GUIDE D'ADMINISTRATION

Commutateurs administrables CiscoSx350, SG350X, SG350XG, Sx550X et SG550XG, version du microprogramme 2.3.5.x, version 0.5

Table des matières

Sommaire

Sommaire

1

Prise en main

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

- Démarrage de l'utilitaire Web de configuration
- PoE (Power over Ethernet)
- Port OOB (Out Of Band, hors bande)
- Port USB
- Mode d'affichage de base ou avancé
- Configuration de l'appareil - Démarrage rapide
- Conventions de nommage de l'interface
- Navigation dans les fenêtres
- Fonction de recherche

Démarrage de l'utilitaire Web de configuration

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

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

Restrictions s'appliquant aux navigateurs

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

Lancement de l'utilitaire de configuration

Pour lancer l'utilitaire de configuration Web :

ÉTAPE 1 Ouvrez un navigateur Web.

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

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

L'adresse IP par défaut 192.168.1.254 des appareils SG350XG et SG550XG est configurée sur le port OOB. Sur les autres modèles, celle-ci est configurée sur le VLAN par défaut (VLAN 1). Pour accéder au périphérique avec l'adresse IP configurée sur le port OOB, vérifiez que le port OOB est connecté à votre réseau ou à votre ordinateur.

Connexion

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

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

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

Pour vous connecter à device configuration utility :

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

ÉTAPE 2 Si vous n'utilisez pas l'anglais, sélectionnez la langue souhaitée dans le menu déroulant Langue. Pour ajouter une nouvelle langue au périphérique ou mettre à jour une langue actuelle, reportez-vous à la description du menu Language (Langue) de la section En-tête d'application.

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

ÉTAPE 4 Indiquez si vous souhaitez sélectionner **Password Complexity Settings** (Paramètres de complexité de mot de passe) sur la page Sécurité du mot de passe.

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

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

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

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

HTTP/HTTPS

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

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

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

Expiration du mot de passe

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

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

Déconnexion

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

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

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

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

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

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

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

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

PoE (Power over Ethernet)

Certains périphériques prennent en charge la fonctionnalité PoE, d'autres non. Les modèles prenant en charge la fonctionnalité PoE comportent un P à la fin de leur nom, par exemple : SF350-48HP.

Les champs PoE sont décrits sur toutes les pages concernées, mais ils ne s'appliquent qu'aux périphériques prenant en charge la fonctionnalité PoE.

Port OOB (Out Of Band, hors bande)

REMARQUE OOB n'est pris en charge que sur les appareils SG350XG et SG550XG.

Le commutateur prend en charge le port hors bande (OOB). Ce port est utilisé pour le réseau de gestion. Étant donné que les ports hors-bande et intrabandes partagent la même table de routage IP, vous ne pouvez pas utiliser le même sous-réseau sur ces deux interfaces.

Le port OOB est attribué à une adresse MAC différente de l'adresse MAC de base et des adresses des ports intra-bandes. Cette adresse MAC est utilisée comme adresse MAC source dans toutes les trames (notamment les trames IP) envoyées par le commutateur sur le port OOB.

L'adresse IP affectée à ce port ne peut pas être attribuée en même temps aux ports intrabandes. En outre, l'adresse IP affectée au port OOB ne doit appartenir à aucun sous-réseau IP configuré sur les interfaces intrabandes des périphériques.

Par défaut, le port OOB est configuré avec l'adresse IP par défaut 192.168.1.254. L'adresse IP par défaut est utilisée lorsqu'aucune autre adresse n'est affectée (de façon dynamique ou statique). Ce sous-réseau est réservé et ne peut pas être affecté sur les interfaces intrabandes.

Pontage

Le pontage entre le port OOB et les interfaces de couche 2 intra-bandes n'est pas pris en charge. Le port OOB ne peut pas être membre d'un VLAN ou d'un LAG et les protocoles du pont (comme STP, GVRP, etc.) ne peuvent pas être activés sur le port OOB.

Seul le trafic non balisé est pris en charge sur le port OOB.

Configuration de port

La configuration Ethernet suivante est prise en charge pour le port OOB :

- Débit (10/100/1000)
- Duplex
- Négociation automatique

Client DHCP

Le client DHCP (IPv4 et IPv6) est activé par défaut sur le port OOB et sur le VLAN par défaut.

Acheminement statique sur le port OOB

Les acheminements statiques sont pris en charge sur le port OOB.

Adresse IPv4 sur le port OOB

Vous ne pouvez définir qu'une seule adresse IPv4 sur le port OOB.

L'adresse IP statique par défaut n'est définie que sur le port OOB.

Applications IP

Toutes les applications IP, comme telnet et SSH, sont prises en charge sur le port OOB, sauf celles indiquées ci-dessous :

- Proxy ARP
- Protocoles de routage
- Applications relais (DHCP, DHCPv6 et UDP)

QoS et ACL

La QoS et les ACL ne sont pas prises en charge sur le port OOB (par conséquent, toutes les fonctionnalités basées sur TCAM, comme la prévention des attaques par déni de service (DoS), ne sont pas prises en charge non plus).

Seules les ACL de gestion sont prises en charge.

Prise en charge de l'empilage

Le nom du port OOB est toujours associé au port OOB physique de l'unité principale. Les ports OOB physiques des unités asservies ne fonctionnent pas et établiront une liaison lors d'une connexion à un appareil voisin ou à un PC.

Port USB

Le port USB peut être utilisé pour connecter des appareils de stockage externes (disque sur clé). Il peut préserver la configuration, le journal SYSLOG et les fichiers image. Dans une pile, seul le port USB de l'unité principale est actif. Le port USB prend totalement en charge le système de fichiers FAT32 et permet une prise en charge partielle (lecture seule) du système de fichiers NTFS.

Vous pouvez utiliser des chemins relatifs ou complets.

Le système prend en charge les actions suivantes sur le port USB via l'interface utilisateur :

- Afficher le contenu USB
- Copier des fichiers vers/depuis le port USB (comme avec TFTP)
- Supprimer, renommer et afficher le contenu des fichiers USB

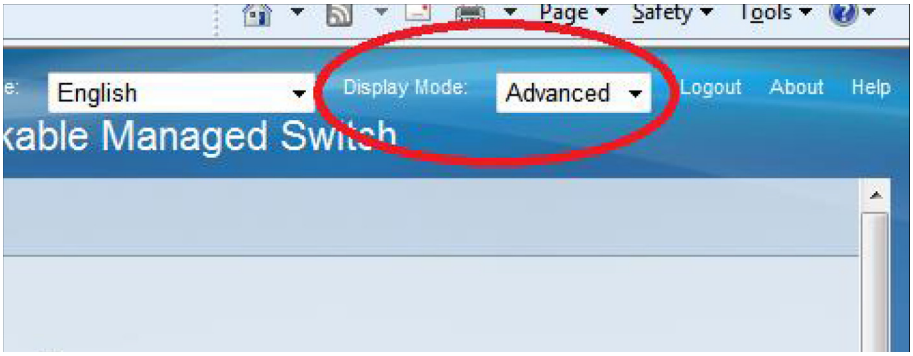
Mode d'affichage de base ou avancé

Le produit prend en charge de nombreuses fonctionnalités, c'est pourquoi l'interface utilisateur Web compte des centaines de pages de configuration et d'affichage. Ces pages sont divisées en modes d'affichage, spécifiés ci-dessous :

- **Basic** (De base) : des options de configuration de sous-réseau de base sont disponibles. Si vous souhaitez accéder à des options de configuration supplémentaires, sélectionnez le mode Advanced (Avancé) dans l'en-tête du périphérique.

- **Advanced** (Avancé) : un ensemble complet d'options de configuration est disponible.

Basculez d'un mode à l'autre, comme illustré ci-dessous :



Quand l'utilisateur passe du mode de base au mode avancé, le navigateur recharge la page. Cependant, après le rechargement, l'utilisateur reste sur la même page.

Quand l'utilisateur passe du mode avancé au mode de base, le navigateur recharge la page. Si celle-ci existe également en mode de base, l'utilisateur reste sur la même page. Si elle n'existe pas, le navigateur charge la première page du dossier dans lequel l'utilisateur travaillait. Si le dossier n'existe pas, la page de mise en route s'affiche.

Si une configuration avancée a été effectuée et si la page est chargée en mode de base, un message s'affichera à l'intention de l'utilisateur (par exemple, 2 serveurs RADIUS sont configurés, mais en mode de base, un seul serveur peut être affiché ; ou l'authentification du port 802.1X est configurée avec une période qui n'est pas visible en mode de base).

Lorsque vous basculez d'un mode à l'autre, la configuration effectuée sur la page (sans l'appliquer) sera supprimée.

Configuration de l'appareil - Démarrage rapide

Pour une configuration initiale rapide, vous pouvez utiliser les assistants de configuration décrits à la section Assistant de configuration des VLAN ou utiliser les liens sur la page de mise en route, comme décrit ci-dessous :

Catégorie	Nom du lien (sur la page)	Page correspondante
Configuration initiale	Manage Stack (Gérer la pile)	Administration : Gestion des piles
	Change Management Applications and Services	Services TCP/UDP
	Change Device IP Address	Interfaces IPv4
	Créer un VLAN	Paramètres VLAN
	Configurer les paramètres de port	Paramètres des ports
État du périphérique	Récapitulatif du système	Récapitulatif du système
	Port Statistics	Interface
	RMON Statistics	Statistiques
	View Log	Mémoire RAM
Accès rapide	Change Device Password	Comptes d'utilisateur
	Upgrade Device Software	Opérations du microprogramme
	Backup Device Configuration	Opérations de fichiers
	Create MAC-Based ACL	Création d'ACL basées sur MAC
	Create IP-Based ACL	Création d'ACL basées sur IPv4
	Configure QoS	Propriétés de QoS
	Configurer SPAN	Analyseur de port commuté (SPAN et RSPAN)

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** (Assistance) pour accéder à la page d'assistance produit du périphérique, puis sélectionnez le lien **Forums** pour accéder à la page Support Community.

Conventions de nommage de l'interface

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

- **Type de l'interface :** les types d'interfaces suivants se retrouvent dans divers types de périphériques :
  - **Fast Ethernet (10/100 bits)** : celles-ci sont désignées par **FE**. Prises en charge uniquement sur les appareils de la gamme 350.
  - **Ports Gigabit Ethernet (10/100/1 000 bits)** : celles-ci sont désignées par **GE**. Prises en charge uniquement sur les appareils de la gamme 350.
  - **Ten Gigabit Ethernet ports (1 000/10 000 Mbit/s)** (Ports Ten Gigabit Ethernet [1 000/10 000 bits]) : celles-ci sont désignées par **XG**.
  - **Port Out-of-Band** (hors bande) : celle-ci est désignée par **OOB**.
  - **LAG (PortChannel)** : celles-ci sont désignées par **LAG**.
  - **VLAN** : celles-ci sont désignées par **VLAN**.
  - **Tunnel** : celles-ci sont désignées par **Tunnel**.
- **Numéro d'unité** : numéro de l'unité dans la pile. Le numéro d'unité, associé au numéro d'interface, permet d'identifier le port. Par exemple, GE1/0/4 est le port numéro 4 de la première unité de la pile.
- **Slot Number** (Numéro de logement) : le numéro de logement est toujours 0.
- **Numéro d'interface :** ID du port, LAG, tunnel ou VLAN.

Navigation dans les fenêtres

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

En-tête d'application

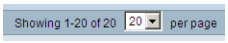
L'en-tête d'application s'affiche sur toutes les pages. Elle propose les liens d'application suivants :

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

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

Boutons de gestion

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

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

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

Fonction de recherche

La *fonction* de recherche vous permet de trouver les pages de l'interface utilisateur qui vous intéressent.

Si vous effectuez une recherche par mot-clé, vous obtiendrez des liens vers les pages correspondantes, mais également des liens vers des pages d'aide.

Pour accéder à la fonction de recherche, saisissez un mot-clé et cliquez sur l'icône de la loupe. Vous trouverez ci-dessous un exemple des résultats de la recherche du mot-clé : CDP :

Si vous êtes en mode de base, des liens vers des pages du mode avancé sont affichés, mais pas disponibles.

2

Tableau de bord

Le tableau de bord se compose de 8 cases, initialement vides, pouvant recevoir différents types d'informations

Vous pouvez sélectionner des modules parmi ceux disponibles et les placer dans cette grille. Vous pouvez par ailleurs personnaliser les paramètres des modules affichés à l'écran.

Lors du chargement du tableau de bord, les modules que vous avez sélectionnés sont chargés à l'emplacement défini dans la grille. Les données contenues dans les modules sont mises à jour régulièrement, à des intervalles différents selon le type de module. Ces intervalles sont configurables pour certains modules.

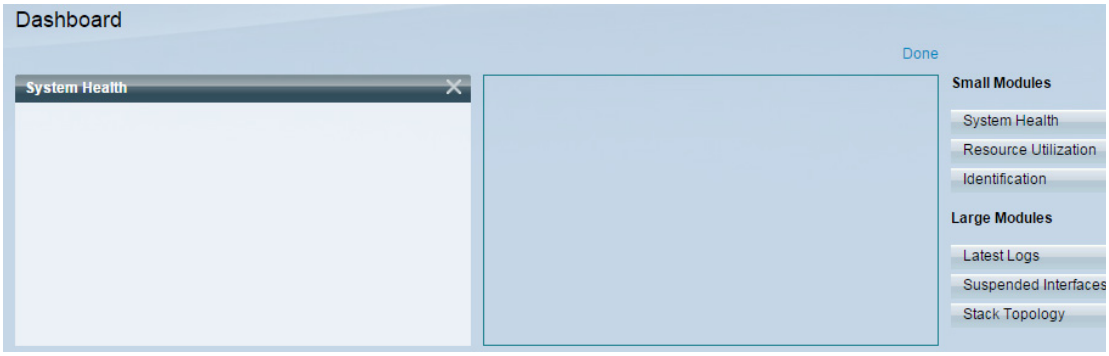
Les sujets suivants sont abordés dans ce chapitre :

- Gestion de la grille
- Intégrité du système
- Utilisation des ressources
- Identification
- Utilisation du port
- Utilisation du PoE
- Derniers journaux
- Interfaces suspendues
- Topologie de la pile
- Erreurs de trafic

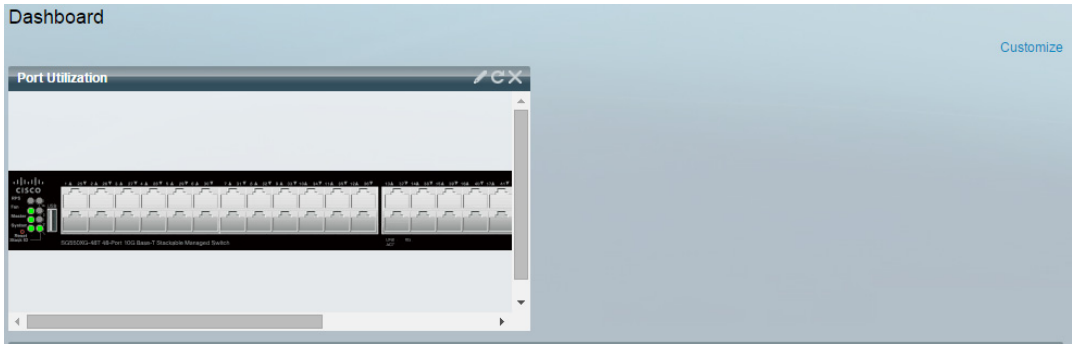
Gestion de la grille

Le tableau de bord se compose de plusieurs modules, mais vous ne pouvez afficher qu'un sous-ensemble des modules simultanément.

Lorsque vous ouvrez le tableau de bord, une vue quadrillée s'affiche, comme illustré ci-dessous (seules 2 cases sont présentées dans cette figure) :



Pour afficher des modules qui ne le sont pas encore, cliquez sur **Personnaliser** en haut à droite du tableau de bord, comme illustré ci-dessous :



Pour ajouter des modules, sélectionnez-en un dans la liste de droite, puis déplacez-le vers un point quelconque de la grille.

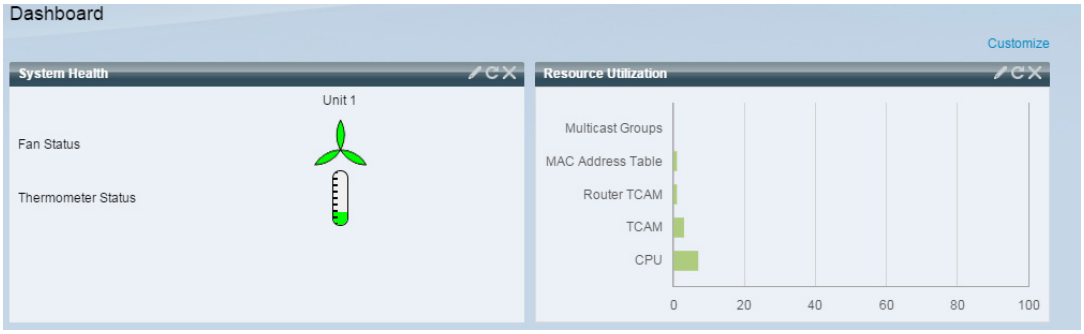
Les modules sont divisés en groupes, spécifiés ci-dessous :

- Les **petits modules** n'occupent qu'une seule case.
- Les **grands modules** peuvent occuper jusqu'à deux cases.

Si vous faites glisser un module vers un point de la grille déjà occupé, le nouveau module remplace l'existant.

Vous pouvez repositionner les modules dans la grille. Pour cela, faites glisser un module d'une position occupée vers une autre. Vous pouvez déplacer le module vers un espace inoccupé ou vers un espace occupé par un module de la même taille. Si l'espace sélectionné est occupé, les modules changent de place.

Lorsque vous cliquez sur **Terminé** à la droite de l'écran, les informations pertinentes sont insérées dans les modules, comme illustré ci-dessous :



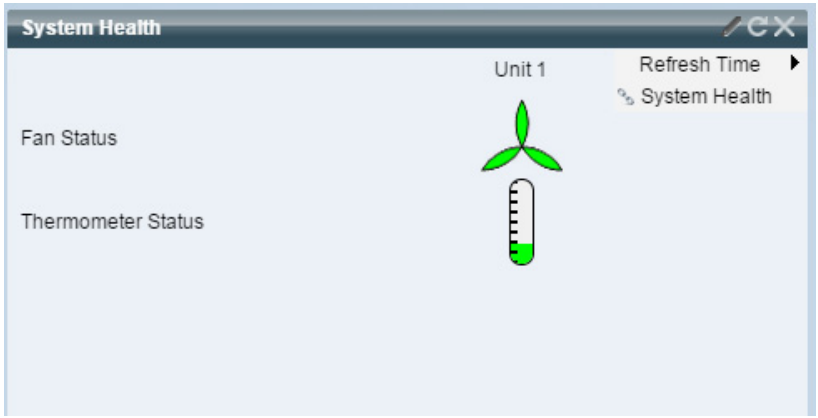
Pour chaque module, une barre de titre ainsi que trois boutons sont affichés : 

Ces boutons permettent d'effectuer les actions suivantes :

- Stylo  : ouvre les options de configuration (en fonction du module).
- Actualiser  : actualise les informations.
- X : supprime le module du tableau de bord.

Intégrité du système

Si celles-ci sont disponibles, ce module affiche des informations sur la température d'un appareil autonome ou de chaque appareil de la pile, comme illustré ci-dessous :



Les icônes suivantes sont affichées :

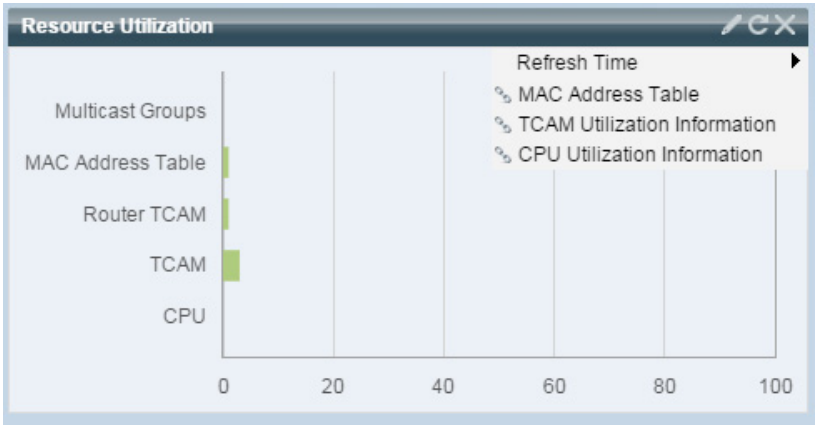
- **État du ventilateur** : jaune si un ventilateur est en panne et est remplacé par le ventilateur redondant ; vert si le ventilateur est opérationnel et rouge s'il est défectueux.
- **État du thermomètre**
  - *La température est satisfaisante* : verte lorsque le thermomètre est presque vide.
  - *La température génère un avertissement* : jaune lorsque le thermomètre est à moitié plein.
  - *La température est critique* : rouge lorsque le thermomètre est plein.

Les options de configuration suivantes (l'icône du stylo située dans le coin supérieur droit) sont disponibles :

- **Délai d'actualisation** : sélectionnez l'une des options affichées.
- **Intégrité du système** : cliquez sur cette option pour ouvrir la page Intégrité et alimentation.

Utilisation des ressources

Ce module affiche le taux d'utilisation des ressources système (en pourcentage) sous forme de graphique à barres comme indiqué ci-dessous :



Les ressources gérées sont les suivantes :

- **Multicast Groups** (Groupes de multidiffusion) : pourcentage des groupes de multidiffusion existants par rapport au nombre maximal de groupes de multidiffusion qu'il est possible de définir.

- **MAC Address Table** (Table des adresses MAC) : pourcentage d'utilisation de la table d'adresses MAC en cours d'utilisation.
- **Router TCAM** (TCAM routeur) : taux d'utilisation du TCAM routeur, en pourcentage.
- **TCAM** : taux d'utilisation de toutes les entrées TCAM non-IP, en pourcentage.
- **CPU** (Processeur) : taux d'utilisation du processeur, en pourcentage.

Chaque barre devient rouge si le taux d'utilisation des ressources est supérieur à 80 %.

Lorsque vous placez le pointeur de la souris sur une barre du graphique, une info-bulle contenant des statistiques d'utilisation s'affiche (ressources utilisées/ressources maximales disponibles).

Les options de configuration suivantes (situées à la droite de l'écran) sont disponibles :

- **Délai d'actualisation** : sélectionnez l'une des options affichées.
- **Groupes de multidiffusion** : cliquez sur cette option pour ouvrir la page Adresse MAC de groupe.
- **Table d'adresses MAC** : cliquez sur cette option pour accéder à la page Adresses dynamiques.
- **Informations d'utilisation TCAM** : cliquez sur cette option pour ouvrir la page Utilisation de TCAM.
- **Informations d'utilisation du processeur** : cliquez sur cette option pour ouvrir la page Utilisation du processeur.

Identification

Ce module affiche des informations de base sur l'appareil et sur la pile, comme illustré ci-dessous :

Il contient les champs suivants :

- **System Description** (Description du système) : description du périphérique.
- **Host Name** (Nom d'hôte) : le nom d'hôte saisi sur la page Paramètres système ou le nom d'hôte par défaut est utilisé. Il est également possible de le spécifier dans l'Assistant de mise en route.
- **Version du micrologiciel** : version du micrologiciel exécuté sur le périphérique.
- **Adresse MAC (unité principale)** : adresse MAC de l'unité.
- **Serial Number (master unit)** (Numéro de série [unité principale]) : numéro de série de l'unité principale.
- **Emplacement du système** : saisissez l'emplacement physique du périphérique.
- **System Contact** : saisissez le nom de la personne à contacter.
- **Puissance totale disponible** : puissance électrique disponible pour le périphérique.
- **Consommation de puissance actuelle** : puissance électrique consommée par le périphérique.

Les options de configuration suivantes (situées à la droite de l'écran) sont disponibles :

- **Délai d'actualisation** : sélectionnez l'une des options affichées.
- **Paramètres système** : cliquez sur cette option pour accéder à la page Paramètres système.
- **Récapitulatif du système** : cliquez sur cette option pour accéder à la page Récapitulatif du système.

Utilisation du port

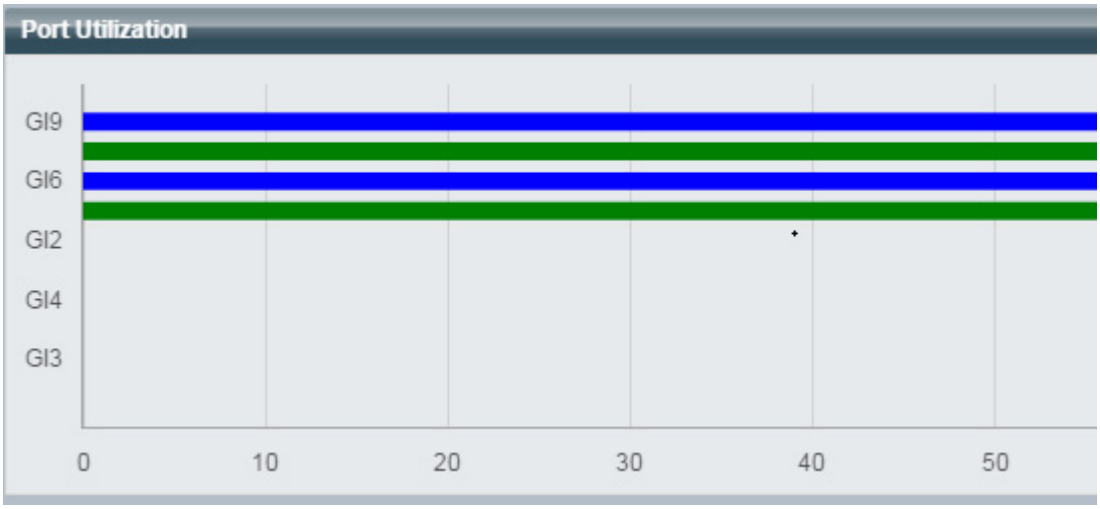
Ce module présente les ports de l'appareil sous forme de graphique ou dans une vue de l'appareil. Vous choisissez la vue dans les options de configuration (l'icône du stylo en haut à droite).

- **Mode d'affichage : appareil**

  Affiche l'appareil. Lorsque vous placez le pointeur de la souris sur un port, des informations relatives à ce port s'affichent.

- **Mode d'affichage : graphique**

  La liste des ports s'affiche. L'utilisation des ports est présentée sous forme de barres :



  Les informations suivantes sont affichées pour chaque port :

  Tx—% (vert)

  Rx—% (bleu)

- **Délai d'actualisation** : sélectionnez l'une des options affichées.
- **Statistiques de l'interface** : vous permettent d'accéder à la page **État et statistiques > Interface**.

Utilisation du PoE

Ce module présente le taux d'utilisation du PoE sous forme graphique, comme illustré ci-dessous :

Pour une unité autonome, ce module affiche une jauge dont les valeurs vont de 0 à 100. La section de la jauge entre le seuil d'interception et 100 s'affiche en rouge. Au centre de la jauge, le taux d'utilisation du PoE actuel est indiqué en watts.

Chaque barre représente un pourcentage d'utilisation du PoE pour le périphérique sur une échelle graduée de 0 à 100. Si l'utilisation du PoE excède le seuil d'interception, la barre s'affiche en rouge. Dans le cas contraire, la barre est verte.

Lorsque vous placez le pointeur de la souris sur une barre, une info-bulle s'affiche indiquant le taux d'utilisation du PoE de l'unité, en watts.

Des vues supplémentaires peuvent être sélectionnées dans les options de configuration (l'icône représentant un stylo en haut à droite).

- **Délai d'actualisation** : sélectionnez l'une des options affichées.
- **Propriétés globales PoE** : lien vers la page **Gestion des ports > PoE > Propriétés**.
- **Propriétés globales PoE** : lien vers la page **Gestion des ports > PoE > Paramètres**.

Derniers journaux

Ce module contient des informations sur les cinq derniers événements consignés par le système sous forme de journaux SYSLOG, comme illustré ci-dessous :

Les options de configuration suivantes (situées à la droite de l'écran) sont disponibles :

- **Seuil de gravité** : cette option est décrite à la section Paramètres des journaux.
- **Délai d'actualisation** : sélectionnez l'une des options affichées.
- **Afficher les journaux** : cliquez sur cette option pour ouvrir la page Mémoire RAM.

REMARQUE Pour plus d'informations, reportez-vous à l'Affichage des journaux.

Interfaces suspendues

Ce module affiche les interfaces suspendues sous forme de tableau ou dans une vue de l'appareil. Vous choisissez la vue dans les options de configuration (l'icône du stylo en haut à droite).

- **Vue Périphérique**

  Dans cette vue, l'appareil est affiché comme illustré ci-dessous :

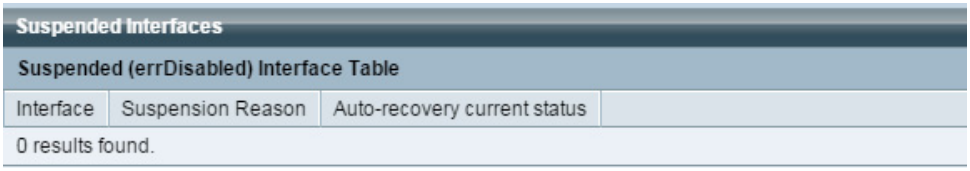
  Lorsque les unités sont connectées dans une pile, l'utilisateur peut sélectionner le périphérique à afficher dans une liste déroulante. Tous les ports suspendus dans l'appareil sont indiqués en rouge.

Lorsque vous placez le pointeur de la souris sur un port suspendu, une info-bulle contenant les informations suivantes s'affiche :

- Nom du port
- Appartenance à un LAG et identité LAG du port
- Motif de la suspension, le cas échéant

- **Vue Tableau**

  En mode d'affichage Tableau, il n'est pas nécessaire de sélectionner une unité de pile spécifique. Les informations sont affichées sous forme de tableau, comme illustré ci-dessous :



  Les champs suivants s'affichent :

  - **Interface** : port ou LAG ayant été suspendu.
  - **Suspension Reason** (Motif de la suspension) : motif pour lequel l'interface a été suspendue.
  - **Auto-recovery current status** (État de la récupération automatique) : indique si la récupération automatique a été activée pour la fonction à l'origine de la suspension.

Les options de configuration suivantes (situées à la droite de l'écran) sont disponibles :

- **Mode d'affichage** : sélectionnez la vue **Appareil** ou **Tableau**.
- **Délai d'actualisation** : sélectionnez l'une des options affichées.
- **Paramètres de reprise après erreur** : cliquez sur cette option pour accéder à la page Paramètres de reprise après erreur.

Topologie de la pile

REMARQUE L'empilage n'est pris en charge que sur les appareils des gammes SG350 (sauf Sx350) et SG550.

Ce module, qui présente la topologie de la pile sous forme graphique, dispose des mêmes fonctions que la section Vue de la topologie de la pile de l'écran Gestion des piles , comme indiqué ci-dessous :

Les champs suivants sont affichés :

- **Topologie de la pile** : les options Chaîne ou Anneau sont disponibles (consultez la page Types de topologie de la pile).
- **Unité princ. de la pile** : nombre d'unités jouant le rôle d'unité principale de la pile.

Lorsque vous placez le pointeur de la souris sur une unité, une info-bulle identifiant l'unité et contenant des informations de base sur ses ports de pile s'affiche.

Lorsque vous placez le pointeur de la souris sur une connexion de la pile dans le module, une info-bulle détaillant les unités connectées et les ports de pile générant la connexion s'affiche.

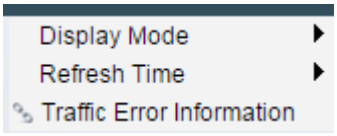
Les options de configuration suivantes (situées à la droite de l'écran) sont disponibles :

- **Gestion des piles** : cliquez sur cette option pour accéder à la page Gestion des piles.

Erreurs de trafic

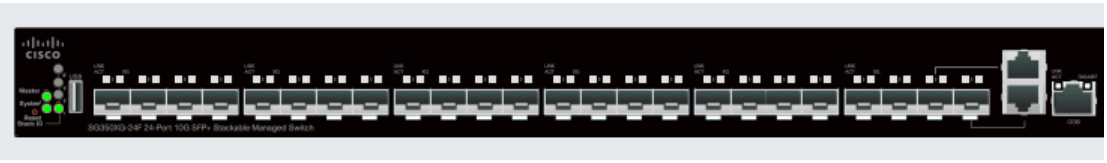
Ce module affiche le nombre de paquets d'erreurs de divers types comptabilisés dans les statistiques RMON. Vous choisissez la vue dans les options de configuration (l'icône du stylo en haut à droite).

Les éléments suivants peuvent être sélectionnés en cliquant sur l'icône représentant un stylo :



- **Mode d'affichage : appareil**

  Ce mode présente un diagramme de l'appareil, comme illustré ci-dessous :



  En mode d'empilage, l'utilisateur peut sélectionner l'appareil à afficher dans une liste déroulante. Tous les ports suspendus dans l'appareil sont indiqués en rouge.

  Lorsque vous placez le pointeur de la souris sur un port suspendu, une info-bulle contenant les informations suivantes s'affiche :

  - Nom du port
  - Appartenance à un LAG et identité LAG du port
  - Détails de la dernière erreur consignée sur le port

- **Mode d'affichage : tableau**

  - *Interface* : nom du port.
  - *Dernière erreur de trafic* : l'erreur de trafic qui a eu lieu sur un port et la dernière occurrence de cette erreur.

- **Délai d'actualisation** : sélectionnez l'un des délais d'actualisation.
- **Informations relatives aux erreurs de trafic** : cliquez pour accéder à la page Statistiques.

3

Assistants de configuration

Cette rubrique décrit les assistants de configuration suivants :

Elle couvre les sujets suivants :

- Assistant de mise en route
- Assistant de configuration des VLAN
- Assistant ACL

Assistant de mise en route

Cet assistant vous aide lors de la configuration initiale du périphérique.

ÉTAPE 1 Cliquez sur **Assistants de configuration** > **Assistant de prise en main**.

ÉTAPE 2 Cliquez sur **Launch Wizard** (Lancer l'assistant), puis sur **Next** (Suivant).

ÉTAPE 3 Renseignez les champs suivants :

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

ÉTAPE 4 Cliquez sur **Next**.

ÉTAPE 5 Renseignez les champs suivants :

- **Interface** : sélectionnez l'interface IP pour le système.
- **IP Interface Source (Source de l'interface IP)** : sélectionnez l'une des options suivantes :
  - *DHCP* : sélectionnez cette option si vous souhaitez que le périphérique reçoive son adresse IP d'un serveur DHCP.
  - *Static* (Statique) : sélectionnez cette option pour saisir manuellement l'adresse IP du périphérique.

Si vous avez sélectionné Statique comme source d'interface IP, renseignez les champs suivants :

- **IP Address** : adresse IP de l'interface.
- **Masque de réseau** : masque IP pour cette adresse.
- **Passerelle administrative par défaut** : saisissez l'adresse IP de la passerelle par défaut.
- **Serveur DNS** : saisissez l'adresse IP du serveur DNS.

ÉTAPE 6 Cliquez sur **Next** (Suivant).

ÉTAPE 7 Renseignez les champs suivants :

- **Username** (Nom d'utilisateur) : saisissez un nouveau nom d'utilisateur comportant 20 caractères maximum. Les caractères UTF-8 sont interdits.
- **Mot de passe** : saisissez un mot de passe (les caractères UTF-8 sont interdits). Si la fiabilité et la complexité du mot de passe sont définies, le mot de passe utilisateur doit être conforme à la stratégie configurée dans Sécurité du mot de passe.
- **Confirm Password** : saisissez à nouveau le mot de passe.
- **Password Strength** (Sécurité du mot de passe) : affiche le niveau de robustesse du mot de passe. Vous pouvez définir la stratégie de sécurité et de complexité du mot de passe sur la page Sécurité du mot de passe.
- **Conserver le nom d'utilisateur et le mot de passe actuels** : sélectionnez cette option pour conserver le nom d'utilisateur et le mot de passe actuels.

ÉTAPE 8 Cliquez sur **Next** (Suivant).

ÉTAPE 9 Renseignez les champs suivants :

- **Clock Source** (Source d'horloge) : sélectionnez l'une des options suivantes :
  - *Paramètres manuels* : sélectionnez cette option pour saisir l'heure système du périphérique. Si vous avez sélectionné cette option, renseignez les champs **Date** et **Time** (Heure).
  - *Default SNTP Servers* (Serveurs SNTP par défaut) : cette option permet d'utiliser les serveurs SNTP par défaut.

  REMARQUE Les serveurs SNTP par défaut sont définis par nom ; par conséquent, le serveur DNS doit être configuré et opérationnel (serveur DNS configuré et accessible). Ceci s'effectue sur la page Paramètres DNS.
  - *Serveur SNTP manuel* : sélectionnez cette option et saisissez l'adresse IP d'un serveur SNTP.

ÉTAPE 10 Cliquez sur **Next** (Suivant) pour afficher un récapitulatif de la configuration saisie.

ÉTAPE 11 Cliquez sur **Apply** (Appliquer) pour enregistrer les données de configuration.

Assistant de configuration des VLAN

Cet assistant vous aide à configurer les VLAN. Chaque fois que vous exécutez cet assistant, vous pouvez configurer l'appartenance des ports dans un seul VLAN. Commencez par configurer le mode du port de liaison (configuration des ports de liaison balisés et non balisés), puis vous passez à la configuration du mode d'accès.

ÉTAPE 1 Cliquez sur **Assistants de configuration** > **Assistant de configuration des VLAN**.

ÉTAPE 2 Cliquez sur **Launch Wizard** (Lancer l'assistant), puis sur **Next** (Suivant).

ÉTAPE 3 Sélectionnez les ports devant être configurés en tant que ports de liaison (en cliquant sur les ports requis dans l'affichage graphique). Les ports déjà configurés en tant que ports de liaison sont présélectionnés.

ÉTAPE 4 Cliquez sur **Next**.

ÉTAPE 5 Renseignez les champs suivants :

- **VLAN ID** (ID VLAN) : sélectionnez le VLAN à configurer. Vous pouvez sélectionner soit un VLAN existant soit un nouveau VLAN.
- **New VLAN ID** (ID du nouveau VLAN) : saisissez l'ID VLAN du nouveau VLAN.
- **VLAN Name** (Nom du VLAN) : saisissez le nom du VLAN (facultatif).

ÉTAPE 6 Sélectionnez les ports de liaison devant être configurés en tant que membres non balisés du VLAN (en cliquant sur les ports requis dans l'affichage graphique). Les ports de liaison qui ne sont pas sélectionnés à cette étape deviennent des membres balisés du VLAN.

ÉTAPE 7 Cliquez sur **Next**.

ÉTAPE 8 Sélectionnez les ports devant être configurés en tant que ports d'accès du VLAN. Les ports d'accès d'un VLAN sont des membres non balisés du VLAN. (Cliquez avec la souris sur les ports requis dans l'affichage graphique.)

ÉTAPE 9 Cliquez sur **Next** (Suivant) pour afficher un récapitulatif des informations saisies.

ÉTAPE 10 Cliquez sur **Appliquer**.

Assistant ACL

Pour créer une nouvelle ACL :

ÉTAPE 1 Cliquez sur **Assistants de configuration** > **Assistant ACL**.

ÉTAPE 2 Cliquez sur **Next**.

ÉTAPE 3 Renseignez les champs suivants :

- **Nom de l'ACL** : saisissez le nom de la nouvelle ACL.
- **Type d'ACL** : sélectionnez le type d'ACL : **IPv4** ou **MAC**.

ÉTAPE 4 Cliquez sur **Next**.

ÉTAPE 5 Renseignez les champs suivants :

- **Action si correspondance** : sélectionnez l'une des options suivantes :
  - *Autoriser le trafic* : réachemine les paquets qui répondent aux critères de l'ACL.
  - *Refuser le trafic* : abandonne les paquets qui répondent aux critères de l'ACL.

- *Fermer l'interface* : abandonne les paquets qui répondent aux critères de l'ACL et désactive le port sur lequel les paquets ont été reçus. Ces ports peuvent être réactivés sur la page Paramètres de reprise après erreur.

ÉTAPE 6 Pour une ACL basée sur MAC, renseignez les champs suivants :

- **Adresse MAC source** : sélectionnez *Indiffér.* si toutes les adresses source sont possibles ou *Défini par l'utilisateur* pour entrer une adresse source ou une plage d'adresses source.
- **Valeur de l'adresse MAC source** : saisissez l'adresse MAC avec laquelle l'adresse MAC source sera mise en correspondance et saisissez également, le cas échéant, son masque.
- **Source MAC Wildcard Mask** : saisissez le masque afin de définir une plage d'adresses MAC.
- **Adresse MAC de destination** : sélectionnez *Indiffér.* si toutes les adresses de destination sont possibles ou *Défini par l'utilisateur* pour entrer une adresse de destination ou une plage d'adresses de destination.
- **Valeur de l'adresse MAC de destination** : saisissez l'adresse MAC avec laquelle l'adresse MAC de destination sera mise en correspondance et saisissez également, le cas échéant, son masque.
- **Destination MAC Wildcard Mask** : saisissez le masque pour définir une plage d'adresses MAC. Veuillez noter que ce masque est différent de ceux employés à d'autres fins comme un masque de sous-réseau. Dans le cas présent, définir un bit sur **1** signifie « ignorer cette valeur » ; définir un bit sur **0** signifie « masquer cette valeur ».

  REMARQUE Prenons l'exemple d'un masque de 0000 0000 0000 0000 0000 0000 1111 1111 (ce qui signifie que vous établissez une correspondance avec les bits égaux à 0, mais pas avec ceux égaux à 1). Vous devez convertir les 1 en un entier décimal et vous remplacez chaque ensemble de quatre zéros par 0. Dans cet exemple, étant donné que 1111 1111 = 255, le masque serait : 0.0.0.255.
- **Nom de période** : si l'option **Période** est sélectionnée, choisissez la période à utiliser. Les périodes sont définies dans la section Configuration de l'heure système. Ce champ n'est affiché que si vous avez créé une période auparavant.

ÉTAPE 7 Pour une ACL basée sur IPv4, renseignez les champs suivants :

- **Protocole** : sélectionnez l'une de ces options pour créer une ACL basée sur un protocole spécifique :
  - *Tout (IP)* : sélectionnez cette option pour accepter tous les protocoles IP.
  - *TCP* : sélectionnez cette option pour accepter les paquets Transmission Control Protocol.

- *UDP* : sélectionnez cette option pour accepter les paquets User Datagram Protocol.
- *ICMP* : sélectionnez cette option pour accepter les paquets ICMP.
- *IGMP* : sélectionnez cette option pour accepter les paquets IGMP.

- **Port source pour TCP/UDP** : sélectionnez un port dans la liste déroulante.
- **Port de destination pour TCP/UDP** : sélectionnez un port dans la liste déroulante.
- **Adresse IP source** : sélectionnez *Indiffér.* si toutes les adresses source sont acceptables ou *Défini par l'utilisateur* pour entrer une adresse source ou une plage d'adresses source.
- **Valeur de l'adresse IP source** : saisissez l'adresse IP avec laquelle l'adresse IP source sera mise en correspondance.
- **Source IP Wildcard Mask** : saisissez le masque pour définir une plage d'adresses IP. Veuillez noter que ce masque est différent de ceux employés à d'autres fins comme un masque de sous-réseau. Pour un bit, 1 indique d'ignorer cette valeur, 0 indique de masquer cette valeur.
- **Adresse IP de destination** : sélectionnez *Tout* si toutes les adresses source sont acceptables ou *Défini par l'utilisateur* pour saisir une adresse source ou une plage d'adresses source.
- **Valeur de l'adresse IP de destination** : saisissez l'adresse IP avec laquelle l'adresse IP source sera mise en correspondance.
- **Destination IP Wildcard Mask** : saisissez le masque pour définir une plage d'adresses IP. Veuillez noter que ce masque est différent de ceux employés à d'autres fins comme un masque de sous-réseau. Pour un bit, 1 indique d'ignorer cette valeur, 0 indique de masquer cette valeur.
- **Nom de période** : si l'option **Période** est sélectionnée, choisissez la période à utiliser. Les périodes sont définies dans la section Configuration de l'heure système. Ce champ n'est affiché que si vous avez créé une période auparavant.

ÉTAPE 8 Cliquez sur **Next**.

ÉTAPE 9 Confirmez que vous voulez bien créer l'ACL et l'ACE.

Les détails de la règle ACL sont affichés. Vous pouvez cliquer sur **Ajouter une autre règle à cette ACL** pour ajouter une autre règle.

ÉTAPE 10 Cliquez sur **Suivant** et saisissez les informations de liaison ACL :

- **Type de liaison** : sélectionnez l'une des options suivantes pour lier l'ACL :
  - *Interfaces physiques uniquement* : liez l'ACL à un port. Dans ce cas, cliquez sur un ou plusieurs ports auxquels lier l'ACL.

- *VLAN uniquement* : liez l'ACL à un VLAN. Saisissez la liste des VLAN dans le champ **Saisissez la liste des VLAN auxquels vous voulez lier l'ACL**.
- *Aucune liaison* : ne liez pas l'ACL.

Cliquez sur **Appliquer**.

4

État et statistiques

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

Elle couvre les sujets suivants :

- Récapitulatif du système
- Utilisation du processeur
- Interface
- Etherlike
- Utilisation du port
- GVRP
- 802.1X EAP
- ACL
- Utilisation de TCAM
- Intégrité et alimentation
- Analyseur de port commuté (SPAN et RSPAN)
- Diagnostics
- RMON
- sFlow
- Affichage des journaux

Récapitulatif du système

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

Pour afficher les informations se rapportant au système, cliquez sur **État et statistiques** > **Récapitulatif du système**.

Informations système :

- **Description du système** : affiche une description du système.
- **Emplacement du système** : indique l'emplacement physique du périphérique. Cliquez sur **Edit** (Modifier) pour accéder à la page Paramètres système et saisir cette information.
- **System Contact** : nom de la personne à contacter. Cliquez sur **Edit** (Modifier) pour accéder à la page Paramètres système et saisir cette information.
- **Nom d'hôte** : nom du périphérique. Cliquez sur **Edit** (Modifier) pour accéder à la page Paramètres système et saisir cette information. Par défaut, le nom d'hôte de l'appareil se compose du mot *commutateur* concaténé avec les trois octets les moins significatifs de l'adresse MAC de l'appareil (les six chiffres hexadécimaux les plus à droite).
- **ID de l'objet système** : identification unique du fournisseur du sous-système de gestion du réseau contenu dans l'entité (utilisée dans SNMP).
- **System Uptime** : temps qui s'est écoulé depuis le dernier redémarrage.
- **Current Time** : heure actuelle du système.
- **Adresse MAC de base** : indique l'adresse MAC du périphérique. Si la pile contient plusieurs unités, l'adresse MAC de base de l'unité principale est affichée.
- **Jumbo Frames** : état de prise en charge des cadres géants. Cette prise en charge peut être activée ou désactivée via la page Paramètres des ports.

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

Informations sur le logiciel :

- **Version du microprogramme (image active)** : numéro de version du microprogramme de l'image active.

  REMARQUE Dans une pile, le numéro de version du microprogramme dépend de la version de l'unité principale.

- **Somme de contrôle MD5 du microprogramme (image active)** : somme de contrôle MD5 de l'image active.
- **Version du microprogramme (non active)** : numéro de version du microprogramme de l'image non active. Si le système appartient à une pile, la version de l'unité principale est affichée.
- **Somme de contrôle MD5 du micrologiciel (non active)** : somme de contrôle MD5 de l'image non active.

  REMARQUE Les trois champs suivants peuvent apparaître deux fois : une fois pour chaque langue sur le périphérique.

- **Paramètres régionaux** : paramètres régionaux de la première langue. (Toujours définis sur Anglais.)
- **Version de langue** : version du module linguistique de la première langue ou de la langue anglaise.
- **Total de contrôle MD5 de langue** : total de contrôle MD5 du fichier de langue.

État des services TCP/UDP :

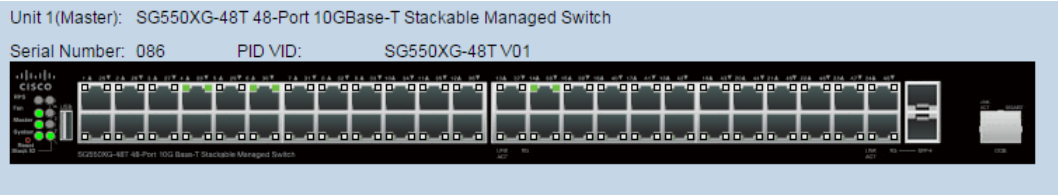
Pour réinitialiser les champs suivants, cliquez sur **Edit** (Modifier) afin d'ouvrir la page Services TCP/UDP.

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

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

- **Informations d'alimentation PoE sur l'unité principale** : cliquez sur **Détails** pour accéder directement à la page Propriétés PoE. Cette page présente les informations d'alimentation PoE relatives à chaque unité.
- **Puissance d'alimentation PoE maximale disponible (W)** : puissance maximale disponible pouvant être fournie par le commutateur.
- **Consommation totale de la puissance PoE (W)** : puissance PoE totale fournie aux périphériques PoE connectés.
- **Mode d'alimentation PoE** : limite du port ou de la classe.

L'unité principale est représentée sous forme graphique, comme illustré ci-dessous :



Placez le pointeur de la souris sur un port pour afficher son nom.

Les informations suivantes sont affichées pour chaque unité :

- **ID d'unité**
- **Numéro de série** : numéro de série.
- **PID VID** : référence de pièce et identifiant de la version.

Utilisation du processeur

Le CPU du périphérique gère les types de trafics suivants en plus du trafic de l'utilisateur final qui contrôle l'interface de gestion :

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

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

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

Pour afficher l'utilisation du CPU :

ÉTAPE 1 Cliquez sur **État et statistiques > Utilisation du processeur**.

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

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

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

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

La fenêtre affiche un graphique de l'utilisation du processeur sur l'appareil.

Interface

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

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

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

ÉTAPE 1 Cliquez sur **État et statistiques** > **Interface**.

ÉTAPE 2 Saisissez les paramètres.

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

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

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

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

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

ÉTAPE 3 Pour consulter les compteurs de statistiques dans la vue Tableau ou Graphique :

- Cliquez sur **View All Interfaces Statistics** (Voir les statistiques de toutes les interfaces) pour visualiser l'ensemble des ports dans la vue Tableau.
- Cliquez sur **Afficher le graphique de l'historique des interfaces** pour afficher ces résultats sous forme graphique. Dans cette vue, vous pouvez sélectionner l'**intervalle de temps** pour lequel les résultats seront présentés et le type de statistique à afficher. Par exemple, si vous sélectionnez les options **5 dernières minutes** et **Paquets de monodiffusion**, vous verrez combien de paquets de destination uniques ont été reçus au cours des 5 dernières minutes.

Etherlike

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

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

ÉTAPE 1 Cliquez sur **État et statistiques** > **Etherlike**.

ÉTAPE 2 Saisissez les paramètres.

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

Les champs sont affichés pour l'interface sélectionnée.

REMARQUE Si l'un des champs suivants affiche un nombre d'erreurs (pas égal à 0), l'heure de la **Dernière mise à jour** s'affiche.

- **Erreurs FCS (Frame Check Sequence)** : trames reçues ayant échoué aux contrôles de redondance cyclique (CRC).
- **Trames de collisions individuelles** : trames impliquées dans une collision individuelle, mais ayant été transmises avec succès.
- **Collisions tardives** : collisions ayant été détectées après les 512 premiers octets de données.
- **Collisions excessives** : transmissions rejetées dues à des collisions excessives.
- **Paquets de taille excessive** : paquets de plus de 2000 octets reçus.
- **Erreurs de réception MAC internes** : trames rejetées en raison d'erreurs de destination.
- **Trames de pause reçues** : trames de pause de contrôle de flux reçues. Ce champ est uniquement disponible pour les ports XG. Lorsque le débit du port est de 1G, le compteur de trames de pause reçues n'est pas opérationnel.
- **Trames de pause transmises** : trames de pause de contrôle de flux transmises à partir de l'interface sélectionnée.

