoS avancé

Utilisez la page Global Settings pour configurer le comportement validé pour le mode QoS avancé. Les paquets entrant dans un domaine QoS sont classifiés à la bordure du domaine QoS.

Pour définir le mode validé :

ÉTAPE 1 Cliquez sur **Quality of Service** > **QoS Advanced Mode** > **Global Settings**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Trust Mode** : sélectionnez un mode validé pendant que le commutateur est en mode QoS avancé. Si le niveau de CoS et la balise DSCP d'un paquet sont mappés sur des files d'attente distinctes, le mode validé détermine la file d'attente à laquelle ce paquet doit être affecté. Les options sont les suivantes :
  - *CoS/802.1p* : le trafic est mappé sur des files d'attente en fonction du champ VPT de la 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 pouvez configurer le mappage VPT vers la file d'attente réelle sur la page CoS/802.1p to Queue.
  - *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 vers file d'attente sur la page DSCP to Queue. Si le trafic n'est pas de type IP, il est mappé sur la file d'attente de meilleur effort.
  - *IP Precedence* : le trafic est mappé sur des files d'attente en fonction de leur priorité IP. Le mappage effectif de la priorité IP sur les files d'attente peut être configuré sur la page IP Precedence to Queue.
  - *CoS/802.1p-DSCP* : sélectionnez cette option pour utiliser le mode CoS validé pour le trafic non IP et le mode DSCP validé pour le trafic IP.
- **Default Mode Status** : sélectionnez le mode validé par défaut (validé ou non validé) pour les interfaces. Vous bénéficiez ainsi de la fonction QoS de base en mode QoS avancé, afin d'approuver CoS/DSCP sur la QoS avancé par défaut (sans devoir créer de stratégie).

  En mode QoS avancé, si Default Mode Status est défini sur Not Trusted, les valeurs CoS par défaut configurées sur l'interface seront utilisées afin d'accorder la priorité au trafic en direction de l'interface.

  Si vous disposez d'une stratégie sur une interface, le mode par défaut ne s'applique pas. L'action s'effectue en fonction de la configuration de stratégie et le trafic sans correspondance est éliminé.

ÉTAPE 3 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration d'un mappage de classe

Un mappage de classe définit un flux de trafic avec des ACL. Vous pouvez combiner une ACL MAC, une ACL IPv4 et une ACL IPv6 en un même mappage de classe. Les mappages de classe sont configurés de façon à correspondre à un critère ou à tous les critères parmi un ensemble de critères de paquet. 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 commutateur. 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, qui permet d'utiliser les mappages de classe 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 des stratégies QoS**).

Pour définir un mappage de classe :

ÉTAPE 1 Cliquez sur **Quality of Service** > **QoS Advanced Mode** > **Class Mapping**.

ÉTAPE 2 Cliquez sur **Add**.

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 informations suivantes :

- **Class Map Name** : saisissez le nom du nouveau mappage de classe.
- **Match ACL Type** : critères qu'un paquet doit satisfaire pour être considéré comme appartenant au flux défini dans le mappage de classe. Les options sont les suivantes :
  - *IP* : un paquet doit correspondre à une ACL IPv4 ou ACL IPv6 du mappage de classe.
  - *MAC* : un paquet doit correspondre à l'ACL MAC du mappage de classe.
  - *MAC or IP* : un paquet doit correspondre soit à l'ACL IP, soit à l'ACL MAC du mappage de classe.

- **IP** : sélectionnez une ACL IPv4 ou IPv6 pour ce mappage de classe.
- **MAC** : sélectionnez une ACL MAC pour ce mappage de classe.
- **Preferred ACL** : indiquez si les paquets sont d'abord comparés à une ACL IP ou à une ACL MAC.

ÉTAPE 4 Cliquez sur **Apply.** La configuration de fonctionnement est mise 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.

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 pouvez créer le gestionnaire de stratégie individuelle sur la page Policy Class Maps.
- **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 pouvez créer un gestionnaire de stratégie d'agrégats sur la page Aggregate Policer.

  Vous créez un gestionnaire de stratégie d'agrégats si vous prévoyez de la partager entre plusieurs classes. Les gestionnaires de stratégie sur un port ne peuvent pas être partagés avec d'autres gestionnaires de stratégie dans un autre périphérique.

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 kbit/s.
- 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.

Action à appliquer aux trames qui dépassent les limites (appelées trafic hors profil) permettant de transmettre ces trames telles quelles ou de les éliminer.