ÉTAPE 3 Pour afficher les compteurs de statistiques dans une vue Tableau, cliquez sur **Voir les statistiques de toutes les interfaces** afin d'afficher l'ensemble des ports dans une vue Tableau.

Utilisation du port

La page Utilisation du port présente l'utilisation large bande (entrante et sortante) par port.

Pour afficher l'utilisation du port :

ÉTAPE 1 Cliquez sur **État et statistiques** > **Utilisation du port**.

ÉTAPE 2 Saisissez la **Fréqu. d'actualisation**, qui correspond à la durée qui s'écoule avant l'actualisation des statistiques de l'interface Ethernet.

Les champs suivants s'affichent pour chaque port :

- **Interface** : nom du port.
- **Utilisation de la transmission** : quantité de bande passante utilisée par les paquets sortants.
- **Utilisation de la réception** : quantité de bande passante utilisée par les paquets entrants.

Pour afficher un graphique sur l'historique de l'utilisation du port, sélectionnez un port et cliquez ensuite sur l'option **Afficher le graphique de l'historique des interfaces**. En plus de cette option, le champ suivant apparaît :

- **Intervalle de temps** : sélectionnez une unité de temps. Le graphique affiche l'utilisation du port dans cette unité de temps.

GVRP

La page GVRP affiche des informations sur les trames du protocole GVRP (GARP VLAN Registration Protocol) qui ont été envoyées ou reçues depuis un port. GVRP est un protocole réseau de couche 2 basé sur des normes permettant la configuration automatique des informations VLAN sur les commutateurs. Il est défini dans l'amendement 802.1ak apporté à la norme 802.1Q-2005.

Les statistiques GVRP d'un port ne s'affichent que si GVRP est activé globalement et sur le port. Reportez-vous à la page Paramètres GVRP.

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

ÉTAPE 1 Cliquez sur **État et statistiques** > **GVRP**.

ÉTAPE 2 Saisissez les paramètres.

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

Le pavé comptabilisant les attributs affiche les compteurs de différents types de paquets par interface. Ces options sont affichées pour les paquets **reçus** et **transmis**.

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

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

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

ÉTAPE 3 Pour gérer les compteurs de statistiques, cliquez sur **Voir les statistiques de toutes les interfaces** afin d'afficher l'ensemble des ports sur une seule et même page.

802.1X EAP

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

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

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

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

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

Les valeurs sont affichées pour l'interface sélectionnée.

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

- **Trames de demandeur EAPOL EAP transmises** : trames de demandeur EAPOL EAP transmises sur le port.
- **Trames de début EAPOL transmises** : trames de début EAPOL qui ont été transmises sur le port.
- **Trames de déconnexion EAPOL transmises** : trames de déconnexion EAPOL qui ont été transmises sur le port.
- **Trames d'annonce EAPOL transmises** : trames d'annonce EAPOL qui ont été transmises sur le port.
- **Trames de demande d'annonce EAPOL transmises** : trames de demande d'annonce EAPOL qui ont été transmises sur le port.
- **Trames d'authentificateur EAPOL EAP transmises** : trames d'authentificateur EAP qui ont été transmises sur le port.
- **Trames EAPOL MKA transmises sans CKN** : trames MKA sans CKN qui ont été transmises sur ce port.

ÉTAPE 4 Pour effacer les compteurs de statistiques :

- Cliquez sur **View All Interfaces Statistics** (Voir les statistiques de toutes les interfaces) pour afficher les compteurs de l'ensemble des interfaces.
- Cliquez sur **Clear Interface Counters** (Effacer les compteurs de l'interface) pour effacer les compteurs de l'ensemble des interfaces.

ACL

Lorsque la fonctionnalité de journalisation ACL est activée, un message d'information SYSLOG est généré pour les paquets qui correspondent aux règles ACL.

Pour voir les interfaces sur lesquelles les paquets ont été transférés ou rejetés sur la base de listes ACL :

ÉTAPE 1 Cliquez sur **État et statistiques** > **ACL**.

ÉTAPE 2 Sélectionnez la **fréquence d'actualisation**, à savoir la durée en secondes qui s'écoule avant l'actualisation de la page. Un nouveau groupe d'interfaces est créé pour chaque période.

Les informations suivantes sont affichées :

- **Global Trapped Packet Counter** (Compteur de paquets interrompus globalement) : nombre de paquets filtré globalement en raison d'un manque de ressources.
- **Paquets filtrés en fonction du port/LAG** : interfaces sur lesquelles les paquets ont été transférés ou rejetés en fonction des règles ACL.
- **Paquets filtrés en fonction du VLAN** : VLAN sur lesquels les paquets ont été transférés ou rejetés en fonction des règles ACL.

ÉTAPE 3 Cliquez sur **Effacer les compteurs** pour effacer les compteurs de statistiques de l'ensemble des interfaces.

Utilisation de TCAM

La mémoire TCAM contient les règles produites par d'autres applications, telles que les règles ACL (listes de contrôle d'accès) et les règles QoS (Qualité de service), tandis que la TCAM du routeur contient les règles de routage IP et les règles créées par l'utilisateur.

Certaines applications attribuent des règles lors de leur mise en œuvre. En outre, les processus qui s'initialisent lors du démarrage système utilisent une partie de leurs règles lors de ce processus de démarrage.

Pour afficher l'utilisation de la mémoire TCAM, cliquez sur **État et statistiques** > **Utilisation de TCAM**.

La page TCAM Utilization (Utilisation de TCAM) répertorie les champs suivants :

- **N° d'unité** : unité de la pile pour laquelle le taux d'utilisation TCAM s'affiche. Ce champ n'est pas affiché lorsque le périphérique n'appartient pas à une pile.
- **Maximum TCAM Entries for Routing and Multicast Routing** (Entrées TCAM maximales pour routage et routage de multidiffusion) : entrées TCAM de routeur maximales disponibles pour le routage et le routage de multidiffusion.
- **Routage IPv4**
  - *Utilisé* : nombre d'entrées TCAM de routeur utilisées pour le routage IPv4.
  - *Maximum* : nombre d'entrées TCAM de routeur disponibles pouvant être utilisées pour le routage IPv4.

- **Routage de multidiffusion IPv4**
  - *Utilisé* : nombre d'entrées TCAM de routeur utilisées pour le routage multidestination IPv4.
  - *Maximum* : nombre d'entrées TCAM de routeur disponibles pouvant être utilisées pour le routage multidestination IPv4.
- **Routage basé sur des stratégies IPv4**
  - *Utilisé* : nombre d'entrées TCAM de routeur utilisées pour le routage en fonction de la stratégie IPv4.
  - *Maximum* : nombre d'entrées TCAM de routeur disponibles pouvant être utilisées pour le routage en fonction de la stratégie IPv4.
- **Routage IPv6**
  - *Utilisé* : nombre d'entrées TCAM de routeur utilisées pour le routage multidestination IPv6.
  - *Maximum* : nombre d'entrées TCAM de routeur disponibles pouvant être utilisées pour le routage multidestination IPv6.
- **Routage de multidiffusion IPv6** : nombre d'entrées TCAM de routeur utilisées pour le routage IPv6.
  - *Utilisé* : nombre d'entrées TCAM de routeur utilisées pour le routage IPv6.
  - *Maximum* : nombre d'entrées TCAM de routeur disponibles pouvant être utilisées pour le routage IPv6.
- **Routage basé sur des stratégies IPv6**
  - *Utilisé* : nombre d'entrées TCAM de routeur utilisées pour le routage en fonction de la stratégie IPv6.
  - *Maximum* : nombre d'entrées TCAM de routeur disponibles pouvant être utilisées pour le routage en fonction de la stratégie IPv6.
- **Mise en correspondance de VLAN**
  - *Utilisé* : nombre d'entrées TCAM de routeur utilisées actuellement pour la mise en correspondance de VLAN.
  - *Maximum* : nombre d'entrées TCAM de routeur disponibles pouvant être utilisées pour la mise en correspondance de VLAN.
- **Nombre maximum d'entrées TCAM pour les règles non IP** : nombre maximum d'entrées TCAM de routeur pouvant être utilisées pour des règles non IP.

- **Règles non-IP**
  - *Utilisé* : nombre d'entrées TCAM utilisées pour les règles non IP.
  - *Maximum* : nombre d'entrées TCAM disponibles pouvant être utilisées par les règles non IP.

Pour savoir comment modifier l'attribution en fonction des divers processus, consultez la section Ressources de routage.

Intégrité et alimentation

La page **Intégrité et alimentation** permet de gérer l'état de la température, de l'alimentation et du ventilateur sur tous les périphériques appropriés. Selon le modèle, un périphérique possède un ou plusieurs ventilateurs. Certains modèles ne possèdent aucun ventilateur.

Alimentation redondante

Cette fonctionnalité n'est prise en charge que sur les modèles de la série SG550.

L'alimentation redondante 2300 prend le relais de l'alimentation CA en cas de besoin. Elle fournit de l'énergie à l'appareil si l'alimentation CA tombe en panne. Elle n'est prise en charge que sur les appareils de la gamme 550.

Si vous devez basculer vers l'alimentation de secours, l'appareil change de source d'énergie sans redémarrage et sans interruption de fonctionnement. L'appareil interroge l'état de l'alimentation redondante toutes les secondes. Si elle fournit de l'énergie, son voyant est allumé. Si elle est active, un message SYSLOG est généré.

Lorsque l'alimentation principale est à nouveau opérationnelle, l'appareil indique à l'alimentation redondante d'arrêter de fournir de l'énergie. Un message SYSLOG est alors généré.

Le voyant de l'alimentation redondante (sur la façade de l'appareil) indique l'état actuel :

- Éteint : l'alimentation redondante n'est pas connectée
- Vert (fixe) : l'alimentation redondante est prête à l'emploi
- Orange (clignotant) : l'alimentation redondante fournit actuellement de l'énergie à l'appareil
- Orange (fixe) : l'alimentation redondante est connectée, mais fournit déjà de l'énergie à deux autres appareils. Dans ce cas, elle ne pourra pas alimenter un appareil supplémentaire

Ventilateurs

Sur certains périphériques, les ventilateurs sont obligatoires pour assurer un bon fonctionnement. En effet, sans eux, le périphérique chauffe trop et s'éteint automatiquement. Le ventilateur étant un composant mobile, il est sujet aux pannes. Un ventilateur redondant est donc installé dans le système. Il ne fonctionne pas, à moins qu'un ou plusieurs ventilateurs tombent en panne. Dans ce cas, il intègre l'environnement de surveillance du périphérique.

Il est recommandé de faire fonctionner le ventilateur redondant au moins 1 minute par jour.

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

Événement	Action
Au moins un capteur de température dépasse le seuil d'avertissement	Les actions suivantes sont générées : • Message SYSLOG • Message « trap » SNMP
Au moins un capteur de température dépasse le seuil critique	Les actions suivantes sont générées : • Message SYSLOG • Message « trap » SNMP Les actions suivantes sont générées : • La LED système s'allume en orange fixe (si le matériel la prend en charge). • Les ports sont désactivés : lorsque la température critique dépasse deux minutes, tous les ports sont arrêtés. • Sur les périphériques qui prennent PoE en charge, les circuits PoE sont désactivés pour abaisser la consommation d'énergie et diminuer la chaleur émise.

Événement	Action
La période de refroidissement qui suit le seuil critique a été dépassée (tous les capteurs indiquent une valeur inférieure de 2 °C au seuil d'avertissement)	Lorsque tous les capteurs ont atteint une valeur inférieure de 2 °C au seuil d'avertissement, le PHY est réactivé et tous les ports sont rétablis. Si l'état du ventilateur est OK, les ports sont activés. Sur les périphériques qui prennent PoE en charge, les circuits PoE sont activés.

Champs Intégrité et alimentation

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

REMARQUE Seuls les champs pertinents pour l'appareil sont affichés.

Cette section affiche l'énergie économisée par le périphérique grâce aux fonctionnalités Green Ethernet et Désactivation des voyants, ainsi qu'en raison de l'inactivité des ports (inactivité physique ou consécutive aux paramètres de plage horaire).

Le champ Économies PoE affiche l'énergie totale économisée en utilisant la fonction de plage horaire PoE qui coupe l'alimentation PoE des ports à des heures spécifiques (généralement lorsque l'élément de réseau PoE n'est pas utilisé).

Les informations suivantes sont affichées (l'ordre des champs peut varier en fonction du périphérique) :

Économies d'énergie

- **Économies d'énergie en cours sur les ports et Green Ethernet** : économies d'énergie en cours sur tous les ports.
- **Économies d'énergie cumulées sur les ports et Green Ethernet** : économies d'énergie cumulées sur tous les ports depuis la mise sous tension du périphérique.
- **Économies d'énergie annuelles prévues sur les ports et Green Ethernet** : prévision des économies d'énergie qui seront réalisées sur le périphérique au cours d'une année. Cette valeur est calculée sur la base des économies réalisées au cours de la semaine écoulée.
- **Économies d'énergie PoE en cours** : quantité d'énergie PoE économisée actuellement sur les ports auxquels sont connectés des appareils alimentés et sur lesquels l'alimentation PoE n'est pas opérationnelle en raison de la fonctionnalité Plage horaire.

- **Économies d'énergie PoE cumulées** : économies d'énergie PoE cumulées, depuis la mise sous tension du périphérique, réalisées sur les ports auxquels sont connectés des appareils alimentés et sur lesquels l'alimentation PoE n'est pas opérationnelle en raison de la fonctionnalité Plage horaire.
- **Économies d'énergie PoE annuelles prévues** : prévision des économies d'énergie PoE qui seront réalisées annuellement sur les ports auxquels sont connectés des appareils alimentés et sur lesquels l'alimentation PoE n'est pas opérationnelle en raison de la fonctionnalité Plage horaire. Cette valeur est calculée sur la base des économies réalisées au cours de la semaine écoulée.

(Pour les familles de dispositifs non-XG) Pour planifier le fonctionnement de l'alimentation pour une plage horaire spécifique, cliquez sur les liens de couleur bleue dans la phrase suivante sur la page : « Vous pouvez augmenter les économies d'énergie en utilisant une Plage horaire afin de planifier les opérations PoE et données ». Les pages suivantes s'affichent :

- **Plage horaire** : la page **Administration > Paramètres d'heure > Plage horaire** s'affiche. Définissez la plage horaire relative aux opérations d'alimentation.
- **Données** : la page **Gestion des ports > Paramètres des ports** s'affiche. Reliez la plage horaire à un ou plusieurs ports :
- **PoE** : la page **Gestion des ports > PoE > Paramètres** s'affiche. Reliez la plage horaire aux opérations PoE sur un ou plusieurs ports :

Si le périphérique fait partie d'une pile, la page Intégrité et alimentation affiche les champs suivants :

Table d'intégrité

- **N° d'unité** : affiche le numéro d'unité dans la pile.
- **Fan Status** (État du ventilateur) : les valeurs suivantes sont disponibles :
  - *OK* : le ventilateur fonctionne normalement.
  - *Échec* : plus d'un ventilateur ne fonctionne pas correctement.
  - *S/O* : le ventilateur n'est pas applicable au modèle en question.
- **État du ventilateur redondant** : les valeurs suivantes sont disponibles :
  - *Ready* (Prêt) : le ventilateur redondant est opérationnel, mais n'est pas requis.
  - *Actif* : l'un des principaux ventilateurs ne fonctionne pas et doit être remplacé.

- **Température** : les options sont les suivantes :
  - *OK* : la température est inférieure au seuil d'avertissement.
  - *Avertissement* : la température est comprise entre le seuil d'avertissement et le seuil critique.
  - *Critique* : la température est supérieure au seuil critique.
  - *N/A* (S/O) : non applicable.

  État de l'alimentation principale (ces champs sont affichés pour les appareils alimentés et ceux qui prennent en charge une alimentation redondante)

  - **État de l'alimentation principale** : affiche l'une des options suivantes pour l'alimentation principale :

    Active : l'alimentation est utilisée.

    Échec : l'alimentation principale a échoué.
  - **Consommation de l'alimentation principale** : quantité d'énergie que l'alimentation principale peut allouer au fonctionnement du PSE.
  - **État de l'alimentation redondante** : affiche l'une des options suivantes pour l'alimentation de secours :

    Active : l'alimentation est utilisée.

    Disponible : la source d'alimentation redondante est connectée, mais pas utilisée.

    Non disponible : l'alimentation redondante est connectée, mais alimente déjà d'autres appareils.

    Non connecté : la source d'alimentation redondante n'est pas connectée.
  - **Consommation de l'alimentation redondante** : quantité d'énergie que l'alimentation de secours peut allouer au fonctionnement du PSE.

  État de l'alimentation PoE (il peut y avoir jusqu'à 2 appareils alimentés)

  - *ID du port d'appareil alimenté 1* : numéro du port d'appareil alimenté 1
  - *Mode de négociation du port 1 de l'appareil alimenté* : mode de négociation (voir la définition ci-dessous)
  - *État du port d'appareil alimenté 1* : indique s'il est connecté ou pas
  - *Type de port d'appareil alimenté 1* : type d'appareil alimenté

- *Consommation du port d'appareil alimenté 1* : quantité maximale d'énergie qui peut être allouée au fonctionnement du PSE
- *ID du port d'appareil alimenté 2* : numéro du port d'appareil alimenté 1
- *Mode de négociation du port 2 de l'appareil alimenté* : mode de négociation (voir la définition ci-dessous)
- *État du port d'appareil alimenté 2* : indique s'il est connecté ou pas
- *Type de port d'appareil alimenté 2* : type d'appareil alimenté
- *Consommation du port d'appareil alimenté 2* : quantité maximale d'énergie qui peut être allouée au fonctionnement du PSE

Si le périphérique ne fait pas partie d'une pile, la page Intégrité et alimentation affiche les champs suivants :

- **Fan Status** (État du ventilateur) : les valeurs suivantes sont disponibles :
  - *OK* : le ventilateur fonctionne normalement.
  - *Failure* (Échec) : le ventilateur ne fonctionne pas correctement.
  - *S/O* : l'ID du ventilateur n'est pas applicable au modèle en question.
- **État du ventilateur redondant** : les valeurs suivantes sont disponibles :
  - *Ready* (Prêt) : le ventilateur redondant est opérationnel, mais n'est pas requis.
  - *Actif* : l'un des principaux ventilateurs ne fonctionne pas et doit être remplacé.
  - *Échec* : les ventilateurs standard sont en panne et le ventilateur redondant ne fonctionne pas correctement.
- **Température** : les options sont les suivantes :
  - *OK* : la température est inférieure au seuil d'avertissement.
  - *Avertissement* : la température est comprise entre le seuil d'avertissement et le seuil critique.
  - *Critique* : la température est supérieure au seuil critique.
  - *N/A* (S/O) : non applicable.

État de l'alimentation principale (ces champs sont affichés pour les appareils alimentés et les périphériques prenant en charge une alimentation redondante)

- **État de l'alimentation** : les options sont les suivantes :
  - *Main* (Principale) : affiche l'une des valeurs suivantes :

    Actif : l'alimentation est utilisée.

    Échec : l'alimentation principale a échoué.
  - *Redondant* : état de l'alimentation redondante. Les options suivantes sont disponibles :

    Active : l'alimentation redondante (RPS) est utilisée.

    Disponible : l'alimentation redondante est connectée, mais n'est pas utilisée.

    Non disponible : l'alimentation redondante est connectée, mais alimente déjà d'autres périphériques.

    Non connecté : l'alimentation redondante n'est pas connectée.

    Présent : l'alimentation redondante est connectée.

Tableau d'alimentation Ethernet (s'affiche uniquement si l'une des unités de la pile prend en charge des ports d'appareils alimentés). Les champs suivants s'affichent :

- **Port** : numéro du port.
- **État de l'appareil alimenté** : affiche l'une des valeurs suivantes :
  - *Connecté* : le port de l'appareil alimenté est connecté à un périphérique PSE qui fournit de l'énergie.
  - *Non connecté* : le port de l'appareil alimenté n'est pas connecté à un périphérique PSE.
- **Mode de négociation** : une des valeurs suivantes :
  - *Auto* : le mode de négociation CDP ou LLDP est utilisé pour déterminer le niveau de puissance.
  - *Forcer 802.3AF* : la norme d'alimentation AF est utilisée des deux côtés.
  - *Forcer 802.3AT* : la norme d'alimentation AT est utilisée des deux côtés.
  - *Forcer 60W* : une puissance de 60 W est utilisée des deux côtés.
- **Réserve d'énergie** : puissance réellement allouée au port.

Analyseur de port commuté (SPAN et RSPAN)

La fonctionnalité SPAN, parfois appelée mise en miroir de ports ou surveillance de ports, sélectionne le trafic réseau qu'un analyseur de réseau est chargé d'étudier. Cet analyseur de réseau peut être un dispositif Cisco SwitchProbe ou une autre sonde de contrôle à distance (RMON).

La mise en miroir des ports est utilisée sur un dispositif réseau pour envoyer une copie des paquets réseau détectés sur un port de périphérique unique, sur plusieurs ports de périphérique ou sur l'intégralité d'un VLAN vers une connexion de contrôle réseau située sur un autre port du périphérique. Cette opération est souvent utilisée lorsqu'une surveillance du trafic réseau (pour un système de détection des intrusions, par exemple) est requise. Un analyseur de réseau, connecté au port de surveillance, traite les paquets de données.

Le périphérique peut mettre en miroir jusqu'à huit interfaces par session.

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 filtré ou abandonné. Les paquets envoyés par l'appareil sont mis en miroir lorsque la mise en miroir des émissions est activée.

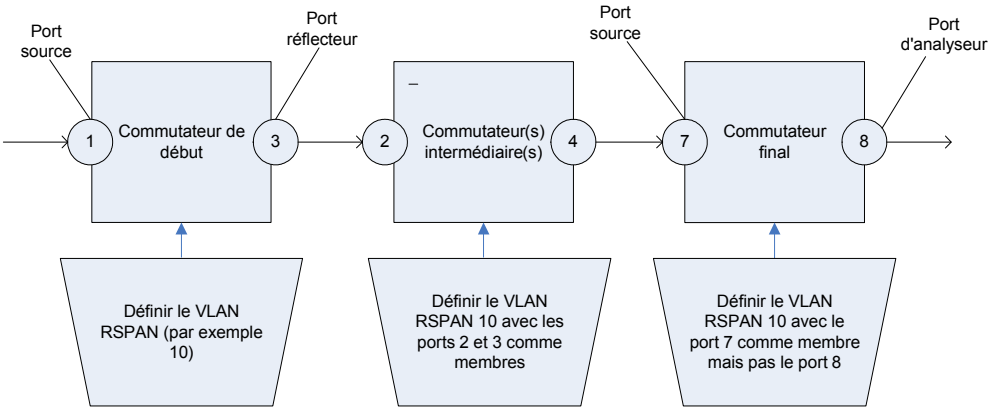
La mise en miroir ne garantit pas que l'ensemble du trafic en provenance du ou des ports source sera reçu sur le port de l'analyseur (de destination). Si le port de l'analyseur reçoit plus de données qu'il ne peut en gérer, une partie de ces données risque d'être perdue.

La mise en miroir VLAN ne peut pas être active sur un VLAN qui n'a pas été créé manuellement. Par exemple, si le VLAN 23 a été créé par GVRP, la mise en miroir de ports ne fonctionnera pas.

RSPAN (Remote SPAN)

RSPAN étend la fonction SPAN en activant le contrôle de plusieurs commutateurs de votre réseau et en autorisant la définition du port de l'analyseur sur un commutateur distant. Outre les commutateurs de début (source) et de fin (destination), vous pouvez définir des commutateurs intermédiaires sur lesquels circule le trafic, comme le montre la Figure 1.

Figure 1 Déploiement de commutateurs RSPAN :



Le trafic de chaque session RSPAN transite par un VLAN RSPAN spécifié par l'utilisateur, lequel est dédié à cette session dans tous les commutateurs participants. Le trafic en provenance des interfaces source sur le périphérique de début est copié sur le VLAN RSPAN via un port réflecteur, puis acheminé via des ports de liaison sur les périphériques intermédiaires vers la session de destination sur le commutateur final, lequel surveille le VLAN RSPAN.

Le port réflecteur est le mécanisme chargé de copier les paquets sur un VLAN RSPAN. Il s'agit d'un port réseau qui traite les différents types de trafic.

Le VLAN RSPAN doit être configuré sur tous les commutateurs intermédiaires.

REMARQUE RSPAN ne copie pas toujours tous les paquets qui proviennent de plusieurs sources simultanément. Si une surveillance précise s'avère indispensable, vous pouvez recourir à la stratégie de mise en miroir basée sur TCAM.

Flux de travail RSPAN

Le flux de travail ci-dessous décrit la configuration des commutateurs de début, intermédiaires et de fin :

- Commutateur de début
- Commutateur(s) intermédiaire(s)
- Commutateur final

Commutateur de début

1. Définissez le VLAN RSPAN. Ce VLAN doit être identique dans tous les commutateurs.
2. Définissez une ou plusieurs interfaces source, qui peuvent être des ports ou un VLAN, et assurez-vous qu'il ne s'agit **pas** d'un membre du VLAN RSPAN.
3. Définissez un port réflecteur (destination, port de sortie) et assurez-vous qu'il ne s'agit pas d'un membre du VLAN RSPAN.
4. Définissez le type de destination sur VLAN distant.
5. Définissez le trafic réseau sur Activer.

Commutateur(s) intermédiaire(s)

1. Définissez le VLAN RSPAN. Ce VLAN RSPAN doit être identique dans les commutateurs de début, intermédiaires et de fin.
2. Assurez-vous qu'au moins deux ports sont membres du VLAN RSPAN. Le trafic va transiter par le commutateur via le VLAN RSPAN.

Commutateur final

1. Définissez le VLAN RSPAN. Ce VLAN RSPAN doit être identique dans les commutateurs de début, intermédiaires et de fin.
2. Assurez-vous que le port source, qui est connecté au commutateur intermédiaire, est membre du VLAN RSPAN.
3. Définissez l'interface source sur VLAN distant.
4. Définissez un port de destination et assurez-vous qu'il ne se trouve pas dans le VLAN RSPAN.
5. Définissez le type de destination sur Interface locale.

VLAN RSPAN

Un VLAN RSPAN doit être défini sur les commutateurs de début, intermédiaires et de fin.

Pour configurer un VLAN comme VLAN RSPAN :

ÉTAPE 1 Cliquez sur **État et statistiques** > **SPAN et RSPAN > VLAN RSPAN**.

Le VLAN RSPAN défini précédemment est affiché.

ÉTAPE 2 Pour configurer un VLAN comme VLAN RSPAN, sélectionnez-le dans la liste déroulante **VLAN RSPAN**.

ÉTAPE 3 Cliquez sur **Appliquer**.

Destinations de sessions SPAN

Un port de destination doit être configuré sur les commutateurs de début et de fin. Sur le périphérique de début, il s'agit du port réflecteur. Sur le périphérique de fin, il s'agit du port analyseur.

Procédure d'ajout d'un port de destination :

ÉTAPE 1 Cliquez sur **État et statistiques > SPAN & RSPAN > SPAN Destinations de sessions**.

Les destinations définies précédemment sont affichées.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants :

- **ID de session** : sélectionnez un ID de session. Il doit correspondre aux ID de session des ports source.
- **Type de destination** : sélectionnez l'une des options suivantes :
  - *Interface locale* : il s'agit du port de destination sur le même périphérique que les ports source (concerne SPAN).
  - *VLAN distant* : il s'agit du port de destination sur un périphérique différent du port source (concerne RSPAN).

  Si le **Type de destination** est défini sur **VLAN distant**, configurez les champs suivants :

  - *Port réflecteur* : sélectionnez une unité/un port qui fait office de port cible sur le premier périphérique.

  Si le **Type de destination** est défini sur **Interface locale**, configurez le champ suivant :

  - *Port* : sélectionnez une unité/un port qui fait office de port analyseur sur le premier périphérique.
- **Trafic réseau** : sélectionnez cette option pour autoriser le trafic autre que celui contrôlé sur le port.

ÉTAPE 4 Cliquez sur **Appliquer**.

Sources de sessions SPAN

Une ou plusieurs sources SPAN ou RSPAN peuvent être configurées sur les périphériques de début et de fin.

Pour configurer les ports source à mettre en miroir :

ÉTAPE 1 Cliquez sur **État et statistiques** > **SPAN et RSPAN > Sources de sessions**.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Sélectionnez le numéro de session dans **ID de session**. Il doit être identique pour tous les ports source et pour le port de destination.

ÉTAPE 4 Pour SPAN ou RSPAN sur le commutateur de début, sélectionnez l'unité et le port ou le VLAN à partir desquels le trafic est contrôlé (**Interface source**). Sur le commutateur de fin, pour RSPAN, sélectionnez **VLAN distant**.

ÉTAPE 5 Dans le champ **Surveiller le type**, indiquez si le trafic entrant, le trafic sortant ou les deux sont mis en miroir.

- *Émission et réception* : mise en miroir des ports sur les paquets entrants et sortants.
- *Rx* : mise en miroir des ports sur les paquets entrants.
- *Tx* : mise en miroir des ports sur les paquets sortants.

ÉTAPE 6 Cliquez sur **Appliquer**. L'interface source pour la mise en miroir est configurée.

Diagnostics

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

Elle couvre les sujets suivants :

- Tests des ports en cuivre
- État des modules optiques
- Informations d'assistance technique

Tests des ports en cuivre

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

VCT réalise deux types de tests :

- La technologie de réflectométrie à dimension temporelle (TDR, Time Domain Reflectometry) teste la qualité et les caractéristiques d'un câble en cuivre relié à un port. Il est possible de tester des câbles faisant jusqu'à 140 mètres de long. Ces résultats apparaissent dans le bloc Résultats de test de la page Test cuivre.
- Les tests s'appuyant sur la technologie DSP sont effectués sur des liaisons XG actives pour en mesurer la longueur de câble. Ces résultats apparaissent dans le bloc Informations avancées de la page Test cuivre. Ce test peut être exécuté uniquement lorsque la vitesse de liaison est de 10G.

Conditions préalables à l'exécution du test des ports cuivre

Avant d'exécuter le test, procédez comme suit :

- (Obligatoire) Désactivez le mode Short Reach (Courte portée) (reportez-vous à la page Propriétés).
- (Facultatif) Désactivez EEE (reportez-vous à la page Propriétés).

Utilisez un câble de données CAT6a pour exécuter le test de tous les câbles (VCT).

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

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

Pour tester les câbles en cuivre reliés aux ports :

ÉTAPE 1 Cliquez sur **État et statistiques** > **Diagnostics** > **Test cuivre**.

ÉTAPE 2 Sélectionnez l'unité/le port sur lequel vous souhaitez exécuter le test.

ÉTAPE 3 Cliquez sur **Copper Test**.

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

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

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

Le bloc **Advanced Information** (Informations avancées) contient les informations suivantes, qui sont actualisées chaque fois que vous accédez à la page :

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

État des modules optiques

La page État des modules optiques affiche les conditions de fonctionnement signalées par l'émetteur-récepteur SFP (Small Form-factor Pluggable).

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.

Les émetteurs-récepteurs SFP+ XG (10 000 Mbit/s) suivants sont pris en charge :

- Cisco SFP-10GSR
- Cisco SFP-10GLRM
- Cisco SFP-10GLR

Les câbles passifs XG suivants (Twinax/DAC) sont pris en charge :

- Cisco SFP-H10GCU1m
- Cisco SFP-H10GCU3m
- Cisco SFP-H10GCU5m

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

Cette page affiche les champs suivants :

- **Port** : numéro du port sur lequel le SFP est connecté.
- **Description** : description de l'émetteur-récepteur optique.
- **Numéro de série** : numéro de série de l'émetteur-récepteur optique.
- **PID** : ID du VLAN.

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

Informations d'assistance technique

Cette page propose un journal détaillé de l'état de l'appareil. C'est utile quand le service d'assistance technique essaie d'aider un utilisateur à résoudre un problème, parce qu'il renvoie le résultat de plusieurs commandes (notamment la commande de débogage) avec une seule commande.

Pour consulter les informations d'assistance technique utiles à des fins de débogage :

ÉTAPE 1 Cliquez sur **État et statistiques** > **Diagnostics** > **Informations d'assistance technique**.

ÉTAPE 2 Cliquez sur **Générer**.

Des informations provenant de plusieurs commandes d'interface de ligne de commande **show** s'affichent.

REMARQUE Vous devrez peut-être patienter quelques instants avant de voir apparaître le résultat de cette commande. Une fois les informations générées, vous pouvez les copier depuis la zone de texte à l'écran en cliquant sur **Sélectionner les données d'assistance technique**.

RMON

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

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

Cette fonction vous permet de réaliser les actions suivantes :

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

Statistiques

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

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

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

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

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

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

Les statistiques suivantes sont affichées pour l'interface sélectionnée.

REMARQUE Si l'un des champs suivants affiche un nombre d'erreurs (pas égal à 0), l'heure de la **Dernière mise à jour** s'affiche.

- **Octets reçus** : octets reçus, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **Événements d'abandon** : paquets abandonnés.
- **Paquets reçus** : paquets corrects reçus, dont les paquets de multidiffusion et de diffusion.
- **Paquets de diffusion reçus** : paquets de diffusion corrects reçus. Ce nombre n'inclut pas les paquets de multidestination.
- **Paquets de multidiffusion reçus** : paquets de multidiffusion corrects reçus.
- **Erreurs d'alignement et CRC** : erreurs d'alignement et CRC qui se sont produites.
- **Paquets de taille insuffisante** : paquets de taille insuffisante (moins de 64 octets) reçus.
- **Paquets de taille excessive** : paquets de taille excessive (plus de 2 000 octets) reçus.
- **Fragments** : fragments (paquets de moins de 64 octets) reçus, à l'exception des bits de synchronisation, mais en incluant les octets FCS.
- **Jabotages** : paquets reçus ayant une longueur supérieure à 1 632 octets. Ce nombre exclut les bits de synchronisation, mais inclut les octets FCS qui comportaient une séquence FCS (Frame Check Sequence) erronée avec un nombre entier d'octets (erreur FCS) ou une séquence FCS erronée avec un nombre non entier d'octets (erreur d'alignement). Un paquet long est une trame Ethernet respectant les critères suivants :
  - La longueur des données du paquet est supérieure à la MRU.
  - Le paquet a un CRC non valide.
  - Un événement d'erreur de réception (Rx) n'a pas été détecté.

- **Collisions** : collisions reçues. Si les trames géantes sont activées, le seuil des trames Jabber est augmenté de façon à correspondre à la taille maximale des trames géantes.
- **Trames de 64 octets** : trames de 64 octets qui ont été envoyées ou reçues.
- **Trames de 65 à 127 octets** : trames de 65 à 127 octets qui ont été envoyées ou reçues.
- **Trames de 128 à 255 octets** : trames de 128 à 255 octets qui ont été envoyées ou reçues.
- **Trames de 256 à 511 octets** : trames de 256 à 511 octets qui ont été envoyées ou reçues.
- **Trames de 512 à 1 023 octets** : trames de 512 à 1 023 octets qui ont été envoyées ou reçues.
- **Trames de 1 024 octets ou plus** : trames de 1 024 à 2 000 octets et trames géantes qui ont été envoyées ou reçues.

ÉTAPE 4 Pour afficher les compteurs dans la vue Tableau ou Graphique :

- Cliquez sur **View All Interfaces Statistics** (Voir les statistiques de toutes les interfaces) pour visualiser l'ensemble des ports dans la vue Tableau.
- Cliquez sur **Vue graphique** pour afficher ces résultats sous forme graphique. Dans cette vue, vous pouvez sélectionner l'**intervalle de temps** pour lequel les résultats seront présentés et le type de statistique à afficher.

Historique RMON

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

Vous pouvez configurer la fréquence d'échantillonnage, la quantité d'échantillons à stocker, ainsi que le port à partir duquel recueillir les données via la page History (Historique).

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

Pour saisir des données de contrôle RMON :

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

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

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

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

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

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

Table de l'historique RMON

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

Pour afficher les statistiques de l'historique RMON :

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

ÉTAPE 2 Cliquez sur **History Table**.

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

Les champs sont affichés pour l'échantillon sélectionné.

- **Propriétaire** : propriétaire de l'entrée dans la table d'historique.
- **N° d'échantillon** : les statistiques ont été récupérées à partir de cet échantillon.

- **Événements d'abandon** : paquets abandonnés en raison d'un manque de ressources réseau lors de l'intervalle d'échantillonnage. Cela peut ne pas correspondre au nombre exact de paquets abandonnés, mais plutôt au nombre de détections de paquets de ce type.
- **Octets reçus** : octets reçus, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **Paquets reçus** : paquets reçus, y compris les paquets erronés, ainsi que les paquets multicast et broadcast.
- **Paquets de diffusion** : paquets de diffusion corrects reçus, à l'exception des paquets de multidiffusion.
- **Multicast Packets** : paquets de multidestination corrects reçus.
- **Erreurs d'alignement et CRC** : erreurs d'alignement et CRC qui se sont produites.
- **Paquets de taille insuffisante** : paquets de taille insuffisante (moins de 64 octets) reçus.
- **Paquets de taille excessive** : paquets de taille excessive (plus de 2 000 octets) reçus.
- **Fragments** : fragments (paquets de moins de 64 octets) reçus, à l'exception des bits de synchronisation, mais incluant les octets FCS.
- **Jabotages** : nombre total de paquets reçus dont la taille dépassait 2 000 octets. Ce nombre exclut les bits de synchronisation, mais inclut les octets FCS qui comportaient une séquence FCS (Frame Check Sequence) erronée avec un nombre entier d'octets (erreur FCS) ou une séquence FCS erronée avec un nombre non entier d'octets (erreur d'alignement).
- **Collisions** : collisions reçues.
- **Utilisation** : pourcentage du trafic actuel de l'interface par rapport au trafic maximum pouvant être géré par cette dernière.

Contrôle des événements RMON

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

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

Pour définir les événements RMON :

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

Cette page affiche les événements précédemment définis.

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

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

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Entrée d'événement** : affiche le numéro d'index d'entrée d'événement pour la nouvelle entrée.
- **Communauté** : saisissez la chaîne de communauté SNMP à inclure lors de l'envoi de messages « trap » (facultatif). Veuillez noter que la communauté doit être définie à l'aide des pages Destinataires de notifications pour que le message de filtre atteigne la station de gestion du réseau.
- **Description** : saisissez un nom pour l'événement. Ce nom est utilisé sur la page **Ajouter une alarme RMON** pour associer une alarme à un événement.
- **Notification Type** : sélectionnez le type d'action résultant de cet événement. Les valeurs possibles sont :
  - *None* : aucune action ne se produit lorsque l'alarme se déclenche.
  - *Journal (Table journal d'événements)* : ajoutez une entrée de journal à la table du journal d'événements lorsque l'alarme se déclenche.
  - *Filtre (gestionnaire SNMP et serveur SYSLOG)* : permet d'envoyer un filtre au serveur de journalisation distant lorsque l'alarme se déclenche.
  - *Journal et interception* : ajoute une entrée de journal à la table du journal d'événements et envoie une interception au serveur de journalisation distant lorsque l'alarme se déclenche.
- **Owner** : saisissez le périphérique ou l'utilisateur ayant défini l'événement.

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

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

Journaux d'événements RMON

La page Events (Événements) affiche le journal des événements (actions) qui se sont produits. Deux types d'événements peuvent être journalisés : *Journal* ou *Journal et interception*. L'action indiquée dans l'événement est mise en œuvre lorsque cet événement est lié à une alarme (reportez-vous à la page Alarmes RMON) et que les conditions de l'alarme sont réunies.

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

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

Vous pouvez sélectionner une interface dans le filtre pour afficher les événements sur une interface spécifique.

Cette page affiche les champs suivants :

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

Alarmes RMON

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

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

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

Pour entrer des alarmes RMON :

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

Toutes les alarmes définies précédemment sont affichées. Les champs sont décrits dans la page Ajouter une alarme RMON ci-dessous. En plus de ces champs, le champ suivant apparaît :

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

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

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

- **Interval** : saisissez l'intervalle (en secondes) entre les alarmes.
- **Owner** : saisissez le nom de l'utilisateur ou du système de gestion du réseau qui reçoit l'alarme.

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

sFlow

La fonctionnalité sFlow permet de collecter des statistiques à l'aide de la technologie d'échantillonnage basée sur sFlow v5.

Cette dernière est intégrée dans les commutateurs et les routeurs. Elle permet de surveiller en permanence les flux de trafic sur une partie ou sur l'intégralité des interfaces, simultanément.

Le système de surveillance sFlow se compose d'un agent (intégré dans un commutateur ou un routeur, ou dans une sonde autonome) et d'un collecteur central de données, appelé collecteur sFlow.

L'agent sFlow utilise la technologie d'échantillonnage pour capturer le trafic et les statistiques sur l'appareil contrôlé, qui sont ensuite réacheminés vers un collecteur à des fins d'analyse avec des datagrammes sFlow.

sFlow v5 définit :

- Le mode de surveillance du trafic.
- La base MIB sFlow qui contrôle l'agent sFlow.
- Le format des échantillons de données utilisé par l'agent sFlow pour réacheminer les données vers un collecteur central. L'appareil prend en charge deux types d'échantillonnage sFlow : échantillonnage des flux et des compteurs. L'échantillonnage des compteurs suivants est effectué avec sFlow v5 (si l'interface le prend en charge) :
  - Les compteurs de l'interface générique (RFC 2233)
  - Les compteurs de l'interface Ethernet (RFC 2358)

Flux de travail

Par défaut, l'échantillonnage des flux et des compteurs est désactivé.

Pour activer l'échantillonnage sFlow :

1. Définissez l'adresse IP d'un récepteur (également appelé collecteur ou serveur) pour les statistiques sFlow. Utilisez la page Paramètres du récepteur sFlow pour ce faire.
2. Activez l'échantillonnage des flux et/ou des compteurs, envoyez les échantillons vers l'index du récepteur et configurez le taux d'échantillonnage moyen. Utilisez la page Paramètres d'interface sFlow pour ce faire.
3. Affichez et effacez les compteurs de statistiques sFlow. Utilisez la page Statistiques sFlow pour ce faire.

Paramètres du récepteur sFlow

Pour définir les paramètres du récepteur sFlow :

ÉTAPE 1 Cliquez sur **État et statistiques > sFlow > Récepteurs sFlow**.

ÉTAPE 2 Renseignez les champs suivants :

- **Interface source IPv4** : sélectionnez l'interface source IPv4.

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

- **Interface source IPv6** : sélectionnez l'interface source IPv6.

Les paramètres sFlow sont affichés dans la table des récepteurs sFlow. Le champ **Adresse du récepteur** est identique au champ **Nom/Adresse IP du serveur** de la page **Ajouter**.

ÉTAPE 3 Pour ajouter un récepteur (analyseur sFlow), cliquez sur **Ajouter** et sélectionnez l'un des index de définition d'échantillonnage prédéfinis dans **Index du récepteur**.

ÉTAPE 4 Renseignez les champs relatifs à l'adresse du récepteur :

- **Définition du serveur** : indiquez si vous souhaitez spécifier le serveur sFlow **Par adresse IP** ou **Par nom**.

Si vous avez choisi **Par adresse IP** comme **Définition du serveur** :

- **Version IP** : indiquez si l'adresse du serveur est de type IPv4 ou IPv6.

- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - **Liaison locale** : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe FE80, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - **Global** : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée)

ÉTAPE 5 Renseignez les champs suivants :

- **Adresse IP/Nom du récepteur** : saisissez l'adresse IP ou le nom du récepteur en fonction des informations requises.
- **Port** : port sur lequel le message SYSLOG est envoyé.
- **Taille maximale du datagramme** : nombre maximal d'octets qui peuvent être envoyés au récepteur dans un seul datagramme d'échantillons (trame).

ÉTAPE 6 Cliquez sur **Appliquer**.

Paramètres d'interface sFlow

Pour échantillonner des datagrammes ou des compteurs depuis un port, ce dernier doit être associé à un récepteur. Les paramètres du port sFlow peuvent être configurés uniquement après avoir défini le récepteur sur la page Paramètres du récepteur sFlow.

Pour activer l'échantillonnage et configurer le port depuis lequel collecter des informations sFlow :

ÉTAPE 1 Cliquez sur **État et statistiques > sFlow > Paramètres d'interface sFlow**.

Les paramètres d'interface sFlow sont affichés.

ÉTAPE 2 Pour associer un récepteur sFlow avec un port, sélectionnez un port, cliquez sur **Modifier** et renseignez les champs suivants :

- **Interface** : sélectionnez l'unité/le port depuis lequel des informations sont collectées.
- **(Échantillonnage des flux) État** : activez/désactivez l'échantillonnage des flux.

- **Taux d'échantillonnage** : si vous saisissez x, un flux de x trames sera échantillonné.
- **Taille maximale d'en-tête** : nombre maximal d'octets qui doivent être copiés depuis un paquet échantillonné.
- **Index du récepteur** : sélectionnez un des indices qui ont été définis sur la page Paramètres du récepteur sFlow.
- **(Échantillonnage des compteurs) État** : activez/désactivez l'échantillonnage des compteurs.
- **Intervalle d'échantillonnage** : si vous saisissez x, un compteur de x secondes sera échantillonné.
- **Index du récepteur** : sélectionnez un des indices qui ont été définis sur la page Paramètres du récepteur sFlow.

ÉTAPE 3 Cliquez sur **Appliquer**.

Statistiques sFlow

Pour afficher les statistiques sFlow :

- Cliquez sur **État et statistiques > sFlow > Statistiques sFlow**.

  Les statistiques sFlow suivantes sont affichées pour chaque interface :

  - **Interface** : port pour lequel l'échantillon a été collecté.
  - **Paquets échantillonnés** : nombre de paquets échantillonnés.
  - **Datagrammes envoyés au récepteur** : nombre de paquets d'échantillonnage sFlow envoyés.

Affichage des journaux

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

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

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

Mémoire RAM

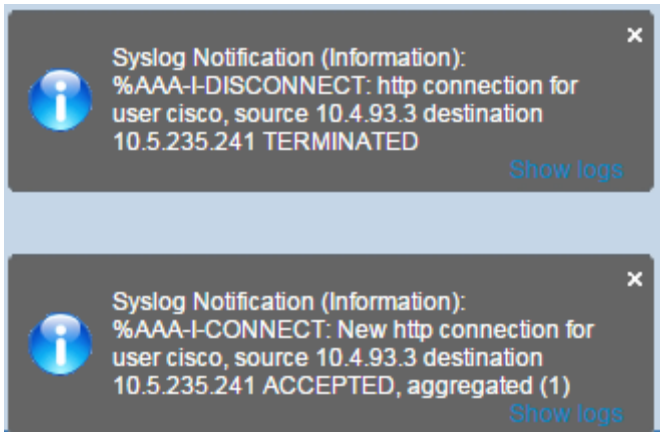
La page Mémoire RAM affiche tous les messages enregistrés dans la RAM (cache) dans l'ordre chronologique. Les entrées sont enregistrées dans le journal de la RAM en fonction de la configuration définie sur la page Paramètres des journaux.

Notifications SYSLOG contextuelles

Quand un nouveau message SYSLOG est consigné dans le fichier journal RAM, une notification détaillant son contenu s'affiche dans l'interface utilisateur Web.

L'interface utilisateur Web interroge le journal RAM toutes les 10 secondes. Les notifications contextuelles pour tous les messages SYSLOG créés au cours des 10 dernières secondes s'afficheront en bas à droite de l'écran.

La notification contextuelle s'affiche comme suit :



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

Les éléments suivants sont affichés en haut de la page :

- **Alert Icon Blinking** (Clignotement de l'icône d'alerte) : activez ou désactivez le clignotement de l'icône d'alerte.
- **Notification Syslog contextuelle** : active la réception de messages SYSLOG contextuels, comme décrit ci-dessus.
- **Current Logging Threshold** (Seuil de journalisation actuel) : spécifie les niveaux de journalisation qui sont générés. Celui-ci peut être modifié en cliquant sur **Modifier** selon le nom du champ.

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

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

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

Mémoire Flash

La page Mémoire Flash affiche, dans l'ordre chronologique, les messages enregistrés dans la mémoire Flash. Le niveau de sévérité minimum à journaliser est configuré sur la page Paramètres des journaux. Les journaux de la mémoire Flash sont conservés au redémarrage du commutateur. Vous pouvez effacer les journaux manuellement.

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

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

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

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

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

5

Administration

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

Elle couvre les rubriques suivantes :

- Modèles d'appareils
- Paramètres système
- Paramètres de console (prise en charge du débit en bauds automatiques)
- Gestion des piles
- Comptes d'utilisateur
- Expiration de la session inactive
- Paramètres d'heure
- Journaux système
- Gestion des fichiers
- Plug-n-Play (PNP)
- Redémarrage
- Ressources de routage
- Détection - Bonjour
- Détection - LLDP
- Détection - CDP
- Localiser le périphérique
- Ping
- Traceroute

Modèles d'appareils

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

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

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

Voici la liste des modèles de périphériques pris en charge :

Nom de la référence	Description	Nombre de ventilateurs	Nombre de ventilateurs redondants
SG350-10	SG350-10 - Commutateur administrable 10 ports Gigabit	0	0
SG350-10P	SG350-10P - Commutateur administrable 10 ports Gigabit PoE	0	0
SG355-10P	SG355-10P - Commutateur administrable 10 ports Gigabit PoE (alimentation interne)	0	0
SG350-10MP	SG350-10MP - Commutateur administrable 10 ports Gigabit Max PoE	0	0
SG350-28	SG350-28 - Commutateur administrable 28 ports Gigabit	0	0
SG350-28P	SG350-28P - Commutateur administrable 28 ports Gigabit PoE	2	0
SG350-28MP	SG350-28MP - Commutateur administrable 28 ports Gigabit Max PoE	3	0
SG350X-24	Commutateur administrable empilable 24 ports Gigabit	1	0
SG350X-24P	Commutateur administrable empilable PoE 24 ports Gigabit	2	0

Nom de la référence	Description	Nombre de ventilateurs	Nombre de ventilateurs redondants
SG350X-24MP	Commutateur administrable empilable PoE 24 ports Gigabit	3	0
SG350X-48	Commutateur administrable empilable 48 ports Gigabit	2	0
SG350X-48P	Commutateur administrable empilable PoE 48 ports Gigabit	4	0
SG350X-48MP	Commutateur administrable empilable PoE 48 ports Gigabit	4	0
SG350XG-24F	SG350XG-24F - Commutateur administrable empilable SFP+ 10 G 24 ports	4	0
SG350XG-24T	SG350XG-24T - Commutateur administrable empilable Base-T 10 G 24 ports	4	0
SG350XG-48T	SG350XG-48T - Commutateur administrable empilable Base-T 10G 48 ports	4	0
SG350XG-2F10	SG350XG-2F10 - Commutateur administrable empilable 10 G à 12 ports	3	0
SG350-8PD	SG SG350-8PD - Commutateur géré 8 ports 2,5 G PoE	0	0
SG350X-8PMD	SG SG350X-8PMD - Commutateur géré empilable 8 ports 2,5 G PoE	1	0
SG350X-24PD	SG SG350X-24PD - Commutateur géré empilable 24 ports 2,5 G PoE	2	0
SF550X-24	Commutateur administrable empilable 24 ports 10/100	1	1
SF550X-24P	Commutateur administrable empilable PoE 10/100 à 24 ports	2	1
SF550X-24MP	Commutateur administrable empilable PoE 10/100 à 24 ports	3	1

Nom de la référence	Description	Nombre de ventilateurs	Nombre de ventilateurs redondants
SF550X-48	Commutateur administrable empilable 10/100 à 48 ports	2	0
SF550X-48P	Commutateur administrable empilable PoE 10/100 à 48 ports	3	1
SF550X-48MP	Commutateur administrable empilable PoE 10/100 à 48 ports	5	1
SG550XG-8F8T	Commutateur empilable 10 Gbit 16 ports avec prise en charge d'une alimentation redondante	3	1
SG550XG-24T	Commutateur empilable Base-T 10G 24 ports (2 ports combo) avec prise en charge d'une alimentation redondante	4	1
SG550XG-48T	Commutateur empilable Base-T 10 G 48 ports (2 ports combo) avec prise en charge d'une alimentation redondante	5	1
SG550XG-24F	Commutateur empilable 10 Gbit SFP+ à 24 ports (2 ports combo) avec prise en charge d'une alimentation redondante	4	1

Paramètres système

Pour accéder aux paramètres système :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres système**.