Configuration de gestionnaires de stratégie d'agrégats

Le gestionnaire de stratégie d'agrégats applique la QoS à un ou plusieurs mappages de classe, c'est-à-dire à un ou plusieurs flux. Un gestionnaire de stratégie d'agrégats peut prendre en charge des mappages de classe issus de différentes stratégies et appliquer la QoS à tous les flux, de façon agrégée, sans tenir compte des stratégies ni des ports.

Pour définir un gestionnaire de stratégie d'agrégats :

ÉTAPE 1 Cliquez sur **Quality of Service** > **QoS Advanced Mode** > **Aggregate Policer**.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **Aggregate Policer Name** : saisissez le nom du gestionnaire de stratégie d'agrégats.
- **Ingress Committed Information Rate (CIR)** : saisissez la bande passante maximale autorisée, en bits par seconde.
- **Exceed Action** : sélectionnez l'action à appliquer aux paquets entrants qui dépassent le seuil CIR. Les options disponibles sont les suivantes :
  - *Forward* : les paquets qui dépassent la limite CIR définie sont réacheminés.
  - *Drop* : les paquets qui dépassent la limite CIR définie sont éliminés.

ÉTAPE 4 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration des stratégies QoS

Utilisez la page Policy Table pour définir des stratégies QoS avancées. Seules les stratégies associées à une interface sont actives (reportez-vous à la section **Configuration des associations 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.

Une fois qu'une stratégie a été ajoutée, vous pouvez ajouter des mappages de classe via la page Policy Class Maps.

Pour créer une stratégie QoS avancée :

ÉTAPE 1 Cliquez sur **Quality of Service** > **QoS Advanced Mode** > **Policy Table**.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez le nom de la nouvelle stratégie dans le champ **New Policy Name**.

ÉTAPE 4 Cliquez sur **Apply**. Le profil de stratégie QoS est ajouté et la configuration de fonctionnement est mise à jour.

ÉTAPE 5 Cliquez sur **Policy Class Map Table** pour afficher la page Policy Class Maps.

Configuration des mappages de classe de stratégies

Vous pouvez ajouter un ou plusieurs mappages de classe à une stratégie. Un mappage de classe définit le type des paquets qui sont considérés comme appartenant au même flux de trafic.

Pour ajouter un mappage de classe à une stratégie :

ÉTAPE 1 Cliquez sur **Quality of Service** > **QoS Advanced Mode** > **Policy Class Maps**.

ÉTAPE 2 Sélectionnez une stratégie et cliquez sur **Go**. Tous les mappages de classe de cette stratégie sont affichés.

ÉTAPE 3 Cliquez sur **Add** pour ajouter un nouveau mappage de classe.

ÉTAPE 4 Saisissez les informations suivantes :

- **Policy Name** : indique la stratégie à laquelle vous ajoutez le mappage de classe.
- **Class Map Name** : sélectionnez le mappage de classe existant à associer à la stratégie.
- **Action Type** : sélectionnez l'action à appliquer concernant la valeur CoS/802.1p et/ou DSCP d'entrée de tous les paquets concordants.
  - *Use default trust mode* : permet d'ignorer la valeur CoS/802.1p et/ou DSCP d'entrée. Les paquets concordants sont envoyés en mode Meilleur effort (Best effort).
  - *Always Trust* : toujours valider les valeurs CoS/802.1p et DSCP du paquet correspondant. 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 to Queue.
  - *Set* : réglez manuellement la file d'attente de sortie pour tous les paquets correspondants. Si cette option est sélectionnée, sélectionnez **Queue** et entrez le numéro de la file d'attente dans le champ **New Value**.
- **Police Type** : sélectionnez le type de gestionnaire de stratégie pour la stratégie. Les options sont les suivantes :
  - *None* : aucune stratégie n'est utilisée.
  - *Single* : la stratégie est associée à un gestionnaire de stratégie individuelle.
  - *Aggregate* : la stratégie est associée à un gestionnaire de stratégie d'agrégats.
- **Aggregate Policer** : si le type de stratégie est Aggregate, sélectionnez un gestionnaire de stratégie d'agrégats.
- **Ingress Committed Information Rate (CIR)** : si le type de stratégie est Single, saisissez la valeur CIR en kbit/s. Consultez la description fournie à la section **Configuration de la bande passante**.