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

- **Description du système** : affiche une description du périphérique.
- **Emplacement du système** : entrez l'emplacement physique du périphérique.
- **System Contact** : saisissez le nom de la personne à contacter.

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

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

  La bannière peut comporter jusqu'à 1 000 caractères. Au bout de 510 caractères, appuyez sur <Entrée> pour continuer.

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

Paramètres de console (prise en charge du débit en bauds automatiques)

Le débit du port de console peut être défini sur l'une des valeurs suivantes : 4 800, 9 600, 19 200, 38 400, 57 600 et 115 200 ou détection automatique.

Si la détection automatique est sélectionnée, le périphérique détecte le débit de la console automatiquement.

Lorsque la détection automatique n'est pas activée, le débit du port de console correspond automatiquement au dernier débit défini manuellement (115 200 par défaut).

Lorsque la détection automatique est activée, mais que le débit en bauds de la console n'a pas encore été détecté, le système utilise la valeur 115 200 pour afficher le texte (par exemple, les informations de démarrage).

Après avoir activé la détection automatique dans la page Paramètres de console, il est possible de l'activer en connectant la console au dispositif et en appuyant deux fois sur la touche Entrée. Le périphérique détecte alors le débit de bauds automatiquement.

Pour activer la détection automatique ou définir manuellement le débit de bauds de la console :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres de console**.

ÉTAPE 2 Sélectionnez l'une des options suivantes dans le champ **Console Port Baud Rate** (Débit en bauds du port de console) :

- **Détection automatique** : le débit de bauds de la console est détecté automatiquement.
- **Statique** : sélectionnez l'un des débits disponibles.

ÉTAPE 3 Cliquez sur **Appliquer**.

Gestion des piles

Reportez-vous à la section Administration : Gestion des piles.

Comptes d'utilisateur

La page Comptes d'utilisateur vous permet de saisir des utilisateurs supplémentaires autorisés à accéder au périphérique (en lecture seule ou en lecture/écriture) ou de modifier les mots de passe d'utilisateurs existants.

Après l'ajout d'un utilisateur de niveau 15 (comme décrit ci-dessous), l'utilisateur par défaut est supprimé du système.

REMARQUE Il est impossible de supprimer tous les utilisateurs. Si tous les utilisateurs sont sélectionnés, le bouton **Supprimer** est désactivé.

Pour ajouter un nouvel utilisateur :

ÉTAPE 1 Cliquez sur **Administration** > **Comptes utilisateurs**.

Cette page affiche les utilisateurs définis dans le système 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 paramètres.

- **Nom d'utilisateur** : saisissez un nouveau nom d'utilisateur comportant 20 caractères maximum. Les caractères UTF-8 sont interdits.
- **Mot de passe** : saisissez un mot de passe (les caractères UTF-8 sont interdits). Si la fiabilité et la complexité du mot de passe sont définies, le mot de passe utilisateur doit être conforme à la stratégie configurée dans Sécurité du mot de passe.
- **Confirm Password** : saisissez à nouveau le mot de passe.
- **Password Strength Meter** : affiche le niveau de sécurité du mot de passe. Vous pouvez définir la stratégie de sécurité et de complexité du mot de passe sur la page Sécurité du mot de passe.
- **Niveau d'utilisateur** : sélectionnez le niveau de privilèges de l'utilisateur que vous ajoutez/modifiez.
  - *Accès CLI en Lecture seule (1)* : l'utilisateur ne peut pas accéder à l'interface utilisateur graphique et peut uniquement accéder aux commandes d'interface de ligne de commande qui ne modifient pas la configuration du périphérique.
  - *Accès CLI en Lecture/Écriture limitée (7)* : l'utilisateur ne peut pas accéder à l'interface utilisateur graphique et peut uniquement accéder aux commandes d'interface de ligne de commande qui modifient la configuration du périphérique. Pour plus d'informations, reportez-vous au *Guide de référence de l'interface de ligne de commande (CLI)*.
  - *Accès de gestion en lecture/écriture (15)* : l'utilisateur peut accéder à l'interface utilisateur graphique et configurer le périphérique.

ÉTAPE 4 Cliquez sur **Appliquer**. L'utilisateur est ajouté au fichier de Configuration d'exécution du périphérique.

Expiration de la session inactive

Le délai d'expiration de la session inactive permet de configurer combien de temps une session de gestion peut rester inactive avant d'expirer et de nécessiter une reconnexion de l'utilisateur, en fonction du type de session :

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

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

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

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

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

Paramètres d'heure

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

Journaux système

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

L'appareil génère les journaux locaux suivants :

- Journal envoyé à l'interface de la console
- Journal enregistré dans une liste cyclique d'événements journalisés dans la mémoire RAM et effacé au redémarrage de l'appareil

- Journal enregistré dans un fichier journal cyclique enregistré dans la mémoire Flash et conservé d'un redémarrage à l'autre

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

Cette section contient les rubriques suivantes :

- Paramètres des journaux
- Paramètres de journalisation distante

Paramètres des journaux

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

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

- Emergency : le système n'est pas utilisable.
- Alert : une action est requise.
- Critical : le système est dans un état critique.
- Error : le système subit une condition d'erreur.
- Warning : un avertissement système a été généré.
- Notice : le système fonctionne correctement, mais une remarque système a été générée.
- Informational : informations sur le périphérique.
- 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 la page Mémoire RAM et sur la page Mémoire Flash.

Si vous choisissez d'enregistrer un niveau de gravité spécifique dans un journal, tous les événements de gravité 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 **Avertissement** n'est enregistré (Remarque, Informatif et Débogage).

Pour définir des paramètres de journalisation globaux :

ÉTAPE 1 Cliquez sur **Administration** > **Journaux système** > **Paramètres des journaux**.

ÉTAPE 2 Saisissez les paramètres.

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

Paramètres de journalisation distante

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

Pour définir les serveurs SYSLOG :

ÉTAPE 1 Cliquez sur **Administration** > **Journaux système** > **Serveurs de journalisation distants**.

ÉTAPE 2 Renseignez les champs suivants :

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

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

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

ÉTAPE 3 Cliquez sur **Ajouter**.

ÉTAPE 4 Saisissez les paramètres.

- **Server Definition** : indiquez si vous souhaitez identifier le serveur de journalisation distante par son adresse IP ou par son nom.
- **Version IP** : sélectionnez le format IP pris en charge.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe FE80::/10, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée).

- **Adresse IP/Nom serveur de journalisation** : saisissez l'adresse IP ou le nom de domaine du serveur de journalisation.
- **UDP Port** : saisissez le numéro du port UDP auquel les messages de journal sont envoyés.
- **Équipement** : sélectionnez une valeur pour l'équipement à partir duquel les journaux système sont envoyés au serveur distant. Une seule valeur d'équipement peut être affectée à un serveur. Si un autre code d'équipement est affecté, la première valeur est remplacée.
- **Description** : saisissez une description pour le serveur.
- **Minimum Severity** : sélectionnez le niveau minimum de gravité des messages de journalisation système à envoyer au serveur.

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

Gestion des fichiers

Reportez-vous à la section Administration : Gestion des fichiers.

Plug-n-Play (PNP)

L'installation manuelle de dispositifs réseau, qu'il s'agisse d'en remplacer ou d'en mettre en œuvre de nouveaux peut être coûteuse, chronophage et source d'erreurs. Généralement, les nouveaux dispositifs sont d'abord envoyés dans une zone de préparation centralisée dans laquelle ils sont déballés, connectés à un réseau intermédiaire, mis à jour avec les licences, les configurations et les images appropriées, puis emballés et livrés sur le site d'installation réel. Une fois ces processus terminés, des spécialistes doivent se déplacer sur les sites concernés pour procéder à l'installation. Même lorsque les appareils sont installés dans le NOC (Network Operations Center)/Centre de données lui-même, il risque de ne pas y avoir suffisamment de techniciens pour le nombre impressionnant d'appareils. Tous ces problèmes entraînent des retards dans le déploiement et augmentent les coûts opérationnels.

La solution Cisco Plug-n-Play réduit les coûts associés au déploiement/à l'installation de dispositifs réseau, accélère leur installation et simplifie les déploiements sans compromettre la sécurité. à l'aide de la solution Cisco Plug-n-Play, vous pouvez effectuer des installations sans intervention des commutateurs dans différents scénarios et sites de déploiement.

Paramètres PNP

Pour configurer les paramètres PNP :

REMARQUE La fonction est activée par défaut.

ÉTAPE 1 Cliquez sur **Administration > PNP > Paramètres PNP**.

ÉTAPE 2 Configurez PNP en renseignant les champs suivants :

- **État PNP** : activé par défaut.

Transport PNP : définit les informations et les paramètres de la session d'agent PNP.

- **Définition des paramètres** : sélectionnez une des options suivantes pour localiser les informations de configuration, concernant le protocole de transport à utiliser, l'adresse du serveur PNP et le port TCP à employer :
  - *Paramètres par défaut* : si cette option est sélectionnée, les paramètres PNP sont pris de l'option DHCP 43. Si tout ou partie des paramètres ne sont pas reçus de l'option DHCP 43, les valeurs par défaut suivantes sont utilisées : protocole de transport par défaut HTTP, nom de DNS « pnpserver » pour le serveur PNP et le port lié à HTTP.

    Lors de la sélection de l'option **Paramètres par défaut** tous les champs de la section **Transport PNP** sont grisés.
  - *Paramètres manuels :* définissez manuellement le port TCP et les paramètres de serveur à utiliser pour le transport PNP.
- **Port TCP** : numéro du port TCP. Il est renseigné automatiquement par le système : 80 pour HTTP.
- **Définition du serveur** : indiquez si vous souhaitez spécifier le serveur PNP **Par adresse IP** ou **Par nom**.
- **Version IP** : sélectionnez le format IP pris en charge.
- **Type d'adresse IPv6 du serveur** : sélectionnez l'une des options suivants, si le type de version d'IP est IPv6 :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.

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

- **Interface de liaison locale** : si le type d'adresse IPv6 source est Liaison locale, sélectionnez son lieu de réception.
- **Adresse IP du serveur/Nom** : saisissez l'adresse IP ou le nom de domaine du serveur PNP.

Utilisateur PNP

- **Définition de l'utilisateur** : informations utilisateur à envoyer au serveur sous forme de paquets PNP. sélectionnez l'une des options suivantes :

  - *Valeur par défaut* : lorsque vous sélectionnez cette option, les paramètres de nom d'utilisateur et de mot de passe sont dérivés de l'option DHCP 43. Si vous sélectionnez cette option, les champs de nom d'utilisateur et de mot de passe sont grisés.

  - *Paramètres manuels* : sélectionnez cette option pour configurer manuellement le nom d'utilisateur et le mot de passe PNP.

- **Nom d'utilisateur** : nom d'utilisateur —Nom d'utilisateur à saisir dans les paquets PNP.
- **Mot de passe**—Mot de passe au format **Crypté** ou **Texte en clair**.

Paramètres de comportement PNP : saisissez les paramètres suivants :

- **Intervalle de reconnexion** : intervalle, en secondes, avant toute tentative de reconnexion de la session une fois celle-ci perdue.
- **Délai d'expiration de découverte** : spécifie le temps à attendre, en secondes, avant toute nouvelle tentative de découverte après que la découverte du serveur PNP ait échoué.
- **Facteur exponentiel de délai d'expiration** : valeur qui déclenche la tentative de détection de manière exponentielle, en multipliant la valeur de délai d'expiration précédente par une valeur exponentielle et en appliquant le résultat comme délai d'expiration (si la valeur est inférieure à la valeur maximale de délai d'expiration).
- **Délai d'expiration de découverte maximal** : valeur maximale du délai d'expiration. Doit être supérieur à la valeur **Délai d'attente de découverte**.
- **Délai d'attente de chien de garde** : intervalle de temps d'attente d'une réponse d'un PnP ou d'un serveur de fichiers pendant une session PNP active (par exemple pendant un processus de téléchargement de fichier).

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres sont copiés dans le fichier de Configuration d'exécution.

Cliquez sur **Afficher les données sensibles sous forme chiffrée** pour afficher le mot de passe s'il est chiffré.

Session PNP

Cet écran affiche la valeur des paramètres PNP actuellement en vigueur. La source du paramètre est affichée entre parenthèses le cas échéant.

Pour afficher des informations sur les paramètres PNP.

ÉTAPE 1 Cliquez sur **Administration > PNP > Session PNP**.

Les champs suivants sont affichés :

- **État administratif** : indique si PNP est activé.
- **État opérationnel** : PNP est-il opérationnel ?
- **État de l'agent PNP** : indique si une session PNP est active. Les valeurs possibles sont **Découverte Attente**; **Découverte**; **Non Prêt**; **Désactivé**; **Session**; **Session Attente**.
- **Port TCP** : Port TCP de la session PNP
- **Adresse du serveur** : adresse IP du serveur PNP.
- **Nom d'utilisateur** : nom d'utilisateur —Nom d'utilisateur à envoyer dans les paquets PNP.
- **Mot de passe MD5** : mot de passe à envoyer dans les paquets PNP.
- **Délai d'attente de détection** : délai d'attente de détection configuré.
- **Délai d'attente d'intervalle de session** : délai d'attente d'intervalle de session configuré (apparaît uniquement lorsque l'**État de l'agent PNP** est **En attente**)
- **Temps d'attente restant** : valeur de temps d'attente restante.

REMARQUE Cliquez sur le bouton Reprise, pour retirer immédiatement l'agent PnP de l'état d'attente, de la manière suivante :

- Si l'agent est à l'état d'attente de découverte, il est paramétré sur l'état de découverte.
- Si l'agent est à l'état d'attente de session PnP, il est paramétré sur l'état de session PnP.

Redémarrage

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

Vous pouvez sauvegarder la configuration du périphérique via la page Opérations de fichiers ou en cliquant sur **Save** (Enregistrer) en haut de la fenêtre. Vous pouvez également charger la configuration depuis un périphérique distant sur la page.

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

- Vous effectuez des actions sur un périphérique distant, et toute erreur peut provoquer une perte de connexion à ce périphérique distant. La préplanification d'un redémarrage restaure la configuration en cours et permet la restauration de la connexion au périphérique distant après expiration du délai spécifié. Si ces actions réussissent, le redémarrage retardé peut être annulé manuellement.
- Le rechargement du périphérique provoque la perte de connexion dans le réseau, en raison du redémarrage retardé, vous pouvez planifier le redémarrage à une heure plus propice pour les utilisateurs (par exemple tard dans la nuit).

Pour redémarrer le périphérique :

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

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

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

Les options suivantes sont disponibles :

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

REMARQUE Vous pouvez uniquement utiliser cette option si l'heure du système a été réglée manuellement ou via SNTP.

REMARQUE Si un redémarrage est prévu, cliquez sur **Annuler le redémarrage** pour l'annuler.

- *In* : redémarre dans le nombre d'heures et de minutes spécifié. La durée maximale pouvant s'écouler est de 24 jours.

- **Rétablir les paramètres d'usine par défaut** : redémarre le périphérique en utilisant sa configuration d'origine. Cette procédure efface tout, sauf l'image active, l'image inactive, la configuration miroir et les fichiers de localisation.

  L'ID d'unité de la pile est défini sur automatique.

- **Effacer le fichier de configuration de démarrage** : choisissez cette option pour effacer la configuration de démarrage du périphérique la prochaine fois qu'il démarrera.

Ressources de routage

Les entrées TCAM sont divisées en groupes, spécifiés ci-dessous :

- **IP Entries** (Entrées IP) : entrées TCAM du routeur réservées pour les routes statiques IP, les interfaces IP et les hôtes IP.
- **Entrées non IP** : entrées TCAM réservées à d'autres applications, telles que les règles ACL, les gestionnaires de stratégie CoS et les limites de débit VLAN.

Le tableau suivant décrit le nombre d'entrées TCAM utilisées par les différentes fonctions :

Entité logique	IPv4	IPv6 (TCAM PCL)	IPv6 (TCAM routeur)
Voisin IP	1 entrée	1 entrée	4 entrées
Adresse IP sur une interface	2 entrées	2 entrées	8 entrées
Acheminement distant IP	1 entrée	1 entrée	4 entrées
Préfixe de lien		1 entrée	4 entrées

Le mappage VLAN utilise les 4 entrées TCAM dans tous les cas.

La page Routing Resources (Ressources de routage) permet d'ajuster l'allocation TCAM du routeur.

Si vous modifiez l'allocation TCAM du routeur de manière incorrecte, un message d'erreur s'affiche. Si votre allocation TCAM du routeur est autorisée, un message s'affiche pour vous indiquer qu'un redémarrage automatique va être effectué avec les nouveaux paramètres. Les ressources de routage peuvent être modifiées de manière incorrecte, de l'une des façons suivantes :

- Le nombre d'entrées TCAM du routeur que vous allouez est inférieur au nombre actuellement utilisé.
- Le nombre d'entrées TCAM du routeur que vous allouez est supérieur au nombre maximal disponible pour cette catégorie (les valeurs maximales s'affichent sur la page).

Pour afficher et modifier les ressources de routage :

ÉTAPE 1 Cliquez sur **Administration** > **Ressources de routage**.

Les champs suivants s'affichent :

Ressources de routage IPv4

- **Nombre de voisins (x entrées TCAM par voisin)** : correspond au nombre de voisins enregistrés sur l'appareil et **Entrées TCAM** représente le nombre d'entrées TCAM du routeur utilisées pour les voisins. Il existe 4 entrées TCAM par voisin pour la gamme SG550XG et 1 pour la gamme SG350XG.
- **Nombre d'interfaces (x entrées TCAM par interface)** : correspond au nombre d'adresses IP sur les interfaces de l'appareil et **Entrées TCAM** représente le nombre d'entrées TCAM du routeur utilisées pour les adresses IP.

- **Nombre de routes (x entrées TCAM par route)** : correspond au nombre de routes enregistrées sur le périphérique et **Entrées TCAM** représente le nombre d'entrées TCAM du routeur utilisées pour les routes.
- **Total** : affiche le nombre d'entrées TCAM du routeur actuellement utilisées.
- **Entrées maximales** : sélectionnez l'une des options suivantes :
  - *Use Default* (Utiliser les valeurs par défaut) : utilisez les valeurs par défaut.
  - *Défini par l'utilisateur* : saisissez une valeur.

Ressources de routage de multidiffusion IPv4

- **Nombre de routes de multidiffusion IPv4 (2 entrées TCAM par route)** : correspond au nombre de routes de multidiffusion enregistrées sur le périphérique et **Entrées TCAM** représente le nombre d'entrées TCAM utilisées pour les routes de multidiffusion.
- **Entrées maximales** : sélectionnez l'une des options suivantes :
  - *Use Default* (Utiliser les valeurs par défaut) : utilisez les valeurs par défaut.
  - *Défini par l'utilisateur* : saisissez une valeur.

Ressources de routage en fonction de la stratégie IPv4

- **Nombre de routes basées sur une stratégie IPv4 (x entrées TCAM par route)** : correspond au nombre de routes de multidiffusion enregistrées sur le périphérique et **Entrées TCAM** représente le nombre d'entrées TCAM utilisées pour les routes de multidiffusion.
- **Entrées maximales** : sélectionnez l'une des options suivantes :
  - *Use Default* (Utiliser les valeurs par défaut) : utilisez les valeurs par défaut.
  - *Défini par l'utilisateur* : saisissez une valeur.

Ressources de routage IPv6

- **Nombre de voisins (x entrées TCAM par voisin)** : correspond au nombre de voisins enregistrés sur l'appareil et **Entrées TCAM** représente le nombre d'entrées TCAM utilisées pour les voisins.
- **Nmbre d'interfaces (x entrées TCAM par interface)** : correspond au nombre d'interfaces sur l'appareil et **Entrées TCAM** représente le nombre d'entrées TCAM utilisées pour les interfaces.
- **Nombre de préfixes de liaison (x entrées TCAM par préfixe)** : correspond au nombre de préfixes de liaison enregistrés sur l'appareil et **Entrées TCAM** représente le nombre d'entrées TCAM utilisées pour les préfixes de liaison.

- **Nombre de routes (x entrées TCAM par route)** : correspond au nombre de préfixes de liaison enregistrés sur l'appareil et **Entrées TCAM** représente le nombre d'entrées TCAM utilisées pour les préfixes de liaison.
- **Total** : nombre total d'entrées TCAM utilisées.
- **Entrées maximales** : sélectionnez l'une des options suivantes :
  - *Use Default* (Utiliser les valeurs par défaut) : utilisez les valeurs par défaut.
  - *Défini par l'utilisateur* : saisissez une valeur.

Ressources de routage de multidiffusion IPv6

- **Nombre de routes de multidiffusion IPv6 (x entrées TCAM par route)** : correspond au nombre de routes de multidiffusion enregistrées sur le périphérique et **Entrées TCAM** représente le nombre d'entrées TCAM utilisées pour les routes de multidiffusion.
- **Entrées maximales** : sélectionnez l'une des options suivantes :
  - *Use Default* (Utiliser les valeurs par défaut) : utilisez les valeurs par défaut.
  - *Défini par l'utilisateur* : saisissez une valeur.

Ressources de routage en fonction de la stratégie IPv6

- **Nombre de routes en fonction de la stratégie IPv6 (4 entrées TCAM par route)** : correspond au nombre de routes de multidiffusion enregistrées sur le périphérique et **Entrées TCAM** représente le nombre d'entrées TCAM utilisées pour les routes de multidiffusion.
- **Entrées maximales** : sélectionnez l'une des options suivantes :
  - *Use Default* (Utiliser les valeurs par défaut) : utilisez les valeurs par défaut.
  - *Défini par l'utilisateur* : saisissez une valeur.

Ressources de routage du mappage VLAN

- **Nombre d'entrées du mappage VLAN (mappage de 4 entrées TCAM)** : correspond au nombre d'entrées de mappage VLAN enregistrées sur le périphérique et **Entrées TCAM** représente le nombre d'entrées TCAM utilisées pour le mappage VLAN.
- **Entrées maximales** : sélectionnez l'une des options suivantes :
  - *Use Default* (Utiliser les valeurs par défaut) : utilisez les valeurs par défaut.
  - *Défini par l'utilisateur* : saisissez une valeur.

ÉTAPE 2 Enregistrez les nouveaux paramètres en cliquant sur **Appliquer**. Le système vérifie si les paramètres des ressources du routage sont possibles. Si l'opération est incorrecte, un message d'erreur s'affiche. Si l'opération est correcte, les paramètres sont copiés dans le fichier de Configuration d'exécution.

Tableau de ressources TCAM : affiche le nombre d'entrées TCAM en cours d'utilisation et disponibles.

- **Numéro d'unité** : numéro d'unité d'un périphérique dans une pile.
- **Entrées TCAM maximales pour le routage et le routage de multidiffusion** : nombre d'entrées TCAM disponibles pour le routage et le routage de multidiffusion.
- **Routage IPv4**
  - *En cours d'utilisation* : nombre d'entrées TCAM utilisées pour le routage IPv4.
  - *Maximum* : nombre maximal d'entrées TCAM disponibles pour le routage IPv4.
- **Routage de multidiffusion IPv4**
  - *En cours d'utilisation* : nombre d'entrées TCAM utilisées pour le routage multidestination IPv4.
  - *Maximum* : nombre maximal d'entrées TCAM disponibles pour le routage multidestination IPv4.
- **Routage en fonction de la stratégie IPv4**
  - *En cours d'utilisation* : nombre d'entrées TCAM de routeur utilisées pour le routage en fonction de la stratégie IPv4.
  - *Maximum* : nombre d'entrées TCAM de routeur disponibles pouvant être utilisées pour le routage en fonction de la stratégie IPv4.
- **Routage IPv6**
  - *En cours d'utilisation* : nombre d'entrées TCAM utilisées pour le routage IPv6.
  - *Maximum* : nombre maximal d'entrées TCAM disponibles pour le routage IPv6.
- **Routage de multidiffusion IPv6**
  - *En cours d'utilisation* : nombre d'entrées TCAM utilisées pour le routage multidestination IPv6.
  - *Maximum* : nombre maximal d'entrées TCAM disponibles pour le routage multidestination IPv6.

- **Routage en fonction de la stratégie IPv6**
  - *En cours d'utilisation* : nombre d'entrées TCAM de routeur utilisées pour le routage en fonction de la stratégie IPv6.
  - *Maximum* : nombre d'entrées TCAM de routeur disponibles pouvant être utilisées pour le routage en fonction de la stratégie IPv6.
- **Maximum TCAM Entries for Non-IP Rules (Entrées TCAM maximales pour règles non-IP)** : nombre d'entrées TCAM disponibles pour les règles non-IP.
- **Règles non-IP**
  - *En cours d'utilisation* : nombre d'entrées TCAM utilisées pour les règles non-IP.
  - *Maximum* : nombre maximal d'entrées TCAM disponibles pour les règles non-IP.
- **Mappage VLAN**
  - *En cours d'utilisation* : nombre d'entrées du mappage VLAN utilisées pour les règles non-IP.
  - *Maximum* : nombre maximal d'entrées du mappage VLAN disponibles pour les règles non-IP.

Détection - Bonjour

Reportez-vous à la section Bonjour.

Détection - LLDP

Reportez-vous à la section Détection - LLDP.

Détection - CDP

Reportez-vous à la section Détection - CDP.

Localiser le périphérique

Cette fonctionnalité permet d'activer tous les voyants de ports réseau sur un périphérique spécifique afin de le localiser physiquement. Elle est utile pour localiser un périphérique dans une pièce comportant de nombreux périphériques interconnectés. Quand cette fonctionnalité est activée, tous les voyants des ports réseau du périphérique clignotent pendant une durée configurée (une minute par défaut). Si un appareil fait partie d'une pile, une unité ou toutes les unités de la pile peuvent être précisées.

ÉTAPE 1 Cliquez sur **Administration > Localiser le périphérique**.

ÉTAPE 2 Renseignez les champs suivants :

- **Durée** : saisissez la durée (en secondes) durant laquelle les voyants doivent clignoter.
- **Durée restante** : ce champ ne s'affiche que si cette fonctionnalité est activée. Il affiche la durée restante de clignotement des voyants.
- **ID d'unité** : ce champ ne s'affiche que si le périphérique fait partie d'une pile. Ce champ précise l'unité sur laquelle les voyants du port réseau clignoteront ou affiche **Toutes** si toutes les unités sont sélectionnées.

ÉTAPE 3 Cliquez sur **Démarrer** pour activer cette fonctionnalité.

Quand cette fonctionnalité est activée, ce bouton devient un bouton **Stop**, ce qui vous permet d'interrompre le clignotement des voyants avant le délai défini.

Ping

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

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

Pour envoyer une requête Ping à un hôte :

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

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

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

  REMARQUE Si l'option Auto est sélectionnée, le système génère l'adresse source en fonction de l'adresse de destination.
- **Destination IPv6 Address Type** (Type d'adresse IPv6 de destination) : sélectionnez l'une des options suivantes :
  - *Link Local* (Liaison locale) : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, sélectionnez son lieu de réception.
- **Nom/adresse IP de destination** : adresse ou nom d'hôte du périphérique auquel la requête Ping est envoyée. C'est la définition de l'hôte qui détermine s'il s'agit d'une adresse IP ou d'un nom d'hôte.
- **Intervalle de Ping** : durée d'attente du système entre les paquets Ping. La requête Ping est réitérée autant de fois que configurée dans le champ **Nombre de Pings**, que la requête aboutisse ou non. Sélectionnez l'intervalle par défaut ou spécifiez votre propre valeur.
- **Nombre de Pings** : nombre de fois que l'opération Ping sera effectuée. Sélectionnez la valeur par défaut ou spécifiez votre propre valeur.
- **État** : indique si la requête Ping a réussi ou échoué.

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

ÉTAPE 4 Vous pouvez consulter le résultat de l'opération Ping dans la section **Compteurs et état du ping** de la page :

- **Nombre de paquets envoyés** : nombre de paquets envoyés par le Ping
- **Nombre de paquets reçus** : nombre de paquets reçus par le Ping
- **Paquets perdus** : pourcentage de paquets perdus pendant une opération Ping
- **Durée minimale d'un aller-retour** : durée la plus courte pour le renvoi d'un paquet
- **Durée maximale d'un aller-retour** : durée la plus longue pour le renvoi d'un paquet
- **Durée moyenne d'un aller-retour** : durée moyenne pour le renvoi d'un paquet
- **État** : échec ou réussite

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 périphérique. La page Traceroute affiche chaque saut entre le dispositif et un hôte cible, ainsi que la durée de l'aller-retour de tels sauts.

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

ÉTAPE 2 Configurez Traceroute en renseignant les champs suivants :

- **Définition de l'hôte** : indiquez si vous souhaitez identifier les hôtes par leur adresse IP ou leur nom.
- **Version IP** : si l'hôte est identifié par son adresse IP, sélectionnez IPv4 ou IPv6 pour indiquer qu'il sera entré au format sélectionné.
- **IP source** : sélectionnez l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source pour les messages de communication. Si le champ Définition de l'hôte a été défini sur Par nom, toutes les adresses IPv4 et IPv6 seront affichées dans ce champ déroulant. Si le champ Définition de l'hôte a été défini sur Par adresse IP, seules les adresses IP existantes du type spécifié dans le champ Version IP seront affichées.
- **Adresse IP/Nom hôte** : entrez l'adresse ou le nom de l'hôte.

- **TTL** : entrez 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**.
- **Délai d'expiration** : entrez la durée pendant laquelle le système attend le retour d'une trame avant de la déclarer perdue. Vous pouvez aussi sélectionner **Valeurs par défaut**.

ÉTAPE 3 Cliquez sur **Activer Traceroute**. L'opération est réalisée.

La page qui apparaît indique la durée de l'aller-retour (RTT) et l'état de chaque « trajet » dans les champs suivants :

- **Index** : affiche le numéro du saut.
- **Hôte** : affiche un arrêt sur l'acheminement vers la destination.

Durée de l'aller-retour *(1 à 3)* : affiche la durée de l'aller-retour en ms pour la trame 1 à 3 et l'état de l'opération 1 à 3.

6

Administration : Gestion des fichiers

Cette section porte sur la gestion des fichiers système.

Les sujets suivants sont traités :

- Fichiers système
- Opérations du microprogramme
- Opérations de fichiers
- Répertoire de fichiers
- Configuration/mise à jour automatique de l'image DHCP

Fichiers système

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

En règle générale, tous les fichiers qui se trouvent dans le dossier **flash://system/** sont des fichiers système.

Diverses actions peuvent être effectuées avec de tels fichiers, notamment : sélectionner le fichier du microprogramme à partir duquel l'appareil doit démarrer, copier différents types de fichiers de configuration en interne sur l'appareil ou copier des fichiers vers ou depuis un appareil externe, comme un serveur.

Les fichiers de configuration du périphérique sont définis en fonction de leur type, et comportent les réglages et valeurs de paramètre du périphérique.

Les autres fichiers sont notamment des 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 dans un éditeur de texte tel que le Bloc-notes une fois copiés sur un appareil externe, un PC par exemple.

Fichiers et types de fichiers

Les types de fichiers présents sur le périphérique sont les suivants :

- **Configuration d'exécution** : paramètres de fonctionnement actuellement utilisés par l'appareil. Ce fichier est modifié lorsque vous changez des valeurs de paramètre sur ce périphérique.

  En cas de redémarrage de l'appareil, la Configuration d'exécution est perdue.

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

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

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

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

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

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

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

- **Fichiers de sauvegarde** : copies manuelles d'un fichier servant à protéger le système en cas d'arrêt ou à maintenir un état de fonctionnement spécifique. Par exemple, vous pouvez copier la Configuration miroir, la Configuration de démarrage ou la Configuration d'exécution dans un fichier de sauvegarde. La sauvegarde est conservée dans la mémoire Flash ou sur un PC ou un lecteur USB, et est préservée en cas de redémarrage du périphérique.

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

- **Fichier de langue** : dictionnaire qui permet d'afficher les fenêtres de l'utilitaire de configuration Web dans la langue sélectionnée.
- **Fichier de journalisation** : messages SYSLOG stockés dans la mémoire Flash.

Opérations du microprogramme

La page Firmware Operations (Opérations du microprogramme) peut être utilisée pour :

- mettre à jour ou sauvegarder l'image du microprogramme ;
- permuter l'image active.

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

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

Les images logicielles des unités d'une pile doivent être identiques afin d'assurer le bon fonctionnement de la pile. Les unités de la pile peuvent être mises à niveau de l'une des façons suivantes.

- Vous pouvez mettre à niveau manuellement le microprogramme d'un périphérique avant d'ajouter ce dernier à la pile (méthode recommandée).
- L'unité principale de la pile met automatiquement à niveau le microprogramme d'une unité récemment ajoutée, à condition que le microprogramme de cette dernière ne soit pas identique à celui de l'unité principale.

Deux images du microprogramme sont conservées sur l'appareil. Une des images est identifiée en tant qu'*image active* et l'autre en tant qu'*image inactive*.

Lors de la mise à jour du microprogramme du périphérique, le nouveau microprogramme remplace toujours l'image inactive. Une fois le nouveau microprogramme téléchargé sur le périphérique, la nouvelle version est utilisée au prochain démarrage. L'ancienne version devient inactive après le redémarrage.

Procédure de mise à jour ou de sauvegarde du microprogramme via HTTP/HTTPS ou USB :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Opérations du microprogramme**.

Les champs suivants s'affichent :

- **Active Firmware File** (Fichier de microprogramme actif) : indique le fichier de microprogramme actif.
- **Active Firmware Version** (Version du microprogramme actif) : indique la version du fichier de microprogramme actif.

ÉTAPE 2 Renseignez les champs suivants :

- **Type d'opération** : sélectionnez **Mettre le micrologiciel à jour Sauvegarder le micrologiciel**.
- **Méthode de copie** : sélectionnez **HTTP/HTTPS** ou **USB**.
- **File Name** (Nom de fichier) : saisissez le nom du fichier à mettre à jour (inutile pour la sauvegarde via HTTP/HTTPS).

ÉTAPE 3 Cliquez sur **Appliquer**.

ÉTAPE 4 Cliquez sur **Redémarrer**.

Procédure de mise à jour ou de sauvegarde du microprogramme via le serveur TFTP :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Opérations du microprogramme**.

Les champs suivants s'affichent :

- **Active Firmware File** (Fichier de microprogramme actif) : indique le fichier de microprogramme actif.
- **Active Firmware Version** (Version du microprogramme actif) : indique la version du fichier de microprogramme actif.

ÉTAPE 2 Renseignez les champs suivants :

- **Operation Type** (Type d'opération) : sélectionnez **Update Firmware** (Mettre à jour le microprogramme) ou **Backup Firmware** (Sauvegarder le microprogramme).
- **Copy Method** (Méthode de copie) : sélectionnez **TFTP**.
- **Définition du serveur** : indiquez si vous souhaitez spécifier le serveur TFTP **par adresse IP** ou **par nom**.

Définition du serveur par adresse :

- **Version IP** : indiquez si une adresse IPv4 ou IPv6 est utilisée pour le serveur.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe FE80, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée)
- **Server IP Address/Name** (Nom/Adresse IP du serveur) : saisissez l'adresse IP ou le nom du serveur TFTP en fonction des informations requises.
- **(Mise à jour) Source** : saisissez le nom du fichier source.
- **(Sauvegarde) Destination** : saisissez le nom du fichier de sauvegarde.

ÉTAPE 3 Cliquez sur **Appliquer** pour commencer l'opération.

Procédure de mise à jour ou de sauvegarde du micrologiciel via SCP :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Opérations du microprogramme**.

Les champs suivants s'affichent :

- **Active Firmware File** (Fichier de microprogramme actif) : indique le fichier de microprogramme actif.
- **Active Firmware Version** (Version du microprogramme actif) : indique la version du fichier de microprogramme actif.

ÉTAPE 2 Renseignez les champs suivants :

- **Operation Type** (Type d'opération) : sélectionnez **Update Firmware** (Mettre à jour le microprogramme) ou **Backup Firmware** (Sauvegarder le microprogramme).
- **Copy Method** (Méthode de copie) : sélectionnez **SCP**.

ÉTAPE 3 Pour activer l'authentification du serveur SSH (qui est désactivée par défaut), cliquez sur **Edit** (Modifier) dans **Remote SSH Server Authentication** (Authentification du serveur SSH distant). Vous accédez à la page Authentification du serveur SSH afin de configurer le serveur SSH.

ÉTAPE 4 Revenez à cette page.

ÉTAPE 5 Sélectionnez l'une des méthodes suivantes pour effectuer l'authentification du client SSH :

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

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

ÉTAPE 6 Renseignez les champs suivants :

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

Définition du serveur **par adresse** :

- **Version IP** : indiquez si l'adresse utilisée est de type IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (si IPv6 est utilisé). Les options sont les suivantes :

  Liaison locale : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.

  Global : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez l'interface de liaison locale dans la liste.

- **Server IP Address/Name** (Nom/Adresse IP du serveur TFTP) : saisissez l'adresse IP ou le nom de domaine du serveur SCP en fonction des informations requises.
- **(Mise à jour) Source** : saisissez le nom du fichier source.
- **(Sauvegarde) Destination** : saisissez le nom du fichier de sauvegarde.

ÉTAPE 7 Cliquez sur **Appliquer**. Si les fichiers, les mots de passe et les adresses du serveur sont corrects, l'une des actions suivantes peut se produire :

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

Pour permuter un fichier image :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Opérations du microprogramme**.

Les champs suivants s'affichent :

- **Active Firmware File** (Fichier de microprogramme actif) : indique le fichier de microprogramme actif.
- **Active Firmware Version** (Version du microprogramme actif) : indique la version du fichier de microprogramme actif.

ÉTAPE 2 Renseignez les champs suivants :

- **Operation Type** (Type d'opération) : sélectionnez **Swap Image** (Permuter l'image).
- **Active Image After Reboot** (Image active après redémarrage) : sélectionnez le fichier de microprogramme qui doit être actif après le redémarrage.
- **Active Image Version Number After Reboot** (Numéro de version de l'image active après redémarrage) : affiche la version du fichier de microprogramme après le redémarrage.

ÉTAPE 3 Cliquez sur **Appliquer**, attendez que le message de réussite s'affiche, puis cliquez sur **Redémarrer** si vous souhaitez recharger immédiatement le nouveau microprogramme.

Opérations de fichiers

Les fonctions disponibles sur la page File Operations (Opérations de fichiers) sont les suivantes :

- Sauvegarde de fichiers de configuration ou de journaux depuis l'appareil vers un périphérique externe.
- Restauration de fichiers de configuration depuis un périphérique externe vers l'appareil.
- Reproduction d'un fichier de configuration.

REMARQUE Si le périphérique fait partie d'une pile, les fichiers de configuration proviennent de l'unité principale.

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

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

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

Lorsque vous cliquez sur **Appliquer** dans une quelconque fenêtre, les modifications que vous avez apportées aux paramètres de configuration de l'appareil sont stockées *uniquement* dans la Configuration d'exécution.

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

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

- De la configuration d'exécution sur la configuration de démarrage ou tout autre fichier de sauvegarde
- De la configuration de démarrage sur la configuration d'exécution ou tout autre fichier de sauvegarde

- D'un fichier de sauvegarde sur la configuration d'exécution ou la configuration de démarrage
- De la configuration miroir sur la configuration d'exécution, la configuration de démarrage ou tout autre fichier de sauvegarde

Les sections suivantes décrivent ces opérations.

Procédure de mise à jour d'un fichier de configuration système via HTTP/HTTPS, USB ou la mémoire interne Flash :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Opérations de fichiers**.

ÉTAPE 2 Renseignez les champs suivants :

- **Type d'opération** : sélectionnez **Mettre à jour le fichier**.
- **Type du fichier de destination** : sélectionnez les types de fichiers de configuration à mettre à jour.
- **Copy Method** (Méthode de copie) : sélectionnez **HTTP/HTTPS**, **USB** ou **Internal Flash** (Mémoire interne Flash).
- **File Name** (Nom de fichier) : saisissez le nom du fichier à partir duquel effectuer la mise à jour (fichier source).

ÉTAPE 3 Cliquez sur **Appliquer** pour commencer l'opération.

Procédure de mise à jour d'un fichier de configuration système via le serveur TFTP :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Opérations de fichiers**.

ÉTAPE 2 Renseignez les champs suivants :

- **Type d'opération** : sélectionnez **Mettre à jour le fichier**.
- **Type du fichier de destination** : sélectionnez les types de fichiers de configuration à mettre à jour.
- **Copy Method** (Méthode de copie) : sélectionnez **TFTP**.
- **Définition du serveur** : indiquez si vous souhaitez spécifier le serveur TFTP par son adresse IP ou son nom de domaine.

Définition du serveur **par adresse** :

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

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

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

  Liaison locale : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.

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

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

- **Server IP Address/Name** (Nom/Adresse IP du serveur) : saisissez l'adresse IP ou le nom du serveur TFTP.
- **Source** : saisissez le nom du fichier de mise à jour.

ÉTAPE 3 Cliquez sur **Appliquer** pour commencer l'opération.

Procédure de mise à jour d'un fichier de configuration système via SCP :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Opérations de fichiers**.

ÉTAPE 2 Renseignez les champs suivants :

- **Type d'opération** : sélectionnez **Mettre à jour le fichier**.
- **Type du fichier de destination** : sélectionnez les types de fichiers de configuration à mettre à jour.
- **Copy Method** (Méthode de copie) : sélectionnez **SCP**.

ÉTAPE 3 Pour activer l'authentification du serveur SSH (qui est désactivée par défaut), cliquez sur **Edit** (Modifier) dans **Remote SSH Server Authentication** (Authentification du serveur SSH distant). Vous accédez à la page Authentification du serveur SSH afin de configurer le serveur SSH.

ÉTAPE 4 Revenez à cette page.

ÉTAPE 5 Sélectionnez l'une des méthodes suivantes pour effectuer **l'authentification du client SSH** :

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

  REMARQUE Le nom d'utilisateur et le mot de passe relatifs aux informations d'identification unique ne seront pas enregistrés dans le fichier de configuration.
- **Définition du serveur** : indiquez si vous souhaitez spécifier le serveur SCP par son adresse IP ou son nom de domaine.

  Définition du serveur **par adresse** :
  - **Version IP** : indiquez si l'adresse utilisée est de type IPv4 ou IPv6.
  - **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (si IPv6 est utilisé). Les options sont les suivantes :

    Liaison locale : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.

    Global : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
  - **Interface de liaison locale** : sélectionnez l'interface de liaison locale dans la liste.
- **Server IP Address/Name** (Nom/Adresse IP du serveur) : saisissez l'adresse IP ou le nom du serveur SCP.
- **Source** : saisissez le nom du fichier source.

ÉTAPE 6 Cliquez sur **Appliquer** pour commencer l'opération.

Procédure de sauvegarde d'un fichier de configuration système via HTTP/HTTPS :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Opérations de fichiers**.

ÉTAPE 2 Renseignez les champs suivants :

- **Type d'opération** : sélectionnez **Sauvegarder le fichier**.
- **Source File Type** (Type du fichier source) : sélectionnez les types de fichiers de configuration à sauvegarder.
- **Copy Method** (Méthode de copie) : sélectionnez **HTTP/HTTPS**.
- **Sensitive Data Handling** (Gestion des données confidentielles) : choisissez la méthode d'inclusion des données confidentielles dans le fichier de sauvegarde. Les options suivantes sont disponibles :
  - *Exclure* : ne pas inclure les données sensibles à la sauvegarde.
  - *Encrypt* (Chiffrer) : inclure les données sensibles dans la sauvegarde, mais en les chiffrant.
  - *Texte en clair* : inclure les données sensibles dans la sauvegarde sous forme de texte en clair.

  REMARQUE Les options disponibles relatives aux données confidentielles sont déterminées par les règles SSD de l'utilisateur actuel. Pour plus d'informations, reportez-vous à la page Règles SSD.

ÉTAPE 3 Cliquez sur **Appliquer** pour commencer l'opération.

Procédure de sauvegarde d'un fichier de configuration système via USB ou la mémoire interne Flash :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Opérations de fichiers**.

ÉTAPE 2 Renseignez les champs suivants :

- **Type d'opération** : sélectionnez **Sauvegarder le fichier**.
- **Source File Type** (Type du fichier source) : sélectionnez les types de fichiers de configuration à sauvegarder.
- **Copy Method** (Méthode de copie) : sélectionnez **USB** ou **Internal Flash** (Mémoire interne Flash).
- **File Name** (Nom de fichier) : saisissez le nom du fichier de sauvegarde de destination.

- **Sensitive Data Handling** (Gestion des données confidentielles) : choisissez la méthode d'inclusion des données confidentielles dans le fichier de sauvegarde. Les options suivantes sont disponibles :
  - *Exclure* : ne pas inclure les données sensibles à la sauvegarde.
  - *Encrypt* (Chiffrer) : inclure les données sensibles dans la sauvegarde, mais en les chiffrant.
  - *Texte en clair* : inclure les données sensibles dans la sauvegarde sous forme de texte en clair.

  REMARQUE Les options disponibles relatives aux données confidentielles sont déterminées par les règles SSD de l'utilisateur actuel. Pour plus d'informations, reportez-vous à la page Règles SSD.

ÉTAPE 3 Cliquez sur **Appliquer** pour commencer l'opération.

Procédure de sauvegarde d'un fichier de configuration système via le serveur TFTP :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Opérations de fichiers**.

ÉTAPE 2 Renseignez les champs suivants :

- **Type d'opération** : sélectionnez **Sauvegarder le fichier**.
- **Source File Type** (Type de fichier source) : sélectionnez le type de fichier à sauvegarder.
- **Copy Method** (Méthode de copie) : sélectionnez **TFTP**.
- **Définition du serveur** : indiquez si vous souhaitez spécifier le serveur TFTP par son adresse IP ou son nom de domaine.

  Définition du serveur **par adresse** :
  - **Version IP** : indiquez si l'adresse utilisée est de type IPv4 ou IPv6.

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

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

  Liaison locale : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.

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

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

- **Server IP Address/Name** (Nom/Adresse IP du serveur) : saisissez l'adresse IP ou le nom du serveur TFTP.
- **Destination** : saisissez le nom du fichier de sauvegarde.
- **Sensitive Data Handling** (Gestion des données confidentielles) : choisissez la méthode d'inclusion des données confidentielles dans le fichier de sauvegarde. Les options suivantes sont disponibles :
  - *Exclure* : ne pas inclure les données sensibles à la sauvegarde.
  - *Encrypt* (Chiffrer) : inclure les données sensibles dans la sauvegarde, mais en les chiffrant.
  - *Texte en clair* : inclure les données sensibles dans la sauvegarde sous forme de texte en clair.

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

ÉTAPE 3 Cliquez sur **Appliquer** pour commencer l'opération.

Procédure de sauvegarde d'un fichier de configuration système via SCP :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Opérations de fichiers**.

ÉTAPE 2 Renseignez les champs suivants :

- **Type d'opération** : sélectionnez **Sauvegarder le fichier**.
- **Source File Type** (Type de fichier source) : sélectionnez le type de fichier à sauvegarder.
- **Copy Method** (Méthode de copie) : sélectionnez **SCP**.

ÉTAPE 3 Pour plus d'informations, consultez la rubrique Authentification des utilisateurs SSH. Renseignez ensuite les champs suivants :

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

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

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

- **Server IP Address/Name** (Nom/Adresse IP du serveur) : saisissez l'adresse IP ou le nom du serveur SCP.
- **Destination** : saisissez le nom du fichier de sauvegarde.
- **Sensitive Data Handling** (Gestion des données confidentielles) : choisissez la méthode d'inclusion des données confidentielles dans le fichier de sauvegarde. Les options suivantes sont disponibles :
  - *Exclure* : ne pas inclure les données sensibles à la sauvegarde.
  - *Encrypt* (Chiffrer) : inclure les données sensibles dans la sauvegarde, mais en les chiffrant.
  - *Texte en clair* : inclure les données sensibles dans la sauvegarde sous forme de texte en clair.

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

ÉTAPE 4 Cliquez sur **Appliquer** pour commencer l'opération.

Procédure de copie d'un fichier de configuration système sur un autre type de fichier de configuration :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Opérations de fichiers**.

ÉTAPE 2 Renseignez les champs suivants :

- **Operation Type** (Type d'opération) : sélectionnez **Duplicate** (Dupliquer).
- **Nom du fichier source** : sélectionnez l'un des types de fichiers de configuration à copier.
- **Destination File Name** (Nom du fichier de destination) : saisissez le fichier de configuration de destination.

ÉTAPE 3 Cliquez sur **Appliquer** pour commencer l'opération.

Répertoire de fichiers

La page File Directory (Répertoire de fichiers) répertorie les fichiers système présents dans le système.

REMARQUE Si la pile contient plusieurs unités, les fichiers affichés proviennent de l'unité principale.

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Répertoire de fichiers**.

ÉTAPE 2 Si nécessaire, activez l'option **Auto Mirror Configuration** (Configuration miroir automatique). Cette option permet d'activer la création automatique de fichiers de configuration miroir. En désactivant cette option, le fichier de configuration miroir est supprimé si vous en aviez créé un. Consultez la section Fichiers système pour obtenir une description des fichiers miroir et pour connaître les raisons qui peuvent vous pousser à éviter la création automatique de fichiers de configuration miroir.

ÉTAPE 3 Sélectionnez le lecteur à partir duquel vous souhaitez afficher les fichiers et les répertoires. Les options suivantes sont disponibles :

- **Flash** : tous les fichiers sont affichés dans le répertoire racine de la station de gestion.
- **USB** : affiche les fichiers sur la clé USB.

ÉTAPE 4 Cliquez sur **Aller à** pour afficher les champs suivants :

- **File Name** (Nom de fichier) : saisissez le système de fichiers ou le nom de fichier en fonction du type de fichier.
- **Autorisations** : définissez les autorisations de lecture/écriture accordées à l'utilisateur du fichier.
- **Size** (Taille) : définissez la taille du fichier.
- **Last Modified** (Dernière modification) : indiquez la date et l'heure de modification du fichier.
- **Full Path** (Chemin d'accès complet) : indiquez le chemin d'accès au fichier.

Configuration/mise à jour automatique de l'image DHCP

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

Cette fonctionnalité comporte les étapes suivantes :

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

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

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

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

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

Protocoles de téléchargement (TFTP ou SCP)

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

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

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

Authentification du client SSH

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

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

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

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

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

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

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

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

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

- Le commutateur utilise le nom de fichier indirect de l'option 125 (DHCPv4) et de l'option 60 (DHCPv6), le cas échéant, dans le message DHCP reçu.
- Si le serveur DHCP n'a pas envoyé le nom de fichier indirect du fichier image du microprogramme, c'est le nom du fichier image indirect de sauvegarde (indiqué sur la page Configuration/mise à jour automatique de l'image DHCP) qui est utilisé.
- Le commutateur télécharge le fichier image indirect, puis en extrait le nom de fichier image sur le serveur TFTP/SCP.
- Le commutateur compare la version du fichier image du serveur TFTP à la version de l'image active du commutateur.
- Si les deux versions sont différentes, la nouvelle version est chargée dans l'image non active, un redémarrage a lieu et l'image non active devient l'image active.
- Lors de l'utilisation du protocole SCP, un message SYSLOG est généré pour indiquer qu'un redémarrage va avoir lieu.
- Lors de l'utilisation du protocole SCP, un message SYSLOG est généré pour confirmer que le processus de mise à jour automatique a eu lieu.

- Lors de l'utilisation du protocole TFTP, des messages SYSLOG sont générés par le processus de copie.

Démarrage de la configuration automatique

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

Options manquantes

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

Sélection du protocole de téléchargement

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

SCP

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

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

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

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

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

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

- Lorsqu'un serveur DHCPv6 envoie des informations à l'appareil. Cet envoi se produit dans les cas suivants :
  - Lorsqu'une interface compatible IPv6 est définie comme client de configuration DHCPv6 sans état.