- **Exceed Action** : si le type de stratégie est Single, sélectionnez l'action à appliquer aux paquets entrants qui dépassent le seuil CIR. Les options disponibles sont les suivantes :
  - *None* : aucune action.
  - *Drop* : les paquets qui dépassent la limite CIR définie sont éliminés.

ÉTAPE 5 Cliquez sur **Apply**. La configuration de fonctionnement est mise à jour.

Configuration des associations de stratégies

Utilisez la page Policy Binding pour associer un profil de stratégie à des interfaces spécifiques. Lorsqu'un profil de stratégie est associé à une interface spécifique, il est actif sur cette interface. Vous ne pouvez configurer qu'un seul profil de stratégie sur chaque interface mais il est possible d'associer un même profil à plusieurs interfaces.

Lorsque vous associez une stratégie à une interface, cette dernière 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 la même interface.

REMARQUE Pour modifier une stratégie, vous devez d'abord la supprimer (annuler la liaison) de tous les ports auxquels elle est liée.

Pour définir une association de stratégie :

ÉTAPE 1 Cliquez sur **Quality of Service** > **QoS Advanced Mode** > **Policy Binding**.

ÉTAPE 2 Sélectionnez une stratégie existante définie sur la page Policy Table et le type d'interface (port ou LAG) et cliquez sur **Go**.

ÉTAPE 3 Cochez la case **Binding** sous les interfaces pour leur associer la stratégie sélectionnée ou décochez-la pour désassocier cette stratégie des interfaces.

ÉTAPE 4 Cliquez sur **Apply**. L'association de stratégie QoS est définie et la configuration de fonctionnement est mise à jour.

ÉTAPE 5 Pour afficher les stratégies associées à toutes les interfaces, cliquez sur **Show Policy Binding Per Port**. La page Policy Binding Table affiche la stratégie associée à chaque interface.

ÉTAPE 6 Cliquez sur **Back** pour revenir à la page précédente.

19

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**
- **Bases MIB prises en charge**
- **ID d'objet de modèles**
- **Configuration de l'ID de moteur SNMP**
- **Configuration de vues SNMP**
- **Configuration de groupes SNMP**
- **Création d'utilisateurs SNMP**
- **Configuration de communautés SNMP**
- **Configuration des destinataires de notifications SNMP**

Versions et flux de travail SNMP

Le Commutateur Cisco 220 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 filtres, à l'aide des filtres définis dans la base d'information pour la gestion (MIB) qu'il prend en charge.

SNMP v1 et v2

Pour contrôler l'accès au système, une liste de communautés SNMP est définie. Chaque communauté est constituée d'une chaîne de communauté et de son privilège d'accès. Le système répond uniquement aux messages SNMP spécifiant la communauté qui dispose des autorisations et des opérations correctes.

Les agents SNMP maintiennent une liste de variables utilisées pour gérer le commutateur. Ces variables sont définies dans la base MIB. La base MIB présente les variables contrôlées par l'agent. Toutes les bases MIB prises en charge par le commutateur sont indiquées dans la section **Bases MIB prises en charge**.

REMARQUE En raison des vulnérabilités en matière de sécurité détectées dans les autres versions, il est recommandé d'utiliser SNMPv3.

SNMP v3

En plus de la fonctionnalité fournie par SNMPv1 et v2, SNMPv3 applique un contrôle d'accès et de nouveaux mécanismes de filtre aux PDU SNMPv1 et SNMPv2. SNMPv3 définit également un modèle de sécurité utilisateur (USM, User Security Model) qui inclut :

- **Authentication** : fournit une intégrité des données et une authentification de leur origine.
- **Privacy** : 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.
- **Timeliness** : 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.
- **Key Managemens** : 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 commutateur pour gérer des fonctionnalités de périphérique.

Flux de travail SNMP

REMARQUE Pour des raisons de sécurité, SNMP est désactivé par défaut. Avant de pouvoir gérer le commutateur via SNMP, vous devez activer le service SNMP sur le commutateur, comme indiqué dans la section **Configuration des 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 :

ÉTAPE 1 Si vous le souhaitez, définissez les vues SNMP sur la page SNMP > Views, comme indiqué dans la section **Configuration de vues SNMP**.

ÉTAPE 2 Définissez les groupes SNMP sur la page SNMP > Groups, comme indiqué dans la section **Configuration de groupes SNMP**. Le groupe peut être associé à la vue SNMP définie.

ÉTAPE 3 Définissez une communauté SNMP sur la page SNMP > Community, comme indiqué dans la section **Configuration de communautés 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.

- **Basic mode** : les droits d'accès d'une communauté peuvent être définis en Read Only ou Read Write. Vous pouvez en outre restreindre l'accès à la communauté à certains objets MIB uniquement, en sélectionnant une vue (définie sur la page SNMP > Views).
- **Advanced Mode** : les droits d'accès à une communauté sont définis par un groupe (défini sur la page SNMP > Groups). Vous pouvez configurer le groupe avec un modèle de sécurité spécifique. Les groupes disposent des droits d'accès de lecture, d'écriture et de notification.

ÉTAPE 4 Définissez les destinataires de la notification sur la page SNMP > Notification Recipients SNMPv1,2, comme indiqué dans la section **Configuration de destinataires de notifications SNMPv1,2**.

Si vous décidez d'utiliser SNMP v3 :

ÉTAPE 1 Définissez le moteur SNMP sur la page SNMP > Engine ID, comme indiqué dans la section **Configuration de l'ID de moteur SNMP**. Créez un ID de moteur unique ou utilisez l'ID de moteur par défaut.

ÉTAPE 2 Si vous le souhaitez, définissez les vues SNMP sur la page SNMP > Views, comme indiqué dans la section **Configuration de vues SNMP**. Vous limitez ainsi la plage des ID d'objet (OID) disponibles pour une communauté SNMP ou un groupe SNMP.

ÉTAPE 3 Définissez les groupes SNMP sur la page SNMP > Groups, comme indiqué dans la section **Configuration de groupes SNMP**. Le groupe peut être associé à la vue SNMP définie.

ÉTAPE 4 Définissez les utilisateurs SNMP sur la page SNMP > Users, comme indiqué dans la section **Création d'utilisateurs SNMP**. Les utilisateurs SNMP peuvent être associés à un groupe SNMP.

ÉTAPE 5 Définissez les destinataires de la notification sur la page SNMP > Notification Recipients SNMPv3, comme indiqué dans la section **Configuration de destinataires de notification SNMPv3**.

Bases MIB prises en charge

Les bases MIB standard suivantes sont prises en charge par le Commutateur Cisco 220 :

- RFC1213 MIB-II
- RFC1215 Generic-Traps MIB
- RFC1493 (4188) Bridge MIB
- RFC2618 RADIUS Client MIB
- RFC2674 Bridge MIB Extension
- RFC2737 Entity MIB
- RFC2819 RMON
- RFC2863 The Interface Group MIB
- RFC3164 Syslog MIB
- RFC3621 PoE MIB (disponibles pour les modèles PoE uniquement)
- RFC3635 Ethernet-Like MIB
- SNMP-COMMUNITY MIB
- SNMP-MIB
- LLDP-MIB
- LLDP-EXT-MED-MIB

- IEEE802.3 Annex 30C MIB
- CISCO-CDP-MIB
- CISCO-ENVMON-MIB
- CISCO-PORT-SECURITY-MIB
- CISCO-IMAGE-MIB

ID d'objet de modèles

Ci-dessous figurent les ID d'objet (OID) des modèles de commutateur :

Modèle	ID d'objet
SF220-24	1.3.6.1.4.1.9.6.1.84.24.1
SF220-24P	1.3.6.1.4.1.9.6.1.84.24.2
SF220-48	1.3.6.1.4.1.9.6.1.84.48.1
SF220-48	1.3.6.1.4.1.9.6.1.84.48.2
SG220-26	1.3.6.1.4.1.9.6.1.84.26.1
SG220-26P	1.3.6.1.4.1.9.6.1.84.26.2
SG220-50	1.3.6.1.4.1.9.6.1.84.50.1
SG220-50P	1.3.6.1.4.1.9.6.1.84.50.2
SG220-28	1.3.6.1.4.1.9.6.1.84.28.5
SG220-28MP	1.3.6.1.4.1.9.6.1.84.28.3
SG220-52	1.3.6.1.4.1.9.6.1.84.52.5

Configuration de l'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 d'interception à un gestionnaire.

Chaque agent SNMP conserve des informations locales utilisées dans des échanges de messages SNMPv3. L'ID de moteur SNMP par défaut est constitué du numéro d'entreprise et de l'adresse MAC par défaut. L'ID de moteur SNMP doit être unique pour le domaine d'administration afin que deux périphériques 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).

Pour définir l'ID de moteur SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Engine ID**.