- Lorsque des messages DHCPv6 sont reçus du serveur (p. ex., lorsque vous appuyez sur le bouton de **redémarrage** d'une page d'interfaces IPv6.
- Lorsque des informations DHCPv6 sont actualisées par l'appareil.
- Lorsque le client DHCPv6 sans état est activé après redémarrage de l'appareil.

- Lorsque les paquets du serveur DHCPv6 contiennent l'option de nom de fichier de configuration.
- Le processus de mise à jour automatique de l'image est déclenché lorsqu'un nom de fichier image indirect est fourni par le serveur DHCP ou qu'un nom de fichier image indirect de sauvegarde a été configuré. Le terme « indirect » signifie qu'il ne s'agit pas de l'image proprement dite, mais d'un fichier qui contient le nom du chemin d'accès à l'image.

Configuration/mise à jour automatique de l'image dans une pile

L'unité principale d'une pile est responsable de la configuration/mise à jour automatique de l'image de la pile entière.

Pour la configuration automatique, le nouveau fichier de configuration est téléchargé vers l'unité principale et synchronisé avec le fichier de sauvegarde avant le rechargement.

Pour la mise à jour automatique de l'image, la nouvelle image est copiée et enregistrée dans l'image non active de l'unité principale. Dans le cadre du processus de copie, l'unité principale synchronise l'image sur toutes les unités de la pile avant de la recharger.

Un fichier de configuration placé sur le serveur TFTP/SCP doit correspondre aux exigences en termes de forme et de format du fichier de configuration pris en charge. La forme et le format du fichier sont vérifiés, mais la validité des *paramètres* de configuration n'est pas contrôlée avant son chargement dans la Configuration de démarrage.

Configuration/mise à jour automatique de l'image DHCP

La Configuration/mise à jour automatique de l'image DHCP permet de configurer le périphérique en tant que client DHCP.

Les valeurs par défaut suivantes existent sur le système :

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

Avant de commencer

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

Préparatifs en vue de la configuration automatique

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

Serveur TFTP/SCP

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

Serveur DHCP

Configurez le serveur DHCP avec les options suivantes :

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

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

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

Serveur TFTP/SCP

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

Serveur DHCP

Configurez le serveur DHCP avec les options suivantes

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

Workflow du client DHCP

ÉTAPE 1 Définissez les paramètres de configuration automatique et/ou de mise à jour automatique de l'image sur la page Configuration/mise à jour automatique de l'image DHCP.

ÉTAPE 2 Définissez le type d'adresse IP sur Dynamique sur la page Configuration IP > Interface IPv4. Définissez le type d'adresse IP sur Dynamique sur la page Interfaces IPv4 et/ou définissez l'appareil en tant que client DHCPv6 sans état sur la page Interfaces IPv6.

Configuration Web

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

ÉTAPE 1 Cliquez sur **Administration** > **Gestion des fichiers** > **Configuration automatique DHCP/ Mise à jour automatique de l'image DHCP**.

ÉTAPE 2 Saisissez les valeurs appropriées.

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

- *TFTP uniquement* : choisissez cette option pour indiquer que seul le protocole TFTP doit être utilisé pour la configuration automatique.
- *SCP uniquement* : choisissez cette option pour indiquer que seul le protocole SCP doit être utilisé pour la configuration automatique.

- **Mise à jour automatique de l'image via DHCP** : sélectionnez ce champ pour activer la mise à jour de l'image du microprogramme depuis le serveur DHCP. Cette fonctionnalité est activée par défaut, mais peut être désactivée ici.
- **Protocole de téléchargement** : sélectionnez une des options suivantes :
  - *Automatique par extension de fichier* : sélectionnez cette option pour indiquer que la mise à jour automatique utilise le protocole TFTP ou SCP en fonction de l'extension du fichier image. Si cette option est sélectionnée, l'extension du fichier du fichier image n'a pas besoin d'être spécifiée. Si vous ne spécifiez rien, l'extension par défaut est utilisée (comme indiqué ci-dessous).
  - *Extension de fichier pour SCP* : si l'option **Automatique par extension de fichier** est sélectionnée, vous pouvez indiquer une extension de fichier ici. Tout fichier portant cette extension est téléchargé via SCP. Si aucune extension n'est saisie, l'extension par défaut **.scp** est utilisée.
  - *TFTP uniquement* : choisissez cette option pour indiquer que seul le protocole TFTP doit être utilisé pour la mise à jour automatique.
  - *SCP uniquement* : choisissez cette option pour indiquer que seul le protocole SCP doit être utilisé pour la mise à jour automatique.
- **Paramètres SSH pour SCP** : lorsque vous utilisez le protocole SCP pour télécharger les fichiers de configuration, sélectionnez l'une des options suivantes :
- **Authentification du serveur SSH distant** : cliquez sur le lien **Activer/désactiver** pour accéder à la page Authentification du serveur SSH. Vous pouvez y activer l'authentification du serveur SSH à utiliser pour le téléchargement et saisir le serveur SSH sécurisé si nécessaire.
- **Authentification du client SSH** : cliquez sur le lien Informations d'identification système pour saisir les informations d'identification utilisateur sur la page Authentification des utilisateurs SSH.
- **Définition du serveur de secours** : indiquez si le serveur de secours sera configuré **Par adresse IP** ou **Par nom**.

ÉTAPE 3 Définition du serveur **par adresse** :

- **Version IP** : indiquez si l'adresse utilisée est de type IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe FE80, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée)

ÉTAPE 4 Saisissez les informations facultatives suivantes qui seront utilisées si le serveur DHCP ne fournit pas les informations requises.

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

  Les champs suivants s'affichent :

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

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres sont copiés dans le fichier de Configuration d'exécution.

7

Administration : Gestion des piles

Cette section décrit la façon dont les piles sont gérées. Elle couvre les sujets suivants :

REMARQUE L'empilage n'est pris en charge que sur les appareils des gammes SG350 (sauf le modèle Sx350) et SG550.

- Vue d'ensemble
- Types d'unités dans une pile
- Topologie de la pile
- Affectation d'ID d'unité
- Processus de sélection de l'unité principale
- Modifications apportées à la pile
- Échec d'unité dans la pile
- Synchronisation automatique du logiciel dans la pile
- Gestion des piles

Vue d'ensemble

Les périphériques peuvent fonctionner de manière autonome ou être connectés à une pile de périphériques opérant dans divers modes d'empilage (reportez-vous à la section Mode de l'unité de pile).

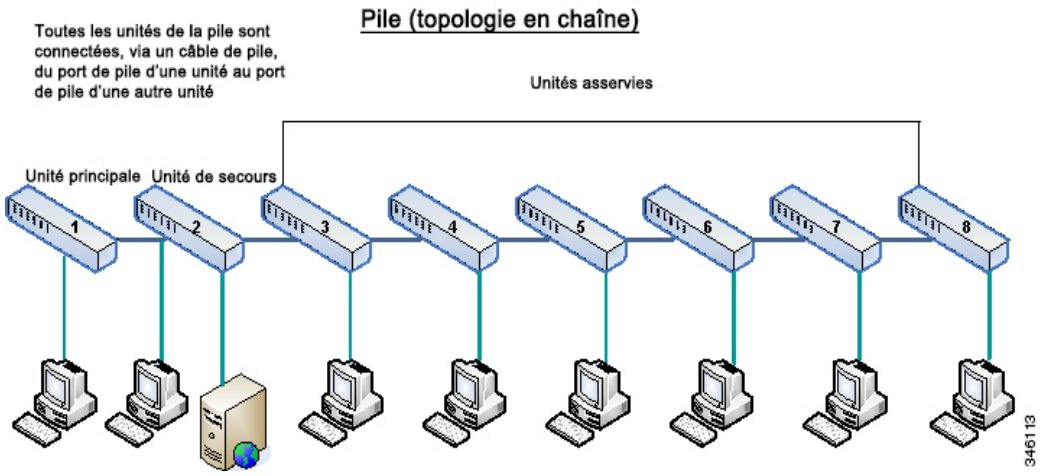
Par défaut, un périphérique est toujours empilable, mais ne dispose d'aucun port configuré comme port de pile. Tous les ports des périphériques sont configurés, par défaut, comme ports réseau. Un périphérique dépourvu de port de pile peut être considéré comme le périphérique principal d'une pile dont il est le seul membre ou comme périphérique autonome. Pour empiler deux ou plusieurs périphériques, reconfigurez les ports réseau souhaités en tant que ports de pile dans les périphériques, puis connectez les périphériques avec les ports de pile résultant selon une topologie en anneau ou en chaîne.

Les périphériques (ou unités) d'une même pile sont connectées via des ports de pile. Ces périphériques sont alors gérés collectivement en tant qu'appareil logique unique. Dans certains cas, les ports de pile peuvent devenir membres d'une pile de LAG (Link Aggregation Group, groupe d'agrégation de liaisons), ce qui augmente la bande passante des interfaces de pile. Reportez-vous à la section Agrégation de liaisons de ports de pile.

La pile est basée sur le modèle suivant : une unité principale/de secours et plusieurs unités asservies.

L'exemple ci-dessous illustre une pile de huit périphériques connectés (pour la gamme 550) :

Architecture de pile (topologie en chaîne)



Une pile offre les avantages suivants :

- La capacité du réseau peut être dynamiquement augmentée ou diminuée. En ajoutant une unité, l'administrateur peut dynamiquement augmenter le nombre de ports de la pile tout en conservant un seul point de gestion. De même, il est possible de supprimer des unités pour réduire la capacité du réseau.
- Le système empilé prend en charge la redondance comme suit :
  - L'unité de secours devient l'unité principale de la pile si l'unité principale d'origine rencontre un problème.
  - Le système de pile prend en charge deux types de topologie : en chaîne et en anneau. Dans une topologie en anneau, si l'un des ports de pile échoue, la pile continue à fonctionner sous la forme d'une topologie de pile (voir Topologie de la pile).

- Un processus appelé Basculement rapide de la liaison de pile (Fast Stack Link Failover) est pris en charge sur les ports d'une pile en chaîne, afin de réduire la durée de la perte des paquets de données lorsque l'un des ports de pile échoue. Jusqu'à ce que la pile soit rétablie dans la nouvelle topologie en chaîne, une unité de pile retourne en boucle les paquets qui devaient transiter par son port de pile défaillant, et transmet aux destinations les paquets renvoyés en boucle via son port de pile. Lors du Basculement rapide de la liaison de pile, les unités principale/de secours restent actives et en état de fonctionnement.

Types d'unités dans une pile

Une unité de pile peut avoir l'un des types suivants :

- **Principale** : l'ID de l'unité principale doit être 1 ou 2. La pile est gérée par l'intermédiaire de l'unité principale qui, elle-même, gère l'unité de secours et les unités asservies.
- **Secours** : en cas d'échec de l'unité principale, c'est l'unité de secours qui endosse le rôle de l'unité principale (basculement). L'ID de l'unité de secours doit être 1 ou 2.
- **Asservies** : ces unités sont gérées par l'unité principale.

Pour qu'un groupe d'unités puisse fonctionner en tant que pile, une unité doit avoir été définie comme unité principale. Lorsque l'unité définie comme unité principale échoue, la pile continue de fonctionner tant qu'il y a une unité de secours (l'unité active qui prend le rôle principal).

Si en plus de l'unité principale, l'unité de secours échoue également, les seules unités qui restent opérationnelles sont les unités asservies qui cessent à leur tour de fonctionner au bout d'une minute. Cela signifie, en d'autres termes, que si au bout d'une minute, vous décidez de raccorder un câble à un port de l'une des unités asservies s'exécutant en l'absence d'unité principale, aucune liaison ne sera établie.

LED d'unité dans la gamme 550

Les périphériques sont pourvus de quatre LED, numérotées de 1 à 4, lesquelles sont utilisées pour indiquer l'ID de chaque unité (par ex., sur l'unité portant l'ID 1, la LED 1 est allumée et les trois autres LED sont éteintes). Pour prendre en charge les ID d'unité dont la valeur dépasse 4, l'allumage des LED a la signification suivante :

- ID d'unité allant de 1 à 4 : la LED 1 est allumée pour identifier l'unité 1, la LED 2, pour identifier l'unité 2, etc., jusqu'à 4.
- ID d'unité 5 : la LED 1 et la LED 4 sont allumées pour identifier l'unité 7.

- ID d'unité 6 : la LED 2 et la LED 4 sont allumées pour identifier l'unité 7.
- ID d'unité 7 : la LED 3 et la LED 4 sont allumées pour identifier l'unité 7.
- ID d'unité 8 : la LED 1, la LED 3 et la LED 4 sont allumées pour identifier l'unité 8.

LED d'unité dans la gamme SG350XG

Les périphériques sont pourvus de quatre LED, numérotées de 1 à 4, lesquelles sont utilisées pour indiquer l'ID de chaque unité (par ex., sur l'unité portant l'ID 1, la LED 1 est allumée et les trois autres LED sont éteintes).

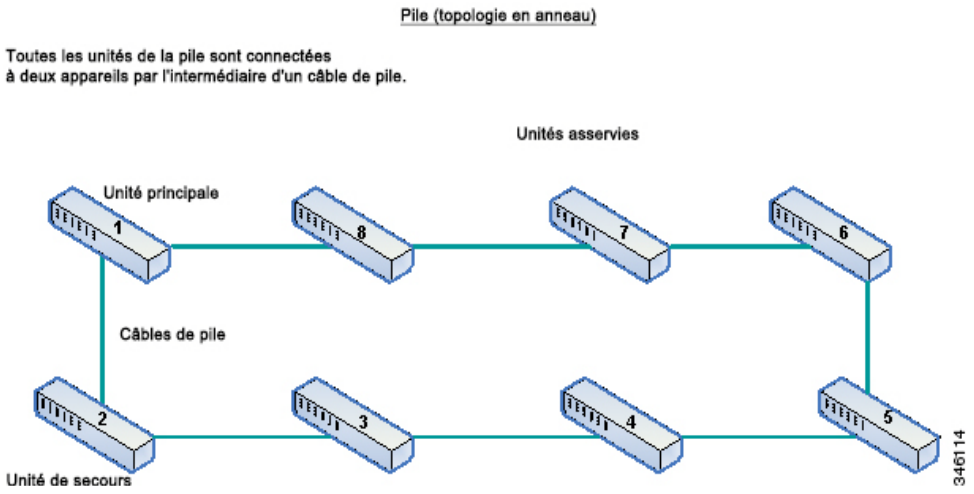
Topologie de la pile

Types de topologie de la pile

Les unités d'une pile peuvent être connectées dans l'un des types de topologie suivants :

- **Topologie en chaîne** : chaque unité est connectée à l'unité voisine, mais il n'existe aucune connexion par câble entre la première et la dernière unité. La figure «Architecture de pile (topologie en chaîne)» illustre une topologie en chaîne.
- **Topologie en anneau** : chaque unité est connectée à l'unité voisine. La dernière unité est connectée à la première unité. L'exemple suivant illustre la topologie en anneau de huit unités :

Pile dans une topologie en anneau (gamme 550)



Une topologie en anneau est plus fiable qu'une topologie en chaîne. L'échec d'une liaison dans un anneau n'affecte pas le fonctionnement de la pile, alors que l'échec d'une liaison dans une connexion en chaîne peut entraîner la division de la pile.

Détection de la topologie

Une pile est établie par un processus appelé la détection de la topologie. Ce processus est déclenché par une modification de l'état actif/inactif d'un port de pile.

Les exemples suivants illustrent des situations dans lesquelles une telle modification peut intervenir :

- Changement de la topologie de la pile d'une formation en anneau à une formation en chaîne
- Fusion de deux piles en une seule pile
- Division de la pile
- Insertion d'autres unités asservies dans la pile (par exemple, parce que les unités ont été précédemment déconnectées de la pile en raison d'une défaillance). Cela peut se produire dans une topologie en chaîne si une unité située au milieu de la pile rencontre un problème.

Lors de la détection de la topologie, chaque unité d'une pile échange des paquets qui contiennent des informations de topologie.

Au terme du processus de détection de la topologie, chaque unité contient les informations de mappage de pile de toutes les unités présentes dans la pile.

Affectation d'ID d'unité

Lorsque la détection de la topologie est terminée, chaque unité présente dans une pile se voit affecter un ID d'unité unique.

L'ID d'unité est défini sur la page Gestion des piles de l'une des façons suivantes :

- **Automatiquement (Auto)** : l'ID d'unité est affecté par le processus de détection de la topologie.
- **Manually** (Manuellement) : l'ID d'unité est défini manuellement sur un nombre entier compris entre 1 et le nombre maximal d'unités dans une pile.

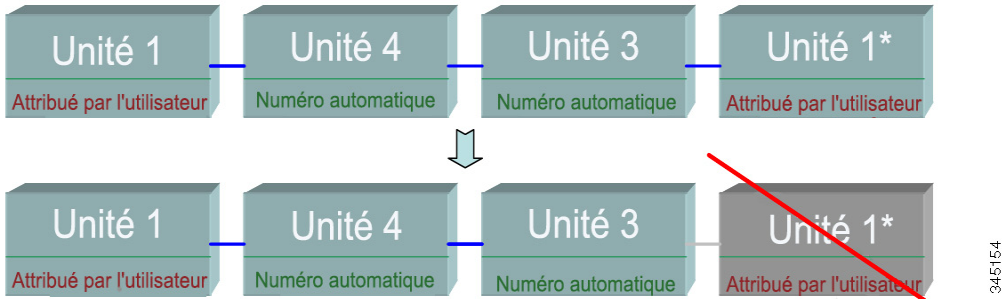
ID d'unité en double

Si vous affectez le même ID d'unité à deux unités distinctes, seule une d'entre elles peut intégrer la pile avec cet ID d'unité.

Si la numérotation automatique a été sélectionnée, l'unité dupliquée se voit affecter un nouveau numéro d'unité. Si la numérotation automatique n'a pas été sélectionnée, l'unité dupliquée est fermée.

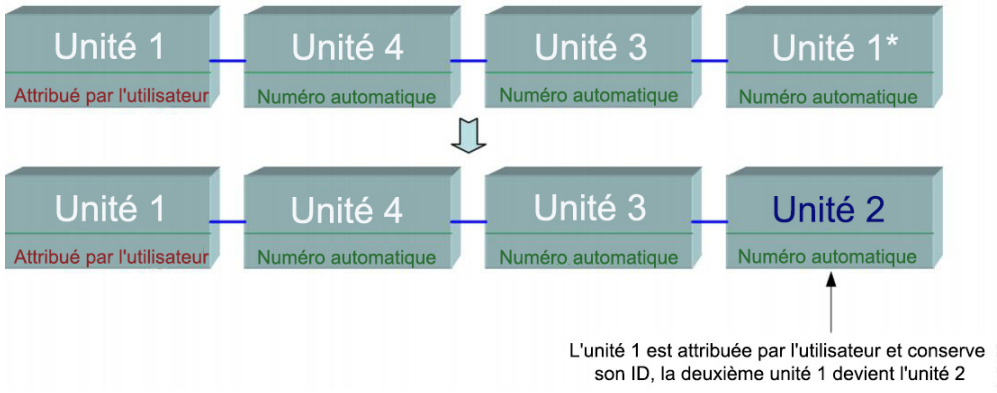
Dans l'exemple ci-dessous, le même ID d'unité est affecté manuellement à deux unités. L'unité 1 n'intègre pas la pile et elle est arrêtée. Elle ne gagne pas le processus de sélection d'unité principale entre les unités définies comme unités principales (1 ou 2).

Unité dupliquée fermée



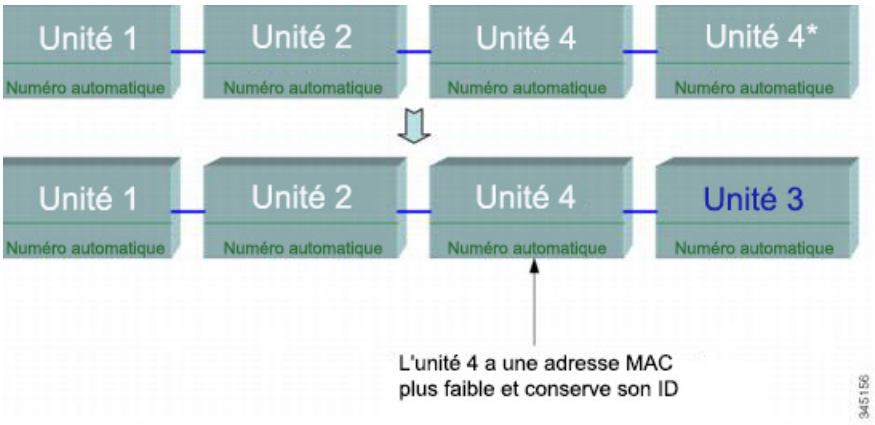
L'illustration suivante présente un exemple dans lequel une des unités dupliquées (numérotées automatiquement) est renumérotée.

Unité dupliquée renumérotée



L'illustration suivante présente un exemple dans lequel une des unités dupliquées est renumérotée. Celle qui a l'adresse MAC la plus basse conserve son ID d'unité (reportez-vous à Processus de sélection de l'unité principale pour obtenir une description de ce processus).

Duplication entre deux unités avec ID d'unité numéroté automatiquement



REMARQUE Si une nouvelle pile comporte plus d'unités que le nombre d'unités maximal, toutes les unités supplémentaires sont arrêtées.

Processus de sélection de l'unité principale

L'unité principale est sélectionnée parmi les unités définies comme unités principales (1 ou 2). Les facteurs de sélection de l'unité principale sont pris en compte selon la priorité suivante :

- **Disponibilité du système** : les unités définies comme unités principales échangent la disponibilité, mesurée par segments de 10 minutes. L'unité qui comporte le plus de segments est alors sélectionnée comme unité principale. Si ces deux unités présentent un nombre identique de segments, c'est l'unité dont l'ID a été défini manuellement qui est sélectionnée comme unité principale, si l'ID de l'autre unité a été définie automatiquement. Dans tous les autres cas, c'est l'unité dont l'ID a la valeur la plus basse qui est sélectionnée. Si l'ID des deux unités est identique, c'est l'unité présentant l'adresse MAC la moins élevée qui est sélectionnée.

  REMARQUE La disponibilité de l'unité de secours est conservée lorsqu'elle est sélectionnée comme unité principale lors du processus de reprise de commutateur.

- **ID d'unité** : si les deux unités ont le même nombre de segments horaires, l'unité ayant l'ID d'unité le plus bas est sélectionnée.

- **Adresse MAC** : si l'ID des deux unités est identique, l'unité ayant l'adresse MAC la plus basse est sélectionnée.

REMARQUE Pour qu'une pile fonctionne, elle doit comporter une unité principale. Une unité principale peut être définie comme l'unité active qui prend le rôle principal. La pile doit contenir une unité 1 et/ou une unité 2 après le processus de sélection de l'unité principale. Sinon, la pile et toutes ses unités sont partiellement fermées, à savoir qu'elles ne sont pas complètement éteintes mais que leurs fonctionnalités de transmission du trafic sont interrompues.

Modifications apportées à la pile

Cette section décrit les différents événements qui peuvent entraîner une modification de la pile. La topologie de la pile change dans l'un des cas suivants :

- Une ou plusieurs unités se connectent à la pile ou se déconnectent de celle-ci.
- Chaque port de la pile a une liaison active ou inactive.
- La pile change entre une formation en anneau et une formation en chaîne.

Lorsque des unités sont ajoutées à une pile ou supprimées de cette pile, elle déclenche des modifications topologiques, un processus de sélection de l'unité principale et/ou l'affectation d'ID d'unité.

Connexion d'une nouvelle unité

Lorsqu'une nouvelle unité est insérée dans la pile, une modification de la topologie de la pile est déclenchée. L'ID d'unité est affecté (en cas de numérotation automatique) et l'unité est configurée par l'unité principale.

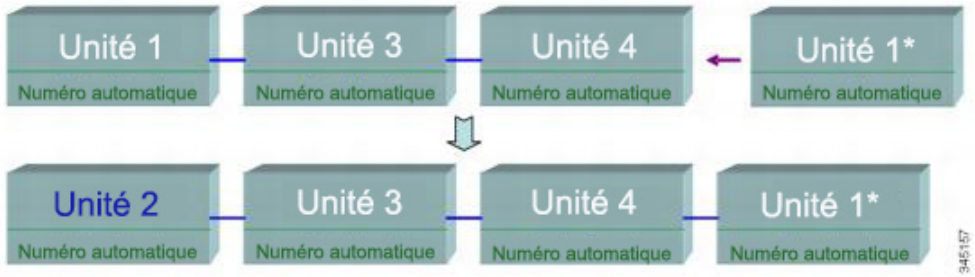
L'un des cas suivants peut se produire lors de la connexion d'une nouvelle unité à une pile existante :

- Aucun ID d'unité n'est dupliqué.
  - Les unités dont les ID sont définis par l'utilisateur conservent leur ID d'unité.
  - Les unités dont les ID sont attribués automatiquement conservent leur ID d'unité.
  - Les unités définies en usine reçoivent automatiquement des ID d'unité, en commençant par l'ID le plus bas disponible.
- Il existe un ou plusieurs ID d'unité dupliqués. La numérotation automatique résout les conflits et affecte des ID d'unité. En cas de numérotation manuelle, seule une unité conserve son ID d'unité et les autres sont fermées.

- Le nombre d'unités dans la pile dépasse le nombre maximal d'unités autorisé. Les nouvelles unités qui viennent de rejoindre la pile sont fermées et un message SYSLOG s'affiche sur l'unité principale.

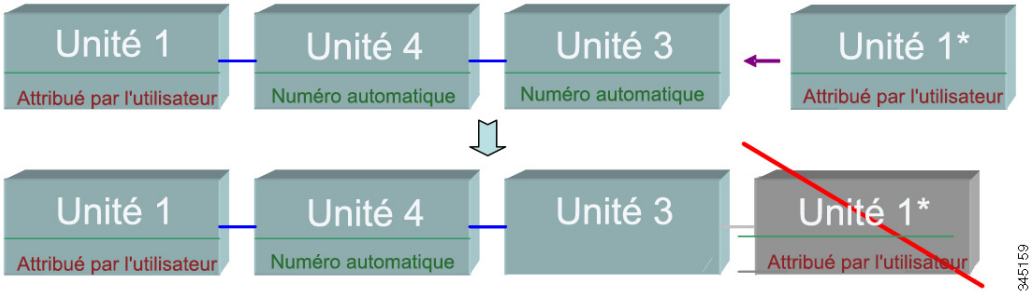
L'illustration suivante présente un exemple de numérotation automatique lorsqu'une unité définie comme unité principale intègre la pile. Deux unités portent l'ID d'unité 1. Le processus de sélection de l'unité principale choisit, parmi ces deux unités, celle qu'il estime être la meilleure pour endosser le rôle de l'unité principale. La meilleure unité est objectivement celle présentant le plus de disponibilités, en d'autres termes le plus grande nombre de segments horaires de 10 minutes. L'autre unité devient alors l'unité de secours.

Unité définie comme unité principale et numérotée automatiquement



L'illustration suivante indique ce qui se passe lorsqu'une unité définie comme unité principale, affectée par l'utilisateur et portant l'ID d'unité 1, intègre une pile qui comporte déjà une unité principale dont l'ID d'unité 1 a été affecté par l'utilisateur. La nouvelle unité 1 n'intègre pas la pile et elle est arrêtée.

Unité définie comme unité principale et affectée par l'utilisateur



Échec d'unité dans la pile

Cette section inclut les rubriques suivantes :

Échec de l'unité principale

Si l'unité principale échoue, l'unité de secours prend le rôle principal et poursuit l'exécution normale de la pile.

Pour que l'unité de secours puisse prendre le relais de l'unité principale, les deux unités restent en permanence à l'état de réserve actif. En état de réserve actif, l'unité principale et son unité de secours sont synchronisées avec la configuration statique (contenue dans les fichiers de Configuration de démarrage et de Configuration d'exécution). Les fichiers de Configuration de secours ne sont pas synchronisés. Le fichier de configuration de sauvegarde reste sur l'unité principale précédente.

Les informations d'état de processus dynamiques, telles que la table des états STP, les adresses MAC apprises dynamiquement, les types de port intelligent appris dynamiquement, les tables de multidiffusion MAC, LACP et GVRP ne sont pas synchronisées.

Lorsqu'une unité principale est configurée, elle synchronise immédiatement l'unité de secours. La synchronisation s'effectue dès l'exécution de la commande. Elle est transparente.

Si une unité est insérée dans une pile en cours d'exécution et qu'elle est sélectionnée en tant qu'unité de secours, l'unité principale procède à sa synchronisation pour qu'elle dispose d'une configuration à jour, puis génère un message SYSLOG pour signaler la fin du processus de synchronisation. Ce message SYSLOG est unique en son genre et s'affiche uniquement en cas de convergence entre l'unité de secours et l'unité principale. Il se présente comme suit : %DSYNCH-I-SYNCH_SUCCEEDED: la synchronisation avec l'unité 2 est présent terminée et s'est déroulée sans incident.

Basculement unité principale/unité de secours

Lorsqu'une unité principale échoue sur la pile, un basculement se produit.

L'unité de secours devient l'unité principale et toutes ses piles de processus et de protocoles sont initialisées pour prendre la responsabilité de l'ensemble de la pile. Ainsi, il n'y a temporairement aucun transfert de trafic dans cette unité, mais les unités asservies restent actives.

REMARQUE Lorsque le protocole STP est utilisé et que la liaison des ports est active, le port STP se trouve de manière temporaire à l'état Blocage et il ne peut donc pas transférer le trafic ou apprendre les adresses MAC. Ceci a pour but d'éviter des boucles Spanning Tree entre les unités actives.

Gestion des unités de secours

Alors que l'unité de secours devient l'unité principale, les unités asservies actives restent actives et continuent à transférer les paquets sur la base de la configuration de l'unité principale d'origine. Cela permet de réduire au maximum l'interruption du trafic de données dans les unités.

Une fois que l'unité de secours a terminé sa transition vers l'état d'unité principale, elle initialise tour à tour chacune des unités asservies en procédant comme suit :

- Supprime et rétablit les valeurs par défaut de la configuration de l'unité asservie (pour empêcher toute configuration incorrecte à partir de la nouvelle unité principale). Ainsi, il n'y a aucun transfert de trafic sur l'unité asservie.
- Appliquer les configurations utilisateur à l'unité asservie.
- Échanger les informations dynamiques comme l'état STP de port, les adresses MAC dynamiques et la liaison active/inactive, entre la nouvelle unité principale et l'unité asservie. Le transfert de paquets sur l'unité asservie reprend lorsque ses ports sont définis par l'unité principale sur l'état de transfert en fonction du STP.

  REMARQUE L'inondation de paquets vers les adresses MAC de monodiffusion inconnues se produit tant que les adresses MAC ne sont pas apprises ou réapprises.

Reconnexion de l'unité principale d'origine après la reprise

Après le basculement, si l'unité d'origine est de nouveau connectée, le processus de sélection de l'unité principale est mis en œuvre. Si l'unité principale d'origine (unité 1) est resélectionnée pour être l'unité principale, alors l'unité principale actuelle (unité 2, qui était l'unité de secours d'origine) est redémarrée et redevient l'unité de secours.

REMARQUE Lors de la reprise de l'unité principale, l'unité de secours reste disponible.

Ports de pile

Par défaut, tous les ports sur le périphérique sont des ports réseau (de liaison montante). Pour connecter les unités, vous devez modifier les types de ports à utiliser pour connecter les périphériques en tant que ports de pile. Ces ports assurent le transfert des paquets de protocole et de données entre les unités.

Vous devez indiquer au système les ports que vous envisagez d'utiliser comme ports de pile (page Gestion des piles). Ces ports sont donc réservés à cet usage.

Les ports suivants peuvent être des ports de pile :

- **Périphériques XG** : tous les ports peuvent être des ports de pile.
- **Périphériques X** : les quatre ports de liaison montante XG peuvent être des ports de pile.

Agrégation de liaisons de ports de pile

Si deux unités voisines sont connectées à plusieurs ports de pile, les ports de pile qui les relient sont automatiquement affectés à un LAG de pile. Cette fonction permet d'augmenter la bande passante de pile du port de pile au-delà de celle d'un port unique.

Il peut exister jusqu'à deux LAG de pile par unité.

Le LAG de pile doit comporter au moins deux ports. Son nombre de ports de pile maximal dépend du type d'unité.

Sur les périphériques Sx550X/SG350, jusqu'à deux interfaces peuvent composer un LAG d'empilage entre 2 unités. La combinaison d'interfaces autorisée pour le même LAG d'empilage est soit composée des interfaces XG1 et XG2, soit des interfaces XG3 et XG4. Aucune autre combinaison d'interfaces n'est prise en charge dans le même LAG de pile.

États des ports de pile

Les ports de pile peuvent présenter l'un des états suivants :

- **Inactif** : l'état opérationnel du port est inactif, ou l'état opérationnel du port de pile est actif, mais le trafic ne peut pas passer sur ce port.
- **Actif** : le port de pile a été ajouté à un LAG de pile dont l'état opérationnel de port de pile est actif et le trafic *peut* passer sur le port ; il fait par ailleurs partie d'un LAG de pile.

- **Standby (Réserve)** : l'état opérationnel du port de pile est actif et le trafic bidirectionnel peut passer sur le port, mais le port ne peut pas être ajouté à un LAG de pile, et le port ne transmet aucun trafic. Un port peut se trouver en mode de réserve pour plusieurs raisons :
  - Des ports de pile présentant des vitesses différentes sont utilisés pour la connexion d'un seul voisin.
  - Sur les périphériques Sx550X/SG350, plus de deux interfaces ou une combinaison d'interfaces non prise en charge sont utilisées pour la connexion à un seul voisin.

Contraintes physiques liées aux LAG de pile

Les facteurs suivants limitent l'utilisation des LAG de pile :

- Un LAG de pile doit contenir des ports présentant la même vitesse.
- En cas de tentative de connexion d'une unité à une pile dont la topologie n'est pas du type Anneau ou Chaîne (par exemple, tentative de connexion d'une unité à plus de deux unités voisines : topologie en étoile), seuls deux LAG de pile peuvent être actifs, les ports de pile restants sont placés en mode de réserve (inactif).

Ports de pile et ports réseau par défaut

Par défaut, tous les ports sont configurés en tant que ports réseau.

Sélection automatique de la vitesse de port

Lorsque le câble d'empilage est connecté au port, son type peut être détecté automatiquement (paramètre par défaut). Lorsque ce paramètre est activé, le système identifie automatiquement le type de câble de pile et sélectionne la vitesse la plus haute prise en charge par ce câble et le port correspondant.

Un message SYSLOG s'affiche au niveau informatif lorsque le type de câble n'est pas reconnu.

Connexion des unités

La connexion entre deux unités au sein d'une même pile peut être établie uniquement si la vitesse des ports de pile situés de part et d'autre de la liaison est identique. Vous devez vérifier que chaque port prend en charge la même vitesse.

Types de câbles

Le tableau suivant décrit les types de câbles pris en charge.

Ports de pile ou ports réseau	
Type de connecteur	Tous les ports
Cisco SFP-H10GB-CU1M – Câble en cuivre passif	1G - 10G
Cisco SFP-H10GB-CU3M – Câble en cuivre passif	1G - 10G
Cisco SFP-H10GB-CU5M – Câble en cuivre passif	1G - 10G
Cisco SFP-10G-SR	10G
Cisco SFP-10G-LRM	Non pris en charge
Cisco SFP-10G-LR	10G
Module SFP 1G MGBSX1	1G
Module SFP 1G MGBT1	1G
Module SFP 1G MGBLX1	1G
Module SFP 1G MGBBX1	1G
100Mbit/s SFP Module MFELX1	Non pris en charge
100Mbit/s SFP Module MFEFX1	Non pris en charge
Module SFP 100Mbs MFEBX1	Non pris en charge
Autres SFP	1G

Synchronisation automatique du logiciel dans la pile

Toutes les unités de la pile doivent exécuter la même version du logiciel. Chaque unité d'une pile télécharge automatiquement le microprogramme à partir de l'unité principale si celui qu'elle exécute est différent de celui de l'unité principale. L'unité redémarre automatiquement pour exécuter la nouvelle version.

Mode de l'unité de pile

Chaque unité présente un mode d'unité de pile qui indique le type des unités de la pile, à savoir :

Pile native

La pile se compose uniquement de périphériques appartenant à la même gamme de produits (350 ou 550) et à la même sous-famille. Cela signifie, par exemple, qu'un périphérique SG350X ne peut être empilé qu'avec un périphérique du même type, et non avec un périphérique SG350XG, et inversement. La même règle s'applique aux périphériques Sx550X et SG550XG.

Pile hybride

En mode Pile hybride, un périphérique SG350X peut être empilé avec un périphérique SG350XG et un périphérique Sx550X peut être empilé avec un périphérique SG550XG.

Pour intégrer une unité dans une pile hybride, elle doit d'abord être configurée en mode Hybride. Pour ce faire, définissez le mode d'empilage sur **Empilage hybride** sur la page Gestion des piles, en suivant la procédure décrite ci-dessous.

Modification du mode d'empilage

La modification du mode d'empilage nécessite un redémarrage du système. Notez également que le passage du mode Natif au mode Hybride efface la configuration du périphérique. Avant de passer du mode Natif au mode Hybride, il est conseillé d'enregistrer le fichier de configuration sur un serveur externe (via TFTP ou HTTP, par exemple).

Le passage du mode Empilage hybride au mode Empilage natif n'efface pas la configuration.

En outre, les 2-4 ports XG des unités Sx350X/Sx550X doivent être configurés comme ports d'empilage et connectés aux ports d'empilage des périphériques SG350XG/SG550XG.

L'ensemble de fonctionnalités est le même pour les périphériques Sx350X et SG350XG (cela vaut également pour les périphériques Sx550X et SG550XG). Il existe toutefois des différences au niveau de la prise en charge des fonctionnalités et de la taille des tables. Pour ces fonctionnalités/tables, la pile hybride prend en charge le plus petit dénominateur commun. Vous trouverez, dans la liste ci-dessous, les différences par type de pile hybride, ainsi que le paramètre utilisé dans chaque type d'unité et dans la pile hybride :

Fonctionnalité/Table	Sx550X	SG550XG	Pile hybride
Port OOB	Non pris en charge	Pris en charge	Non pris en charge
Taille de table MAC	16 000	64 000	16 000
ACL TCAM	3 000 - Réservé	2 000 - Réservé	2 000 - Réservé
Taille de table ARP	4 000 - Réservé	8 000 - Réservé	4 000 - Réservé
Expiration de la table MAC max.	400	630	400

Fonctionnalité/Table	SG350X	SG350XG	Pile hybride
Port OOB	Non pris en charge	Pris en charge	Non pris en charge
Taille de table MAC	16 000	64 000	16 000
ACL TCAM	1 000 - Réservé	2 000 - Réservé	1 000 - Réservé
TCAM routeur	992 (affecte également le paramètre par défaut et maximum pour chaque type)	7168 (affecte également le paramètre par défaut et maximum pour chaque type)	992 (affecte également le paramètre par défaut et maximum pour chaque type)
Taille de table ARP	1 000 - Réservé	8 000 - Réservé	1 000 - Réservé
Nombre de groupes de multidiffusion	2 000	4 000	2 000
Nombre maximum d'interfaces IPv6	106	200	106
Nombre maximum d'hôtes IPv6	210	1776	210
Préfixe IPv6 On-link max.	200	256	200
Expiration de la table MAC max.	400	630	400
Tunnel manuel IPv6 / Tunnel 6tp4 / Tunnel de routage ISATAP	Non pris en charge	Pris en charge	Non pris en charge

Homogénéité des modes d'unité de pile au sein de la pile

Toutes les unités de la pile doivent utiliser le même mode d'unité de pile.

À l'initialisation de la pile, un algorithme de détection de la topologie est exécuté afin de recueillir des informations sur les unités en présence.

Après sélection d'une unité comme unité principale, celle-ci peut rejeter les demandes de connexion émises par les autres unités si leur mode d'unité de pile n'est pas cohérent. En cas de rejet de l'une des unités pour ce motif, cette unité est logiquement fermée (les ports de cette unité ne peuvent plus ni envoyer/ni recevoir du trafic) et toutes ses LED (système, ventilation, ID, ports réseaux et ports de pile) sont allumées. Les informations relatives au mode d'unité de pile discordant sont affichées sous la forme d'un message d'erreur SYSLOG, sur l'unité principale.

Notez que, pour sortir de cet état, la seule méthode consiste à débrancher l'unité de la source électrique, puis à la rebrancher. Cette opération doit être effectuée lorsqu'une unité concernée est déconnectée de la pile. Une fois cette opération effectuée, le mode de l'unité concernée peut être défini sur le mode de pile en cours et l'unité peut intégrer la pile.

Type de l'unité de pile

Si une unité d'un type (GE/FE/XG) est retirée de la pile et remplacée par une unité d'un autre type, le périphérique tente d'appliquer la configuration de l'unité précédente à la nouvelle unité. En règle générale, cela s'effectue sans problème. Il peut toutefois y avoir des exceptions, comme décrit ci-dessous :

- Configuration des ports de liaison descendante : si la pile comprenait une unité d'un type (une unité GE, par exemple) qui a été remplacée par une unité d'un autre type (une unité FE, par exemple), la majeure partie de la configuration basée sur les ports (VLAN, STP, ACL, 802.1x, etc.) est appliquée automatiquement au nouveau type de port. Une partie de la configuration relative à un type de port statique échouera et il se peut que des erreurs soient signalées (par exemple, si la vitesse du port a été configurée sur 1GB et que ce numéro de port sur la nouvelle unité prend en charge une vitesse pouvant atteindre 100 Mbit/s). Cependant, cela n'entraînera pas l'échec du reste de la configuration. Les commandes qui ont échoué sont conservées dans le fichier de configuration d'exécution et de démarrage. Cependant, elles seront supprimées du nouveau fichier de configuration d'exécution au rechargement du système.
- Configuration des ports de liaison montante : si des unités GE/FE sont remplacées par des unités FE/GE, la configuration est la même sur ces deux types d'unité (étant donné que les ports de liaison montante sont toujours des ports XG). La configuration des ports de liaison montante est donc appliquée aux nouvelles unités sans aucune erreur.

Lors du remplacement d'un périphérique FE/GE (prenant en charge le type de port de liaison montante) par un périphérique XG (qui ne prend pas en charge ce type de port), la configuration des ports de liaison montante sur le périphérique XG qui vient d'être inséré est enregistrée dans un type d'interface spécial dont l'ID est compris entre 49 et 52. Ce type d'interface est réservé pour indiquer l'absence de l'interface.

Lors du remplacement d'un type d'unité/interface, les fichiers de configuration d'exécution et de démarrage sont modifiés afin d'afficher correctement le type d'interface. Par exemple, en cas de remplacement d'une ancienne unité de type FE avec l'ID d'interface FE1/0/1 par une unité de type GE, la configuration d'exécution/démarrage (et les commandes show de l'interface de ligne de commande) affiche(nt) automatiquement la configuration sous GE1/0/1.

Gestion des piles

Pour configurer la pile :

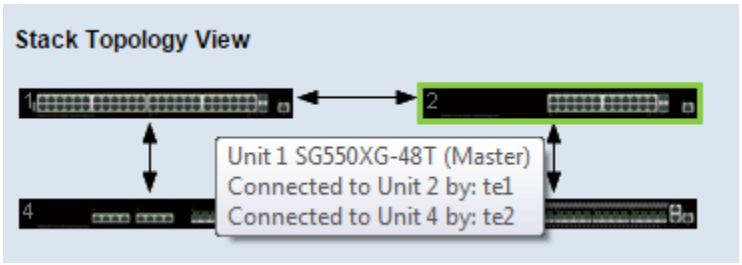
ÉTAPE 1 Cliquez sur **Administration** > **Gestion des piles**.

L'état opérationnel d'un périphérique autonome ou d'une pile s'affiche dans le bloc **État opérationnel de la pile**.

- **Mode de pile** : affiche l'une des options suivantes :
  - *Empilage natif* : le périphérique fait partie d'une pile dans laquelle toutes les unités sont du même type.
  - *Empilage hybride* : le périphérique fait partie d'une pile qui peut être constituée de périphériques 350 de types mixtes ou de périphériques 550 de types mixtes (mais pas d'une combinaison de périphériques 350 et 550).
- **Topologie de la pile** : indique si la topologie de la pile est en chaîne ou en anneau.
- **Unité principale de la pile** : affiche l'ID de l'unité principale de la pile.

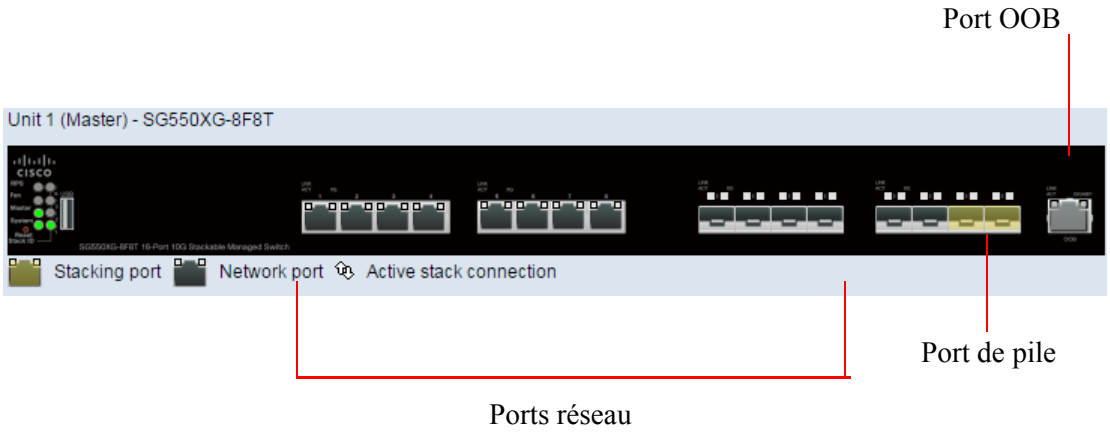
Vue de la topologie de la pile

Cette vue contient une représentation graphique du périphérique. Placez le pointeur de la souris dessus pour afficher le numéro de l'unité, sa fonction dans la pile (unité principale, de secours ou asservie) et les appareils qui y sont connectés dans la pile et via quels ports de pile. Un exemple est illustré ci-dessous :



Vue de l'unité et configuration des ports de pile

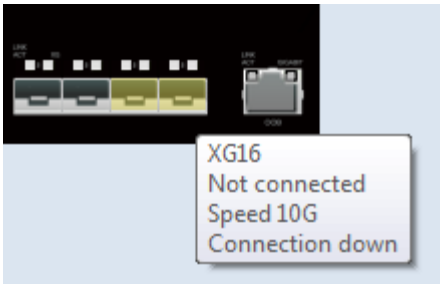
Lorsque vous cliquez sur un périphérique spécifique dans la vue de topologie de la pile, une représentation graphique du périphérique s'affiche. Un exemple est illustré ci-dessous :



ÉTAPE 2 Procédure de sélection de ports de pile pour un périphérique :

a. Cliquez sur un périphérique dans la vue de la topologie de la pile. Les ports de cet appareil sont affichés dans la **Vue de l'unité et configuration des ports de pile**.

b. Lorsque vous placez le pointeur de la souris sur un port, une info-bulle affiche le numéro du port de pile, l'unité qui y est connectée (le cas échéant), le débit du port et son état de connexion. Voici un exemple. Cliquez sur les ports réseau (en noir) à sélectionner en tant



que ports de pile. Le port réseau passe au jaune pour indiquer qu'il jouera le rôle de port de pile. (Si vous cliquez sur un port de pile jaune, celui-ci devient un port réseau (noir)).

ÉTAPE 3 Pour configurer l'ID d'unité après réinitialisation des appareils de la pile, cliquez sur l'appareil dans la vue de la topologie de la pile et renseignez le champ suivant :

- **Unit ID After Reset (ID d'unité après réinitialisation)** : sélectionnez un ID d'unité ou Automatique pour que l'ID d'unité soit affecté par le système.
- **Vitesse de connexion de la pile unité x** : affiche la vitesse de connexion de la pile.

ÉTAPE 4 Cliquez sur **Appliquer et redémarrer**. Les paramètres sont copiés dans le fichier Configuration d'exécution et la pile est redémarrée.

8

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 : il est essentiel que les heures de modification soient cohérentes, quelle que soit la machine sur laquelle se trouvent les systèmes de fichiers.

Pour ces raisons, l'heure configurée sur tous les périphériques du réseau doit être précise.

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

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

- Configuration de l'heure système
- Modes SNTP
- Heure système
- SNTP monodiffusion
- SNTP multidestination/pluridiffusion
- Authentification SNTP
- Plage horaire
- Période récurrente

Configuration de l'heure système

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

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

Time

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

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

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

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

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

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

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

Fuseau horaire et heure d'été

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

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

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

Modes SNTP

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

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

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

Heure système

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

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

Pour définir l'heure système :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres d'heure** > **Heure système**.

Les champs suivants s'affichent :

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

ÉTAPE 2 Saisissez les paramètres suivants :

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

  REMARQUE Le paramètre de source d'horloge doit être défini à l'une des valeurs ci-dessus pour que l'authentification MD5 RIP fonctionne.
- **Paramètres manuels** : définissez la date et l'heure manuellement. L'heure locale est utilisée lorsqu'aucune source d'horloge alternative, telle qu'un serveur SNTP, n'est disponible :
  - *Date* : saisissez la date du système.
  - *Local Time* : saisissez l'heure système.

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

    REMARQUE Le client DHCP prend en charge l'option 100 permettant le réglage dynamique du fuseau horaire.
  - *Fuseau horaire de DHCP* : affiche l'acronyme du fuseau horaire configuré à partir du serveur DHCP. L'acronyme s'affiche dans le champ **Heure actuelle**.
  - *Décalage du fuseau horaire* : sélectionnez la différence en heures entre le *temps du méridien de Greenwich* (GMT) et l'heure locale. Par exemple, le décalage de fuseau horaire pour Paris et GMT+1 et celui pour New York est GMT- 5.
  - *Acronyme du fuseau horaire* : saisissez un nom qui représente ce fuseau horaire. L'acronyme s'affiche dans le champ **Actual Time**.
- **Paramètres d'heure d'été** : sélectionnez le mode de définition de l'heure d'été :
  - *Heure d'été* : sélectionnez cette option pour activer l'heure d'été.
  - *Compensation d'heure définie* : entrez le nombre de minutes de décalage par rapport à l'heure GMT (entre 1 et 1 440). La valeur par défaut est 60.
  - *Type d'heure d'été* : cliquez sur l'un des éléments suivants :

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

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

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

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

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

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

ÉTAPE 3 Sélectionnez *Récurrent* pour personnaliser différemment le début et la fin de l'heure d'été :

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

ÉTAPE 4 Cliquez sur **Appliquer**. Les valeurs d'heure système sont écrites dans le fichier de Configuration d'exécution.

SNTP monodiffusion

Seize serveurs de monodiffusion SNTP maximum peuvent être configurés.

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

Pour ajouter un serveur de monodiffusion SNTP :

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

ÉTAPE 2 Renseignez les champs suivants :

- **Client SNTP monodiffusion** : sélectionnez cette option pour permettre au périphérique d'utiliser des clients monodiffusion SNTP prédéfinis avec des serveurs SNTP monodiffusion.

- **Interface source IPv4** : sélectionnez l'interface IPv4 dont l'adresse IPv4 sera utilisée comme adresse IPv4 source dans les messages utilisés pour les communications avec le serveur SNTP.
- **Interface source IPv6** : sélectionnez l'interface IPv6 dont l'adresse IPv6 sera utilisée comme adresse IPv6 source dans les messages utilisés pour les communications avec le serveur SNTP.

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

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

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

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

ÉTAPE 4 Cliquez sur **Ajouter**.

REMARQUE Pour supprimer tous les serveurs SNTP définis par l'utilisateur, cliquez sur **Restore Default Servers** (Restaurer les serveurs par défaut).