ÉTAPE 2 Dans la zone **Local Engine ID**, définissez l'ID de moteur local :

- **Use Default** : utilisez l'ID de moteur généré par le périphérique. 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* : réglé sur 3 pour indiquer l'adresse MAC qui suit.
  - *6 derniers octets* : adresse MAC du commutateur.
- **User Defined** : saisissez l'ID de moteur de l'unité locale. La valeur du champ est une chaîne hexadécimale (plage : 10 à 64). Chaque octet dans les chaînes de caractères hexadécimales est représenté par deux chiffres hexadécimaux.

ÉTAPE 3 Cliquez sur **Apply**. L'ID de moteur local est défini et la configuration de fonctionnement est mise à jour.

ÉTAPE 4 Le tableau **Remote Engine ID Table** affiche tous les ID de moteur SNMP distant pris en charge par le commutateur. Pour ajouter un ID de moteur distant, cliquez sur **Add**.

ÉTAPE 5 Saisissez les informations suivantes :

- **Server Definition** : indiquez si vous souhaitez spécifier le serveur d'ID de moteur par son adresse IP ou son nom.
- **IP Version** : sélectionnez **Version 4** ou **Version 6** si le serveur est identifié par adresse IP.
- **Server IP Address/Name** : saisissez l'adresse IP ou le nom de domaine du serveur distant qui reçoit les filtres.
- **Engine ID** : saisissez l'ID de moteur.

ÉTAPE 6 Cliquez sur **Apply.** L'ID de moteur distant est défini et la configuration de fonctionnement est mise à jour.

Configuration de vues SNMP

Une vue est une étiquette définie par l'utilisateur pour une collection de sous-arborescences de l'arborescence de la base MIB. Chaque ID de sous-arborescence est défini par l'OID de la racine des sous-arborescences concernées. Vous pouvez utiliser des noms connus pour spécifier la racine de la sous-arborescence souhaitée ou entrer un OID.

Chaque sous-arborescence est soit incluse, soit exclue dans la vue en cours de définition.

Utilisez la page Views pour configurer les vues SNMP. Les vues par défaut ne peuvent pas être modifiées. Vous pouvez associer des vues à des groupes via la page SNMP > Groups ou à une communauté qui utilise le mode d'accès de base via la page SNMP > Communities.

Pour définir des vues SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Views**.

ÉTAPE 2 Pour ajouter une nouvelle vue SNMP, cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **View Name** : saisissez un nom de vue.
- **Object ID Subtree** : sélectionnez **User Defined** pour définir manuellement un OID ou sélectionnez un OID existant dans la liste. Tous les descendants de ce nœud seront inclus dans la vue ou exclus.
- **Include In View** : cochez cette option pour inclure les bases MIB sélectionnées dans cette vue, ou décochez-la pour les exclure.

ÉTAPE 4 Cliquez sur **Apply**. La vue SNMP est définie et la configuration de fonctionnement est mise à jour.

Configuration de groupes SNMP

Dans SNMPv1 et SNMPv2, une chaîne de communauté est envoyée accompagnée des trames SNMP. La chaîne de communauté agit en tant que mot de passe pour accéder à un agent SNMP. Cependant, ni les trames, ni la chaîne de communauté ne sont cryptées. Par conséquent, SNMPv1 et SNMPv2 ne sont pas sécurisés.

Dans SNMPv3, les fonctions de sécurité suivantes peuvent être configurées :

- **Authentication** : le commutateur vérifie que l'utilisateur SNMP est un administrateur système autorisé. Cette opération est effectuée pour chaque trame.
- **Privacy** : les trames SNMP peuvent accueillir des données cryptées.

Dans SNMPv3, il existe trois niveaux de sécurité :

- No security (Aucune authentification et aucune confidentialité)
- Authentication (Authentification et aucune confidentialité)
- Authentification et confidentialité (réglages de confidentialité du groupe)

SNMPv3 permet de contrôler le contenu que chaque utilisateur peut lire ou écrire, ainsi que les notifications qu'il reçoit. Un groupe définit des privilèges de lecture/écriture et un niveau de sécurité. Il devient opérationnel lorsqu'il est associé à un utilisateur ou une communauté SNMP.

REMARQUE Pour associer à un groupe une vue qui n'est pas une vue par défaut, créez d'abord la vue sur la page SNMP > Views.

Pour définir des groupes SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Groups**.