ÉTAPE 5 Saisissez les paramètres suivants :

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

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

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

- **ID de clé d'authentification** : si l'authentification est activée, sélectionnez la valeur de l'ID de clé. Créez des clés d'authentification à l'aide de la page Authentification SNTP.

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

SNTP multidestination/pluridiffusion

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

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

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

Sélectionnez l'une des options suivantes :

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

ÉTAPE 2 Cliquez sur **Ajouter** pour sélectionner l'interface pour SNTP.

Sélectionnez une Interface.

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

Authentification SNTP

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

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

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

Flux de travail

ÉTAPE 1 Activez l'authentification sur la page SNTP Authentication (Authentification SNTP) ci-dessous.

ÉTAPE 2 Créez une clé sur la page SNTP Authentication (Authentification SNTP) ci-dessous.

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

Pour activer l'authentification SNTP et définir des clés :

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

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

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

ÉTAPE 4 Cliquez sur **Ajouter**.

ÉTAPE 5 Saisissez les paramètres suivants :

- **ID de clé d'authentification** : saisissez le numéro utilisé pour identifier cette clé d'authentification SNTP en interne.
- **Clé d'authentification (chiffrée)** : saisissez la clé utilisée pour l'authentification (huit caractères maximum) au format chiffré. Le serveur SNTP doit envoyer cette clé pour que le périphérique se synchronise dessus.
- **Clé d'authentification (texte en clair)** : saisissez la clé utilisée pour l'authentification (huit caractères maximum) au format texte en clair. Le serveur SNTP doit envoyer cette clé pour que le périphérique se synchronise dessus.

- **Clé de confiance** : sélectionnez cette option pour recevoir les informations de synchronisation uniquement à partir d'un serveur SNTP utilisant cette clé d'authentification.

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

Plage horaire

Les périodes peuvent être définies et associées aux types de commandes suivants, afin que ces commandes ne soient appliquées que pendant la période concernée :

- Listes de contrôle d'accès
- Authentification des ports 8021X
- Paramètres des ports
- PoE basé sur une période

Les deux types de plages horaires sont les suivants :

- **Absolu** : ce type de période débute à une date spécifique ou immédiatement et se termine à une date spécifique ou se prolonge indéfiniment. Il est créé dans les pages Période. Un élément récurrent peut lui être ajouté.
- **Récurrent** : ce type de période contient un élément de période qui est ajouté à une plage absolue, et il débute et se termine de manière récurrente. Il est créé dans les pages Plage récurrente.

Si une période comprend à la fois des plages absolues et des plages récurrentes, les opérations des commandes associées ne sont activées que si l'heure de début absolue et la période récurrente ont été atteintes. Les opérations des commandes associées sont inactives si l'une des plages horaires a été atteinte.

Le périphérique prend en charge 10 périodes absolues au maximum.

Toutes les spécifications horaires sont interprétées en heure locale (l'heure d'été n'a aucune incidence). Afin de s'assurer que les entrées de la période prennent effet aux heures souhaitées, l'heure système doit être définie.

La fonction Période permet d'effectuer les tâches suivantes :

- Limiter l'accès des ordinateurs au réseau aux horaires de travail (par exemple) : par la suite, les ports réseau sont ainsi verrouillés et l'accès au reste du réseau est bloqué (voir Paramètres des ports et Agrégation de liaisons).
- Limiter l'alimentation PoE à une période définie.

Période absolue

Pour définir une période absolue :

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

Les périodes existantes s'affichent.

ÉTAPE 2 Pour ajouter une nouvelle période, cliquez sur **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants :

- **Nom de période** : saisissez un nouveau nom de période.
- **Heure de début absolue** : pour définir l'heure de début, renseignez les champs suivants :
  - *Immédiat* : sélectionnez cette option pour que la période démarre immédiatement.
  - *Date, Heure* : saisissez la date et l'heure auxquelles la période débute.
- **Heure de fin absolue** : pour définir l'heure de fin, renseignez les champs suivants :
  - *Infini* : sélectionnez cette option pour que la période ne se termine jamais.
  - *Date, Heure* : saisissez la date et l'heure auxquelles la période se termine.

ÉTAPE 4 Cliquez sur **Appliquer**.

ÉTAPE 5 Pour ajouter une période récurrente, cliquez sur **Plage récurrente**.

Période récurrente

Il est possible d'ajouter un élément de temps récurrent à une période absolue. Cela limite l'opération à certaines périodes au sein de la plage absolue.

Pour ajouter un élément de période récurrent à une période absolue :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres d'heure** > **Plage récurrente**.

Les périodes récurrentes existantes s'affichent (filtrées par période spécifique absolue).

ÉTAPE 2 Sélectionnez la période absolue à laquelle ajouter la plage récurrente.

ÉTAPE 3 Pour ajouter une nouvelle période récurrente, cliquez sur **Ajouter**.

ÉTAPE 4 Renseignez les champs suivants :

- **Heure de début récurrente** : saisissez la date et l'heure auxquelles la période débute sur une base récurrente.
- **Heure de fin récurrente** : saisissez la date et l'heure auxquelles la période se termine de façon récurrente.

ÉTAPE 5 Cliquez sur **Appliquer**.

ÉTAPE 6 Cliquez sur **Période** pour accéder à la page **Période absolue**.

9

Administration : Détection

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

Elle couvre les rubriques suivantes :

- Bonjour
- LLDP et CDP
- Détection - LLDP
- Détection - CDP

Bonjour

En tant que client Bonjour, le périphérique diffuse périodiquement des paquets de protocole de détection Bonjour vers un ou plusieurs sous-réseaux IP à connexion directe, annonçant ainsi sa propre existence et les services qu'il offre ; par exemple HTTP, HTTPs et Telnet. Utilisez la page Services TCP/UDP pour activer ou désactiver les services de l'appareil. Le périphérique peut être détecté par un système de gestion du réseau ou une autre application tierce. Par défaut, Bonjour est activé sur le VLAN de gestion.

Lorsque vous activez Bonjour sur le périphérique, celui-ci envoie des paquets de détection Bonjour vers les interfaces dotées d'adresses IP qui ont été associées à Bonjour sur la table de contrôle des interfaces de détection Bonjour. Utilisez l'Interfaces IPv4 pour configurer une adresse IP sur une interface.

Si une interface telle que VLAN est supprimée, le périphérique lui envoie des paquets Bonjour Goodbye pour désenregistrer l'interface et ses services. Les périphériques voisins qui reçoivent les paquets Goodbye suppriment les services de leurs tables de services locales. La table de contrôle des interfaces de détection Bonjour montre les interfaces dont les adresses IP sont associées à la fonction Bonjour. Les notifications Bonjour peuvent être diffusées uniquement sur les interfaces qui sont mentionnées dans cette table. Si un service est activé ou désactivé, le

périphérique envoie des paquets Bonjour afin d'enregistrer ou de désenregistrer le service en conséquence. Si un service est modifié, le périphérique envoie des paquets Bonjour avec les nouvelles informations. Si l'adresse IP du périphérique est modifiée, le périphérique notifie également sa nouvelle adresse IP.

Si Bonjour est désactivé, le périphérique cesse d'envoyer les annonces de détection Bonjour et n'écoute plus les annonces de détection Bonjour envoyées par d'autres périphériques.

Pour configurer le protocole Bonjour :

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

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

ÉTAPE 3 Pour activer Bonjour sur une interface spécifique, cliquez sur **Ajouter**.

ÉTAPE 4 **Sélectionnez** l'interface. Si une adresse IP a été attribuée à l'interface, celle-ci est affichée.

ÉTAPE 5 Cliquez sur **Appliquer** pour mettre à jour le fichier de Configuration d'exécution.

REMARQUE Cliquez sur **Supprimer** pour désactiver Bonjour sur une interface (le système effectue alors la suppression sans réaliser d'autres opérations, telles qu'**Appliquer**).

LLDP et CDP

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

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

- CDP/LLDP peut être activé ou désactivé globalement, ou pour chaque port. La fonctionnalité CDP/LLDP d'un port ne s'applique que si CDP/LLDP est globalement activé.
- Si CDP/LLDP est globalement activé, le périphérique élimine les paquets CDP/LLDP entrants provenant des ports où CDP/LLDP est désactivé.

- Si CDP/LLDP est globalement désactivé, le périphérique peut être configuré pour ignorer l'inondation tenant compte du VLAN, ou l'inondation ne tenant pas compte du VLAN, de tous les paquets CDP/LLDP entrants. L'inondation tenant compte du VLAN transmet un paquet CDP/LLDP entrant au VLAN où le paquet est reçu, mais pas au port d'entrée. L'inondation ne tenant pas compte du VLAN transmet un paquet CDP/LLDP entrant à tous les ports, sauf au port d'entrée. Par défaut, le système élimine les paquets CDP/LLDP lorsque CDP/LLDP est désactivé au niveau global. Vous pouvez configurer l'élimination/l'inondation des paquets CDP et LLDP entrants respectivement sur les pages Propriétés CDP et Propriétés LLDP.
- La fonction Port intelligent automatique requiert l'activation de CDP et/ou LLDP. La fonction Port intelligent automatique configure automatiquement une interface basée sur l'annonce CDP/LLDP reçue de l'interface.
- Les périphériques d'extrémité CDP et LLDP, tels que les téléphones IP, apprennent la configuration VLAN voix des annonces CDP et LLDP. Par défaut, le périphérique est activé pour envoyer une annonce CDP et LLDP basée sur le VLAN voix qui est configuré sur le périphérique. Pour plus d'informations, reportez-vous à la section VLAN voix.

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

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

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

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

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

Détection - LLDP

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

Présentation de LLDP

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

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

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

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

Flux de travail de configuration de LLDP

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

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

Propriétés LLDP

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

Pour saisir des propriétés LLDP :

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

ÉTAPE 2 Saisissez les paramètres.

- **État LLDP** : sélectionnez cette option pour activer LLDP sur le périphérique (activée par défaut).
- **Traitement des trames LLDP** : si LLDP n'est pas activé, sélectionnez l'action à réaliser en cas de réception d'un paquet correspondant aux critères sélectionnés :
  - *Filtrage* : supprime le paquet.
  - *Inondation* : transfère le paquet à tous les membres du VLAN.
- **Intervalle d'annonce TLV** : définissez, en nombre de secondes, la fréquence d'envoi des mises à jour des annonces LLDP ou utilisez la valeur par défaut.

- **Intervalle de notification SNMP de changement de topologie** : saisissez le délai minimal entre deux notifications SNMP.
- **Multiplicateur de conservation** : saisissez la durée de conservation des paquets LLDP avant leur élimination, en multiples de l'intervalle d'annonce TLV. Par exemple, si l'intervalle d'annonce TLV est de 30 secondes et que le multiplicateur de conservation (Hold Multiplier) est 4, les paquets LLDP seront supprimés après 120 secondes.
- **Délai de réinitialisation** : saisissez l'intervalle en secondes qui sépare la désactivation et la réactivation de LLDP, suite à un cycle d'activation ou de désactivation de LLDP.
- **Délai de transmission** : saisissez le délai en secondes qui séparera deux transmissions de trames LLDP successives en cas de modification dans la MIB de systèmes locaux LLDP.
- **Notification d'ID de châssis** : sélectionnez l'une des options suivantes pour une notification dans les messages LLDP :
  - *Adresse MAC* : spécifiez l'adresse MAC du périphérique.
  - *Nom d'hôte* : spécifiez le nom d'hôte de ce périphérique.

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

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

Paramètres des ports

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

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

Pour définir les paramètres des ports LLDP :

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

Cette page affiche les informations LLDP des ports.

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

Cette page contient les champs suivants :

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

  L'intervalle entre deux notifications est défini dans le champ Topology Change SNMP Notification Interval (Intervalle de notification SNMP de changement de topologie) de la page Propriétés LLDP. Définissez les destinataires des notifications SNMP à l'aide de la page Destinataires de notifications SNMPv1.2.
- **TLV facultatives sélectionnées** : sélectionnez les informations que le périphérique doit publier en déplaçant la TLV voulue depuis la liste **TLV facultatives disponibles**. Les TLV disponibles contiennent les informations suivantes :
  - *Description du port* : informations sur le port, notamment son fabricant, son nom de produit et la version du matériel/logiciel.
  - *Nom du système* : nom attribué au système, au format alphanumérique. Cette valeur est identique à l'objet sysName.
  - *Description du système* : description de l'entité réseau, au format alphanumérique. Inclut le nom du système et la version du matériel, le système d'exploitation et les logiciels réseau pris en charge par le périphérique. Cette valeur est identique à l'objet sysDescr.

- *Fonctionnalités du système* : fonctions principales du périphérique. L'écran indique aussi si ces fonctions sont activées sur le périphérique. Les fonctionnalités sont indiquées par deux octets. Les bits 0 à 7 indiquent respectivement Autres, Répéteur, Pont, Point d'accès WLAN, Routeur, Téléphone, Système de câble DOCSIS et Station. Les bits 8 à 15 sont réservés.
- *802.3 MAC-PHY* : fonction duplex et débit, avec les paramètres duplex et de débit actuels du périphérique d'envoi. L'écran indique également si les paramètres actuels sont obtenus par négociation automatique ou par configuration manuelle.
- *Alimentation 802.3 via MDI* : alimentation maximale transmise via MDI.
- *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.
- *Alimentation à 4 fils via MDI* : (concerne les ports PoE prenant en charge un PoE de 60 watts) TLV conçue par Cisco pour prendre en charge l'alimentation PoE (Power over Ethernet) qui fournit 60 watts (de série, vous ne bénéficiez que de 30 watts).

TLV facultative d'adresse de gestion

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

VLAN et protocole 802.1

- **PVID** : sélectionnez cette option pour annoncer le PVID dans la TLV.
- **Port and Protocol VLAN ID** : ID VLAN du port et du protocole.
- **ID VLAN** : sélectionnez les VLAN qui feront l'objet d'une annonce.
- **ID des protocoles** : sélectionnez les protocoles qui feront l'objet d'une annonce.
- **ID des protocoles sélectionnés** : sélectionnez les protocoles à utiliser dans la case **ID des protocoles**, puis placez-les dans la case **ID des protocoles sélectionnés**.

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

Stratégie réseau LLDP MED

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

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

Configuration d'une stratégie réseau LLDP MED

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

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

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

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

Pour définir une stratégie réseau LLDP MED :

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

Cette page contient les stratégies réseau précédemment créées.

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

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

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

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

ÉTAPE 5 Saisissez les valeurs appropriées :

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

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

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

Paramètres des ports LLDP MED

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

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

Pour configurer LLDP MED sur chaque port :

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

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

- **Stratégie réseau définie par l'utilisateur** : stratégies définies pour les types de trafic (appelées applications). Vous utilisez pour ce faire la Stratégie réseau LLDP MED. Dans ce cas, les informations suivantes sont affichées pour la stratégie sur le port :
  - *Actif* : le type de trafic actif sur le port.
  - *Application* : le type de trafic pour lequel la stratégie est définie.
- **Lieu** : indique si la TLV de lieu est transmise.
- **PoE** : indique si la TLV PoE-PSE est transmise.
- **Inventaire** : indique si la TLV d'inventaire est transmise.

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

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

ÉTAPE 4 Configurez les paramètres suivants :

- **Interface** : sélectionnez l'interface à configurer.
- **État LLDP MED** : activez/désactivez LLDP MED sur ce port.
- **Notification SNMP** : indiquez si la notification SNMP doit être envoyée, port par port, lorsqu'une station de travail prenant en charge MED est détectée (un système de gestion SNMP, par exemple), lors d'un changement de topologie.
- **TLV facultatives sélectionnées** : sélectionnez les TLV que le périphérique peut publier en les déplaçant de la liste **TLV facultatives disponibles** vers la liste TLV facultatives sélectionnées.
- **Selected Network Policies** (Stratégies réseau disponibles) : sélectionnez les stratégies LLPD MED que LLDP va publier en les déplaçant de la liste **Available Network Policies** (Stratégies réseau disponibles) vers la liste **Selected Network Policies** (Stratégies réseau sélectionnées). Vous les aviez précédemment créées sur la page Stratégie réseau LLDP MED. Pour inclure une ou plusieurs stratégies réseau définies par l'utilisateur dans l'annonce, vous devez aussi sélectionner **Stratégie réseau** dans les **TLV facultatives disponibles**.

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

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

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

État des ports LLDP

La page LLDP Port Status (État des ports LLDP) contient des informations globales LLDP pour chaque port.

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

Les informations concernant tous les ports, notamment le port OOB, s'affichent.

ÉTAPE 2 Sélectionnez un port spécifique, puis cliquez sur **LLDP Local Information Detail** (Détails sur les informations locales LLDP) pour consulter le détail des TLV LLDP et LLDP MED envoyées au port.

ÉTAPE 3 Sélectionnez un port spécifique, puis cliquez sur **Détails sur les informations de voisinage LLDP** pour consulter les informations relatives aux TLV LLDP et LLDP MED reçues du port.

- **Informations globales d'état des ports LLDP**
- **Sous-type de l'ID du châssis** : type d'ID de châssis (adresse MAC, par exemple).
- **Chassis ID** : identificateur du châssis. Si vous avez choisi l'adresse MAC comme sous-type d'ID de châssis, l'adresse MAC du périphérique s'affiche.
- **Nom du système** : nom du périphérique.
- **Description du système** : description du périphérique, au format alphanumérique.
- **Supported System Capabilities** : fonctions principales du périphérique telles que Bridge (pont), WLAN AP (point d'accès WLAN) ou Router (routeur).
- **Fonctionnalités système activées** : fonctions principales activées sur le périphérique.
- **Port ID Subtype** : type d'ID de port affiché.
- **Table d'état des ports LLDP**
- **Interface** : identificateur de port.
- **État LLDP** : option de publication LLDP.
- **État LLDP MED** : indique si la fonction est activée ou désactivée.
- **Local PoE (Power Type, Power Source, Power Priority, Power Value)** (PoE local [Type d'alimentation, Source d'alimentation, Priorité d'alimentation]) : informations PoE locales annoncées.

- **Remote PoE (Power Type, Power Source, Power Priority, Power Value)** (PoE distant [Type d'alimentation, Source d'alimentation, Priorité d'alimentation]) : informations PoE annoncées par le voisin.
- **# of neighbors** : nombre de voisins détectés.
- **Fonctionnalités de voisinage du 1er périphérique** : affiche les fonctions principales du voisin, par exemple : pont ou routeur.

Informations locales LLDP

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

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

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

Cette page contient les champs suivants pour l'interface sélectionnée (notamment le port OOB) :

Global

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

Management Address (adresse de gestion)

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

- **Adresse IPv4** : adresse IPv4 renvoyée qui convient le mieux pour la gestion.
- **Adresse IPv6 globale** : adresse IPv6 globale renvoyée qui convient le mieux pour la gestion.
- **Adresse IPv6 liaison locale** : adresse IPv6 liaison locale renvoyée qui convient le mieux pour la gestion.

MAC/PHY Details (informations MAC/PHY)

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

802.3 Details (informations relatives à 802.3)

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

802.3 Link Aggregation (agrégation de liaisons 802.3)

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

Alimentation 802.3 via MDI

- **Classe de port de prise en charge de l'alimentation MDI** : classe de port annoncée pour la prise en charge de l'alimentation.
- **Prise en charge de l'alimentation MDI PSE** : indique si l'alimentation MDI est prise en charge sur le port.
- **État de l'alimentation MDI PSE** : indique si l'alimentation MDI est activée sur le port.
- **Capacité de contrôle des paires d'alimentation PSE** : indique si le contrôle des paires d'alimentation est pris en charge sur le port.
- **Paire d'alimentation PSE** : type de contrôle des paires d'alimentation pris en charge sur le port.
- **Classe d'alimentation PSE** : classe de port annoncée pour l'alimentation.
- **Type d'alimentation** : type d'appareil alimenté connecté au port.
- **Source d'alimentation** : source d'alimentation du port.
- **Priorité d'alimentation** : priorité d'alimentation du port.
- **Valeur d'alimentation exigée par l'appareil alimenté** : quantité d'énergie allouée par le PSE à l'appareil alimenté.
- **Valeur d'alimentation allouée au PSE** : quantité d'énergie allouée à l'équipement source d'alimentation (PSE).

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

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

Alimentation à 4 fils via MDI

- **Prise en charge de PoE à 4 paires** : indique que le système et le port prennent en charge les câbles à 4 paires (uniquement pour les ports spécifiques qui disposent de cette capacité matérielle).
- **Détection des paires de rechange/Classification requise** : indique qu'un câble à 4 paires est nécessaire.
- **État voulu de la paire de rechange de l'appareil alimenté** : indique qu'un appareil alimenté demande à activer la fonctionnalité 4 paires.
- **État opérationnel de la paire de rechange de l'appareil alimenté** : indique si la fonctionnalité 4 paires est activée ou désactivée.

MED Details (informations MED)

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

- **Manufacturer Name** : nom du fabricant du périphérique.
- **Model Name** : nom du modèle de périphérique.
- **Asset ID** : ID de la ressource.

Location Information (informations sur l'emplacement)

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

Network Policy Table (table des stratégies réseau)

- **Type d'application** : type d'application de la stratégie réseau. Exemple : Voix.
- **VLAN ID** : ID du VLAN pour lequel la stratégie réseau est définie.
- **Type de VLAN** : 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.
- **Priorité d'utilisateur** : priorité d'utilisateur de la stratégie réseau.
- **DSCP** : DSCP de la stratégie réseau.

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

Informations de voisinage LLDP

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

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

Pour afficher les informations LLDP des voisins :

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

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

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

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

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

La page Informations de voisinage LLDP comporte les champs suivants :

Détails du port

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

Détails de base

- **Sous-type de l'ID du châssis** : type d'ID de châssis (adresse MAC, par exemple).
- **ID du châssis** : identifiant du châssis du périphérique de voisinage réseau (LAN) 802.
- **Port ID Subtype** : type d'ID de port affiché.
- **Port ID** : identificateur du port.
- **Description du port** : informations sur le port, notamment son fabricant, son nom de produit et la version du matériel/logiciel.
- **Nom du système** : nom du système publié.

- **Description du système** : description de l'entité réseau, au format alphanumérique. Inclut le nom du système et la version du matériel, le système d'exploitation et les logiciels réseau pris en charge par le périphérique. Cette valeur est identique à l'objet sysDescr.
- **Fonctionnalités système prises en charge** : fonctions principales du périphérique. Les fonctionnalités sont indiquées par deux octets. Les bits 0 à 7 indiquent respectivement Autres, Répéteur, Pont, Point d'accès WLAN, Routeur, Téléphone, Système de câble DOCSIS et Station. Les bits 8 à 15 sont réservés.
- **Fonctionnalités système activées** : fonctions principales activées sur le périphérique.

Table des adresses de gestion

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

MAC/PHY Details (informations MAC/PHY)

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

Alimentation 802.3 via MDI

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

- **Capacité de contrôle des paires d'alimentation PSE** : indique si le contrôle des paires d'alimentation est pris en charge sur le port.
- **Paire d'alimentation PSE** : type de contrôle des paires d'alimentation pris en charge sur le port.
- **Classe d'alimentation PSE** : classe de port annoncée pour l'alimentation.
- **Type d'alimentation** : type d'appareil alimenté connecté au port.
- **Source d'alimentation** : source d'alimentation du port.
- **Priorité d'alimentation** : priorité d'alimentation du port.
- **Valeur d'alimentation exigée par l'appareil alimenté** : quantité d'énergie demandée par l'appareil alimenté.
- **Valeur d'alimentation allouée par le PSE** : quantité d'énergie allouée par le PSE à l'appareil alimenté.

Alimentation à 4 fils via MDI

- **Prise en charge de PoE à 4 paires** : indique que le système et le port prennent en charge les câbles à 4 paires (uniquement pour les ports spécifiques qui disposent de cette capacité matérielle).
- **Détection des paires de rechange/Classification requise** : indique qu'un câble à 4 paires est nécessaire.
- **État voulu de la paire de rechange de l'appareil alimenté** : indique qu'un appareil alimenté demande à activer la fonctionnalité 4 paires.
- **État opérationnel de la paire de rechange de l'appareil alimenté** : indique si la fonctionnalité 4 paires est activée ou désactivée.

802.3 Details (informations relatives à 802.3)

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

802.3 Link Aggregation (agrégation de liaisons 802.3)

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

802.3 Energy Efficient Ethernet (EEE)

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

MED Details (informations MED)

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

- **Serial Number** : numéro de série du périphérique.
- **Manufacturer Name** : nom du fabricant du périphérique.
- **Model Name** : nom du modèle de périphérique.
- **Asset ID** : ID de la ressource.

VLAN et protocole 802.1

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

PPVID

Table PPVID

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

ID VLAN

Table des ID VLAN

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

Table des ID de protocole

- **ID des protocoles** : ID des protocoles annoncés.

Location Information (informations sur l'emplacement)

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

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

Network Policy Table (table des stratégies réseau)

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

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

Statistiques LLDP

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

Pour afficher les statistiques LLDP :

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

Pour chaque port, les champs suivants sont affichés :

- **Interface** : identificateur de l'interface (peut également correspondre au port OOB).
- **Trames émises (total)** : nombre de trames transmises.
- **Trames reçues**
  - *Total* : nombre des trames reçues.
  - *Éliminé* : nombre des trames reçues qui ont été éliminées.
  - *Erreurs* : nombre total des trames reçues comportant des erreurs.
- **TLV reçues**
  - *Éliminée* : nombre de TLV reçues qui ont été éliminées.
  - *Non reconnue* : nombre de TLV reçues non reconnues.
- **Nombre de suppressions d'informations du voisin** : nombre d'expirations du délai maximal du voisin sur l'interface.

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

Surcharge LLDP

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

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

Pour afficher les informations de surcharge LLDP :

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

Cette page contient les champs suivants, pour chaque port :

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

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

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

- **LLDP Mandatory TLVs (TLV LLDP obligatoires)**
  - *Taille (octets)* : taille totale des TLV obligatoires, en octets.
  - *État* : indique si un groupe de TLV obligatoires est en cours de transmission ou si une surcharge est intervenue.
- **LLDP MED Capabilities (fonctionnalités LLDP MED)**
  - *Taille (octets)* : taille totale des paquets de fonctionnalités LLDP MED, en octets.
  - *État* : indique si les paquets de fonctionnalités LLDP MED ont été envoyés ou si une surcharge est survenue.

- **LLDP MED Location (emplacement LLDP MED)**
  - *Taille (octets)* : taille totale des paquets d'emplacement LLDP MED, en octets.
  - *État* : indique si les paquets d'emplacement LLDP MED ont été envoyés ou si une surcharge est survenue.
- **LLDP MED Network Policy (stratégie réseau LLDP MED)**
  - *Taille (octets)* : taille totale des paquets de stratégie réseau LLDP MED, en octets.
  - *État* : indique si les paquets de stratégie réseau LLDP MED ont été envoyés ou si une surcharge est survenue.
- **Alimentation LLDP MED étendue via MDI**
  - *Taille (octets)* : taille totale des paquets d'alimentation LLDP MED étendue via MDI, en octets.
  - *État* : indique si les paquets d'alimentation LLDP MED étendue via MDI ont été envoyés ou si une surcharge est survenue.
- **TLV 802.3**
  - *Taille (octets)* : taille totale des paquets de TLV 802.3 LLDP MED, en octets.
  - *État* : indique si les paquets de TLV 802.3 LLDP MED ont été envoyés ou si une surcharge est survenue.
- **LLDP Optional TLVs (TLV LLDP facultatives)**
  - *Taille (octets)* : taille totale des paquets de TLV LLDP MED facultatives, en octets.
  - *État* : indique si les paquets de TLV facultatives LLDP MED ont été envoyés ou si une surcharge est survenue.
- **LLDP MED Inventory (inventaire LLDP MED)**
  - *Taille (octets)* : taille totale des paquets de TLV d'inventaire LLDP MED, en octets.
  - *État* : indique si les paquets d'inventaire LLDP MED ont été envoyés ou si une surcharge est survenue.
- **Total**
  - *Total (octets)* : nombre total d'octets d'informations LLDP dans chaque paquet.
  - *Octets restants disponibles* : nombre total d'octets disponibles restants pour envoyer des informations LLDP supplémentaires dans chaque paquet.

Détection - CDP

Cette section explique comment configurer CDP.

Elle couvre les rubriques suivantes :

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

Propriétés CDP

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

Flux de travail de configuration de CDP

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

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

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

ÉTAPE 3 Si la fonction Auto Smartport (Port intelligent automatique) est utilisée pour détecter les fonctionnalités des périphériques CDP, activez CDP sur la page Propriétés.

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

Pour saisir les paramètres généraux CDP :

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

ÉTAPE 2 Saisissez les paramètres.

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

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

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

Paramètres d'interface CDP

La page Paramètres d'interface vous permet d'activer/de désactiver CDP sur chaque 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.

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

Vous pouvez sélectionner les TLV LLDP MED à annoncer sur la page Paramètres des ports LLDP MED.

Pour définir les paramètres d'interface CDP :

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

Cette page affiche les informations CDP suivantes pour chaque interface, y compris le port OOB.

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

Quatre boutons sont disponibles en bas de la page :

- **Copier les paramètres** : sélectionnez ce bouton pour copier une configuration d'un port vers un autre.
- **Modifier** : les différents champs sont décrits à l'étape 2 ci-dessous.
- **CDP Local Information Details** (Détail des informations locales CDP) : vous accédez à la page Informations locales CDP.
- **CDP Neighbor Information Details** (Détail des informations de voisinage CDP) : vous accédez à la page Informations de voisinage CDP.

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

Cette page contient les champs suivants :

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

  REMARQUE Les trois champs suivants sont opérationnels si le périphérique a été configuré pour envoyer des interceptions à la station de gestion.
- **Non-concordance VLAN voix Syslog** : cochez cette option pour permettre l'envoi d'un message SYSLOG lorsqu'une non-concordance VLAN voix est détectée. Cela signifie que les informations de VLAN voix dans la trame entrante ne correspondent pas à ce qu'indique le périphérique local.

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

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

Informations locales CDP

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

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

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

- **Interface** : numéro du port local. Le port OOB peut également être sélectionné.
- **État CDP** : indique si CDP est activé.
- **Device ID TLV (TLV d'ID de périphérique)**
  - *Type d'ID de périphérique* : type d'ID de périphérique annoncé dans la TLV d'ID de périphérique.
  - *ID de périphérique* : ID de périphérique annoncé dans la TLV d'ID de périphérique.
- **Durée de vie du nom du système**
  - *Nom du système* : nom système de l'appareil.
- **Address TLV (TLV de l'adresse)**
  - *Adresses 1 à 3* : adresses IP (annoncées dans la TLV d'adresse de périphérique).
- **Port TLV (TLV du port)**
  - *ID du port* : identificateur du port annoncé dans la TLV de port.

- **Capabilities TLV (TLV des fonctionnalités)**
  - *Fonctionnalités* : fonctionnalités annoncées dans la TLV de port.
- **Version TLV (TLV de la version)**
  - *Version* : informations sur la version logicielle sous laquelle le périphérique fonctionne.
- **Platform TLV (TLV de la plateforme)**
  - *Plate-forme* : identificateur de la plate-forme annoncée dans la TLV de plate-forme.
- **Native VLAN TLV (TLV du VLAN natif)**
  - *VLAN natif* : identificateur du VLAN natif annoncé dans la TLV de VLAN natif.
- **Full/Half Duplex TLV (TLV duplex intégral/semi-duplex)**
  - *Duplex* : port semi-duplex ou duplex intégral annoncé dans la TLV semi-duplex ou duplex intégral.
- **Appliance TLV (TLV du dispositif)**
  - *ID du dispositif* : type de périphérique associé au port annoncé dans la TLV de dispositif.
  - *ID du VLAN du dispositif* : VLAN du périphérique utilisé par le dispositif ; par exemple, si le dispositif est un téléphone IP, il s'agit du VLAN voix.
- **Extended Trust TLV (TLV de confiance étendue)**
  - *Confiance étendue* : l'activation de cette option indique que le port est sécurisé. L'hôte/serveur à partir duquel le paquet est reçu est ainsi sécurisé pour le marquage des paquets. Dans ce cas, les paquets reçus sur ce port ne sont pas marqués à nouveau. La désactivation de cette option indique que le port n'est pas validé, auquel cas le champ suivant peut être défini.
- **CoS for Untrusted Ports TLV (CoS pour le TLV des ports non validés)**
  - *CoS pour les ports non sécurisés* : si l'option Confiance étendue est désactivée sur le port, ce champ affiche la valeur CoS Layer 2, à savoir une valeur de priorité 802.1D/802.1p. Il s'agit de la valeur COS par l'intermédiaire de laquelle tous les paquets reçus sur un port non validé sont à nouveau marqués par le périphérique.

- **TLV d'alimentation disponible**
  - *ID de demande* : l'ID de dernière demande d'alimentation reçu correspond au dernier champ ID de demande reçu dans une TLV de demande d'alimentation. Sa valeur est 0 si aucune TLV de demande d'alimentation n'a été reçue depuis le dernier passage de l'interface vers l'état activé (Up).
  - *ID de gestion de l'alimentation* : valeur incrémentée de 1 (ou 2 pour éviter 0) à chaque fois que l'un des événements suivants se produit :

    Modification des valeurs Puissance disponible ou Niveau de gestion d'alimentation.

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

    L'interface passe à l'état Désactivé.
  - *Puissance disponible* : puissance consommée par le port.
  - *Niveau de gestion d'alimentation* : affiche la demande du fournisseur au périphérique alimenté pour connaître sa TLV de consommation électrique. Le périphérique affiche toujours « Aucune préférence » dans ce champ.
- **TLV d'alimentation à 4 fils via MDI (UPOE)**

  Indique si cette TLV est prise en charge.
  - *Prise en charge de PoE à 4 paires* **:** indique si PoE est pris en charge.
  - *Détection des paires de rechange/Classification requise* **:** indique si cette classification est requise.
  - *État voulu de la paire de rechange de l'appareil alimenté* **:** indique l'état souhaité de la paire de rechange de l'appareil alimenté.
  - *État opérationnel de la paire de rechange de l'appareil alimenté* **:** indique l'état de la paire de rechange du PSE.

Informations de voisinage CDP

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

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

Pour afficher les informations de voisinage CDP :

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

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

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

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

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

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

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

Cette page contient les champs suivants relatifs au voisin :

- **Device ID** : ID du périphérique de voisinage.
- **Nom du système** : nom de l'ID de périphérique de voisinage.
- **Local Interface** : numéro d'interface du port via lequel la trame a été reçue.
- **Advertisement Version** : version du protocole CDP.
- **Time to Live** : durée en secondes à l'issue de laquelle les informations concernant ce voisin sont supprimées.
- **Capabilities** : fonctions principales du périphérique. Les fonctionnalités sont indiquées par deux octets. Les bits 0 à 7 indiquent respectivement Autres, Répéteur, Pont, Point d'accès WLAN, Routeur, Téléphone, Système de câble DOCSIS et Station. Les bits 8 à 15 sont réservés.

- **Plate-forme** : identificateur de la plate-forme des voisins.
- **Neighbor Interface** : numéro d'interface du voisin via lequel la trame a été reçue.
- **VLAN natif** : VLAN natif du voisin.
- **Application** : nom de l'application qui s'exécute sur le voisin.
- **Duplex** : indique si l'interface de voisinage est semi-duplex ou duplex intégral.
- **Adresses** : adresses des voisins.
- **Alimentation prélevée** : puissance consommée par le voisin sur l'interface.
- **Version** : version logicielle des voisins.
- **Demande d'énergie** : énergie demandée par l'appareil alimenté connecté au port.
- **Liste de demande d'énergie** : chaque appareil alimenté peut envoyer une liste de niveaux d'énergie pris en charge (jusqu'à 3).
- **Puissance disponible**
  - *ID de demande* : l'ID de dernière demande d'alimentation reçu correspond au dernier champ ID de demande reçu dans une TLV de demande d'alimentation. Sa valeur est 0 si aucune TLV de demande d'alimentation n'a été reçue depuis le dernier passage de l'interface vers l'état activé (Up).
  - *ID de gestion de l'alimentation* : valeur incrémentée de 1 (ou 2 pour éviter 0) à chaque fois que l'un des événements suivants se produit :

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

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

    L'interface passe à l'état Désactivé.
  - *Puissance disponible* : puissance consommée par le port.
  - *Niveau de gestion d'alimentation* : affiche la demande du fournisseur au périphérique alimenté pour connaître sa TLV de consommation électrique. Le périphérique affiche toujours « Aucune préférence » dans ce champ.
- **Alimentation à 4 fils via MDI**
  - *Prise en charge de PoE à 4 paires* : indique que le système et le port prennent en charge les câbles à 4 paires (uniquement pour les ports spécifiques qui disposent de cette capacité matérielle).

- *Détection des paires de rechange/Classification requise* : indique qu'un câble à 4 paires est nécessaire.
- *État voulu de la paire de rechange de l'appareil alimenté* : indique qu'un appareil alimenté demande à activer la fonctionnalité 4 paires.
- *État opérationnel de la paire de rechange de l'appareil alimenté* : indique si la fonctionnalité 4 paires est activée ou désactivée.

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

Statistiques CDP

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

Les statistiques CDP d'un port ne s'affichent que si CDP est activé globalement et sur le port. Ceci s'effectue sur la page Propriétés CDP et sur la page Paramètres d'interface CDP.

Pour afficher les statistiques CDP :

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

Les champs suivants s'affichent pour chaque interface, y compris le port OOB :

Paquets reçus/transmis :

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

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

- **Somme de contrôle incorrecte** : nombre de paquets reçus ayant une valeur de somme de contrôle incorrecte.
- **Autres erreurs** : nombre de paquets reçus comportant d'autres erreurs que des sommes de contrôle incorrectes.

- **Voisinages supérieurs au maximum** : nombre de fois que les informations de paquet n'ont pas pu être stockées dans le cache en raison d'un manque d'espace disponible.

ÉTAPE 2 Pour effacer tous les compteurs sur toutes les interfaces, cliquez sur **Effacer tous les compteurs de l'interface**. Pour effacer tous les compteurs sur une interface, sélectionnez-la et cliquez sur **Effacer les compteurs de l'interface**.

10

Gestion des ports

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

Elle couvre les sujets suivants :

- Flux de travail
- Paramètres des ports
- Paramètres de reprise après erreur
- Paramètres de détection de bouclage
- Agrégation de liaisons
- UDLD
- PoE
- Green Ethernet

Flux de travail

Pour configurer les ports, procédez comme suit :

1. Configurez le port à l'aide de la page Paramètres des ports.
2. Activez/désactivez le protocole LACP (Link Aggregation Control Protocol), puis configurez les ports membres potentiels sur les LAG souhaités via la page Gestion des LAG. Par défaut, tous les LAG sont vides.
3. Configurez les paramètres Ethernet, comme le débit et la négociation automatique pour les LAG, via la page Paramètres des LAG.
4. Configurez les paramètres LACP des ports membres d'un LAG ou candidats à l'adhésion à un LAG dynamique, via la page LACP.
5. Configurez Green Ethernet et 802.3 Energy Efficient Ethernet via la page Propriétés.

6. Configurez le mode d'économie d'énergie Green Ethernet et 802.3 Energy Efficient Ethernet pour chaque port, via la page Paramètres des ports.
7. Si l'alimentation PoE est prise en charge et activée sur le périphérique, configurez ce dernier en suivant les instructions de la section Gestion des ports : PoE.

Paramètres des ports

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

Pour configurer les paramètres des ports :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Paramètres des ports**.

Les paramètres des ports sont affichés pour tous les ports.

ÉTAPE 2 Renseignez les champs suivants :

- **Prévention des interruptions de liaison** : sélectionnez cette option pour minimiser les interruptions sur votre réseau. Si cette commande est activée, elle désactive automatiquement les ports sur lesquels la liaison est perturbée.
- **Trames géantes** : sélectionnez cette option pour prendre en charge les paquets dont les tailles sont inférieures ou égales à 9 Ko. Si l'option Trames Jumbo (Trames Jumbo) n'est pas activée (par défaut), le système prend en charge les tailles de paquets allant jusqu'à 2 000 octets. Notez que la réception de paquets dont la taille excède 9 Ko peut entraîner l'arrêt du port de réception. De la même manière, l'envoi de paquets dont la taille excède 10 Ko peut entraîner l'arrêt du port de réception.

  Pour que les trames Jumbo soient appliquées, vous devez redémarrer le périphérique une fois la fonction activée. Dans les systèmes de pile, il est possible que les unités de pile redémarrent deux fois pour que ce paramètre prenne effet. Ces redémarrages sont effectués automatiquement.

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

Les modifications apportées à la configuration des trames géantes prennent effet *uniquement* après un enregistrement explicite de la configuration d'exécution dans le fichier de configuration de démarrage via la page Opérations de fichiers et après un redémarrage de l'appareil.

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

ÉTAPE 5 Modifiez les paramètres suivants :

- **Interface** : sélectionnez le numéro du port.
- **Port Description** : saisissez le nom défini par l'utilisateur pour ce port ou un commentaire.
- **Type de port** : affiche le type et le débit du port. Les options possibles sont les suivantes :
  - *Ports cuivre* : les ports standard, non mixtes, prennent en charge les valeurs suivantes : 10M, 100M, 1000M (type : cuivre) et 10G.
  - *Ports mixtes* : le port mixte connecté avec un câble CAT6a cuivre ou *une interface Gigabit fibre SFP.*
  - Fibre optique 10 G : ports avec débit de 1 G ou de 10 G.
  - OOB : port hors bande (pris en charge uniquement sur les modèles SG550XG et SG350XG).

  REMARQUE La fibre SFP est prioritaire dans les ports mixtes lorsque les deux ports sont utilisés.
- **État administratif** : sélectionnez si le port doit être démarré ou arrêté au redémarrage du périphérique.
- **État opérationnel** : indique si le port est actuellement actif ou inactif. Si le port est fermé en raison d'une erreur, la description de cette erreur s'affiche.
- **Interceptions SNMP d'état de lien** : sélectionnez cette option pour activer la génération des interceptions SNMP notifiant que l'état du lien du port a subi des modifications. Cela ne concerne pas le port OOB.
- **Période** : sélectionnez pour activer la période pendant laquelle le port est à l'état Actif. Lorsque la période n'est pas active, le port est à l'arrêt. Si vous configurez une période, celle-ci n'est effective que lorsque le port est administrativement à l'état Actif.
- **Nom de période** : sélectionnez le profil qui spécifie la période. Cela ne concerne pas le port OOB. Si vous n'avez pas encore défini de période, cliquez sur **Modifier** ou accédez à la page Plage horaire. Cela ne concerne pas le port OOB.
- **État de période opérationnelle** : indique si la période est actuellement active ou inactive.

- **Négociation automatique** : sélectionnez cette option pour activer la négociation automatique sur le port. La négociation automatique permet à un port d'annoncer sa vitesse de transmission, son mode duplex et ses fonctions de contrôle de flux à son partenaire de liaison.
- **Operational Auto Negotiation** : affiche l'état actuel de la négociation automatique sur le port.
- **Vitesse du port administratif** : sélectionnez la vitesse du port. Le type de port détermine les vitesses disponibles. Vous ne pouvez choisir *Vitesse administrative* que si la négociation automatique est désactivée pour le port.
- **Operational Port Speed** : affiche le débit actuel du port, obtenu par négociation.
- **Mode duplex administratif** : (affiché uniquement sur les ports non XG) sélectionnez le mode duplex du port. Ce champ ne peut être configuré que lorsque la négociation automatique est désactivée et que le débit du port est réglé sur 10M ou 100M. Lorsque le port a un débit de 1G, le mode est toujours Duplex intégral. Les options possibles sont les suivantes :
  - *Semi-duplex* : l'interface prend en charge la transmission entre le périphérique et le client dans une seule direction à la fois.
  - *Duplex intégral* : l'interface prend en charge la transmission entre le périphérique et le client dans les deux directions simultanément.
- **Mode duplex opérationnel** : (affiché uniquement sur les ports non XG) affiche le mode duplex actuel des ports.
- **Annonce automatique** : sélectionnez les fonctionnalités annoncées par la négociation automatique lorsqu'elle est activée.

  REMARQUE Certaines options ne s'appliquent pas à tous les périphériques.

  Les options sont les suivantes :
  - *Capacité maximale* : tous les débits de port et paramètres de mode duplex sont acceptés.
  - *10 Semi duplex* : débit de 10 Mbit/s et mode Semi-duplex (non disponible sur les périphériques XG).
  - *10 Duplex intégral* : débit de 10 Mbit/s et mode Duplex intégral (non disponible sur les périphériques XG).
  - *100 Semi-duplex* : débit de 100 Mbit/s et mode Semi-duplex (non disponible sur les périphériques XG).
  - *100 Duplex intégral* : débit de 100 Mbit/s et mode Duplex intégral.

- *1000 Duplex intégral* : débit de 1 000 Mbit/s et mode Duplex intégral.
- *2500 Duplex intégral* : le LAG annonce un débit de 2 500 Mbit/s et le mode est Duplex intégral. Cette option n'est prise en charge que sur les appareils de la gamme 550.
- *5000 Duplex intégral* : le LAG annonce un débit de 5 000 Mbit/s et le mode est Duplex intégral. Cette option n'est prise en charge que sur les appareils de la gamme 550.
- *10000 Duplex intégral* : le LAG annonce un débit de 10 000 Mbit/s et le mode est Duplex intégral. Cette option n'est prise en charge que sur les appareils de la gamme 550.

- **Annonce opérationnelle** : affiche les fonctionnalités actuellement publiées à l'attention du voisin des ports. Les options disponibles sont celles spécifiées dans le champ *Annonce administrative*.
- **Mode Préférence** : disponible uniquement si la négociation automatique est activée. Sélectionnez le mode unité principale/asservie de l'interface pour l'opération de négociation automatique. Sélectionnez l'une des options suivantes :
  - *Unité asservie* : commencez la négociation avec la préférence selon laquelle le port du périphérique est l'esclave dans le processus de négociation automatique.
  - *Unité principale* : commencez la négociation avec la préférence selon laquelle le port du périphérique est le maître dans le processus de négociation automatique.
- **Annonce de voisin** : affiche les fonctionnalités publiées par le périphérique de voisinage réseau (partenaire de liaison).
- **Contre-pression** : (pris en charge uniquement sur les ports non XG) sélectionnez le mode de contre-pression du port (utilisé en mode semi duplex) à appliquer pour ralentir la vitesse de réception des paquets en cas de surcharge de l'appareil. La sélection de cette option désactive le port distant, ce qui l'empêche d'envoyer des paquets en brouillant le signal.
- **Contrôle de flux** : activez ou désactivez le contrôle de flux 802.3x ou activez la négociation automatique du contrôle de flux sur le port (uniquement en mode Duplex intégral). La négociation automatique du contrôle de flux ne peut pas être activée sur les ports mixtes.
- **MDI/MDIX** : état *MDI (Media Dependent Interface*, interface dépendant du support)/ *MDIX (Media Dependent Interface with Crossover*, interface dépendant du support avec croisement) sur le port.

Les options sont les suivantes :

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

- **MDI/MDIX opérationnel** : affiche le paramètre MDI/MDIX actuel.
- **Port protégé** : sélectionnez cette option pour définir ce port en tant que port protégé. (Un port protégé est également appelé PVE (Private VLAN Edge).) Les fonctions d'un port protégé sont les suivantes :
  - Les ports protégés fournissent une isolation Couche 2 entre les interfaces (ports Ethernet et LAG) qui partagent le même 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. Les LAG protégés sont décrits à la section Paramètres des LAG.
- **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 **Appliquer**. Les paramètres des ports sont écrits dans le fichier de Configuration d'exécution.

Paramètres de reprise après erreur

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

Pour configurer les paramètres de reprise sur erreur :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Paramètres de reprise après erreur**.

ÉTAPE 2 Renseignez les champs suivants :

- **Automatic Recovery Interval** (Intervalle de récupération automatique) : spécifie le délai de la récupération d'erreur automatique, si celle-ci est activée, après la fermeture d'un port.
- **Récupération ErrDisable automatique**
  - **Sécurité des ports** : sélectionnez cette option pour activer la récupération d'erreur automatique lorsque le port a été fermé en raison d'une violation de la sécurité des ports.
  - **Violation d'hôte unique 802.1x** : sélectionnez cette option pour activer la récupération d'erreur automatique lorsque le port a été fermé par 802.1x.
  - **Déni de service ACL** : sélectionnez cette option pour activer le mécanisme de reprise automatique après erreur par une action ACL.
  - **Protection BPDU STP** : sélectionnez cette option pour activer la surveillance IGMP globalement sur toutes les interfaces.
  - **Protection de bouclage STP** : activez la reprise automatique lorsque le port a été fermé par une protection de bouclage STP.
  - **UDLD** : sélectionnez cette option pour activer le mécanisme de reprise après erreur automatique pour l'état de fermeture UDLD.
  - **Détection de bouclage** : sélectionnez cette option pour activer le mécanisme de reprise après erreur pour les ports fermés par la détection de bouclage.
  - **Storm Control** (Contrôle des tempêtes) : sélectionnez cette option pour activer le mécanisme de récupération d'erreur pour les ports fermés par le contrôle des tempêtes.
  - **Prévention des interruptions de liaison** : sélectionnez cette option pour minimiser les interruptions sur votre réseau. Si cette commande est activée, elle désactive automatiquement les ports sur lesquels la liaison est perturbée.

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

Pour réactiver manuellement un port :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Paramètres de reprise après erreur**.

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

ÉTAPE 2 Sélectionnez l'interface que vous souhaitez réactiver.

ÉTAPE 3 Cliquez sur **Réactiver**.

Paramètres de détection de bouclage

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

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

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

- **Câble court-circuité** : port qui renvoie en boucle tout le trafic reçu.
- **Direct multi-ports loop (Diriger la boucle multi-ports)** : le commutateur est connecté à un autre commutateur avec plusieurs ports et STP est désactivé.
- **LAN segment loop (Boucle de segment LAN)** : le commutateur est connecté avec un ou plusieurs ports à un segment LAN qui comporte des boucles.

Fonctionnement de la fonction LBD

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

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

- La fonction LBD est activée globalement.
- La fonction LBD est activée sur le port.

- L'état opérationnel du port est actif.
- Le port se trouve dans l'état STP de redirection ou désactivé (état de redirection d'instance MSTP, instance 0).

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

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

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

Configuration et paramètres par défaut

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

Interactions avec les autres fonctions

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

Configuration de la fonction LBD

Pour activer et configurer LBD :

ÉTAPE 1 Activez la détection de bouclage à l'échelle du système sur la page des paramètres de détection du bouclage (ci-dessous).

ÉTAPE 2 Activez la détection de bouclage sur les ports d'accès sur la page des paramètres de détection du bouclage (ci-dessous).

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

Pour configurer la détection du bouclage :

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

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

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

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

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

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

ÉTAPE 5 Choisissez d'activer LBD sur les ports ou les LAG dans le champ **Type d'interface égal à** dans le filtre.

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

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

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

Agrégation de liaisons

Cette section explique comment configurer les LAG. Elle couvre les sujets suivants :

- Présentation de l'agrégation de liaisons
- Configuration et paramètres par défaut
- Flux de travail des LAG statiques et dynamiques
- Gestion des LAG
- Paramètres des LAG
- LACP

Présentation de l'agrégation de liaisons

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

Deux types de LAG sont pris en charge :

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

Équilibrage de la charge

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

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

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

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

Gestion des LAG

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

Les dispositifs SG350XG prennent en charge jusqu'à 8 LAG. Les dispositifs SG550XG prennent en charge jusqu'à 32 LAG. Tous les appareils prennent en charge jusqu'à 8 ports dans un groupe de LAG.

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 huit ports à un LAG statique. Il est également impossible de définir plus de 16 ports comme candidats à 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.

Configuration et paramètres par défaut

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

Flux de travail des LAG statiques et dynamiques

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

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

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

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

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

Gestion des LAG

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

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

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

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

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

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

Pour définir les ports membres ou candidats dans un LAG :

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

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

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

ÉTAPE 2 Entrez les valeurs des champs suivants :

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

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

Paramètres des LAG

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

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

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

Les LAG du système sont affichés.