ÉTAPE 2 Pour ajouter un nouveau groupe SNMP, cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **Group Name** : saisissez le nom du nouveau groupe.
- **Security Model** : sélectionnez la version SNMP (SNMPv1, SNMPv2 ou SNMPv3) associée au groupe.

Il est possible de définir trois types de vues avec différents niveaux de sécurité. Pour chaque niveau de sécurité, sélectionnez les vues correspondant aux privilèges de lecture, d'écriture et de notification en renseignant les champs suivants :

- **Security Level** : cochez la case **Enable** pour activer le niveau de sécurité relatif associé au groupe. SNMPv1 et SNMPv2 ne prennent pas en charge l'authentification, ni la confidentialité. Si SNMPv3 est sélectionné comme mode de sécurité, choisissez l'une des options suivantes :
  - *No Authentication and No Privacy* : les niveaux de sécurité d'authentification et de confidentialité ne sont pas affectés au groupe.
  - *Authentication and No Privacy* : 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.
  - *Authentication and Privacy* : authentifie les messages SNMP messages et les crypte si leur origine est authentifiée.
- **View** : sélectionnez une vue précédemment définie pour les privilèges de lecture, d'écriture et de notification. L'association d'une vue aux privilèges d'accès de lecture, écriture et notification du groupe limite l'étendue de l'arborescence de la base MIB sur laquelle le groupe dispose d'un accès en lecture, écriture et notification.
  - *Read* : l'accès est en lecture seule pour la vue sélectionnée. Il est possible de choisir le mode de lecture seule pour un groupe SNMP.
  - *Write* : l'accès à la gestion est en écriture pour la vue sélectionnée. Sinon, un utilisateur ou une communauté associés à ce groupe peuvent écrire dans toutes les bases MIB, à l'exception de celles qui contrôlent le SNMP lui-même.

- *Notify* : envoie uniquement des filtres dont le contenu est inclus dans la vue SNMP sélectionnée. Sinon, il n'existe aucune restriction sur le contenu des filtres. En général, il n'est pas nécessaire de sélectionner Notify.

ÉTAPE 4 Cliquez sur **Apply**. Le groupe SNMP est défini et la configuration de fonctionnement est mise 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.

L'utilisateur configuré a les attributs de son groupe et dispose des privilèges d'accès définis dans la vue associée.

Les groupes permettent aux gestionnaires de réseaux d'affecter des droits d'accès à un groupe d'utilisateurs plutôt qu'à un utilisateur unique. Un utilisateur ne peut être membre que d'un seul groupe.

Pour créer un utilisateur SNMPv3, vous devez disposer d'un groupe SNMPv3. Le groupe SNMPv3 peut être défini sur la page SNMP > Groups.

Pour définir des utilisateurs SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Users**.

ÉTAPE 2 Pour créer un utilisateur SNMP et lui affecter des privilèges de contrôle d'accès SNMP, cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **User Name** : saisissez un nom d'utilisateur.
- **Group Name** : sélectionnez le groupe SNMP auquel appartient l'utilisateur SNMP.

  REMARQUE Les utilisateurs appartenant à des groupes qui ont été supprimés sont conservés, mais sont inactifs.

- **Authentication Method** : sélectionnez la méthode d'authentification qui varie en fonction du nom de groupe qui a été attribué. Si le groupe ne requiert pas d'authentification, alors l'utilisateur ne peut configurer aucune authentification. Les options sont les suivantes :
  - *None* : aucune authentification d'utilisateur n'est utilisée.
  - *MD5* : utilise un mode de passe ou une clé MD5 pour l'authentification.
  - *SHA* : utilise un mot de passe ou une clé SHA (Secure Hash Algorithm, algorithme de cryptage irréversible) pour l'authentification.
- **Authentication Password** : sélectionnez **Encrypted** pour entrer un mot de passe d'authentification crypté ou sélectionnez **Plaintext** pour entrer le mot de passe en texte clair. Le mot de passe qui est utilisé pour générer une clé via la méthode d'authentification MD5 ou SHA.
- **Privacy Method** : sélectionnez **None** ou **DES** comme méthode de confidentialité.
- **Privacy Password** : sélectionnez **Encrypted** pour entrer un mot de passe d'authentification crypté ou sélectionnez **Plaintext** pour entrer le mot de passe en texte clair. Le mot de passe sert à générer une clé via la méthode DES.

ÉTAPE 4 Cliquez sur **Apply**. L'utilisateur SNMPv3 est ajouté et la configuration de fonctionnement est mise à jour.

Configuration de communautés SNMP

Vous pouvez gérer les droits d'accès dans SNMPv1 et SNMPv2 en définissant des communautés sur la page SNMP > Communities. Le nom de la communauté correspond à un type de mot de passe partagé entre la station de gestion SNMP et l'unité. Il sert à authentifier la station de gestion SNMP.

Les communautés sont uniquement définies dans SNMPv1 et v2, car SNMPv3 fonctionne avec des utilisateurs et non avec des communautés. Les utilisateurs appartiennent à des groupes qui disposent de droits d'accès qui leur sont affectés.

La page Communities associe des communautés à des droits d'accès, soit directement (mode de base), soit via des groupes (mode avancé) :

- **Basic mode** : les droits d'accès d'une communauté peuvent être définis en Read Only ou Read Write. Vous pouvez en outre restreindre l'accès à la communauté à certains objets MIB uniquement, en sélectionnant une vue.
- **Advanced Mode** : les droits d'accès à une communauté sont définis par un groupe. Vous pouvez configurer le groupe avec un modèle de sécurité spécifique. Les groupes disposent des droits d'accès de lecture, d'écriture et de notification.

Pour définir des communautés SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Communities**.

ÉTAPE 2 Pour ajouter une nouvelle communauté SNMP, cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **Community String** : saisissez le nom de la communauté (mot de passe) servant à authentifier la station de gestion auprès du périphérique.
- **Basic** : 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 système) 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, renseignez les champs suivants :
  - *Access Mode* : sélectionnez les droits d'accès de la communauté. Les options sont les suivantes :

    Read Only : l'accès à la gestion se fait en lecture seule uniquement. Aucune modification ne peut être apportée à la communauté.

    Read Write : l'accès à la gestion se fait en lecture et écriture. Des modifications ne peuvent être apportées qu'à la configuration du commutateur, pas à la communauté.

    SNMP Admin : l'accès à la gestion se fait en lecture et écriture. Des modifications peuvent être apportées à l'ensemble de la configuration du commutateur, par conséquent la vue en lecture/écriture concerne l'ensemble.
  - *View Name* : sélectionnez une vue SNMP (collection de sous-arborescences de bases MIB auxquelles un accès est accordé).
- **Advanced** : dans ce mode, les droits d'accès sont déterminés par groupe SNMP. Sélectionnez un groupe SNMP existant dans le menu déroulant de la communauté.

ÉTAPE 4 Cliquez sur **Apply.** La communauté SNMP est définie et la configuration de fonctionnement est mise à jour.

Configuration des destinataires de notifications SNMP

Des filtres sont générés pour signaler des événements système, tels que défini dans la RFC 1215. Le système peut générer des filtres définis dans la base MIB qu'il prend en charge.

Les destinations du filtre (connus sous le nom de destinataires de notification) sont des nœuds réseau où des messages d'interception sont envoyés par le commutateur. Plusieurs destinataires de notification sont répertoriés comme cibles des filtres. Une entrée de destination du filtre contient l'adresse IP du nœud et les informations SNMP qui correspondent à la version qui doit être incluse dans le message d'interception. Lorsqu'un événement nécessite l'envoi d'un message d'interception, ce dernier est envoyé vers chaque nœud répertorié dans la Table des destinataires de notifications.

La page Notification Recipients SNMPv1,2 et la page Notification Recipients SNMPv3 permettent de configurer la destination d'envoi des notifications SNMP, ainsi que les types de notifications SNMP envoyées vers chaque destination (filtres ou informations).

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.

Configuration de destinataires de notifications SNMPv1,2

Pour définir un destinataire dans SNMPv1,2 :

ÉTAPE 1 Cliquez sur **SNMP** > **Notification Recipients SNMPv1,2**.

ÉTAPE 2 Pour créer un destinataire de notification SNMPv1,2, cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **Server Definition** : indiquez si vous souhaitez spécifier le destinataire de notification par son adresse IP ou son nom.