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

ÉTAPE 3 Entrez les valeurs des champs suivants :

- **LAG** : sélectionnez l'ID du LAG.
- **LAG Type** : affiche le type de port inclus dans le LAG.
- **Description** : saisissez le nom du LAG ou un commentaire.
- **État administratif** : définissez le LAG sélectionné comme étant démarré ou arrêté.
- **Operational Status** : indique si le LAG est actuellement opérationnel.

- **Interceptions SNMP d'état de lien** : sélectionnez cette option pour activer la génération des interceptions SNMP notifiant que l'état du lien des ports a subi des modifications dans le LAG.
- **Période** : sélectionnez pour activer la période pendant laquelle le port est à l'état Actif. Lorsque la période n'est pas active, le port est à l'arrêt. Si vous configurez une période, celle-ci n'est effective que lorsque le port est administrativement à l'état Actif.
- **Nom de période** : sélectionnez le profil qui spécifie la période. Si vous n'avez pas encore défini de période, cliquez sur **Modifier** ou accédez à la page Plage horaire.
- **État de période opérationnelle** : indique si la période est actuellement active ou inactive.
- **Négociation automatique administrative** : permet d'activer ou de désactiver la négociation automatique sur le LAG. La négociation automatique est un protocole établi entre deux partenaires de liaison qui permet à un LAG d'annoncer sa vitesse de transmission et son contrôle de flux à son partenaire (la valeur par défaut pour le contrôle de flux est *Désactivé*). Il est recommandé de maintenir la négociation automatique activée des deux côtés d'une liaison agrégée (ou de la désactiver des deux côtés), tout en s'assurant que les débits de liaison sont identiques.
- **Négociation automatique opérationnelle** : affiche le paramètre de négociation automatique.
- **Administrative Speed** (Vitesse du port administratif) : sélectionnez la vitesse des ports dans le LAG.
- **Operational LAG Speed** : affiche le débit actuel de fonctionnement du LAG.
- **Annonce administrative** : sélectionnez les fonctionnalités que le LAG doit annoncer. Les options sont les suivantes :
  - *Capacité maximale* : tous les débits de LAG et modes duplex sont acceptés.
  - *10 Duplex intégral* : le LAG annonce un débit de 10 Mbit/s et le mode est Duplex intégral.
  - *100 Duplex intégral* : le LAG annonce un débit de 100 Mbit/s et le mode est Duplex intégral.
  - *1000 Duplex intégral* : le LAG annonce un débit de 1 000 Mbit/s et le mode est Duplex intégral.
  - *2500 Duplex intégral* : le LAG annonce un débit de 2 500 Mbit/s et le mode est Duplex intégral. Cette option n'est prise en charge que sur les appareils de la gamme 550.

- *5000 Duplex intégral* : le LAG annonce un débit de 5 000 Mbit/s et le mode est Duplex intégral. Cette option n'est prise en charge que sur les appareils de la gamme 550.
- *10000 Duplex intégral* : le LAG annonce un débit de 10 000 Mbit/s et le mode est Duplex intégral. Cette option n'est prise en charge que sur les appareils de la gamme 550.

- **Annonce opérationnelle** : affiche l'état d'annonce administrative. Le LAG annonce ses capacités à son LAG voisin pour lancer le processus de négociation. Les options disponibles sont celles spécifiées dans le champ *Annonce administrative*.
- **Contrôle de flux administratif** : définissez le contrôle de flux à **Activer** ou **Désactiver**, ou activez la **négociation automatique** du contrôle de flux sur le LAG.
- **Contrôle de flux opérationnel** : affiche le paramètre de contrôle de flux actuel.
- **LAG protégé** : sélectionnez cette option pour définir ce LAG comme port protégé pour l'isolation de couche 2. Consultez la description de la configuration des ports à la rubrique Paramètres des ports pour en savoir plus sur les ports et LAG protégés.

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

LACP

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

Priorité et règles LACP

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

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

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

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

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

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

LACP sans membre de liaison

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

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

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

Paramètres LACP

Utilisez la page LACP pour configurer les ports candidats au LAG et pour configurer les paramètres LACP pour chaque port.

Lorsque tous les facteurs sont égaux, si le LAG est configuré avec davantage de ports candidats que le maximum de ports actifs autorisé (8), le périphérique sélectionne des ports et les marque comme actifs à partir du LAG dynamique dont la priorité est la plus élevée sur le périphérique.

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

Pour définir les paramètres LACP :

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

ÉTAPE 2 Définissez le paramètre **LACP System Priority** (Priorité du système LACP).

ÉTAPE 3 Sélectionnez un port et cliquez sur **Modifier**.

ÉTAPE 4 Entrez les valeurs des champs suivants :

- **Port** : sélectionnez le numéro du port auquel s'appliquent les valeurs de délai et de priorité.
- **Priorité des ports LACP** : saisissez la valeur de priorité LACP du port.
- **Délai LACP** : intervalle qui sépare l'envoi et la réception de deux PDU LACP consécutives. Sélectionnez les transmissions périodiques des PDU LACP, qui s'effectuent à une vitesse de transmission **longue** ou **courte**, selon la préférence de délai LACP définie.

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

UDLD

Cette section décrit la fonction Unidirectional Link Detection (UDLD).

Elle couvre les sujets suivants :

- Présentation de la fonction UDLD
- Paramètres globaux UDLD
- Paramètres d'interface UDLD
- Voisins UDLD

Présentation de la fonction UDLD

UDLD est un protocole de couche 2 qui permet aux périphériques connectés par des câbles Ethernet à fibre optique ou à paire torsadée de détecter des liaisons unidirectionnelles. Une liaison unidirectionnelle est établie lorsque le trafic provenant d'un périphérique de voisinage est reçu par le périphérique local, mais que le trafic issu du périphérique local n'est pas reçu par le voisin.

L'objectif du protocole UDLD est de détecter les ports sur lesquels le voisin ne reçoit pas de trafic du périphérique local (liaison unidirectionnelle) et de fermer ces ports.

Tous les périphériques connectés doivent prendre en charge UDLD pour que le protocole puisse détecter les liaisons unidirectionnelles. Si seul le périphérique local prend en charge UDLD, le périphérique ne pourra pas détecter l'état de la liaison. Dans ce cas, l'état de la liaison est défini sur indéterminé. L'utilisateur peut spécifier si les ports ayant l'état indéterminé sont fermés ou déclenchent simplement des notifications.

États et modes de UDLD

Sous le protocole UDLD, les ports se voient attribuer les états suivants :

- **Détection** : le système tente de déterminer si la liaison est bidirectionnelle ou unidirectionnelle. Il s'agit d'un état temporaire.
- **Bidirectionnel** : le trafic envoyé par un périphérique local est reçu par son voisin et le trafic envoyé par le voisin est reçu par le périphérique local.
- **Fermer** : la liaison est unidirectionnelle. Le trafic envoyé par un périphérique local est reçu par son voisin, mais le trafic envoyé par le voisin n'est pas reçu par le périphérique local.
- **Indéterminé** : le système ne peut pas déterminer l'état du port, car l'une des situations suivantes se produit :
  - Le voisin ne prend pas en charge UDLD.

    Ou

  - Le voisin ne reçoit pas de trafic du périphérique local.

  Dans ce cas, l'action UDLD dépend du mode UDLD du périphérique, comme expliqué ci-après.

UDLD prend en charge les modes de fonctionnement suivants :

- **Normal**

  Si l'état de liaison du port est déterminé être bidirectionnel et que les informations UDLD expirent alors que la liaison sur le port fonctionne toujours, UDLD tente de rétablir l'état du port.

- **Agressif**

  Si l'état de liaison du port est déterminé être bidirectionnel et que les informations UDLD expirent, UDLD arrête le port au bout d'une période prolongée, lorsqu'il peut déterminer que la liaison est défectueuse. L'état du port pour UDLD est marqué comme Indéterminé.

UDLD est activé sur un port lorsque l'une des situations suivantes se produit :

- Le port est un port fibre et UDLD est activé globalement.
- Le port est un port cuivre et vous activez spécifiquement UDLD sur celui-ci.

Fonctionnement de UDLD

Lorsque UDLD est activé sur un port, les actions suivantes sont réalisées :

- UDLD initie l'état de détection sur le port.

  Dans cet état, UDLD envoie régulièrement des messages sur chaque interface active vers tous les voisins. Ces messages contiennent l'ID de périphérique de tous les voisins connus. Il envoie ces messages en fonction du délai de message défini par l'utilisateur.

- UDLD reçoit les messages UDLD des périphériques de voisinage. Il met en cache ces messages jusqu'à ce que le délai d'expiration soit atteint (3 fois le délai de message). Si un nouveau message est reçu avant l'heure d'expiration, les informations contenues dans ce message remplacent les précédentes.

- Lorsque le délai d'expiration est atteint, le périphérique procède comme suit avec les informations reçues :

  - **Si le message du voisin contient l'ID du périphérique local** : l'état de liaison du port est défini sur bidirectionnel.

  - **Si le message du voisin ne contient pas l'ID du périphérique local** : l'état de liaison du port est défini sur unidirectionnel et le port est fermé.

- Si les messages UDLD ne sont pas reçus d'un périphérique voisin avant l'expiration du délai, l'état de liaison du port est défini sur indéterminé et le système procède comme suit :
  - **Le périphérique est en mode UDLD normal :** une notification est émise.
  - **Le périphérique est en mode UDLD agressif :** le port est fermé.

Si l'interface a l'état bidirectionnel ou indéterminé, le périphérique envoie régulièrement un message à chaque seconde du délai de message. Les étapes suivantes sont effectuées à maintes reprises.

Un port qui a été fermé peut être réactivé manuellement via la page Paramètres de reprise après erreur. Pour obtenir plus d'informations, reportez-vous à la section Réactivation d'un port fermé.

Si une interface est arrêtée et que UDLD est activé, le périphérique supprime toutes les informations de voisinage et envoie au moins un message ULDL aux voisins pour leur indiquer que le port est fermé. Lorsque le port est réactivé, l'état UDLD devient Détection.

UDLD non pris en charge ou désactivé sur un voisin

Si UDLD n'est pas pris en charge ou désactivé sur un voisin, aucun message UDLD n'est reçu de ce voisin. Dans ce cas, le périphérique ne peut pas déterminer si la liaison est unidirectionnelle ou bidirectionnelle. L'état de l'interface est alors définie sur indéterminé.

Réactivation d'un port fermé

Vous pouvez réactiver un port qui a été fermé par UDLD en procédant de l'une des manières suivantes :

- **Automatically** (Automatiquement) : vous pouvez configurer le système pour qu'il réactive automatiquement les ports fermés par UDLD sur la page Paramètres de reprise après erreur. Dans ce cas, lorsqu'un port est fermé par UDLD, il est automatiquement réactivé à l'expiration de l'intervalle de récupération automatique. UDLD est alors de nouveau exécuté sur le port. Si la liaison est toujours unidirectionnelle, UDLD la ferme à nouveau, par exemple à l'issue du délai d'expiration de UDLD.
- **Manually** (Manuellement) : vous pouvez réactiver un port via la page Paramètres de reprise après erreur.

Instructions d'utilisation

Cisco vous recommande de ne pas activer UDLD sur les ports connectés aux périphériques sur lesquels UDLD n'est pas pris en charge ou désactivé. L'envoi de paquets UDLD sur un port connecté à un périphérique qui ne prend pas en charge UDLD génère davantage de trafic sur le port sans offrir d'avantages.

En outre, tenez compte des éléments suivants lorsque vous configurez UDLD :

- Définissez le délai du message selon l'urgence qu'il y a de fermer les ports avec une liaison unidirectionnelle. Plus le délai de message est petit, plus les paquets UDLD envoyés et analysés sont nombreux, mais plus le port est fermé rapidement si la liaison est unidirectionnelle.
- Si vous souhaitez activer UDLD sur un port cuivre, vous devez l'activer sur chaque port. Si vous activez UDLD globalement, il est uniquement activé sur les ports fibre.
- Définissez le mode UDLD sur normal si vous ne souhaitez pas fermer les ports sauf s'il est certain que la liaison est unidirectionnelle.
- Définissez le mode UDLD sur Agressif quand vous voulez une perte de liaison à la fois unidirectionnelle et bidirectionnelle.

Dépendances envers les autres fonctions

- UDLD et couche 1

  Lorsque UDLD est activé sur un port, UDLD s'exécute activement sur ce port tant que le port est actif. Lorsque le port est fermé, UDLD passe à l'état de fermeture UDLD. Dans cet état, UDLD supprime tous les voisins appris. Lorsque le port repasse de fermé à ouvert, UDLD est de nouveau exécuté activement.

- UDLD et protocoles de couche 2

  UDLD s'exécute sur un port indépendamment des autres protocoles de couche 2 exécutés sur le même port, tels que STP ou LACP. Par exemple, UDLD attribue un état au port quel que soit l'état STP du port ou peu importe si le port appartient à un LAG ou pas.

Configuration et paramètres par défaut

Les valeurs par défaut suivantes sont disponibles pour cette fonction :

- UDLD est désactivé par défaut sur tous les ports du périphérique.
- Le délai de message par défaut est de 15 secondes.
- Le délai d'expiration par défaut est de 45 secondes (3 fois le délai de message).
- État UDLD du port par défaut :
  - Les interfaces fibre ont l'état UDLD global.
  - Les interfaces non fibre ont l'état désactivé.

Avant de commencer

Aucune tâche préalable n'est requise.

Tâches UDLD courantes

Cette section décrit quelques tâches courantes permettant de configurer UDLD.

Flux de travail 1 : pour activer globalement UDLD sur les ports fibre, procédez comme suit :

ÉTAPE 1 Ouvrez la page Paramètres globaux UDLD.

a. Saisissez le **Délai de message**.

b. Dans le champ État UDLD par défaut du port fibre, entrez **Désactivé**, **Normal** ou **Agressif** comme état UDLD global.

ÉTAPE 2 Cliquez sur **Appliquer**.

Flux de travail 2 : pour changer la configuration UDLD sur un port fibre ou pour activer UDLD sur un port cuivre, procédez comme suit :

ÉTAPE 1 Ouvrez la page Paramètres globaux UDLD.

a. Sélectionnez un port.

b. Sélectionnez l'état UDLD du port **Par défaut**, **Désactivé**, **Normal** ou **Agressif**. Si vous sélectionnez Par défaut, le port se voit appliquer le paramètre global.

ÉTAPE 2 Cliquez sur **Appliquer**.

Flux de travail 3 : pour réactiver un port après sa fermeture par UDLD si la réactivation automatique n'a pas été configurée, procédez comme suit :

ÉTAPE 1 Ouvrez la page Paramètres de reprise après erreur.

a. Sélectionnez un port.

b. Cliquez sur **Réactiver**.

Configuration de UDLD

La fonction UDLD peut être configurée pour tous les ports fibre à la fois (sur la page Paramètres globaux UDLD) ou pour chaque port (sur la page Paramètres d'interface UDLD).

Paramètres globaux UDLD

L'État UDLD par défaut du port fibre s'applique uniquement aux ports fibre.

Le champ Délai de message s'applique aux ports cuivre et fibre.

Pour configurer UDLD globalement :

ÉTAPE 1 Cliquez sur **Gestion des ports > UDLD** > **Paramètres globaux UDLD**.

ÉTAPE 2 Renseignez les champs suivants :

- **Délai de message** : entrez l'intervalle entre deux messages UDLD envoyés. Ce champ est destiné aux ports fibre et cuivre.
- **État UDLD par défaut du port fibre** : ce champ est uniquement destiné aux ports **fibre**. L'état UDLD des ports cuivre doit être défini individuellement sur la page Paramètres d'interface UDLD. Les états possibles sont :
  - *Désactivé* : UDLD est désactivé sur tous les ports du périphérique.
  - *Normal* : le périphérique arrête une interface si la liaison est unidirectionnelle. Si la liaison est indéterminée, une notification est émise.
  - *Agressif* : le périphérique arrête une interface si la liaison est unidirectionnelle. Si la liaison est bidirectionnelle, le périphérique s'arrête après expiration des informations UDLD. L'état du port est marqué comme Indéterminé.

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

Paramètres d'interface UDLD

Utilisez la page Paramètres d'interface UDLD pour changer l'état UDLD d'un port spécifique. Vous pouvez ici définir l'état pour les ports cuivre et fibre.

Pour copier un ensemble de valeurs spécifique vers plusieurs ports, définissez la valeur pour un port, puis utilisez le bouton **Copier** pour la copier sur les autres ports.

Pour configurer UDLD sur une interface :

ÉTAPE 1 Cliquez sur **Gestion des ports > UDLD** > **Paramètres d'interface UDLD**.

Les informations sont affichées pour tous les ports sur lesquels UDLD est activé. Toutefois, si vous avez effectué un filtrage sur un groupe de ports spécifique, les informations sont affichées pour ce groupe de ports uniquement.

- **Port** : l'identifiant du port.
- **État UDLD** : les états possibles sont :
  - *Default* (Par défaut) : le port reçoit la valeur du paramètre Fiber Port UDLD Default State (État UDLD par défaut du port fibre) définie sur la page Paramètres globaux UDLD.
  - *Désactivé* : UDLD est désactivé sur tous les ports fibre du périphérique.
  - *Normal* : le périphérique arrête une interface s'il détecte que la liaison est unidirectionnelle. Si la liaison est indéterminée, il émet une notification.
  - *Agressif* : le périphérique arrête une interface si la liaison est unidirectionnelle. Si la liaison est bidirectionnelle, le périphérique s'arrête après expiration des informations UDLD. L'état du port est marqué comme Indéterminé.
- **État bidirectionnel** : les états possibles sont :
  - *Détection* : le dernier état UDLD du port est en cours de détermination. Le délai d'expiration n'a pas encore été atteint depuis la dernière détermination (le cas échéant) ou depuis le début de l'exécution de UDLD sur le port ; l'état n'a donc pas encore été déterminé.
  - *Bidirectionnel* : le trafic envoyé par le périphérique local est reçu par son voisin et le trafic envoyé par le voisin est reçu par le périphérique local.
  - *Indéterminé* : l'état de la liaison entre le port et son port connecté ne peut pas être déterminé, car aucun message UDLD n'a été reçu ou le message UDLD ne contenait pas l'ID du périphérique local.
  - *Désactivé (par défaut)* : UDLD a été désactivé sur ce port.
  - *Fermer* : le port a été fermé car sa liaison avec le périphérique connecté est indéterminée en mode agressif.
  - *Inactif* : le port est inactif.
- **Nombre de voisins** : nombre de périphériques connectés détectés.

ÉTAPE 2 Pour modifier l'état UDLD d'un port spécifique, sélectionnez-le et cliquez sur **Modifier**.

ÉTAPE 3 Modifiez la valeur de l'état UDLD. Si vous sélectionnez **Default** (Par défaut), le port reçoit la valeur du paramètre **Fiber Port UDLD Default State** (État UDLD par défaut du port fibre) définie sur la page Paramètres globaux UDLD.

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

Voisins UDLD

Pour afficher tous les périphériques connectés au périphérique local, cliquez sur **Gestion des ports > UDLD** > **Voisins UDLD**.

Les champs suivants sont affichés pour tous les ports sur lesquels UDLD est activé.

- **Nom de l'interface** : nom du port UDLD local.
- **Informations de voisinage :**
  - *ID du périphérique* : ID du périphérique distant.
  - *MAC du périphérique* : adresse MAC du périphérique distant.
  - *Nom du périphérique* : nom du périphérique distant.
  - *ID du port* : nom du port distant.
- **État** : état de la liaison entre le périphérique local et le périphérique voisin sur le port local. Les valeurs suivantes sont possibles :
  - *Détection* : le dernier état UDLD du port est en cours de détermination. Le délai d'expiration n'a pas encore été atteint depuis la dernière détermination (le cas échéant) ou depuis le début de l'exécution de UDLD sur le port ; l'état n'a donc pas encore été déterminé.
  - *Bidirectionnel* : le trafic envoyé par le périphérique local est reçu par son voisin et le trafic envoyé par le voisin est reçu par le périphérique local.
  - *Indéterminé* : l'état de la liaison entre le port et son port connecté ne peut pas être déterminé, car aucun message UDLD n'a été reçu ou le message UDLD ne contenait pas l'ID du périphérique local.
  - *Désactivé* : UDLD a été désactivé sur ce port.
  - *Fermer* : le port a été fermé car sa liaison avec le périphérique connecté est indéterminée en mode agressif.

- **Délai d'expiration du voisin (s)** : indique le délai à respecter avant que le périphérique tente de déterminer l'état UDLD du port. Il correspond à trois fois le délai de message.
- **Heure du message du voisin (s)** : indique le délai entre les messages UDLD.

PoE

Cette section décrit comment utiliser la fonctionnalité PoE.

REMARQUE PoE n'est pris en charge que sur les appareils autonomes, qui ne font pas partie d'une pile.

Elle couvre les sujets suivants :

- Vue d'ensemble
- Propriétés PoE
- Paramètres
- Statistiques
- Présentation de la fonction Green Ethernet

Vue d'ensemble

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

Fonctionnalités

PoE offre les fonctions suivantes :

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

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

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

Fonctionnement

Le processus de mise en œuvre de PoE comprend les étapes suivantes :

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

Le PoE prend en charge deux modes :

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

Appareils PoE

Les ports de liaison montante peuvent fonctionner en tant qu'appareil alimenté (PD, Powered Device), avec 1 ou 2 ports d'appareil alimenté. Sur les appareils comptant 8 ports, le port le plus élevé sera celui de l'appareil alimenté (les ports d'appareil alimenté ne disposent pas de la fonctionnalité PSE). En présence de 2 ports d'appareil alimenté, il est conseillé de les connecter à un seul PSE. Les 2 ports d'appareil alimenté sont fonctionnels s'ils utilisent le même standard d'alimentation (tous les deux AF, AT ou 60 W PoE).

Pour les appareils PSE 60 W PoE, les types de ports PSE sont les suivants :

	Appareils à 24 ports	Appareils à 48 ports
350	4 ports 60 W PoE, 20 ports AT	8 ports 60 W PoE, 40 ports AT
550	8 ports 60 W PoE, 16 ports AT	16 ports 60 W PoE, 32 ports AT

La fonctionnalité PoE (Power over Ethernet) n'est disponible que sur les appareils suivants basés sur PoE.

Nom de la référence	Appareil alimenté PoE AT/ AF/60 W PoE	PSE PoE AF/AT
SF350-08	AT	N/A
SF352-08	AT	N/A
SF352-08P	AT/AF/60 W PoE	AF/AT
SF352-08MP	AT/AF/60 W PoE	AF/AT
SF350-24P	N/A	AT/AF/60 W PoE
SF350-24MP	N/A	AT/AF/60 W PoE
SF350-48	N/A	N/A
SF350-48P	N/A	AT/AF/60 W PoE
SF350-48MP	N/A	AT/AF/60 W PoE
SG350-10P	AT/AF/60 W PoE	AF/AT
SG355-10P	AT/AF/60 W PoE	AF/AT
SG350-10MP	AT/AF/60 W PoE	AF/AT
SG350-10SFP	AF/AT	N/A

Nom de la référence	Appareil alimenté PoE AT/ AF/60 W PoE	PSE PoE AF/AT
SG350-28P	N/A	AT/AF/60 W PoE
SG350-28MP	N/A	AT/AF/60 W PoE
SG350-52P	N/A	AT/AF/60 W PoE
SG350-52MP	N/A	AT/AF/60 W PoE
SG350X-24P	N/A	AT/AF/60 W PoE
SG350X-24MP	N/A	AT/AF/60 W PoE
SG350X-48P	N/A	AT/AF/60 W PoE
SG350X-48MP	N/A	AT/AF/60 W PoE
SG350-8PD	N/A	AF/AT
SG350X-8PMD	N/A	UPoE/AF/AT
SG350X-24PD	N/A	UPoE/AF/AT
SF550X-24P	N/A	AT/AF/60 W PoE
SF550X-24MP	N/A	AT/AF/60 W PoE
SF550X-48P	N/A	AT/AF/60 W PoE
SF550X-48MP	N/A	AT/AF/60 W PoE
SG550X-24P	N/A	AT/AF/60 W PoE
SG550X-24MP	N/A	AT/AF/60 W PoE
SG550X-24MPP	N/A	AT/AF/60 W PoE

Nom de la référence	Appareil alimenté PoE AT/ AF/60 W PoE	PSE PoE AF/AT
SG550X-48P	N/A	AT/AF/60 W PoE
SG550X-48MP	N/A	AT/AF/60 W PoE

Considérations relatives à la configuration PoE

Veuillez tenir compte des points suivants lors de la configuration de PoE :

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

Les options suivantes peuvent être configurées :

- Puissance maximale qu'un PSE est autorisé à fournir à un appareil alimenté.
- Modification du mode de Limite de classe en Limite du port et vice versa alors que l'appareil fonctionne. Les valeurs de puissance par port qui ont été configurées pour le mode Limite du port sont conservées.

  REMARQUE Remplacer le mode Limite de classe par Limite de port et inversement tandis que l'appareil PSE fonctionne provoque le redémarrage forcé de l'appareil alimenté.
- De la limite de port maximale autorisée en tant que limite numérique par port en mW (mode Port Limit).
- De générer un filtre lorsqu'un appareil alimenté essaie de consommer trop d'énergie et à quel pourcentage de la puissance maximale ce filtre est généré.

Le matériel PoE spécifique détecte automatiquement la classe du PD et sa limite de puissance en fonction de la classe de l'appareil connecté à chaque port spécifique (mode Limite de classe).

Si, à tout moment au cours de la connexion, un PD relié nécessite plus de puissance de la part du PSE que l'allocation configurée ne le permet (que le PSE soit en mode Limite de classe ou Limite du port), le PSE en question :

- maintient l'état actif/inactif de la liaison du port PoE ;
- désactive l'alimentation du port PoE ;
- consigne le motif de l'arrêt de l'alimentation ;
- génère une interception SNMP.

Propriétés PoE

REMARQUE Cette section concerne uniquement les appareils prenant en charge la fonctionnalité PoE.

La page Propriétés PoE permet de sélectionner le mode PoE Limite du port ou Limite de classe, 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.

La puissance de sortie est désactivée lors du redémarrage, de l'initialisation et de la configuration système pour veiller à ne pas endommager les appareils alimentés.

Pour configurer PoE sur l'appareil et surveiller la puissance consommée :

ÉTAPE 1 Cliquez sur **Gestion des ports > PoE > Propriétés**.

ÉTAPE 2 Entrez les valeurs des champs suivants :

- **Mode d'alimentation** : sélectionnez l'une des options suivantes :
  - *Limite de classe* : la limite maximale de puissance par port est déterminée par la classe de l'appareil, elle-même résultant de l'étape de classification.
  - *Limite du port* : la limite maximale de puissance de chaque port est configurée par l'utilisateur.

  REMARQUE Lorsque vous modifiez le mode de Limite de port à Limite de classe ou inversement, vous devez d'abord désactiver les ports PoE, puis les réactiver après avoir modifié les options de configuration de l'alimentation.
- **Interceptions** : permet d'activer ou de désactiver les interceptions. Si les interceptions sont activées, vous devez également activer SNMP et configurer au moins un destinataire de notification SNMP.
- **Seuil des interceptions d'alimentation** : saisissez le seuil d'utilisation sous la forme d'un pourcentage de la limite de puissance. Une alarme se déclenche si la puissance dépasse cette valeur.
- **Version du logiciel** : affiche la version logicielle de la puce PoE.

Les compteurs suivants sont affichés pour l'appareil ou pour toutes les unités de la pile :

- **Puissance nominale** : quantité totale d'énergie que l'appareil peut fournir à l'ensemble des appareils alimentés connectés.
- **Consommation** : puissance actuellement consommée par les ports PoE.

- **Puissance disponible** : puissance nominale moins la quantité d'énergie consommée.
- **Puces PSE et révision matérielle** : numéro de révision du matériel et des puces PoE.

ÉTAPE 3 Cliquez sur **Appliquer** pour enregistrer les propriétés PoE.

Paramètres

La page Paramètres affiche les informations PoE système sur l'activation de PoE sur les interfaces, la surveillance de la consommation actuelle et la limite maximale de puissance par port en mode Limite du port.

REMARQUE La fonctionnalité PoE de l'appareil peut être configurée pour une période donnée. Cette configuration vous permet d'indiquer les jours de la semaine et les heures auxquels la fonctionnalité PoE est activée pour chaque port. La fonctionnalité PoE est désactivée en dehors des périodes de temps ainsi spécifiées. Pour utiliser cette option, une période doit d'abord être définie sur la page Plage horaire.

Cette page limite la puissance par port à une consommation en watts spécifique. Pour que ces paramètres soient actifs, le système doit être en mode Limite du port PoE. Ce mode est configuré sur la page Propriétés PoE.

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

Exemple de priorité PoE :

Supposition : un appareil doté de 48 ports fournit un total de 375 watts.

L'administrateur configure tous les ports pour qu'ils allouent jusqu'à 30 watts. Au final, si les 48 ports allouent 30 watts chacun, on obtient 1440 watts, ce qui est beaucoup trop. L'appareil ne peut pas fournir suffisamment d'énergie à chaque port ; il suit donc certaines priorités.

L'administrateur définit la priorité de chaque port, en lui allouant autant de puissance que possible.

Vous devez entrer ces priorités sur la page Paramètres PoE.

Reportez-vous à la section Modèles d'appareils pour obtenir une description des modèles d'appareils qui prennent en charge la fonctionnalité PoE et connaître la puissance maximale pouvant être allouée aux ports PoE.

Pour configurer les paramètres de limite du port PoE :

ÉTAPE 1 Cliquez sur **Gestion des ports > PoE > Paramètres**.

Les ports sont affichés avec les informations PoE appropriées. Ces champs sont décrits sur la page Modifier, sauf les champs suivants :

- **Affectation de puissance administrative (mW)** : indiquez la quantité d'énergie qui peut être allouée.
- **État opérationnel** : indique si la fonction PoE est actuellement active sur le port.
- **Standard PoE** : affiche le type de fonctionnalité PoE pris en charge, comme 60 W PoE et 802.3 AT.

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

ÉTAPE 3 Renseignez les champs suivants :

- **Interface** : sélectionnez le port à configurer.
- **État administratif** : permet d'activer ou de désactiver PoE sur le port.
- **Période** : sélectionnez cette option pour activer la fonctionnalité PoE sur le port.
- **Nom de la période** : si l'option Période est activée, choisissez la plage temporelle à utiliser. Les périodes sont définies sur la page Période. Pour définir une nouvelle période, cliquez sur **Modifier**.
- **Niveau de priorité** : sélectionnez la priorité du port (faible, élevée ou critique) à utiliser lorsque l'alimentation est faible. Par exemple, si 99 % de la puissance disponible est consommée, et que le port 1 a une priorité élevée et le port 3 une priorité faible, le port 1 sera alimenté, contrairement au port 3.
- **Affectation de puissance administrative** : ce champ s'affiche uniquement si le mode d'alimentation Limite du port est défini sur la page Propriétés PoE. Si le mode d'alimentation Limite du port est sélectionné, saisissez la puissance affectée au port (en milliwatts).
- **Forcer quatre paires** : sélectionnez cette option pour obliger la paire de rechange à fournir de l'énergie. Cette option permet de fournir une alimentation PoE de 60 watts aux appareils alimentés ne prenant pas en charge la négociation PoE CDP/LLDP.
- **Affectation de puissance maximale** : ce champ s'affiche uniquement si le mode d'alimentation Limite de puissance est défini sur la page Propriétés PoE. Affiche la puissance maximale autorisée sur ce port.
- **Puissance négociée** : puissance allouée à l'appareil.

- **Protocole de négociation de la puissance** : protocole qui détermine la puissance négociée.
- **Consommation électrique** : affiche la puissance (en milliwatts) affectée sous Paramètres (Limite de classe).
- **Classe** : affiche la classe de puissance générée.

La page Paramètres (Limite de classe) affiche les informations PoE système sur l'activation de PoE sur les interfaces, la surveillance de la consommation actuelle et la limite maximale de puissance par port.

REMARQUE La fonctionnalité PoE de l'appareil peut être configurée pour une période donnée. Cette configuration vous permet d'indiquer les jours de la semaine et les heures auxquels la fonctionnalité PoE est activée pour chaque port. La fonctionnalité PoE est désactivée en dehors des périodes de temps ainsi spécifiées. Pour utiliser cette option, une période doit d'abord être définie sur la page *Plage horaire*.

Cette page permet de limiter la puissance par port en fonction de la classe de l'appareil alimenté connecté. Pour que ces paramètres soient actifs, le système doit être en mode Limite de classe PoE. Vous pouvez configurer ce mode sur la page Propriétés PoE.

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

Exemple de priorité PoE :

Reportez-vous à la section Modèles d'appareils pour obtenir une description des modèles d'appareils qui prennent en charge la fonctionnalité PoE et connaître la puissance maximale pouvant être allouée aux ports PoE.

Pour configurer les paramètres de limite de classe PoE :

ÉTAPE 1 Cliquez sur **Gestion des ports > PoE > Paramètres (Limite de classe)**.

Les ports sont affichés avec les informations PoE appropriées. Ces champs sont décrits sur la page Modifier, sauf les champs suivants :

- **Standard PoE** : affiche le type de fonctionnalité PoE pris en charge, comme 60 W PoE et 802.3 AT.
- **État opérationnel** : indique si la fonction PoE est actuellement active sur le port.

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

ÉTAPE 3 Renseignez le champ suivant :

- **Interface** : sélectionnez le port à configurer.
- **État administratif** : permet d'activer ou de désactiver PoE sur le port.
- **Période** : sélectionnez cette option pour spécifier la période d'activation de la fonctionnalité PoE sur le port.
- **Nom de la période** : si l'option Période est activée, choisissez la plage temporelle à utiliser. Les plages temporelles sont définies sur la page *Plage horaire*. Cliquez sur **Modifier** pour accéder à la page **Période**.
- **Niveau de priorité** : sélectionnez la priorité du port (faible, élevée ou critique) à utiliser lorsque l'alimentation est faible. Par exemple, si 99 % de la puissance disponible est consommée, et que le port 1 a une priorité élevée et le port 3 une priorité faible, le port 1 sera alimenté, contrairement au port 3.
- **Forcer quatre paires** : activez cette fonctionnalité pour proposer une meilleure alimentation.
- **Affectation de puissance maximale** : ce champ s'affiche uniquement si le mode d'alimentation Limite de puissance est défini sur la page Propriétés PoE. Affiche la puissance maximale autorisée sur ce port.
- **Consommation électrique** : affiche la puissance (en milliwatts) affectée Paramètres (Limite de classe).
- **Classe** : affiche la classe de l'appareil, ce qui indique son niveau de puissance maximum :

Classe	Puissance maximale fournie par le port de l'appareil
0	30,0 watts
1	4,0 watts
2	7,0 watts
3	15,4 watts
4	30,0 watts

- **Affectation de puissance maximale** : ce champ s'affiche uniquement si le mode d'alimentation Limite de puissance est défini sur la page Propriétés PoE. Affiche la puissance maximale autorisée sur ce port.
- **Puissance négociée** : puissance allouée à l'appareil.

- **Protocole de négociation de la puissance** : protocole qui détermine la puissance négociée.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres PoE du port sont consignés dans le fichier de Configuration d'exécution.

Statistiques

Cette page présente les tendances en matière de consommation électrique, c'est-à-dire la consommation électrique moyenne au fil du temps. Ces données s'avèrent utiles pour surveiller le comportement de la fonctionnalité PoE et corriger les erreurs.

L'appareil stocke les valeurs de consommation des ports PoE (en watts) au fil du temps. Cela permet de calculer et d'afficher la consommation PoE moyenne sur la période spécifiée (jour/semaine/mois) et de dégager des tendances. Les informations sont fournies pour chaque interface ainsi que pour l'appareil dans son intégralité.

Les valeurs de consommation PoE sont prélevées toutes les minutes. Les statistiques quotidiennes, hebdomadaires et mensuelles sont enregistrées dans la mémoire Flash, de sorte qu'elles restent disponibles après un redémarrage.

Voici un exemple de consommation PoE moyenne par port/appareil :

> Somme de toutes les valeurs de consommation PoE sur une période/Nombre de minutes dans la période d'échantillonnage.

Pour afficher la tendance de consommation PoE sur l'appareil et définir les paramètres de la vue :

ÉTAPE 1 Cliquez sur **Gestion des ports > PoE > Statistiques**.

ÉTAPE 2 Sélectionnez l'unité et le port dans les champs **Unité** et **Port**.

ÉTAPE 3 Sélectionnez la **Fréquence d'actualisation**.

ÉTAPE 4 Les champs suivants s'affichent pour l'interface sélectionnée :

Historique de consommation

- **Consommation moyenne au cours de la dernière heure** : moyenne de toutes les mesures de consommation PoE au cours de la dernière heure.
- **Consommation moyenne au cours du dernier jour** : moyenne de toutes les mesures de consommation PoE au cours du dernier jour.

- **Consommation moyenne au cours de la dernière semaine** : moyenne de toutes les mesures de consommation PoE au cours de la dernière semaine.

Compteurs d'événements PoE

- **Compteur de surcharges** : nombre de conditions de surcharge détectées.
- **Compteur de courts-circuits** : nombre de conditions de court-circuit détectées.
- **Compteur de rejets** : nombre de conditions de rejet détectées.
- **Compteur d'absences** : nombre de conditions d'absence détectées.
- **Compteur de signatures non valides** : nombre de conditions de signature non valide détectées.

Les opérations suivantes peuvent être effectuées sur la page principale :

- **Effacer les compteurs d'événements** : efface les compteurs d'événements affichés.
- **Afficher les statistiques de toutes les interfaces** : affiche les statistiques ci-dessus pour toutes les interfaces.
- **Voir le graphique de l'historique des interfaces** : affiche les compteurs sous forme graphique.
- **Actualiser** : actualise les compteurs affichés.

Vous pouvez effectuer les opérations suivantes en cliquant sur **Afficher les statistiques de toutes les interfaces** :

- **Effacer les compteurs d'événements** : efface les compteurs d'événements affichés.
- **Afficher les statistiques de l'interface** : affiche les statistiques ci-dessus pour une interface.
- **Afficher le graphique de l'historique des interfaces** : affiche les compteurs sous forme graphique pour l'interface sélectionnée.
- **Actualiser** : actualise les compteurs affichés.

Vous pouvez effectuer les opérations suivantes en cliquant sur **Afficher le graphique de l'historique des interfaces** :

- **Afficher les statistiques de l'interface** : affiche les statistiques d'une interface sélectionnée sous la forme d'un tableau. Indiquez l'**intervalle de temps** en heures, jours, semaines ou années.

- **Afficher les statistiques de toutes les interfaces** : affiche les statistiques ci-dessus pour toutes les interfaces sous la forme d'un tableau. Indiquez l'**intervalle de temps** en heures, jours, semaines ou années.
- **Effacer les compteurs d'événements** : efface les compteurs.

Green Ethernet

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

Elle contient les sections suivantes :

Présentation de la fonction Green Ethernet

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

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

- **Mode Détection d'énergie** : sur une liaison inactive, le port passe en mode inactif, ce qui permet d'économiser l'énergie tout en maintenant le port à l'état administratif Démarré. La sortie de ce mode et le retour au mode entièrement opérationnel sont rapides, transparents et sans aucune perte de trame. Ce mode est pris en charge sur les ports GE comme sur les ports FE. Il est désactivé par défaut.
- **Mode Courte portée** : cette fonction permet d'économiser de l'énergie sur une courte longueur de câble. Une fois que la longueur du câble a été analysée, la consommation d'énergie est ajustée en fonction de cette longueur. Si la longueur de câble est inférieure à 30 mètres pour des ports 10 Gigabit et 50 mètres pour d'autres types de ports, le périphérique a besoin de moins de puissance pour envoyer des trames sur ce câble, ce qui représente une économie d'énergie. Ce mode n'est pris en charge que sur les ports GE RJ45 ; il ne s'applique pas aux ports mixtes. Il est désactivé par défaut.

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

EEE est activé par défaut au niveau global. Sur un port donné, si EEE est activé, le mode Courte portée est désactivé. L'utilisateur doit désactiver EEE avant d'activer le mode Courte portée.

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

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

Sur la page Récapitulatif du système, les voyants qui sont représentés sur les illustrations des cartes des appareils ne sont pas affectés par la désactivation des voyants.

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

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

Économie d'énergie par la désactivation des LED de port

La fonctionnalité de désactivation des LED des ports permet d'économiser l'énergie consommée par les LED des périphériques. Étant donné que les périphériques se trouvent souvent dans une pièce inoccupée, le fait de maintenir ces LED allumées est un gaspillage d'énergie. La fonction Green Ethernet permet de désactiver les LED des ports (liaison, vitesse et PoE) lorsqu'elles ne sont pas nécessaires et de les activer lorsqu'elles le sont (débogage, raccordement de périphériques supplémentaires, etc.).

Sur la page Récapitulatif du système, les voyants qui sont représentés sur les illustrations des cartes des appareils ne sont pas affectés par la désactivation des voyants.

Les LED du port peuvent être désactivées via la page Propriétés.

Fonction 802.3az Energy Efficient Ethernet (EEE)

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

Elle couvre les sujets suivants :

- Présentation de 802.3az EEE
- Négociation des fonctionnalités d'annonce
- Détection du niveau de liaison pour 802.3az EEE
- Disponibilité de 802.3az EEE
- Configuration par défaut
- Interactions entre les fonctions
- Flux de travail de configuration de 802.3az EEE

Présentation de 802.3az EEE

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

802.3az EEE n'est pas prise en charge sur le port OOB.

REMARQUE L'état du partenaire de liaison distante peut être affiché uniquement lorsque le débit de la liaison est de 1G ou 10G.

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

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

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

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

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

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

Négociation des fonctionnalités d'annonce

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

REMARQUE Si la négociation automatique n'est pas activée sur un port, la fonction EEE est désactivée. Une seule exception s'applique : si le débit de la liaison est de 1G ou 10G, la fonction EEE est toujours activée même si la négociation automatique est désactivée.

Détection du niveau de liaison pour 802.3az EEE

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

Disponibilité de 802.3az EEE

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

Configuration par défaut

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

Interactions entre les fonctions

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

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

Flux de travail de configuration de 802.3az EEE

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

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

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

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

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

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

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

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

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

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

ÉTAPE 5 Pour consulter les informations associées à 802.3az EEE sur l'appareil distant, ouvrez les pages Informations de voisinage LLDP, puis affichez les informations contenues dans le bloc 802.3 Energy Efficient Ethernet (EEE).

Propriétés

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

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

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Green Ethernet** > **Propriétés**.

ÉTAPE 2 Entrez les valeurs des champs suivants :

- **Mode Détection d'énergie** : (pour les périphériques non XG) cochez cette case pour activer ce mode.
- **Courte portée** : (pour les périphériques non XG) cochez cette case pour activer ce mode.
- **LED des ports** : sélectionnez cette option pour activer les LED des ports. Lorsque les LED des ports sont désactivés, ils n'affichent pas l'état des liaisons, l'activité, etc.
- **802.3 EEE (Energy Efficient Ethernet)** : permet d'activer ou de désactiver globalement le mode EEE.

ÉTAPE 3 Cliquez sur **Reset Energy Saving Counter (Réinitialiser le compte d'économie d'énergie)** pour réinitialiser les informations sur les économies d'énergie réalisées.

ÉTAPE 4 Cliquez sur **Appliquer**. Les propriétés Green Ethernet sont écrites dans le fichier de Configuration d'exécution.

Paramètres des ports

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

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

Les fonctionnalités Courte portée et Détection d'énergie sont toujours activées sur les périphériques XG ; elles ne peuvent pas être désactivées. Sur les périphériques équipés de ports FE ou GE, ces fonctionnalités peuvent être activées ou désactivées.

Pour définir les paramètres Green Ethernet de chaque port :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Green Ethernet** > **Paramètres des ports**.

La page Paramètres des ports affiche les éléments suivants :

- **État des paramètres globaux** : affiche les éléments suivants :
  - *Mode Détection d'énergie* : indique si ce mode est activé ou non.
  - *Mode Courte portée* : indique si ce mode est activé ou non.
  - *Mode 802.3 Energy Efficient Ethernet (EEE)* : indique si ce mode est activé ou non.

Pour chaque port, les champs suivants sont décrits :

REMARQUE Il est possible que certains champs ne s'affichent pas sur certaines références.

- **Port** : numéro du port.
- **Détection d'énergie** : état du mode de détection d'énergie sur le port :
  - Administratif : indique si le mode de détection d'énergie est activé.
  - Opérationnel : indique si le mode de détection d'énergie est actuellement opérationnel sur le port local. Vous savez ainsi si elle a été activée (État administratif), si elle a été activée sur le port local et si elle est opérationnelle sur le port local.
  - Motif : précise pourquoi le mode de détection d'énergie n'est pas opérationnel même s'il est activé.

- **Courte portée** : état du mode Courte portée sur le port :
  - *Administratif* : indique si le mode Courte portée est activé.
  - *Opérationnel* : indique si le mode Courte portée est actuellement opérationnel sur le port local. Vous savez ainsi si elle a été activée (État administratif), si elle a été activée sur le port local et si elle est opérationnelle sur le port local.
  - *Motif* : précise pourquoi le mode Courte portée n'est pas opérationnel même s'il est activé.
  - *Longueur de câble*—longueur du câble.
- **802.3 Energy Efficient Ethernet (EEE)** : état du port concernant la fonction EEE :
  - *Administratif* : indique si la fonction EEE est activée.
  - *Opérationnel* : indique si la fonction EEE est actuellement opérationnelle sur le port local. Vous savez ainsi si elle a été activée (État administratif), si elle a été activée sur le port local et si elle est opérationnelle sur le port local.
  - *LLDP administratif* : indique si l'annonce des compteurs EEE via LLDP est activée.
  - *LLDP opérationnel* : indique si l'annonce des compteurs EEE via LLDP est actuellement opérationnelle.
  - *Support EEE sur la distance* : indique si la fonction EEE est prise en charge sur le partenaire de liaison. La fonction EEE doit être prise en charge sur les partenaires de liaison local et distant.

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

ÉTAPE 3 (Périphériques non XG uniquement) Activez ou désactivez le mode **Détection d'énergie** sur le port.

ÉTAPE 4 (Périphériques non XG uniquement) Activez ou désactivez le mode **Courte portée** sur le port si le périphérique comporte des ports GE.

ÉTAPE 5 Activez ou désactivez le mode **802.3 Energy Efficient Ethernet (EEE)** sur le port.

ÉTAPE 6 Activez ou désactivez le mode **802.3 Energy Efficient Ethernet (EEE) LLDP** sur le port (annonce des fonctionnalités EEE via LLDP).

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

11

Port intelligent

Ce document décrit la fonction Port intelligent.

Il contient les rubriques suivantes :

Vue d'ensemble

La fonction Port intelligent constitue un moyen pratique d'enregistrer et de partager des configurations communes. En appliquant la même macro Port intelligent à plusieurs interfaces, ces dernières partagent un ensemble commun de configurations. Une macro Port intelligent est un script de commandes de l'interface de ligne de commande (CLI).

Il est possible d'appliquer une macro Port intelligent à une interface par nom de macro ou par Type de port intelligent associé à la macro. L'application d'une macro Port intelligent par nom de macro s'effectue uniquement via l'interface de ligne de commande. Pour plus d'informations, reportez-vous au guide de l'interface de ligne de commande (CLI).

Il y a deux façons d'appliquer une macro Port intelligent par type de port intelligent à une interface :

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

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

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

Les flux de travail classiques sont également décrits dans la section Tâches courantes de port intelligent.

Qu'est-ce qu'un port intelligent ?

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

Types de port intelligent

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

- Imprimante
- Bureau
- Invité

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

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

Vous pouvez appliquer une macro Port intelligent à l'aide des méthodes suivantes :

- Le Type de port intelligent associé.
- De manière statique à partir d'une macro Port intelligent, par son nom uniquement depuis l'interface de ligne de commande (CLI).

Une macro Port intelligent peut être appliquée par son Type de port intelligent, de manière statique à partir de l'interface de ligne de commande (CLI) et de l'interface utilisateur graphique (GUI), et de manière dynamique par le Port intelligent automatique. L'option Port intelligent automatique détecte les types de port intelligent des appareils associés, sur la base des fonctionnalités CDP, des fonctionnalités système LLDP et/ou des fonctionnalités LLDP-MED.

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

Type de port intelligent	Pris en charge par le Port intelligent automatique	Pris en charge par le Port intelligent automatique par défaut
Inconnu	Non	Non
Par défaut	Non	Non
Imprimante	Non	Non
Bureau	Non	Non

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

Types de port intelligent spéciaux

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

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

- **Par défaut**

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

  Si l'option Port intelligent automatique attribue un type de port intelligent à une interface et que l'interface n'est pas configurée pour être Port intelligent automatique persistant, alors son type de port intelligent est réinitialisé à la valeur par défaut dans les cas suivants :

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

- **Inconnu**

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

  Pour obtenir des conseils de dépannage, reportez-vous à la partie flux de travail dans Tâches courantes de port intelligent.

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

Macros Port intelligent

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

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

Le code source de la macro peut être trouvé en exécutant la commande show parser macro name [macro_name] en mode d'exécution privilégiée de l'interface de ligne de commande (CLI) ou en cliquant sur le bouton **Afficher la source de la macro** sur la page Paramètres de type.

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

Il existe deux types de macros Port intelligent :

- **Intégré** : ces macros sont fournies par le système. Une macro applique le profil de configuration et l'autre le supprime. Les noms des macros Port intelligent intégrées et du Type de port intelligent auquel elles sont associées sont indiqués ci-dessous :
  - macro_name (par exemple : printer)
  - no_nom_macro (par exemple : no_printer)

- **Défini par l'utilisateur** : ces macros sont écrites par les utilisateurs. Pour plus d'informations, reportez-vous au *Guide de référence de l'interface de ligne de commande (CLI)*. Pour associer une macro définie par l'utilisateur à un Type de port intelligent, vous devez également définir son anti-macro.
  - smartport-type-name (par exemple : my_printer)
  - no_smartport-type-name (par exemple : no_my_printer)

Les macros Port intelligent sont liées aux types de port intelligent sur la page Paramètres de type.

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

Application d'un Type de port intelligent à une interface

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

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

Échec de la macro et opération de réinitialisation

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

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

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

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

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

Fonctionnement de la fonction Port intelligent

Il est possible d'appliquer une macro Port intelligent à une interface par le nom de la macro ou par le type de port intelligent associé à la macro. L'application d'une macro Port intelligent par nom de macro s'effectue uniquement via l'interface de ligne de commande. Pour plus d'informations, reportez-vous au guide de l'interface de ligne de commande (CLI).

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

Il y a deux façons d'appliquer une macro Port intelligent par type de port intelligent à une interface :

- **Port intelligent statique**

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

- **Port intelligent automatique**

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

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

Port intelligent automatique

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

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

Activation du Port intelligent automatique

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

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

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

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

Identification du Type de port intelligent

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

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

À moins que le Port intelligent automatique persistant ne soit activé sur une interface, le Type de port intelligent et la configuration générée qui est appliquée par le Port intelligent automatique sont supprimés si le ou les périphériques en cours d'association arrivent à expiration, passent en liaison inactive ou redémarrent, ou si le périphérique connecté reçoit des fonctionnalités conflictuelles. Les délais d'expiration sont déterminés par l'absence d'annonces CDP et/ou LLDP en provenance de l'appareil pendant une durée spécifiée.

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

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

Ce mappage est présenté dans les tableaux suivants :

Mise en correspondance des fonctionnalités CDP avec le type de port intelligent

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

Mise en correspondance des fonctionnalités LLDP avec le type de port intelligent

Nom de la fonctionnalité	Bit LLDP	Type de port intelligent
Autre	1	Ignorer
Répéteur IETF RFC 2108	2	Ignorer
Pont MAC IEEE Std. 802.1D	3	Commutateur
Point d'accès WLAN IEEE Std. 802.11 MIB	4	Point d'accès sans fil
Routeur IETF RFC 1812	5	Routeur
Téléphone IETF RFC 4293	6	ip_phone
Système de câble DOCSIS IETF RFC 4639 et IETF RFC 4546	7	Ignorer

Mise en correspondance des fonctionnalités LLDP avec le type de port intelligent (suite)

Nom de la fonctionnalité	Bit LLDP	Type de port intelligent
Station uniquement IETF RFC 4293	8	Hôte
Composant C-VLAN d'un pont VLAN IEEE Std. 802.1Q	9	Commutateur
Composant S-VLAN d'un pont VLAN IEEE Std. 802.1Q	10	Commutateur
Relais MAC à deux ports (TPMR) IEEE Std. 802.1Q	11	Ignorer
Réservé	12-16	Ignorer

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

Plusieurs appareils associés au port

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

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

- Si tous les appareils présents sur une interface annoncent la même fonctionnalité (il n'y a pas de conflit), le Type de port intelligent correspondant est appliqué à l'interface.
- Si l'un des appareils est un commutateur, le Type de port intelligent *Commutateur* est utilisé.
- Si l'un des appareils est un point d'accès, le Type de port intelligent *Point d'accès sans fil* est utilisé.
- Si l'un des appareils est un téléphone IP et qu'un autre appareil est un hôte, le type de port intelligent *ip_phone_desktop* est utilisé.
- Si l'un des appareils est un téléphone IP de bureau et que l'autre est un téléphone IP ou un hôte, le type de port intelligent *ip_phone_desktop* est utilisé.
- Dans tous les autres cas, le Type de port intelligent par défaut est utilisé.

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

Interface du Port intelligent automatique persistant

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

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

Gestion des erreurs

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

Configuration par défaut

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

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

Relations avec les autres fonctions

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

Tâches courantes de port intelligent

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

Flux de travail 1 : pour activer globalement le Port intelligent automatique sur l'appareil et configurer un port avec la fonction Port intelligent automatique, procédez comme suit :

ÉTAPE 1 Pour activer la fonction Auto Smartport (Port intelligent automatique) sur l'appareil, ouvrez la page Propriétés. Définissez **Port intelligent automatique administratif** sur **Activer** ou **Activer par VLAN voix**.

ÉTAPE 2 Spécifiez si l'appareil doit traiter les annonces CDP et/ou LLDP des appareils connectés.

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

ÉTAPE 4 Cliquez sur **Appliquer.**

ÉTAPE 5 Pour activer la fonction Auto Smartport (Port intelligent automatique) sur une ou plusieurs interfaces, ouvrez la page Paramètres d'interface.

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

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

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

ÉTAPE 9 Cliquez sur **Appliquer**.

Flux de travail 2 : pour configurer une interface en tant que port intelligent statique, procédez comme suit :

ÉTAPE 1 Pour activer la fonction Smartport (Port intelligent) sur l'interface, ouvrez la page Paramètres d'interface.

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

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

ÉTAPE 4 Définissez les paramètres de macro souhaités.

ÉTAPE 5 Cliquez sur **Appliquer**.

Flux de travail 3 : pour définir les valeurs par défaut des paramètres de macro Port intelligent et/ou lier une paire de macros définies par l'utilisateur à un type de port intelligent, procédez comme suit :

Cette procédure vous permet d'effectuer les tâches suivantes :

- Afficher la source de la macro.
- Modifier les valeurs par défaut des paramètres.
- Restaurer les paramètres d'usine.
- Lier une paire de macros définies par l'utilisateur (une macro et son anti-macro correspondante) à un Type de port intelligent.

ÉTAPE 1 Ouvrez la page Paramètres de type.

ÉTAPE 2 Sélectionnez le Type de port intelligent.

ÉTAPE 3 Cliquez sur **Afficher la source de la macro** pour afficher la macro Port intelligent actuelle qui est associée au Type de port intelligent sélectionné.

ÉTAPE 4 Cliquez sur **Modifier** pour ouvrir une nouvelle fenêtre dans laquelle vous pouvez lier des macros définies par l'utilisateur au type de port intelligent sélectionné et/ou modifier les valeurs par défaut des paramètres dans les macros qui sont liées à ce type de port intelligent. Les valeurs par défaut de ces paramètres sont utilisées lorsque le Port intelligent automatique applique le Type de port intelligent sélectionné (le cas échéant) à une interface.

ÉTAPE 5 Sur la page Modifier, modifiez les champs.

ÉTAPE 6 Cliquez sur **Appliquer** pour rétablir la macro si les paramètres ont changé.

Flux de travail 4 : pour réexécuter une macro Port intelligent si celle-ci a échoué, procédez comme suit :

ÉTAPE 1 Sur la page Paramètres d'interface, sélectionnez une interface avec le type de port intelligent Unknown (Inconnu).

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

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

ÉTAPE 4 Cliquez sur **Modifier**. Une nouvelle fenêtre s'ouvre. Cliquez sur **Réinitialiser** pour réinitialiser l'interface.

ÉTAPE 5 Revenez à la page principale et réappliquez la macro en utilisant **Réappliquer** (pour les appareils qui ne sont ni des commutateurs, ni des routeurs ni des points d'accès) ou **Réappliquer la macro de port intelligent** (pour les commutateurs, routeurs ou points d'accès) afin d'exécuter la macro Port intelligent sur l'interface.

Il existe une deuxième méthode de réinitialisation d'une ou plusieurs interfaces inconnues :

ÉTAPE 1 Sur la page Paramètres d'interface, activez la case à cocher Port Type equals to (Type de port est égal à).

ÉTAPE 2 Sélectionnez *Inconnu* et cliquez sur **OK**.

ÉTAPE 3 Cliquez sur **Réinitialiser tous les ports intelligents inconnus**. Réappliquez ensuite la macro comme indiqué ci-dessus.

ASTUCE L'échec de la macro peut être dû à un conflit avec une configuration de l'interface qui a été effectuée avant l'application de la macro (le plus souvent rencontré dans les paramètres de sécurité et de contrôle des tempêtes), un type de port incorrect, une typo ou une commande incorrecte dans la macro définie par l'utilisateur ou encore une valeur de paramètre non valide. Les paramètres sont contrôlés, sans prise en compte du type ou de la limite, avant la tentative d'application de la macro. Par conséquent, une entrée incorrecte ou non valide pour une valeur de paramètre se soldera presque assurément par un échec lors de l'application de la macro.

Configuration de port intelligent à l'aide de l'interface Web

Vous pouvez configurer la fonction Port intelligent sur les pages Port intelligent > Propriétés, Paramètres de type de port intelligent et Paramètres d'interface.

Pour la configuration du VLAN vocal, reportez-vous à la section VLAN voix.

Pour la configuration de LLDP/CDP, reportez-vous respectivement aux sections Détection - LLDP et Détection - CDP.

Propriétés

Pour configurer la fonction Port intelligent globalement :

ÉTAPE 1 Cliquez sur **Port intelligent > Propriétés**.

ÉTAPE 2 Saisissez les paramètres.

- **Port intelligent automatique administratif** : sélectionnez cette option pour activer ou désactiver globalement le Port intelligent automatique. Les options suivantes sont disponibles :
  - *Désactiver* : sélectionnez cette option pour désactiver le Port intelligent automatique sur l'appareil.
  - *Activer* : sélectionnez cette option pour activer le Port intelligent automatique sur l'appareil.
  - *Activer par VLAN voix automatique* : cette option active le Port intelligent automatique, mais ne le rend opérationnel que lorsque le VLAN voix automatique est aussi activé et opérationnel. Activer par VLAN voix automatique est la valeur par défaut.
- **Port intelligent automatique opérationnel** : affiche l'état de la fonction Port intelligent automatique.
- **Méthode de détection périphérique de port intelligent auto.** : indiquez si les types de paquets entrants CDP et/ou LLDP doivent être utilisés pour détecter le type de port intelligent des appareils en cours d'association. Vous devez cocher au moins un type pour que le Port intelligent automatique puisse identifier les appareils.
- **État CDP opérationnel** : affiche l'état opérationnel de CDP. Activez CDP si le Port intelligent automatique doit détecter le type de port intelligent à partir de l'annonce CDP.

- **État LLDP opérationnel** : affiche l'état opérationnel de LLDP. Activez LLDP si le Port intelligent automatique doit détecter le type de port intelligent à partir de l'annonce LLDP/LLDP-MED.
- **Détection périphérique de port intelligent auto.** : sélectionnez chaque type d'appareil pour lequel le Port intelligent automatique peut attribuer des types de port intelligent aux interfaces. Si vous ne cochez pas cette option, le Port intelligent automatique n'attribue ce Type de port intelligent à aucune interface.

ÉTAPE 3 Cliquez sur **Appliquer**. Vous appliquez ainsi les paramètres de Port intelligent globaux sur l'appareil.

Paramètres de type

Utilisez la page Paramètres de type de port intelligent pour modifier les paramètres de type de port intelligent et afficher la source de la macro.

Par défaut, chaque Type de port intelligent est associé à une paire de macros Port intelligent intégrées. Pour plus d'informations sur la macro et l'anti-macro, reportez-vous à la section Types de port intelligent. Vous pouvez aussi associer votre propre paire de macros définies par l'utilisateur avec des configurations personnalisées à un Type de port intelligent. Les macros définies par l'utilisateur peuvent seulement être préparées via l'interface de ligne de commande (CLI). Pour plus d'informations, reportez-vous au Guide de référence de l'interface de ligne de commande (CLI).

Les macros intégrées ou définies par l'utilisateur peuvent comporter des paramètres. Les macros intégrées peuvent intégrer jusqu'à trois paramètres.

La modification de ces paramètres pour les Types de port intelligent qui sont appliqués par le Port intelligent automatique sur la page Paramètres de type de port intelligent configure les valeurs par défaut de ces paramètres. Ces valeurs par défaut sont utilisées par le Port intelligent automatique.

REMARQUE Une fois les modifications apportées aux types Port intelligent automatique, les nouveaux paramètres sont appliqués aux interfaces auxquelles le Port intelligent automatique a déjà attribué ce type. Dans ce cas, si vous liez une macro non valide ou définissez une valeur par défaut non valide pour un paramètre, tous les ports de ce Type de port intelligent deviennent inconnus.

ÉTAPE 1 Cliquez sur **Port intelligent > Paramètres de type de port intelligent**.

ÉTAPE 2 Pour afficher la macro Port intelligent associée à un Type de port intelligent, sélectionnez un Type de port intelligent, puis cliquez sur **Afficher la source de la macro**.

ÉTAPE 3 Pour modifier les paramètres d'une macro ou attribuer une macro définie par l'utilisateur, sélectionnez un Type de port intelligent, puis cliquez sur **Modifier**.

ÉTAPE 4 Renseignez les champs.

- **Type de port** : sélectionnez un type de port intelligent.
- **Nom de la macro** : affiche le nom de la macro Port intelligent actuellement associée au type de port intelligent.
- **Type de macro** : indiquez si la paire macro/anti-macro associée à ce type de port intelligent est **intégrée** (voir Macros Port intelligent intégrées) ou **définie par l'utilisateur**.
- **Macro définie par l'utilisateur** : si vous le souhaitez, sélectionnez la macro définie par l'utilisateur à associer au type de port intelligent sélectionné. La macro doit déjà avoir été couplée avec une anti-macro.

  Le couplage des deux macros s'effectue par nom et est décrit dans la section Macro Port intelligent.
- **Paramètres de macro** : affiche les champs suivants pour trois paramètres dans la macro :
  - *Nom du paramètre* : nom du paramètre dans la macro.
  - *Valeur du paramètre* : valeur actuelle du paramètre dans la macro. Vous pouvez la modifier ici.
  - *Description du paramètre* : description du paramètre.

ÉTAPE 5 Cliquez sur **Appliquer** pour enregistrer les modifications dans la configuration d'exécution. Si la macro Port intelligent et/ou ses valeurs de paramètre associées au Type de port intelligent sont modifiées, le Port intelligent automatique réapplique automatiquement la macro aux interfaces qui sont actuellement attribuées avec le Type de port intelligent par le Port intelligent automatique. Le Port intelligent automatique n'applique pas les modifications aux interfaces auxquelles un Type de port intelligent a été attribué de façon statique.

REMARQUE Il n'existe aucune méthode permettant de valider les paramètres de macro, car ils n'ont aucune association de type. Toutefois, n'importe quelle entrée est valide à ce stade. Néanmoins, des valeurs de paramètre non valides peuvent entraîner des erreurs lorsque le Type de port intelligent est attribué à une interface appliquant la macro associée.

Paramètres d'interface

Utilisez la page Paramètres d'interface pour effectuer les tâches suivantes :

- Appliquez de manière statique un type de port intelligent spécifique à une interface, avec des valeurs propres à l'interface pour les paramètres de macro.
- Activez le Port intelligent automatique sur une interface.
- Diagnostiquez une macro Port intelligent dont l'application a échoué et a généré l'état Inconnu du Type de port intelligent.
- Appliquez à nouveau une macro Port intelligent après son échec pour toutes les interfaces ou l'un des types d'interface suivants : commutateur, routeur et point d'accès (AP). Vous devez avoir effectué les corrections nécessaires avant de cliquer sur **Apply** (Appliquer). Pour obtenir des conseils de dépannage, reportez-vous à la partie flux de travail dans Tâches courantes de port intelligent.
- Réappliquez une macro Port intelligent à une interface. Dans certaines circonstances, il se peut que vous souhaitiez réappliquer une macro Port intelligent pour mettre à jour la configuration sur une interface. Par exemple, en réappliquant une macro Port intelligent d'appareil sur une interface de commutateur, l'interface devient membre des VLAN qui ont été créés depuis la dernière application de la macro. Vous devez connaître les configurations actuelles de l'appareil et la définition de la macro pour déterminer si une réapplication aura un impact sur l'interface.
- Réinitialisez les interfaces inconnues. Le mode des interfaces inconnues est ainsi défini sur Par défaut.

Pour appliquer une macro Port intelligent :

ÉTAPE 1 Cliquez sur **Port intelligent > Paramètres d'interface**.

Pour réappliquer les dernières macro Port intelligent qui étaient associées à un groupe d'interfaces, cliquez sur l'une des options suivantes :

- **Tous les commutateurs, routeurs et point d'accès sans fil** : les macros sont réappliquées à toutes les interfaces.
- **All Switches** (Tous les commutateurs) : les macros sont réappliquées à toutes les interfaces définies en tant que commutateurs.
- **All Routers** (Tous les routeurs) : les macros sont réappliquées à toutes les interfaces définies en tant que routeurs.

- **Tous les points d'accès sans fil** : les macros sont réappliquées à toutes les interfaces définies en tant que points d'accès.

  Pour réappliquer les macros Port intelligent associées à une interface spécifique, sélectionnez cette interface (elle doit être opérationnelle) et cliquez sur **Reapply** (Réappliquer) pour réappliquer la dernière macro appliquée à l'interface.

  L'action **Réappliquer** ajoute aussi l'interface à tous les VLAN nouvellement créés.

ÉTAPE 2 Diagnostic de port intelligent.

Si une macro Port intelligent échoue, le Type de port intelligent de l'interface est Inconnu. Sélectionnez une interface dont le type est inconnu, puis cliquez sur **Afficher les diagnostics.** Le système affiche la commande où l'application de la macro a échoué. Pour obtenir des conseils de dépannage, reportez-vous à la partie flux de travail dans Tâches courantes de port intelligent. Corrigez le problème et réappliquez la macro.

ÉTAPE 3 Réinitialisation de toutes les interfaces inconnues au type Par défaut.

- Cochez la case *Type de port intelligent est égal à*.
- Sélectionnez *Inconnu.*
- Cliquez sur **Go**.
- Cliquez sur **Réinitialiser tous les ports intelligents inconnus**. Réappliquez ensuite la macro comme indiqué ci-dessus. Cette opération réinitialise l'ensemble des interfaces de type Inconnu, ce qui signifie que le type Par défaut est réattribué à toutes les interfaces. Une fois que vous avez corrigé l'erreur dans la macro et/ou dans la configuration d'interface actuelle, vous pouvez appliquer une nouvelle macro.

REMARQUE La réinitialisation de l'interface de type inconnu ne réinitialise pas la configuration effectuée par la macro qui a échoué. Ce nettoyage doit être réalisé manuellement.

Pour attribuer un type de port intelligent à une interface ou activer la fonction Port intelligent automatique sur l'interface :

ÉTAPE 1 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 2 Renseignez les champs.

- **Interface** : sélectionnez le port ou LAG.
- **Type de port intelligent** : affiche le type de port intelligent actuellement attribué au port/LAG.
- **Application de port intelligent** : sélectionnez le type de port intelligent dans le menu déroulant Application de port intelligent.

- **Méthode d'application de port intelligent** : si Port intelligent automatique est sélectionné, le type de port intelligent est automatiquement attribué en fonction de l'annonce CDP et/ou LLDP reçue des appareils en cours de connexion, et la macro Port intelligent correspondante est appliquée. Pour attribuer un Type de port intelligent de manière statique et appliquer la macro Port intelligent correspondante à l'interface, sélectionnez le Type de port intelligent souhaité.
- **État persistant** : sélectionnez cette option pour activer l'état persistant. S'il est activé, l'association d'un Type de port intelligent à une interface est conservée même si l'interface est désactivée ou que l'appareil est redémarré. L'État persistant s'applique uniquement si l'Application de port intelligent de l'interface est Port intelligent automatique. L'activation de l'État persistant sur une interface élimine le retard de détection de l'appareil.
- **Paramètres de macro** : affiche les champs suivants pour un maximum de trois paramètres dans la macro :
  - *Nom du paramètre* : nom du paramètre dans la macro.
  - *Valeur du paramètre* : valeur actuelle du paramètre dans la macro. Vous pouvez la modifier ici.
  - *Description du paramètre* : description du paramètre.

ÉTAPE 3 Cliquez sur **Réinitialiser** pour définir une interface sur Par défaut si son état est Inconnu (en raison d'un échec d'application de macro). La macro peut être réappliquée sur la page principale.

ÉTAPE 4 Cliquez sur **Appliquer** pour mettre à jour les modifications et attribuer le Type de port intelligent à l'interface.

Macros Port intelligent intégrées

Vous trouverez ci-dessous une description de la paire de macros intégrées pour chaque Type de port intelligent. Pour chaque Type de port intelligent, une macro permet de configurer l'interface et une anti-macro permet de supprimer la configuration.

Le code de macro des types de port intelligent suivants est indiqué ci-après :

- desktop
- printer
- guest
- server

- host
- ip_camera
- ip_phone
- ip_phone_desktop
- switch
- router
- ap

desktop

```
[desktop]
#interface configuration, for increased network security and reliability when
connecting a desktop device, such as a PC, to a switch port. (configuration
d'interface pour une sécurité et une fiabilité réseau accrues au moment de
connecter un périphérique de bureau, tel qu'un PC à un port de commutateur.)
#macro description Desktop
#macro keywords $native_vlan $max_hosts
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                       $max_hosts: Nombre maximum de périphériques autorisés
sur le port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_desktop

```
[no_desktop]
#macro description No Desktop
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

printer

```
[printer]
#macro description printer
#macro keywords $native_vlan
#
#macro key description: $native_vlan: VLAN sans balise qui sera configuré sur
le port
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_printer

```
[no_printer]
#macro description No printer
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

guest

```
[guest]
#macro description guest
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré
sur le port
#Default Values are
#$native_vlan = Default VLAN
#
#the port type cannot be detected automatically
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_guest]]

```
[no_guest]
#macro description No guest
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

server

```
[server]
#macro description server
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                        $max_hosts: Nombre maximum de périphériques autorisés
sur le port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_server

```
[no_server]
#macro description No server
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
spanning-tree portfast auto
#
@
```

host

```
[host]
#macro description host
#macro keywords $native_vlan $max_hosts
#
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                        $max_hosts: Nombre maximum de périphériques autorisés
sur le port
#Default Values are
#$native_vlan = Default VLAN
#$max_hosts = 10
#
#the port type cannot be detected automatically
#
#the default mode is trunk
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_host

```
[no_host]
#macro description No host
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_camera

```
[ip_camera]
#macro description ip_camera
#macro keywords $native_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré
sur le port
#Default Values are
#$native_vlan = Default VLAN
#
switchport mode access
switchport access vlan $native_vlan
#
#single host
port security max 1
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_camera

```
[no_ip_camera]
#macro description No ip_camera
#
no switchport access vlan
no switchport mode
#
no port security
no port security mode
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone

```
[ip_phone]
#macro description ip_phone
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                          $voice_vlan: ID du VLAN voix
#                        $max_hosts: Nombre maximum de périphériques autorisés
sur le port
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone

```
[no_ip_phone]
#macro description no ip_phone
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: ID du VLAN voix
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

ip_phone_desktop

```
[ip_phone_desktop]
#macro description ip_phone_desktop
#macro keywords $native_vlan $voice_vlan $max_hosts
#
#macro key description:   $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                          $voice_vlan: ID du VLAN voix
#                        $max_hosts: Nombre maximum de périphériques autorisés
sur le port
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#$max_hosts = 10
#
#the default mode is trunk
smartport switchport trunk allowed vlan add $voice_vlan
smartport switchport trunk native vlan $native_vlan
#
port security max $max_hosts
port security mode max-addresses
port security discard trap 60
#
smartport storm-control broadcast level 10
smartport storm-control include-multicast
```

```
smartport storm-control broadcast enable
#
spanning-tree portfast
#
@
```

no_ip_phone_desktop

```
[no_ip_phone_desktop]
#macro description no ip_phone_desktop
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: ID du VLAN voix
#
#Default Values are
#$voice_vlan = 1
#
smartport switchport trunk allowed vlan remove $voice_vlan
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no port security
no port security mode
no port security max
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
no smartport storm-control include-multicast
#
spanning-tree portfast auto
#
@
```

switch

```
[switch]
#macro description switch
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                        $voice_vlan: ID du VLAN voix
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
spanning-tree link-type point-to-point
```

```
#
@
```

no_switch

```
[no_switch]
#macro description No switch
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: ID du VLAN voix
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no spanning-tree link-type
#
@
```

router

```
[router]
#macro description router
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré
sur le port
#                        $voice_vlan: ID du VLAN voix
#
#Default Values are
#$native_vlan = Default VLAN
#$voice_vlan = 1
#
#the default mode is trunk
smartport switchport trunk allowed vlan add all
smartport switchport trunk native vlan $native_vlan
#
smartport storm-control broadcast level 10
smartport storm-control broadcast enable
#
spanning-tree link-type point-to-point
#
@
```

no_router

```
[no_router]
#macro description No router
#macro keywords $voice_vlan
#
#macro key description:   $voice_vlan: ID du VLAN voix
#
no smartport switchport trunk native vlan
smartport switchport trunk allowed vlan remove all
#
no smartport storm-control broadcast enable
no smartport storm-control broadcast level
#
no spanning-tree link-type
#
@
```

ap