- **IP Version** : sélectionnez **Version 4** ou **Version 6** si le destinataire de notification est identifié par adresse IP.
- **Recipient IP Address/Name** : saisissez l'adresse IP ou le nom d'hôte du destinataire des filtres.
- **UDP Port** : saisissez le port UDP utilisé pour les notifications sur l'unité du destinataire.
- **Notification Type** : indiquez le type de données à envoyer (**Traps** ou **Informs**). Si les deux sont nécessaires, deux destinataires doivent être créés.
- **Timeout** : saisissez la durée pendant laquelle le commutateur doit attendre avant de renvoyer des informations, en secondes. La valeur par défaut est 15 secondes.
- **Retries** : saisissez le nombre de fois que le commutateur peut renvoyer une demande d'information. La valeur par défaut est 3.
- **Community String** : sélectionnez la communauté SNMP pour le gestionnaire des filtres.
- **Notification Version** : sélectionnez la version SNMP du filtre. SNMPv1 ou SNMPv2 peut être utilisé, une seule version ne pouvant être activée à la fois.

ÉTAPE 4 Cliquez sur **Apply.** Le destinataire de notification SNMPv1,2 est ajouté et la configuration de fonctionnement est mise à jour.

Configuration de destinataires de notification SNMPv3

Pour définir un destinataire dans SNMPv3 :

ÉTAPE 1 Cliquez sur **SNMP** > **Notification Recipients SNMPv3**.

ÉTAPE 2 Pour ajouter un destinataire de notification SNMPv3, cliquez sur **Add**.

ÉTAPE 3 Saisissez les informations suivantes :

- **Server Definition** : indiquez si vous souhaitez spécifier le destinataire de notification par son adresse IP ou son nom.
- **IP Version** : sélectionnez **Version 4** ou **Version 6** si le destinataire de notification est identifié par adresse IP.
- **Recipient IP Address/Name** : saisissez l'adresse IP ou le nom d'hôte du destinataire de notification auquel les filtres sont envoyés.

- **UDP Port** : saisissez le port UDP utilisé pour les notifications sur l'unité du destinataire.
- **Notification Type** : indiquez le type de données à envoyer (**Traps** ou **Informs**). Si les deux sont nécessaires, deux destinataires doivent être créés.
- **Timeout** : saisissez la durée pendant laquelle le commutateur doit attendre avant de renvoyer des informations, en secondes. La valeur par défaut est 15 secondes.
- **Retries** : saisissez le nombre de fois que le commutateur peut renvoyer une demande d'information. La valeur par défaut est 3.
- **User Name** : sélectionnez l'utilisateur auquel sont envoyées les notifications SNMP. Pour recevoir les notifications, cet utilisateur doit être défini sur la page Users, et son ID de moteur doit être distant.
- **Security Level** : sélectionnez le niveau d'authentification appliqué au paquet. Les options sont les suivantes :
  - *No Authentication* : indique que le paquet n'est pas authentifié ni crypté.
  - *Authentication* : indique que le paquet est authentifié, mais pas crypté.
  - *Privacy* : indique que le paquet est à la fois authentifié et crypté.

  REMARQUE Le niveau de sécurité dépend du nom d'utilisateur qui a été sélectionné. Si le paramètre No Authentication a été défini pour ce nom d'utilisateur, le niveau de sécurité sera uniquement No Authentication. Cependant, si le paramètre Authentication and Privacy a été défini pour ce nom d'utilisateur sur la page Users, le niveau de sécurité sur cet écran peut être No Authentication, Authentification ou Authentication ou Privacy.

ÉTAPE 4 Cliquez sur **Apply**. Le destinataire de notification SNMPv3 est défini et la configuration de fonctionnement est mise à jour.

A

Pour en savoir plus

Cisco fournit une gamme étendue de ressources pour vous aider, ainsi que votre client, à profiter de tous les avantages du système Commutateurs Smart Cisco série 220.

Communauté d'assistance Cisco	www.cisco.com/go/smallbizsupport
Assistance et ressources Cisco	www.cisco.com/go/smallbizhelp
Coordonnées de l'assistance téléphonique	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Téléchargements de microprogrammes Cisco	www.cisco.com/go/smallbizfirmware Sélectionnez un lien pour télécharger le microprogramme d'un produit Cisco. Aucune connexion n'est requise.
Demandes Open Source Cisco	www.cisco.com/go/smallbiz_opensource_request
Commutateurs Cisco série 220	www.cisco.com/go/220switches
Informations sur la garantie	www.cisco.com/go/warranty
Informations relatives à la conformité et à la sécurité	www.cisco.com/en/US/docs/switches/lan/csb_switching_general/rcsi/Switch_ClassA_RCSI.pdf
Cisco Partner Central (connexion partenaire requise)	www.cisco.com/web/partners/sell/smb