```
[ap]
#macro description ap
#macro keywords $native_vlan $voice_vlan
#
#macro key description:  $native_vlan: VLAN sans balise qui sera configuré
sur le port
```

12

Gestion des VLAN

Cette section couvre les sujets suivants :

- VLAN standard
- Paramètres de VLAN privé
- Paramètres GVRP
- Groupes VLAN
- VLAN voix
- Accès VLAN TV port de multidestination
- VLAN TV port client multidiffusion

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

Description des VLAN

Les VLAN sont configurés avec un ID VLAN unique (VID) dont la valeur est comprise entre 1 et 4 094. Un port sur un périphérique d'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 seul VLAN non balisé ou de plusieurs VLAN balisés.

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

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

Si une trame est balisée VLAN, une balise VLAN à quatre octets est ajoutée à chaque trame Ethernet. La balise contient un ID VLAN compris entre 1 et 4 094, et une balise de priorité VLAN (VPT, VLAN Priority Tag) comprise entre 0 et 7. Pour plus d'informations sur VPT, reportez-vous à la section Qualité de service.

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

S'il n'existe aucune balise VLAN dans la trame ou si la trame comporte une balise de priorité, elle est catégorisée dans le VLAN selon le PVID (identificateur de port VLAN) configuré au port de réception de la trame.

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

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

Le port de sortie :

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

Rôles du VLAN

Les réseaux VLAN fonctionnent au niveau de la couche 2. Tout le trafic VLAN (monodiffusion/diffusion/multidiffusion) demeure au sein du VLAN. Les périphériques reliés à différents VLAN n'ont pas de connectivité directe entre eux sur la couche MAC Ethernet. Des périphériques de VLAN différents peuvent communiquer entre eux uniquement via des routeurs de couche 3. Un routeur IP, par exemple, est requis pour acheminer le trafic IP entre les VLAN si chaque VLAN représente un sous-réseau IP.

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

Les périphériques adjacents tenant compte du VLAN échangent des informations VLAN entre eux via le protocole GVRP (Generic VLAN Registration Protocol). En conséquence, les informations VLAN sont propagées via un réseau 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 plus d'informations sur le protocole GVRP, reportez-vous à la section Paramètres GVRP.

Certains VLAN peuvent avoir des rôles supplémentaires, notamment :

- VLAN voix : pour en savoir plus, reportez-vous à la section VLAN voix.
- VLAN invité : défini sur la page Propriétés.
- VLAN par défaut : VLAN1.

QinQ

QinQ fournit l'isolation entre les réseaux de fournisseur de services et les réseaux de client. Le périphérique est un pont fournisseur qui prend en charge l'interface de service « c-tagged » basée sur les ports.

Avec QinQ, le périphérique ajoute une balise ID appelée ServiceTag (S-tag) qui permet de transférer les paquets sur le réseau du fournisseur. La balise S-tag permet de répartir le trafic entre plusieurs clients, tout en conservant les balises VLAN du client.

Le trafic du client est encapsulé avec une balise S-tag avec TPID 0x8100, indépendamment du fait qu'il soit au départ balisé « c-tagged » ou non balisé. La balise S-tag permet à ce trafic d'être traité comme un agrégat au sein d'un réseau de pont fournisseur, dans lequel le pontage est uniquement basé sur le VID S-tag (S-VID).

La balise S-Tag est conservée lorsque le trafic est transféré par le biais de l'infrastructure du fournisseur de services réseau ; elle est ensuite supprimée par un périphérique de sortie.

Un autre avantage de QinQ est qu'il n'est pas nécessaire de configurer les dispositifs de bordure du client.

Le mode QinQ peut être activé sur la page Paramètres d'interface.

VLAN privé

La fonction VLAN privé fournit une isolation de couche 2 entre les ports. Cela signifie qu'au niveau du trafic de pontage, par opposition au routage IP, les ports qui partagent le même domaine de diffusion ne peuvent pas communiquer les uns avec les autres. Les ports dans un VLAN privé peuvent être situés n'importe où sur le réseau de couche 2, ce qui signifie qu'ils ne sont pas obligatoirement sur le même commutateur. Le VLAN privé est conçu pour recevoir du trafic non balisé ou contenant des balises de priorité et pour transmettre du trafic non balisé.

Les types de ports suivants peuvent être membres d'un VLAN privé :

- **Proximité** : un port de proximité peut communiquer avec tous les ports du même VLAN privé. Ces ports connectent les serveurs et les routeurs.
- **Communauté (hôte)** : les ports de communauté peuvent définir un groupe de ports qui sont membres du même domaine de couche 2. Ils sont isolés au niveau de la couche 2 des autres communautés et des ports isolés. Ces ports connectent les ports d'hôtes.
- **Isolé (hôte)** : Un port isolé possède une isolation complète de couche 2 des autres ports isolés ou des ports de communauté au sein du même VLAN privé. Ces ports connectent les ports d'hôtes.

Les types suivants de VLAN privés existent :

- **VLAN principal** : le VLAN principal est utilisé pour permettre une connectivité de couche 2 des ports de proximité aux ports isolés et aux ports de communauté. Il ne peut y avoir qu'un seul VLAN principal par VLAN privé.
- **VLAN isolé (également appelé VLAN secondaire)** : un VLAN isolé permet aux ports isolés d'envoyer du trafic vers le VLAN principal. Il ne peut y avoir qu'un seul VLAN isolé par VLAN privé.
- **VLAN de communauté (également appelé VLAN secondaire)** : pour créer un sous-groupe de ports (communauté) au sein d'un VLAN, les ports doivent être ajoutés à un VLAN de communauté. Le VLAN de communauté permet une connectivité de couche 2 des ports de communauté aux ports de proximité et aux ports de la même communauté. Il ne peut y avoir qu'un seul VLAN de communauté pour chaque communauté et plusieurs VLAN de communauté peuvent coexister dans le système pour le même VLAN privé.

Reportez-vous à la Figure 1 et à la Figure 2 pour des exemples d'utilisation de ces VLAN.

Le trafic de l'hôte est envoyé sur les VLAN isolés et de communauté, alors que le trafic du serveur et du routeur est envoyé sur le VLAN principal.

L'apprentissage des adresses MAC partagées existe entre tous les VLAN qui sont membres du même VLAN privé (même si le commutateur prend en charge l'apprentissage indépendant du VLAN). Cela permet le trafic de monodiffusion, malgré le fait que les adresses MAC des hôtes sont apprises par les VLAN isolés et de communauté, tandis que les adresses MAC des routeurs et du serveur sont apprises par le VLAN principal.

Un port VLAN privé ne peut être ajouté qu'à un VLAN privé. D'autres types de port, comme les ports d'accès ou de liaison, peuvent être ajoutés à des VLAN individuels qui composent le VLAN privé (car ce sont des VLAN 802.1Q standard).

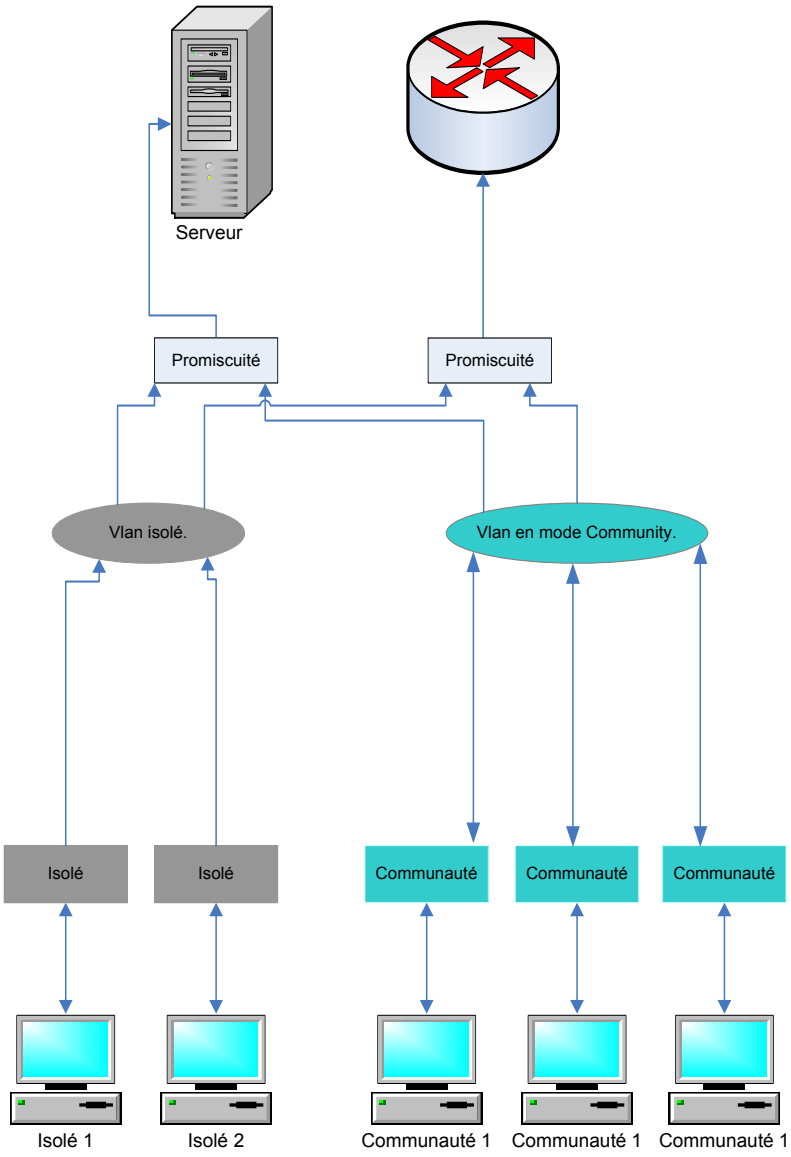
Un VLAN privé peut être configuré pour s'étendre sur plusieurs commutateurs en réglant les ports inter-commutateur comme des ports de liaison et en les ajoutant à tous les VLAN dans le VLAN privé. Les ports de liaison inter-commutateur envoient et reçoivent le trafic balisé des divers VLAN du VLAN privé (principal, isolés et communautés).

Le commutateur prend en charge 16 VLAN principaux et 256 VLAN secondaires.

Flux de trafic

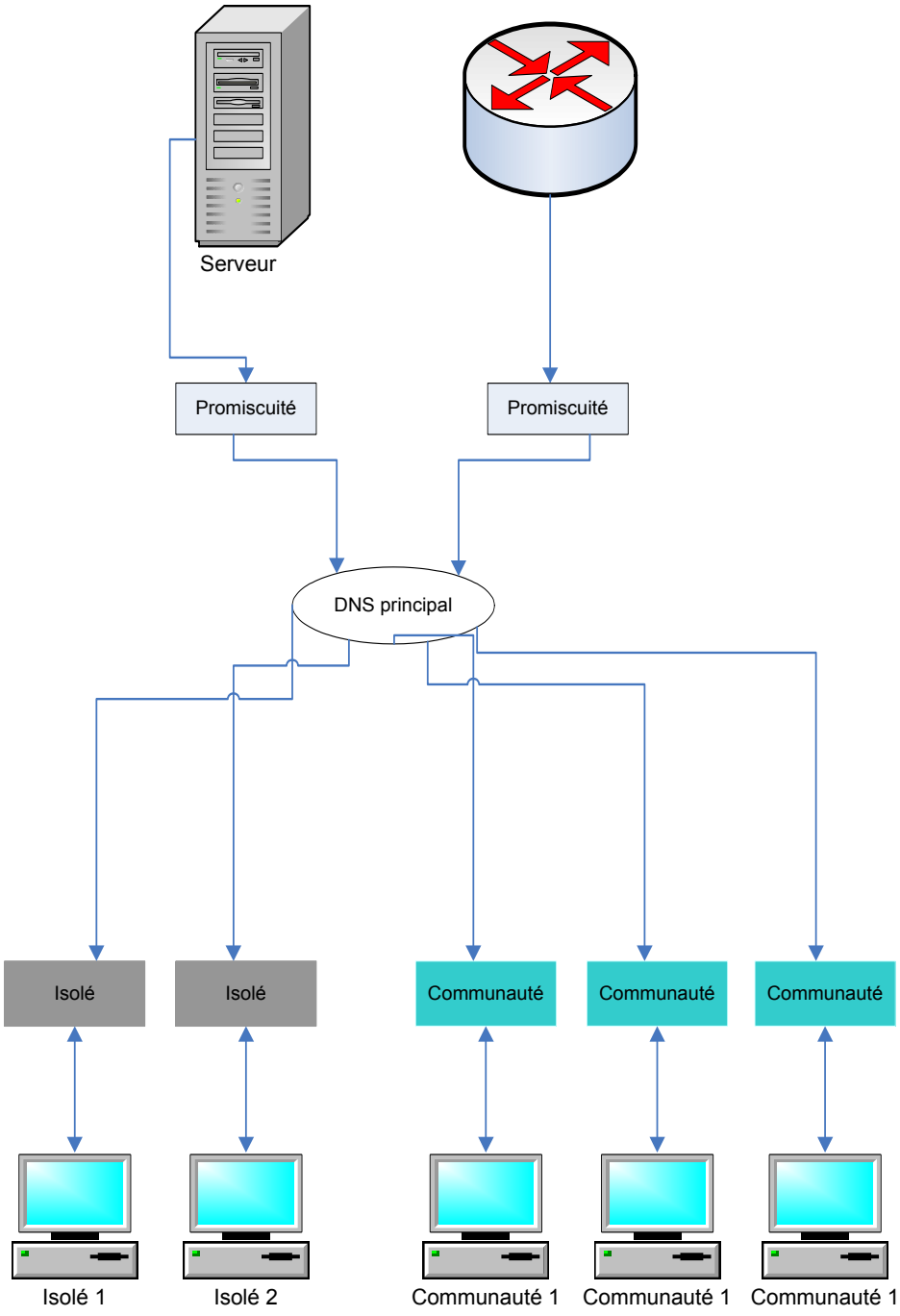
La section suivante décrit le trafic entre les hôtes et les serveurs/routeurs ou d'autres hôtes.

Figure 1 Trafic des hôtes vers les serveurs/routeurs



La section suivante décrit le trafic serveur/routeur (réponse à l'hôte).

Figure 2 Trafic des serveurs/routeurs vers les hôtes



Interaction avec les autres fonctions

Cette section décrit l'interaction entre les VLAN privés et d'autres fonctions du système.

Fonctions prises en charge sur un VLAN privé

Les fonctions suivantes peuvent être activées uniquement sur un VLAN principal (et pas sur un VLAN isolé ni sur un VLAN de communauté), bien qu'elles affectent tous les VLAN dans le VLAN privé.

- Surveillance IGMP et surveillance MLD. Les rapports et les requêtes IGMP sont détectés sur tous les VLAN dans le VLAN privé, tandis que les entrées de multidiffusion résultantes ne sont ajoutées qu'à la base de données FDB du VLAN principal. Cela permet de transférer le trafic de multidiffusion vers le VLAN principal plutôt qu'inonder ce dernier. Les VLAN isolés et les VLAN de communauté continuent d'inonder avec le trafic de multidiffusion.
- Surveillance DHCP
- Inspection ARP
- Protection de la source IP

Le système empêche l'ajout ou le retrait des VLAN isolés ou de communauté dans un VLAN privé, tant que les fonctions ci-dessus sont activées.

Fonctions non prises en charge sur un VLAN privé

Les fonctions suivantes ne sont pas prises en charge sur les VLAN privés et sur tous les VLAN constituant le VLAN privé :

- VLAN voix automatique
- VLAN par défaut
- Relais DHCP
- VLAN non authentifié 802.1x
- VLAN invité
- IPv4 et IPv6. Toutes deux peuvent être définies sur un VLAN principal. Les ports isolés et de communauté ne permettent pas la connectivité IP. La connectivité IP nécessite de faire passer le trafic sur un VLAN principal.

Fonctions non prises en charge sur les modes de port VLAN privé

Les fonctions suivantes ne sont pas prises en charge sur les modes de port VLAN privé :

- GVRP
- Détection automatique d'OUI de VLAN voix
- VLAN invité avec port 802.1x
- Affectation VLAN dynamique de port 802.1x
- VLAN TV multidiffusion

REMARQUE Notez les clarifications suivantes :

- Port de sécurité : les entrées MAC dans la table de la FDB du VLAN sont vidées lorsque le port est déverrouillé.
- L'appartenance des ports à un VLAN privé est équivalente à l'appartenance des ports aux VLAN 802.1Q en ce qui concerne les limitations de l'interaction entre les fonctions, par exemple :
  - Un port ne doit pas être ajouté à un LAG/LACP.
  - Un port ne doit pas être configuré en tant que destination du port moniteur.

Ressources requises

Comme un VLAN privé est composé de plusieurs VLAN 802.1Q, le système exige des ressources supplémentaires pour chaque VLAN secondaire dans un VLAN privé. Les ressources pour les fonctions suivantes sont allouées par VLAN dans le VLAN privé.

- **Adresses MAC dynamiques** : les adresses MAC apprises sur les VLAN principaux sont copiées sur tous les VLAN de communauté et sur le VLAN isolé. Les adresses MAC apprises sur les VLAN isolés ou de communauté sont copiées sur le VLAN principal.
- **Surveillance DHCP** : une règle TCAM est nécessaire pour capturer le trafic DHCP.
- **Inspection ARP** : une règle TCAM est nécessaire pour capturer le trafic ARP.
- **Protection de la source IP** : une règle TCAM est nécessaire pour transférer/omettre le trafic IP.
- **Sécurité du premier saut** : une règle TCAM est nécessaire pour capturer le trafic IPv6 (lorsque la protection de la source IPv6 est activée).

Consignes relatives à la configuration

Prenez note des consignes suivantes pour la configuration des fonctions :

- **MSTP** : la même instance MSTP doit être affectée à tous les VLAN dans un VLAN privé.
- **Protection de la source IP** : la liaison d'une ACL aux ports de protection de la source IP n'est pas recommandée sur un VLAN privé en raison de la quantité de ressources TCAM nécessaires.

VLAN standard

Cette section décrit les pages de l'interface utilisateur permettant de configurer les différents types de VLAN. Cette section décrit les éléments suivants :

- Présentation du VLAN standard
- Paramètres VLAN
- Paramètres d'interface
- Port vers VLAN
- Appartenance VLAN des ports
- Traduction de VLAN
- Paramètres GVRP
- Présentation des groupes de VLAN basés sur MAC
- Présentation des groupes de VLAN basés sur un sous-réseau
- Présentation des groupes de VLAN basés sur un protocole

Présentation du VLAN standard

Flux de travail de la configuration VLAN

Pour configurer les VLAN :

ÉTAPE 1 Créez les VLAN requis en suivant les instructions de la section Paramètres VLAN.

ÉTAPE 2 Définissez la configuration VLAN souhaitée pour les ports et activez QinQ sur une interface, comme décrit dans la section *Paramètres d'interface*.

ÉTAPE 3 Assignez des interfaces aux VLAN comme décrit dans la section Port vers VLAN ou la section Appartenance VLAN des ports.

ÉTAPE 4 Affichez l'appartenance actuelle des ports au VLAN pour toutes les interfaces, comme décrit dans la section Appartenance VLAN des ports.

1. Si nécessaire, configurez les groupes VLAN comme indiqué dans les sections Présentation des groupes de VLAN basés sur MAC et Présentation des groupes de VLAN basés sur un sous-réseau.
2. Si nécessaire, configurez le VLAN TV comme indiqué dans les sections Accès VLAN TV port de multidestination et VLAN TV port client multidiffusion.

Paramètres VLAN par défaut

Le commutateur crée automatiquement un VLAN par défaut appelé VLAN 1. L'état de l'interface par défaut de tous les ports est défini sur Access (Accès) et tous les ports sont configurés en tant que membres non balisés du VLAN par défaut.

Le VLAN par défaut présente les caractéristiques suivantes :

- Il est distinct, non statique/non dynamique et tous les ports sont des membres non balisés par défaut.
- Il peut être supprimé.
- Il ne peut recevoir d'étiquette.
- Il est automatiquement utilisé en tant que VLAN voix pour le VLAN voix basé sur OUI.
- Si un port n'est plus membre d'un VLAN, le périphérique le configure automatiquement en tant que membre non balisé du VLAN par défaut. Un port n'est plus membre d'un VLAN si le VLAN est supprimé ou si le port est supprimé du VLAN.
- Les serveurs RADIUS ne peuvent pas attribuer le VLAN par défaut aux demandeurs 802.1x via l'affectation dynamique de VLAN.

Paramètres VLAN

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

Le périphérique prend en charge jusqu'à 4 000 VLAN, y compris le VLAN par défaut.

Chaque VLAN doit être configuré avec un ID VLAN unique (VID) dont la valeur est comprise entre 1 et 4 094. Le périphérique réserve le VID 4095 comme VLAN d'abandon. Tous les paquets classés comme VLAN d'abandon sont abandonnés à l'entrée et ne sont pas transférés vers un port.

Pour créer un VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres VLAN**.

Les informations s'affichent pour tous les VLAN définis. Les champs ci-dessous sont définis sur la page **Ajouter**. Le champ suivant n'est pas sur la page **Ajouter**.

- **Originators** (Initiateurs) : façon dont le VLAN a été créé.
  - *GVRP* : le VLAN a été créé dynamiquement via le protocole GVRP (Generic VLAN Registration Protocol).
  - *Statique* : le VLAN a été défini par l'utilisateur.
  - *Par défaut* : c'est le VLAN par défaut.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un ou plusieurs nouveaux VLAN.

La page permet la création d'un VLAN unique ou d'une plage de VLAN.

ÉTAPE 3 Pour créer un seul VLAN, sélectionnez le bouton **VLAN**, saisissez l'**ID de VLAN** et le **Nom du VLAN** (facultatif).

Pour créer une plage de VLAN, sélectionnez le bouton **Plage** et spécifiez la plage de VLAN à créer en saisissant le VID de départ et le VID de fin (ces valeurs sont comprises). Si vous utilisez la fonction **Plage**, le nombre maximal de VLAN que vous pouvez créer en une seule fois est 100.

REMARQUE Le système nécessite certains VLAN pour une utilisation interne ; ils ne peuvent donc pas être créés ni configurés par l'utilisateur. Ces VLAN sont les suivants :

- Un VLAN pour chaque interface IP, défini directement sur un port Ethernet ou un canal de port (LAG).
- Un VLAN pour chaque tunnel IPv6.
- Un VLAN pour 802.1x.

Les VLAN pour les tunnels IPv6 et pour 802.1x sont pré-attribués, tandis que les VLAN pour la configuration IP des ports Ethernet/canaux de port sont affectés lors de l'application de la configuration IP. Des VLAN internes sont alloués en commençant par le VLAN libre dont le numéro est le plus élevé (par défaut, VLAN 4094).

ÉTAPE 4 Ajoutez les champs suivants pour les nouveaux VLAN.

- **État de l'interface VLAN** : sélectionnez cette option pour arrêter le VLAN. Dans cet état, le VLAN ne transmet/reçoit pas de messages en provenance/vers des niveaux plus élevés. Par exemple, si vous arrêtez un VLAN sur lequel une interface IP est configurée, le pontage dans le VLAN continue, mais le commutateur ne peut pas transmettre et recevoir le trafic IP sur le VLAN.
- **Interceptions SNMP d'état de lien** : sélectionnez cette option pour activer la génération des interceptions SNMP relatives à l'état de la liaison.

ÉTAPE 5 Cliquez sur **Appliquer** pour créer le ou les VLAN.

Paramètres d'interface

La page *Paramètres d'interface* affiche et active la configuration des paramètres du VLAN pour toutes les interfaces.

Pour configurer les paramètres du VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres d'interface**.

ÉTAPE 2 Sélectionnez la méthode **Balisage Ethertype global** pour la balise S-VLAN.

- Dot1q-8100
- Dot1ad-88a8
- 9100
- 9200

ÉTAPE 3 Sélectionnez un type d'interface (Port ou LAG) et cliquez sur **Go**. Les ports ou LAG et leurs paramètres VLAN s'affichent.

ÉTAPE 4 Pour configurer un port ou LAG, sélectionnez-le puis cliquez sur **Modifier**.

ÉTAPE 5 Entrez les valeurs des champs suivants :

- **Interface** : sélectionnez un port/LAG.
- **Mode Port commuté** : sélectionnez Couche 2 ou Couche 3.
- **Mode d'interface VLAN** : sélectionnez le mode d'interface du VLAN. Les options sont les suivantes :
  - *Général* : l'interface peut prendre en charge toutes les fonctions telles qu'elles sont définies dans la spécification IEEE 802.1q. Elle peut être un membre balisé ou non balisé d'un ou de plusieurs VLAN.
  - *Accès* : l'interface est un membre non balisé d'un VLAN unique. Un port configuré dans ce mode est appelé un port d'accès.
  - *Liaison* : l'interface est membre non balisé d'un VLAN au maximum, ainsi que membre balisé de zéro ou plusieurs VLAN. Un port configuré dans ce mode est appelé un port de liaison.
  - *Client* : sélectionnez cette option pour mettre l'interface en mode QinQ. Vous pouvez ainsi appliquer votre propre agencement VLAN (PVID) sur le réseau du fournisseur. Le périphérique est en mode Q-in-Q lorsqu'il comporte un ou plusieurs ports client. Reportez-vous à la section QinQ.
  - VLAN privé - Hôte : sélectionnez cette option pour définir l'interface comme isolée ou de communauté. Puis, sélectionnez un VLAN isolé ou de communauté dans le champ VLAN secondaire - Hôte.
  - VLAN privé - Proximité : sélectionnez cette option pour définir l'interface comme interface de proximité.
  - Mise en correspondance de VLAN – Tunnel : sélectionnez cette option pour définir l'interface comme port de bordure de tunnel VLAN.
  - Mise en correspondance de VLAN – Un à un : sélectionnez cette option pour définir l'interface à utiliser comme port de bordure un à un pour la mise en correspondance de VLAN.
- **Balisage Ethertype** : sélectionnez une méthode de balisage Ethertype pour la balise S-VLAN (reportez-vous au champ **Balisage Ethertype global** ci-dessus).
- **Type de trame** : (disponible uniquement en mode Général) sélectionnez le type de trame que l'interface peut recevoir. Les trames qui ne sont pas du type configuré sont abandonnées à l'entrée. Les valeurs possibles sont les suivantes :
  - *Tout admettre* : l'interface accepte tous les types de trames : trames non balisées, trames balisées et trames avec balise de priorité.

- *Admettre balisées uniquement* : l'interface accepte uniquement les trames balisées.
- *Admettre non balisées uniquement* : l'interface accepte uniquement les trames de priorité et les trames non balisées.

- **Filtrage d'entrée** : (uniquement disponible en mode Général) sélectionnez cette option pour activer le filtrage en entrée. Lorsqu'une interface est en mode de filtrage d'entrée, elle abandonne toutes les trames entrantes classées comme appartenant aux VLAN dont elle n'est pas membre. Le filtrage d'entrée peut être désactivé ou activé sur les ports généraux. Il est toujours activé sur les ports d'accès et les ports de liaison.
- **VLAN principal** : sélectionnez le VLAN principal dans le VLAN privé. Le VLAN principal est utilisé pour permettre une connectivité de couche 2 des ports de proximité aux ports isolés et ports de communauté. Si vous sélectionnez **None** (Aucun), l'interface n'est pas en mode VLAN privé.
- **VLAN secondaire - Hôte** : sélectionnez un VLAN isolé ou de communauté pour les hôtes qui ne nécessitent qu'un seul VLAN secondaire.
- **VLAN secondaires disponibles pour les VLAN secondaires sélectionnés** : pour les ports de proximité, déplacez tous les VLAN secondaires qui sont requis pour le transfert normal des paquets à partir des **VLAN secondaires disponibles**. Les ports de proximité et de liaison peuvent être membres de plusieurs VLAN.

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

Traduction de VLAN

La traduction de VLAN comprend la fonctionnalité de tunneling de VLAN, ainsi que la fonction de mise en correspondance de VLAN « un à un ».

Le tunneling de VLAN est une amélioration de la fonctionnalité VLAN en mode QinQ/Nested VLAN/Client. Elle permet aux fournisseurs de services d'utiliser un seul VLAN pour prendre en charge des clients qui possèdent plusieurs VLAN, tout en conservant les ID de VLAN du client et en séparant le trafic sur les différents VLAN du client. Cette fonctionnalité est connue sous le nom de « double balisage » ou QinQ car, outre la balise 802.1Q standard (VLAN client/C-VLAN), le commutateur ajoute une balise ID, désignée sous le nom de balise de service (S-VLAN), pour réacheminer le trafic sur le réseau. Sur une interface de bordure, c'est-à-dire l'interface sur laquelle un réseau client est connecté au commutateur de bordure du fournisseur, les C-VLAN sont mappés à des S-VLAN et les balises C-VLAN d'origine sont conservées dans le cadre de la capacité utile. Les trames non balisées sont abandonnées.

Lorsqu'une trame est envoyée sur une interface balisée « non-edge », elle est encapsulée avec une autre couche de balise S-VLAN sur laquelle l'ID C-VLAN d'origine est mappé. Les paquets transmis sur des trames d'interfaces de ce type font donc l'objet d'un double balisage, avec une balise S-VLAN externe et une balise C-VLAN interne. La balise S-VLAN est conservée, tandis que le trafic est acheminé sur l'infrastructure du fournisseur de services réseau. Sur un périphérique de sortie, la balise S-VLAN est supprimée lorsqu'une trame est envoyée vers une interface de bordure. Les trames non balisées sont abandonnées.

La fonction de tunneling VLAN utilise un ensemble de commandes différent de l'implémentation QinQ/Nested VLAN d'origine et y ajoute les fonctionnalités suivantes :

- Elle fournit, pour chaque interface de bordure, plusieurs mappages de C-VLAN différents à des VLAN distincts.
- Elle permet de configurer une action d'abandon pour certains C-VLAN reçus sur des interfaces de bordure.
- Elle permet de configurer l'action pour des C-VLAN qui ne sont pas mappés de façon spécifique à un S-VLAN (abandon ou mappage à certains S-VLAN).
- Elle permet de configurer, globalement et par interface NNI (Network Node Interface - Ports de dorsale), l'EtherType de la balise S-VLAN. Dans l'implémentation QinQ précédente, seul l'EtherType 0x8100 était pris en charge pour une balise S-VLAN.

Le S-VLAN spécifié par l'utilisateur doit être créé sur le périphérique avant d'être configuré sur une interface en tant que telle. Si ce VLAN n'existe pas, la commande échouera.

Le réacheminement IPv4/IPv6 et le tunneling VLAN sont des fonctionnalités qui s'excluent mutuellement. Cela signifie que si le réacheminement IPv4 ou IPv6 est activé, une interface ne peut pas être définie sur le mode de tunneling VLAN. De même, si une interface est définie sur le mode de tunneling VLAN, le réacheminement IPv4 ou IPv6 ne peut pas être activé sur ce périphérique.

Les fonctionnalités suivantes sont aussi mutuellement exclusives avec le tunneling VLAN :

- VLAN voix automatique
- Port intelligent automatique
- VLAN voix

Les interfaces IPv4 et IPv6 ne peuvent pas être définies sur les VLAN qui comportent des interfaces de bordure.

Les fonctionnalités de couche 2 ci-dessous ne sont pas prises en charge sur les VLAN qui comportent des interfaces de bordure :

- Surveillance IGMP/MLD
- Surveillance DHCP
- Sécurité du premier saut IPv6

Les protocoles suivants ne peuvent pas être activés sur les interfaces de bordure (UNI - Interfaces de réseau utilisateur) :

- STP
- GVRP

Les fonctionnalités suivantes ne sont pas prises en charge sur les interfaces de bordure (UNI - Interfaces de réseau utilisateur) :

- Affectation VLAN RADIUS
- VLAN 802.1x
- SPAN/RSPAN – En tant que port de destination avec le mot-clé réseau ou en tant que port réflecteur avec le mot-clé réseau ou port réflecteur.

Pour appliquer le mode de tunneling VLAN sur une interface, l'utilisation de règles TCAM de routeur est requise. Si la quantité de ressources TCAM de routeur s'avère insuffisante, la commande échouera. Les utilisateurs peuvent ajouter/supprimer l'allocation de ressources TCAM de routeur en vue du tunneling (et de la mise en correspondance) VLAN en sélectionnant **Administration > Ressources de routage** (un redémarrage du système est requis).

L'implémentation QinQ d'origine (commandes relatives au mode client) coexiste avec la nouvelle implémentation du tunneling VLAN. Le mode du port client constitue un cas particulier de port de tunnel de mise en correspondance de VLAN et ne nécessite aucune allocation de ressources TCAM.

Outre le tunneling VLAN, le périphérique prend en charge la mise en correspondance de VLAN de type « un à un ». Avec ce type de mise en correspondance, sur une interface de bordure (c'est-à-dire l'interface sur laquelle un réseau client est connecté au commutateur de bordure du fournisseur), les C-VLAN sont mappés à des S-VLAN et les balises C-VLAN d'origine sont remplacées par le S-VLAN spécifié. Les trames non balisées sont abandonnées.

Lorsqu'une trame est envoyée sur une interface balisée « non-edge », elle est accompagnée d'une seule balise VLAN, à savoir celle du S-VLAN spécifié. La balise S-VLAN est conservée, tandis que le trafic est acheminé sur le réseau d'infrastructure du fournisseur de services. Sur un périphérique de sortie, la balise S-VLAN est remplacée par la balise C-VLAN lorsqu'une trame est envoyée vers une interface de bordure.

Dans le mode de mise en correspondance de VLAN « un à un », une interface appartient à tous les SVLAN pour lesquels la mise en correspondance est définie en tant qu'interface avec balise de sortie. Le PVID d'interface est défini sur 4095.

Mise en correspondance de VLAN

Pour configurer une mise en correspondance de VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Traduction de VLAN > Mise en correspondance de VLAN**.

La table des paramètres de mise en correspondance de VLAN définis précédemment s'affiche.

ÉTAPE 2 Sélectionnez l'un des types de mise en correspondance suivants :

- **Un à un** : sélectionnez cette option pour afficher et modifier les paramètres de l'interface définie sur le mode de mise en correspondance de VLAN « Un à un ».
- **Mise en correspondance de tunnels** : sélectionnez cette option pour afficher et modifier les paramètres de l'interface définie sur le mode de mise en correspondance de VLAN « Tunnel ».

ÉTAPE 3 Cliquez sur **Ajouter**, puis renseignez les champs suivants :

- **Interface** : sélectionnez le port.
- **Mode VLAN d'interface** : affiche le mode d'interface actuel.
- **Type de mise en correspondance** : sélectionnez l'une des options suivantes :
  - *Un à un* : sélectionnez cette option pour définir des paramètres de mise en correspondance de VLAN « Un à un ».
  - *Mise en correspondance de tunnels* : sélectionnez cette option pour définir des paramètres de mise en correspondance de VLAN « Tunnel ».
- **Traduction « un à un »** : cette option s'affiche si vous avez sélectionné l'option « Un à un » comme type de mise en correspondance. Sélectionnez l'une des options suivantes :
  - *VLAN source* : configurez l'ID du VLAN client (C-VLAN) qui sera traduit (converti) en S-VLAN (VLAN traduit).
  - *VLAN traduit* : configurez le S-VLAN qui remplacera le C-VLAN spécifié.

- **Mise en correspondance de tunnels** : cette option s'affiche si vous avez sélectionné l'option « Mise en correspondance de tunnels » comme type de mise en correspondance. Sélectionnez l'une des options suivantes :
  - *VLAN client* : sélectionnez **Par défaut** pour définir l'action requise pour les C-VLAN qui ne sont pas indiqués de façon spécifique ou **Liste des VLAN** pour définir précisément le comportement de tunnel VLAN pour les VLAN répertoriés.
  - *Tunneling* : sélectionnez **Abandonner** ou **ID de VLAN extérieur**. Si l'option ID de VLAN extérieur est sélectionnée, indiquez les VLAN.

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

Port vers VLAN

Les pages **Port vers VLAN** et Appartenance VLAN des ports affichent les appartenances VLAN des ports dans diverses présentations. Vous pouvez les utiliser pour ajouter des appartenances aux VLAN ou en supprimer de ces derniers.

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

Pour transférer correctement les paquets, les périphériques intermédiaires tenant compte du VLAN qui acheminent le trafic VLAN entre les nœuds d'extrémité doivent être configurés manuellement, ou doivent apprendre dynamiquement les VLAN ainsi que leurs appartenances de port via le protocole GVRP (Generic VLAN Registration Protocol).

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

Les trames balisées VLAN peuvent traverser 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.

Utilisez la page Port vers VLAN pour afficher et configurer les ports dans un VLAN spécifique.

Pour mapper des ports ou des LAG à un VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Port vers VLAN**.

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

Le mode actuel de chaque port ou LAG s'affiche (Access [Accès], Trunk [Liaison], General [Général], Private-Host [Hôte privé], Private-Promiscuous [Hôte de proximité] ou Customer [Client]). Vous pouvez configurer ce mode sur la page Paramètres d'interface.

Chaque port ou LAG s'affiche avec son enregistrement actuel sur le VLAN.

Les champs suivants s'affichent :

- **VLAN Mode** (Mode VLAN) : affiche le type des ports dans le VLAN.
- **Type d'appartenance** : sélectionnez l'une des options suivantes :
  - *Interdit* : l'interface n'est pas autorisée à rejoindre le VLAN même à partir de l'enregistrement GVRP. Lorsqu'un port n'est pas membre d'un autre VLAN, l'activation de cette option sur le port l'intègre au VLAN interne 4095 (VID réservé).
  - *Exclu* : l'interface n'est actuellement pas membre du VLAN. Ceci est le paramètre par défaut pour tous les ports et LAG lorsqu'un nouveau VLAN vient d'être créé.
  - *Balisé* : l'interface est un membre balisé du VLAN.
  - *Non balisé* : l'interface est un membre non balisé du VLAN. Les trames du VLAN sont envoyées non balisées à l'interface VLAN.
  - *VLAN TV multidiffusion* : interface utilisée pour la TV numérique à l'aide d'IP de multidestination. Le port se connecte au VLAN avec une balise VLAN de VLAN TV multidiffusion. Pour plus d'informations, reportez-vous à l'Accès VLAN TV port de multidestination.
- **PVID** : sélectionnez cette option pour définir le PVID de l'interface avec le VID du VLAN. Le PVID est un paramètre propre à chaque port.

ÉTAPE 3 Cliquez sur **Appliquer**. Les interfaces sont attribuées au VLAN et écrites dans le fichier de Configuration d'exécution.

Vous pouvez continuer d'afficher et/ou de configurer l'appartenance de port à un autre VLAN en sélectionnant l'ID d'un autre VLAN.

Appartenance VLAN des ports

La page Appartenance VLAN des ports affiche tous les ports du périphérique, ainsi qu'une liste des VLAN auxquels chaque port appartient.

Si la méthode d'authentification basée sur les ports pour une interface est 802.1x et que le Contrôle de port administratif est Auto, alors :

- Tant que le port n'est pas authentifié, il est exclu de tous les VLAN, à l'exception des VLAN invités et non authentifiés. Sur la page VLAN vers port, le port est marqué d'un « P » majuscule.
- Lorsque le port est authentifié, il reçoit l'appartenance dans le VLAN où il a été configuré.

REMARQUE Le mode VLAN IS est pris en charge. Cela signifie que l'appartenance du port VLAN peut être configurée au préalable pour plusieurs modes VLAN. Lorsque le port passe en mode VLAN spécifique, la configuration devient active. Lorsque vous changez de mode, les paramètres du mode quitté sont sauvegardés et seront réappliqués si vous le réactivez sur l'interface.

Pour attribuer un port à un ou plusieurs VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Appartenance VLAN des ports**.

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

- **Interface** : ID du port/LAG.
- **Mode** : mode de l'interface VLAN sélectionné sur la page Paramètres d'interface.
- **VLAN administratifs** : liste déroulante qui affiche tous les VLAN dont l'interface peut être membre.
- **VLAN opérationnels** : liste déroulante qui affiche tous les VLAN dont l'interface est actuellement membre.
- **LAG** : si l'interface sélectionnée est Port, affiche le LAG dont elle est membre.

ÉTAPE 3 Sélectionnez un port et cliquez sur le bouton **Connecter le VLAN**.

ÉTAPE 4 Entrez les valeurs des champs suivants :

- **Interface** : sélectionnez un port/LAG.
- **Current VLAN Mode** (Mode VLAN actuel) : affiche le mode VLAN du port qui a été sélectionné sur la page Paramètres d'interface.

- **Appartenance du mode d'accès (actif)**
  - *Access VLAN ID* (ID VLAN d'accès) : lorsque le port est en mode d'accès, il est membre de ce VLAN.
  - *VLAN TV multidiffusion* : lorsque le port est en mode d'accès, il est membre de ce VLAN TV multidiffusion.
- **Appartenance du mode de liaison**
  - *Native VLAN ID* (ID VLAN natif) : lorsque le port est en mode de liaison, il est membre de ce VLAN.
  - *Tagged VLANs* (VLAN balisés) : lorsque le port est en mode de liaison, il est membre de ces VLAN. Les options suivantes sont disponibles :

    All VLANs (Tous les VLAN) : lorsque le port est en mode de liaison, il est membre de tous les VLAN.

    User Defined (Définis par l'utilisateur) : lorsque le port est en mode de liaison, il est membre des VLAN définis ici.
- **Appartenance du mode général**
  - *Untagged VLANs* (VLAN non balisés) : lorsque le port est en mode général, il est membre non balisé de ce VLAN.
  - *Tagged VLANs* (VLAN balisés) : lorsque le port est en mode général, il est membre balisé de ce VLAN.
  - *Forbidden VLANs* (VLAN interdits) : lorsque le port est en mode général, l'interface n'est pas autorisée à joindre le VLAN, même depuis 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).
  - *General PVID* (PVID général) : lorsque le port est en mode général, il appartient à ces VLAN.
- **Appartenance du mode client**
  - *Customer VLAN ID* (ID VLAN client) : lorsque le port est en mode client, il est membre de ces VLAN.
  - *VLAN client multidiffusion* : lorsque le port est en mode client, il est membre de ces VLAN TV multidiffusion.

ÉTAPE 5 Sélectionnez un port et cliquez ensuite sur **Détails** pour afficher les champs suivants :

- **Administrative VLANs** (VLAN administratifs) : le port est configuré pour ces VLAN.
- **Operational VLANs** (VLAN opérationnels) : le port est actuellement membre de ces VLAN.

ÉTAPE 6 Cliquez sur **Apply** (Appliquer) (pour rejoindre le VLAN). Les paramètres sont modifiés et écrits dans le fichier de Configuration d'exécution.

Paramètres de VLAN privé

La page Paramètres de VLAN privé affiche les VLAN privés qui ont été définis.

Pour créer un nouveau VLAN privé :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres de VLAN privé**.

ÉTAPE 2 Cliquez sur le bouton **Ajouter**.

ÉTAPE 3 Entrez les valeurs des champs suivants :

- **ID de VLAN principal** : sélectionnez un VLAN à définir comme le VLAN principal dans le VLAN privé. Le VLAN principal est utilisé pour permettre une connectivité de couche 2 des ports de proximité aux ports isolés et ports de communauté.
- **ID de VLAN isolé** : un VLAN isolé permet aux ports isolés d'envoyer du trafic vers le VLAN principal.
- **Available Community VLANs (VLAN de communauté disponibles)** : déplacez les VLAN à définir comme VLAN de communauté vers la liste **Selected Community VLANs (VLAN de communauté sélectionnés)**. Les VLAN de communauté permettent une connectivité de couche 2 des ports de communauté aux ports de proximité et aux ports de la même communauté. C'est qui s'appelle **Plage de VLAN de communauté** sur la page principale.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres sont modifiés et écrits dans le fichier de Configuration d'exécution.

Paramètres GVRP

Les périphériques adjacents tenant compte du VLAN peuvent s'échanger les 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.

Pour activer le protocole GVRP sur une interface, celle-ci doit être configurée en mode Général.

Lorsqu'un port est connecté à un VLAN via GVRP, il est ajouté au VLAN en tant que membre dynamique balisé, sauf si cette action a été expressément interdite sur la page Appartenance VLAN des ports. Si le VLAN n'existe pas, il est dynamiquement créé lorsque la création de VLAN dynamiques est activée pour ce port (sur la page Paramètres GVRP).

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.

Par défaut, le protocole GVRP est désactivé globalement et sur les ports.

Paramètres GVRP

Pour définir les paramètres GVRP d'une interface :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres GVRP**.

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

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

ÉTAPE 4 Sélectionnez un type d'interface (Port ou LAG) et cliquez sur **OK** pour afficher toutes les interfaces de ce type.

ÉTAPE 5 Pour définir les paramètres GVRP pour un port, sélectionnez-le et cliquez sur **Modifier**.

ÉTAPE 6 Entrez les valeurs des champs suivants :

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

ÉTAPE 7 Cliquez sur **Appliquer**. Les paramètres GVRP sont modifiés et écrits dans le fichier de Configuration d'exécution.

Groupes VLAN

Cette section explique comment configurer les groupes de VLAN. Elle décrit les fonctionnalités suivantes :

- Présentation des groupes de VLAN basés sur MAC
- Présentation des groupes de VLAN basés sur un protocole
- Présentation des groupes de VLAN basés sur un sous-réseau

Les groupes VLAN sont utilisés pour l'équilibrage de charge du trafic sur un réseau de couche 2.

Les paquets sont affectés à un VLAN en fonction des diverses classifications.

Si plusieurs schémas de classification sont définis, les paquets sont affectés à un VLAN dans l'ordre suivant :

- **Balise** : si le paquet est balisé, le VLAN est extrait de la balise.
- **VLAN basé sur MAC** : si un VLAN basé sur MAC a été défini, le VLAN est extrait du mappage source MAC au VLAN de l'interface d'entrée.
- **VLAN basé sur un sous-réseau** : si un VLAN basé sur un sous-réseau a été défini, le VLAN est extrait du mappage source IP au VLAN de l'interface d'entrée.
- **Protocol-Based VLAN** (VLAN basé sur protocole) : si un VLAN basé sur protocole a été défini, le VLAN est extrait du mappage Protocole (de type Ethernet) au VLAN de l'interface d'entrée.
- **PVID** : le VLAN est extrait de l'ID de VLAN par défaut du port.

Présentation des groupes de VLAN basés sur MAC

La classification des VLAN basés sur MAC permet au système de classer les paquets en fonction de leur adresse MAC source. Vous pouvez alors définir le mappage MAC au VLAN pour chaque interface.

Vous pouvez définir plusieurs groupes VLAN basés sur MAC, chaque groupe contenant différentes adresses MAC.

Ces groupes basés sur MAC peuvent être attribués à des ports/LAG spécifiques. Les groupes VLAN basés sur MAC ne peuvent pas contenir de plages d'adresses MAC qui se chevauchent sur le même port.

Flux de travail

Pour définir un groupe de VLAN basé sur MAC :

1. Attribuez une adresse MAC à un ID de groupe VLAN (à l'aide de la page Groupes basés sur MAC).
2. Pour chaque interface requise :
   a. Affectez le groupe VLAN à un VLAN (à l'aide de la page Groupes basés sur MAC aux VLAN). Les interfaces doivent être en mode Général.
   b. Si l'interface n'appartient pas au VLAN, affectez-la manuellement au VLAN à l'aide de la page Port vers VLAN.

Groupes basés sur MAC

Reportez-vous au Tableau 1 pour obtenir une description de la disponibilité de cette fonction.

Pour assigner une adresse MAC à un groupe de VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Groupes VLAN** > **Groupes basés sur MAC**.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Entrez les valeurs des champs suivants :

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

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

- **Masque de préfixe** : saisissez l'une des informations suivantes :
  - *Hôte (48)* : permet d'inclure tous les bits de l'adresse MAC dans le masque de préfixe (48 bits)
  - *Longueur* : *préfixe* de l'adresse MAC
- **ID de groupe** : saisissez un ID de groupe VLAN créé par l'utilisateur.

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

Groupes basés sur MAC aux VLAN

Reportez-vous au Tableau 1 pour obtenir une description de la disponibilité de cette fonction.

Les ports/LAG doivent être en mode Général.

Pour attribuer un groupe de VLAN basé sur MAC à un VLAN sur une interface :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Groupes VLAN** > **Groupes basés sur MAC aux VLAN**.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Entrez les valeurs des champs suivants :

- **Type de groupe** : indique que le groupe est basé sur une adresse MAC.
- **Interface** : saisissez une interface générale (port/LAG) via laquelle le trafic est reçu.
- **ID de groupe** : sélectionnez un groupe VLAN, défini sur la page Présentation des groupes de VLAN basés sur MAC.
- **ID de VLAN** : sélectionnez le VLAN vers lequel le trafic est transféré depuis le groupe VLAN.

ÉTAPE 4 Cliquez sur **Appliquer** pour définir le mappage du groupe VLAN au VLAN. Ce mappage ne lie pas l'interface dynamiquement au VLAN ; l'interface doit être ajoutée manuellement au VLAN.

Présentation des groupes de VLAN basés sur un sous-réseau

La classification Groupe de VLAN basé sur un sous-réseau permet de classer les paquets en fonction de leur sous-réseau. Vous pouvez alors définir le mappage sous-réseau au VLAN pour chaque interface.

Vous pouvez configurer plusieurs groupes de VLAN basés sur un sous-réseau, chacun d'eux contenant différents sous-réseaux.

Ces groupes peuvent être attribués à des ports/LAG spécifiques. Les groupes de VLAN basés sur un sous-réseau ne peuvent pas contenir de plages de sous-réseaux qui se chevauchent sur le même port.

Flux de travail

Pour définir un groupe de VLAN basé sur un sous-réseau :

1. Définissez un groupe basé sur un sous-réseau (à l'aide de la page Groupes basés sur un sous-réseau).
2. Pour chaque interface requise, affectez le groupe basé sur un sous-réseau à un VLAN (en utilisant la page Groupes basés sur un sous-réseau au VLAN). Les interfaces ne peuvent pas être affectées à un VLAN dynamique (DVA). En mode IS, le paramètre peut être sauvegardé même si l'appareil n'est pas en mode général, afin d'être activé ultérieurement.

   REMARQUE Si l'interface ne fait pas partie du VLAN, affectez-la manuellement au VLAN à l'aide de la page Port vers VLAN. Sinon, le paramètre Groupes de VLAN basés sur un sous-réseau ne prendra pas effet.
3. Il n'y a aucune limite entre DVA et les groupes basés sur un sous-réseau.

Groupes basés sur un sous-réseau

Pour ajouter un groupe basé sur un sous-réseau :

ÉTAPE 1 Cliquez sur **Gestion des VLAN > Groupes VLAN > Groupes basés sur un sous-réseau**.

ÉTAPE 2 Cliquez sur le bouton **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants :

- **Adresse IP** : saisissez l'adresse IP sur laquelle le sous-groupe est basé.
- **Masque de préfixe** : saisissez le masque de préfixe qui définit le sous-réseau.
- **ID de groupe** : saisissez un ID de groupe.

ÉTAPE 4 Cliquez sur **Appliquer**. Le groupe est ajouté et consigné dans le fichier de Configuration d'exécution.

Groupes basés sur un sous-réseau au VLAN

Pour faire correspondre un groupe de sous-réseaux à un port, le DVA ne doit pas être configuré sur le port (reportez-vous à la section Paramètres d'interface).

Il est possible de lier plusieurs groupes à un même port, chaque port étant associé à son propre VLAN.

Il est également possible de mapper plusieurs groupes à un même VLAN.

Pour mettre en correspondance le groupe de sous-réseaux et un VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Groupes VLAN** > **Groupes basés sur un sous-réseau au VLAN**.

Les mappages actuellement définis s'affichent.

ÉTAPE 2 Pour associer une interface à un groupe basé sur un protocole et au VLAN, cliquez sur **Ajouter**.

Le champ Type de groupe affiche le type de groupe à mettre en correspondance.

ÉTAPE 3 Renseignez les champs suivants.

- **Interface** : numéro du port ou du LAG affecté au VLAN en fonction du groupe basé sur un protocole.
- **ID de groupe** : ID du groupe de protocoles.
- **ID VLAN** : associe le groupe spécifié pour cette interface à un ID de VLAN défini par l'utilisateur.

ÉTAPE 4 Cliquez sur **Appliquer**. Les ports du groupe basé sur un sous-réseau sont mappés à des VLAN et consignés dans le fichier de Configuration d'exécution.

Présentation des groupes de VLAN basés sur un protocole

Des groupes de protocoles peuvent être définis, puis liés à un port. Lorsqu'un groupe de protocoles a été lié à un port, chaque paquet originaire d'un protocole du groupe est affecté au VLAN configuré sur la page Groupes basés sur les protocoles.

Flux de travail

Pour définir un groupe VLAN basé sur protocole :

1. Définissez un groupe de protocoles (à l'aide de la page Groupes basés sur les protocoles).
2. Pour chaque interface requise, affectez le groupe de protocoles à un VLAN (en utilisant la page Groupes basés sur un protocole aux VLAN). Les interfaces doivent être en mode Général et aucun VLAN dynamique (ADV) ne peut leur être affecté.

Groupes basés sur les protocoles

Pour définir un ensemble de protocoles :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Groupes VLAN** > **Groupes basés sur un protocole**.

La page Groupes basés sur les protocoles contient les champs suivants :

- **Encapsulation** : affiche le protocole sur lequel le groupe VLAN est basé.
- **Valeur de protocole (Hex)** : affiche la valeur du protocole sous forme hexadécimale.
- **ID du groupe** : affiche l'ID du groupe de protocoles auquel l'interface est ajoutée.

ÉTAPE 2 Cliquez sur le bouton **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants :

- **Encapsulation** : type de paquet de protocole. Les options suivantes sont disponibles :
  - *Ethernet V2* : si cette option est sélectionnée, sélectionnez le **Type Ethernet**.
  - *LLC-SNAP (rfc1042)* : si cette option est sélectionnée, saisissez la **Valeur de protocole**.
  - *LLC* : si cette option est sélectionnée, sélectionnez les **Valeurs DSAP-SSAP**.
- **Type Ethernet** : sélectionnez le type Ethernet pour l'encapsulation Ethernet V2. Il s'agit du champ à deux octets dans la trame Ethernet utilisé pour indiquer quel protocole est encapsulé dans la charge utile du paquet Ethernet pour le groupe VLAN.
- **Valeur de protocole** : entrez le protocole pour l'encapsulation LLC-SNAP (rfc 1042).
- **ID du groupe** : saisissez un ID de groupe de protocoles.

ÉTAPE 4 Cliquez sur **Appliquer**. Le groupe de protocoles est ajouté et écrit dans le fichier de Configuration d'exécution.

Groupes basés sur un protocole aux VLAN

Pour mapper un groupe de protocoles à un port, ce dernier doit être en mode Général et ne pas posséder d'ADV configuré (voir Paramètres d'interface).

Il est possible de lier plusieurs groupes à un même port, chaque port étant associé à son propre VLAN.

Il est également possible de mapper plusieurs groupes à un même VLAN.

Pour mapper le port de protocole à un VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Groupes VLAN** > **Groupes basés sur un protocole aux VLAN**.

Les mappages actuellement définis s'affichent.

ÉTAPE 2 Pour associer une interface à un groupe basé sur un protocole et au VLAN, cliquez sur **Ajouter**.

Le champ **Type de groupe** affiche le type de groupe à mettre en correspondance.

ÉTAPE 3 Renseignez les champs suivants.

- **Interface** : numéro du port ou du LAG affecté au VLAN en fonction du groupe basé sur un protocole.
- **ID de groupe** : ID du groupe de protocoles.
- **ID VLAN** : associe l'interface à un ID de VLAN défini par l'utilisateur.

ÉTAPE 4 Cliquez sur **Appliquer**. Les ports de protocoles sont mappés à des VLAN et écrits dans le fichier de Configuration d'exécution.

VLAN voix

Dans un LAN, les périphériques vocaux tels que les téléphones IP, les points d'extrémité VoIP et les systèmes vocaux sont placés dans le même VLAN. On appelle ce VLAN un VLAN voix. Si les périphériques vocaux se trouvent dans d'autres VLAN voix, des routeurs IP (couche 3) sont requis pour établir la communication.

Cette section couvre les sujets suivants :

- Présentation du VLAN voix
- Configuration du VLAN voix
- OUI de téléphonie

Présentation du VLAN voix

Cette section couvre les sujets suivants :

- Modes VLAN voix dynamiques
- VLAN voix automatique, Port intelligent automatique, CDP et LLDP
- QoS VLAN voix
- Contraintes du VLAN voix
- Workflows de VLAN voix

Vous trouverez ci-après des exemples de déploiement vocal classiques, accompagnés des configurations appropriées :

- **UC3xx/UC5xx hébergé :** tous les téléphones et points d'extrémité VoIP Cisco prennent en charge ce modèle de déploiement. Pour ce modèle (UC3xx/UC5xx), les téléphones et points d'extrémité VoIP Cisco résident sur le même VLAN voix. Par défaut, le VLAN voix de UC3xx/UC5xx est le VLAN 100.
- **PBX IP tiers hébergé :** les téléphones SBTG CP-79xx et SPA5xx ainsi que les points d'extrémité SPA8800 Cisco prennent en charge ce modèle de déploiement. Dans ce modèle, le VLAN utilisé par les téléphones est déterminé par la configuration réseau. Il peut éventuellement y avoir des VLAN voix et données séparés. Les téléphones et points d'extrémité VoIP s'inscrivent avec un PBX IP sur site.
- **Centrex IP/ITSP hébergé :** les téléphones CP-79xx et SPA5xx ainsi que les points d'extrémité SPA8800 Cisco prennent en charge ce modèle de déploiement. Dans ce modèle, le VLAN utilisé par les téléphones est déterminé par la configuration réseau. Il peut éventuellement y avoir des VLAN voix et données séparés. Les téléphones et points d'extrémité VoIP s'inscrivent sur un proxy SIP hors site dans le cloud.

En ce qui concerne le VLAN, les modèles ci-dessus fonctionnent dans des environnements tenant compte du VLAN et ne tenant pas compte du VLAN. Dans l'environnement tenant compte du VLAN, le VLAN voix fait partie des nombreux VLAN configurés dans une installation. L'exemple ne tenant pas compte du VLAN est équivalent à un environnement tenant compte du VLAN avec un seul VLAN.

Le périphérique fonctionne toujours en tant que commutateur tenant compte du VLAN.

Le périphérique prend en charge un seul VLAN voix. Par défaut, le VLAN voix est VLAN 1. Le VLAN voix est défini par défaut sur VLAN 1. Un autre VLAN voix peut être configuré manuellement. Il peut aussi être appris dynamiquement lorsque la fonction VLAN voix automatique est activée.

Vous pouvez ajouter manuellement des ports au VLAN voix à l'aide de la configuration VLAN de base décrite à la section Configuration des paramètres d'interface VLAN, ou en appliquant manuellement aux ports la macro Port intelligent relative à la voix. Vous avez aussi la possibilité de les ajouter dynamiquement si le périphérique est en mode OUI de téléphonie ou que la fonction Ports intelligents automatiques est activée pour celui-ci.

Modes VLAN voix dynamiques

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

- **OUI de téléphonie**

  En mode OUI de téléphonie, le VLAN voix doit être un VLAN configuré manuellement et ne peut pas être le VLAN par défaut.

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

- **VLAN voix automatique**

  En mode VLAN voix automatique, le VLAN voix peut être le VLAN voix par défaut manuellement configuré ou peut être appris à partir de périphériques externes comme UC3xx/5xx et de commutateurs qui annoncent le VLAN voix dans CDP ou VSDP. VSDP est un protocole défini par Cisco pour la détection des services vocaux.

  À la différence du mode OUI de téléphonie qui détecte les périphériques vocaux basés sur le mode OUI de téléphonie, le mode VLAN voix automatique dépend de la fonction Port intelligent automatique pour ajouter dynamiquement les ports au VLAN voix. Si elle est activée, la fonction Port intelligent automatique ajoute un port au VLAN voix lorsqu'elle détecte sur le port un périphérique en cours d'association qui s'annonce en tant que téléphone ou points d'extrémité de média, par l'intermédiaire de CDP et/ou LLDP-MED.

Points d'extrémité vocaux

Pour qu'un VLAN voix fonctionne correctement, les périphériques vocaux tels que les téléphones et points d'extrémité VoIP Cisco doivent être attribués au VLAN pouvant envoyer et recevoir leur trafic vocal. Voici quelques exemples possibles :

- Un téléphone/point d'extrémité peut être configuré de manière statique avec le VLAN voix.
- Un téléphone/point d'extrémité peut obtenir le VLAN voix dans le fichier d'amorçage qu'il télécharge à partir d'un serveur TFTP. Un serveur DHCP peut spécifier le fichier d'amorçage et le serveur TFTP lorsqu'il attribue une adresse IP au téléphone.
- Un téléphone/point d'extrémité peut obtenir les informations VLAN voix à partir des annonces CDP et LLDP-MED qu'il reçoit de ses systèmes vocaux et commutateurs voisins.

Le périphérique attend des périphériques vocaux en cours de raccordement qu'ils envoient des paquets VLAN balisés. Sur les ports où le VLAN voix est également le VLAN natif, les paquets VLAN voix non balisés sont possibles.

VLAN voix automatique, Port intelligent automatique, CDP et LLDP

Valeurs par défaut

Selon les paramètres par défaut définis en usine, CDP, LLDP, LLDP-MED, le mode Port intelligent automatique et le mode de base de QoS avec DSCP validé sont activés. Tous les ports sont membres du VLAN 1 par défaut, qui est le VLAN voix par défaut.

Déclenchements de VLAN voix

Lorsque le mode VLAN voix dynamique est activé sur VLAN voix automatique, cela signifie que le VLAN voix automatique ne devient opérationnel que si un ou plusieurs déclenchements se produisent. Les déclenchements possibles sont la configuration de VLAN voix statique, la réception d'informations VLAN voix dans une annonce de voisinage CDP et la réception d'informations VLAN voix dans le protocole VSDP (Voice VLAN Discovery Protocol). Si vous le souhaitez, vous pouvez rendre le mode VLAN voix automatique immédiatement opérationnel sans attendre de déclenchement.

Si la fonction Port intelligent automatique est activée en fonction du mode VLAN voix automatique, la fonction Port intelligent automatique est activée lorsque le mode VLAN voix automatique devient opérationnel. Si vous le souhaitez, vous pouvez activer la fonction Port intelligent automatique indépendamment du mode VLAN voix automatique.

REMARQUE La liste de configuration par défaut s'applique ici aux commutateurs dont la version du micrologiciel prend directement en charge le mode VLAN voix automatique. Elle s'applique également aux commutateurs non configurés qui ont été mis à niveau vers la version du micrologiciel prenant en charge le mode VLAN voix automatique.

REMARQUE Les valeurs par défaut et les déclenchements de VLAN voix sont conçus pour n'avoir aucun effet sur les installations ne comportant pas de VLAN voix, ni sur les commutateurs qui ont déjà été configurés. Vous pouvez désactiver et activer manuellement le mode VLAN voix automatique et/ou Port intelligent automatique en fonction de votre déploiement.

VLAN voix automatique

Le mode VLAN voix automatique permet de gérer le VLAN voix, mais dépend de la fonction Port intelligent automatique pour gérer l'appartenance des ports VLAN voix. Le mode VLAN voix automatique offre les fonctions suivantes lorsqu'il est opérationnel :

- Il détecte les informations VLAN voix dans les annonces CDP provenant des périphériques voisins directement connectés.
- Si plusieurs commutateurs et/ou routeurs voisins, tels que des périphériques Cisco Unified Communication (UC), annoncent leur VLAN voix, le VLAN voix du périphérique ayant l'adresse MAC la plus basse est utilisé.

  REMARQUE En cas de connexion du périphérique à un périphérique UC Cisco, vous devrez peut-être configurer le port sur le périphérique UC à l'aide de la commande *`switchport voice vlan`* afin de vous assurer que le périphérique UC annonce son VLAN voix dans CDP sur le port.
- Il synchronise les paramètres VLAN voix avec les autres commutateurs activés pour le mode VLAN voix automatique, par l'intermédiaire du protocole VSDP (Voice Service Discovery Protocol). Le périphérique se configure toujours lui-même avec le VLAN voix provenant de la source de priorité la plus élevée qu'il détecte. La priorité est basée sur le type de source et l'adresse MAC de la source qui fournit les informations de VLAN voix. Les priorités du type de source, de la plus haute à la plus basse, sont la configuration VLAN statique, l'annonce CDP et la configuration par défaut basée sur le VLAN par défaut modifié, ainsi que le VLAN voix par défaut. Une adresse MAC numériquement basse a une priorité plus élevée qu'une adresse MAC numériquement haute.
- Il conserve le VLAN voix jusqu'à ce qu'un nouveau VLAN voix provenant d'une source de priorité plus élevée soit détecté ou jusqu'à ce que le mode VLAN voix automatique soit redémarré par l'utilisateur. Après le redémarrage, le périphérique rétablit le VLAN voix par défaut et relance la détection VLAN voix automatique.

- Lorsqu'un nouveau VLAN voix est configuré ou détecté, le périphérique le crée automatiquement et remplace toutes les appartenances de port du VLAN voix existant par celles du nouveau VLAN voix. Cette opération est susceptible d'interrompre ou de terminer des sessions vocales existantes, notamment lorsque la topologie réseau a été modifiée.

  REMARQUE Le périphérique peut se synchroniser avec des commutateurs basés sur VSDP dans le même VLAN de gestion et, dans les sous-réseaux IP connectés directement, configurés sur le périphérique.

L'option Port intelligent automatique fonctionne avec CDP/LLDP pour gérer les appartenances de port du VLAN voix lorsque des points d'extrémité vocaux sont détectés à partir des ports :

- Lorsque CDP et LLDP sont activés, le périphérique envoie périodiquement des paquets CDP et LLDP pour annoncer au VLAN voix les points d'extrémité vocaux à utiliser.
- Lorsqu'un périphérique en cours d'association à un port s'annonce lui-même en tant que point d'extrémité vocal, par l'intermédiaire de CDP et/ou LLDP, la fonction Port intelligent automatique ajoute automatiquement le port au VLAN voix en appliquant au port la macro Port intelligent correspondante (si aucun autre périphérique provenant du port n'annonce une fonctionnalité conflictuelle ou supérieure). Si un périphérique s'annonce lui-même en tant que téléphone, la macro Port intelligent par défaut est le téléphone. Si un périphérique s'annonce lui-même en tant que téléphone et hôte, ou téléphone et pont, la macro Port intelligent par défaut est le téléphone + bureau.

QoS VLAN voix

Le VLAN voix peut propager les paramètres CoS/802.1p et DSCP à l'aide des stratégies réseau LLDP-MED. Par défaut, le protocole LLDP-MED est défini pour répondre avec le paramètre QoS voix lorsqu'un dispositif envoie des paquets LLDP-MED. Les périphériques prenant en charge MED doivent envoyer leur trafic vocal avec les mêmes valeurs CoS/802.1p et DSCP que celles reçues avec la réponse LLDP-MED.

Vous pouvez désactiver la mise à jour automatique entre le VLAN voix et LLDP-MED, et utiliser vos propres stratégies réseau.

S'il utilise le mode OUI, le périphérique peut en outre configurer le mappage et le re-marquage (CoS/802.1p) du trafic vocal basé sur le OUI.

Par défaut, toutes les interfaces sont approuvées pour CoS/802.1p. Le périphérique applique la qualité de service basée sur la valeur CoS/802.1p qui a été trouvée dans le flux vocal. En mode VLAN voix automatique, vous pouvez remplacer la valeur des flux vocaux par le biais du QoS avancé. Pour les flux vocaux OUI de téléphonie, vous pouvez remplacer la qualité de service et éventuellement re-marquer la valeur 802.1p des flux vocaux en spécifiant les valeurs CoS/802.1p souhaitées et en utilisant l'option de re-marquage sous OUI de téléphonie.

Contraintes du VLAN voix

Les contraintes suivantes doivent être prises en compte :

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

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

- Le VLAN voix ne peut pas être activé pour le mode Port intelligent.
- Le VLAN voix ne peut pas prendre en charge l'affectation dynamique de VLAN (ADV).
- Le VLAN voix ne peut pas être le VLAN invité si le mode VLAN voix est OUI. Si le mode VLAN voix est Automatique, alors le VLAN voix peut être le VLAN invité.
- 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.
- Un nouvel ID VLAN peut être configuré pour le VLAN voix uniquement si le VLAN voix actuel n'a pas de ports candidats.
- L'interface VLAN d'un port candidat doit être en mode Général ou Liaison.
- La QoS du VLAN voix est appliquée aux ports statiques ainsi qu'aux ports candidats qui ont rejoint le VLAN voix.
- Le flux vocal est accepté si l'adresse MAC peut être apprise par la base de données de transfert (FDB, Forwarding Database). (S'il n'existe aucun espace disponible dans la FDB, aucune action ne se produit.)

Workflows de VLAN voix

La configuration par défaut du périphérique sur VLAN voix automatique, Ports intelligents automatiques, CDP et LLDP regroupe la plupart des exemples de déploiement vocal courants. Cette section décrit la façon de déployer un VLAN voix lorsque la configuration par défaut ne peut pas être utilisée.

Flux de travail 1 : pour configurer le VLAN voix automatique :

ÉTAPE 1 Ouvrez la page Propriétés du VLAN voix.

ÉTAPE 2 Sélectionnez l'ID du VLAN voix. Il ne peut pas être défini sur l'ID de VLAN 1 (cette étape n'est pas obligatoire pour le VLAN voix dynamique).

ÉTAPE 3 Sélectionnez **VLAN voix dynamique** pour activer le mode VLAN voix automatique.

ÉTAPE 4 Sélectionnez la méthode **Activation du VLAN voix automatique**.

REMARQUE Si le périphérique est actuellement en mode OUI de téléphonie, vous devez le désactiver pour pouvoir configurer le mode VLAN voix automatique.

ÉTAPE 5 Cliquez sur **Appliquer**.

ÉTAPE 6 Configurez les ports intelligents comme décrit dans la section Tâches courantes de port intelligent.

ÉTAPE 7 Configurez LLDP/CDP comme décrit respectivement dans les sections Détection - LLDP et Détection - CDP.

ÉTAPE 8 Activez la fonction Smartport (Port intelligent) sur les ports appropriés via la page Paramètres d'interface.

REMARQUE Les étapes 7 et 8 sont facultatives, car elles sont activées par défaut.

Flux de travail 2 : pour configurer la méthode OUI de téléphonie :

ÉTAPE 1 Ouvrez la page Gestion des VLAN > VLAN voix > Propriétés. Sélectionnez **VLAN voix dynamique** pour activer le mode OUI de téléphonie.

REMARQUE Si le périphérique est actuellement en mode VLAN voix automatique, vous devez le désactiver pour pouvoir activer le mode OUI de téléphonie.

ÉTAPE 2 Configurez le mode Telephony OUI (OUI de téléphonie) sur la page Table des OUI de téléphonie.

ÉTAPE 3 Configurez l'appartenance VLAN OUI de téléphonie pour les ports sur la page Interface des OUI de téléphonie.

Configuration du VLAN voix

Cette section explique comment configurer le VLAN voix. Elle couvre les sujets suivants :

- Propriétés du VLAN voix
- Paramètres de VLAN voix automatique
- OUI de téléphonie

Propriétés du VLAN voix

Utilisez la page Propriétés du VLAN voix pour effectuer les opérations suivantes :

- Afficher les paramètres de configuration actuels du VLAN voix
- Configurer l'ID de VLAN du VLAN voix
- Configurer les paramètres QoS du VLAN voix
- Configurer le mode VLAN voix (OUI de téléphonie ou VLAN voix automatique)
- Configurer la façon dont le VLAN voix automatique se déclenche

Pour afficher et configurer les propriétés du VLAN voix :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **Propriétés**.

- Les paramètres VLAN voix configurés sur le périphérique s'affichent dans le bloc **Paramètres du VLAN voix (État administratif)**.
- Les paramètres VLAN voix actuellement appliqués au déploiement VLAN voix s'affichent dans le bloc **Paramètres du VLAN voix (État opérationnel)**.

ÉTAPE 2 Renseignez les champs **Administrative Status** (État administratif) suivants :

- **ID VLAN voix** : entrez le VLAN qui sera le VLAN voix.

  REMARQUE Les modifications apportées à l'ID du VLAN voix, CoS/802.1p et/ou DSCP obligent le périphérique à annoncer le VLAN voix administratif en tant que VLAN voix statique. Si l'option *Activation du VLAN voix automatique* déclenchée par le VLAN voix externe est sélectionnée, les valeurs par défaut doivent être conservées.

- **CoS/802.1p** : sélectionnez une valeur CoS/802.1p utilisée par LLDP-MED en tant que stratégie de réseau voix. Pour plus d'informations, reportez-vous à *Administration > Détection > LLDP > Stratégie réseau LLD PMED*.
- **DSCP** : sélection de valeurs DSCP utilisées par LLDP-MED en tant que stratégie de réseau voix. Pour plus d'informations, reportez-vous à *Administration > Détection > LLDP > Stratégie réseau LLD PMED*.

Les champs **Operational Status** (État opérationnel) suivants s'affichent :

- **Voice VLAN ID** (ID VLAN voix) : VLAN voix.
- **CoS/802.1p** : valeur utilisée par LLDP-MED en tant que stratégie de réseau voix. Pour plus d'informations, reportez-vous à *Administration > Détection > LLDP > Stratégie réseau LLD PMED*.
- **DSCP** : valeur utilisée par LLDP-MED en tant que stratégie de réseau voix.

Les champs **Dynamic Voice VLAN Settings** (Paramètres du VLAN voix dynamique) s'affichent :

- **VLAN voix dynamique** : sélectionnez ce champ pour désactiver ou activer la fonction VLAN voix de l'une des manières suivantes :
  - *Activer le VLAN voix automatique* : active le VLAN voix dynamique en mode VLAN voix automatique.
  - *Activer OUI de téléphonie* : active le VLAN voix dynamique en mode OUI de téléphonie.
  - *Désactiver* : désactive le VLAN voix automatique ou le OUI de téléphonie.
- **Activation du VLAN voix automatique** : sélectionnez l'une des options suivantes pour activer le VLAN voix automatique :
  - *Immédiat* : le VLAN voix automatique du périphérique est activé et immédiatement opérationnel.
  - *Par déclenchement du VLAN voix externe* : le VLAN voix automatique du périphérique est activé et opérationnel uniquement si le périphérique détecte un périphérique qui annonce le VLAN voix.

  REMARQUE La reconfiguration manuelle de l'ID de VLAN voix, CoS/802.1p et/ou DSCP à partir de leurs valeurs par défaut génère un VLAN voix statique ayant une priorité plus élevée que le VLAN voix automatique qui a été appris des sources externes.

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

Paramètres de VLAN voix automatique

Si le mode VLAN voix automatique est activé, utilisez la page VLAN voix automatique pour afficher les paramètres globaux et d'interface appropriés.

Vous pouvez aussi utiliser cette page pour redémarrer manuellement le VLAN voix automatique, en cliquant sur **Redémarrer VLAN voix automatique**. Au bout de quelques instants, le système rétablit le VLAN voix par défaut, et relance la détection VLAN voix automatique et le processus de synchronisation sur tous les commutateurs du LAN pour lesquels le mode VLAN voix automatique est activé.

REMARQUE Cette opération rétablit uniquement le VLAN voix par défaut si le type de source est dans l'état *Inactif*.

Pour afficher les paramètres de VLAN voix automatique :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **VLAN voix automatique**.

Le bloc **Operation Status** (État opérationnel) figurant sur cette page affiche les informations sur le VLAN voix actuel et sur sa source :

- **État de VLAN voix automatique** : indique si le VLAN voix automatique est activé.
- **ID du VLAN voix** : identificateur du VLAN voix actuel.
- **Type de source** : affiche le type de source où le VLAN voix a été détecté par le périphérique racine.
- **CoS/802.1p** : affiche les valeurs CoS/802.1p utilisées par LLDP-MED en tant que stratégie de réseau voix.
- **DSCP** : affiche les valeurs DSCP utilisées par LLDP-MED en tant que stratégie de réseau voix.
- **Adresse MAC commutateur racine** : adresse MAC du périphérique racine VLAN voix automatique qui détecte ou est configuré avec le VLAN voix à partir duquel le VLAN voix est appris.
- **Adresse MAC du commutateur** : adresse MAC de base du périphérique. Si l'adresse MAC du commutateur du périphérique est l'adresse MAC du commutateur racine, le périphérique est le périphérique racine VLAN voix automatique.
- **Heure de changement de l'ID VLAN voix** : heure de la dernière mise à jour du VLAN voix.

ÉTAPE 2 Cliquez sur **Redémarrer VLAN voix automatique** pour rétablir le VLAN voix par défaut et relancer la détection VLAN voix automatique sur tous les commutateurs du LAN pour lesquels la fonction VLAN voix automatique est activée.

Le paramètre **Voice VLAN Local Source Table** (Table de source locale VLAN voix) affiche le VLAN voix configuré sur le périphérique, ainsi que toute configuration VLAN voix annoncée par des périphériques voisins à connexion directe. Elle contient les champs suivants :

- **Interface** : affiche l'interface sur laquelle la configuration VLAN voix a été reçue ou configurée. Si S/O est affiché, cela signifie que la configuration a été effectuée sur le périphérique lui-même. Si une interface est affichée, cela signifie qu'une configuration de voix a été reçue d'un voisin.
- **Adresse MAC source** : adresse MAC de l'UC de provenance de la configuration de voix.

- **Type de source** : type d'UC de provenance de la configuration de voix. Les options suivantes sont disponibles :
  - *Par défaut* : configuration VLAN voix par défaut sur le périphérique.
  - *Statique* : configuration VLAN voix définie par l'utilisateur programmée sur le périphérique.
  - *CDP* : indique que l'UC qui a annoncé la configuration VLAN voix exécute CDP.
  - *LLDP* : indique que l'UC qui a annoncé la configuration VLAN voix exécute LLDP.
  - *ID du VLAN voix* : identificateur du VLAN voix annoncé ou configuré.
- **ID du VLAN voix** : identificateur du VLAN voix actuel.
- **CoS/802.1p** : valeurs CoS/802.1p annoncées ou configurées qui sont utilisées par LLDP-MED en tant que stratégie de réseau voix.
- **DSCP** : valeurs DSCP annoncées ou configurées qui sont utilisées par LLDP-MED en tant que stratégie réseau de voix.
- **Meilleure source locale** : indique si ce VLAN voix a été utilisé par le périphérique. Les options suivantes sont disponibles :
  - *Oui* : le périphérique utilise ce VLAN voix pour se synchroniser avec les autres commutateurs pour lesquels la fonction VLAN voix automatique est activée. Ce VLAN voix est celui utilisé pour le réseau, sauf si un VLAN voix provenant d'une source de priorité plus élevée est détecté. Une seule source locale peut être la meilleure source locale.
  - *Non* : il ne s'agit pas de la meilleure source locale.

ÉTAPE 3 Cliquez sur **Actualiser** pour actualiser les informations figurant sur la page.

OUI de téléphonie

Les OUI (Organizationally Unique Identifiers) sont attribués par l'autorité d'enregistrement intégrée IEEE (Institute of Electrical and Electronics Engineers). Étant donné que le numéro des fabricants de téléphones IP est limité et connu, les valeurs d'OUI connues entraînent l'affectation automatique au VLAN voix des trames concernées et du port sur lequel elles sont détectées.

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

Cette section couvre les sujets suivants :

- Table des OUI de téléphonie
- Interface des OUI de téléphonie

Table des OUI de téléphonie

Utilisez la page OUI de téléphonie pour configurer les propriétés QoS des OUI de téléphonie. Vous pouvez également configurer le Délai d'expiration d'appartenance automatique. Si la période expire sans aucune activité téléphonique, le port est supprimé du VLAN voix.

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

Pour configurer les OUI de téléphonie et/ou ajouter un nouveau OUI de VLAN voix :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **OUI de téléphonie**.

La page OUI de téléphonie contient les champs suivants :

- **État opérationnel OUI de téléphonie** : indique si les OUI sont utilisés pour identifier le trafic vocal.
- **CoS/802.1p** : sélectionnez la file d'attente CoS à attribuer au trafic vocal.
- **Remarquer CoS/802.1p** : sélectionnez cette option pour remarquer le trafic sortant.
- **Délai d'expiration d'appartenance automatique** : entrez le délai à l'issue duquel supprimer un port du VLAN voix une fois que toutes les adresses MAC des téléphones détectés sur les ports ont expiré.

ÉTAPE 2 Cliquez sur **Appliquer** pour intégrer ces valeurs à la Configuration d'exécution du périphérique.

La Table des OUI de téléphonie s'affiche :

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

ÉTAPE 3 Cliquez sur **Restaurer les OUI par défaut** pour supprimer tous les OUI créés par l'utilisateur et conserver uniquement les OUI par défaut dans la table. Les informations OUI risquent d'être inexactes tant que la restauration n'est pas terminée. Cette opération peut prendre plusieurs secondes. Au bout de quelques secondes, actualisez la page en la quittant et y accédant à nouveau.

Pour supprimer tous les OUI, cochez la case du haut. Tous les OUI sont sélectionnés et peuvent être supprimés en cliquant sur **Supprimer**. Si vous cliquez ensuite sur **Restaurer les OUI par défaut**, le système récupère les OUI connus.

ÉTAPE 4 Pour ajouter un nouveau OUI, cliquez sur **Ajouter**.

ÉTAPE 5 Entrez les valeurs des champs suivants :

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

ÉTAPE 6 Cliquez sur **Appliquer**. Le OUI est ajouté à la Table des OUI de téléphonie.

Interface des OUI de téléphonie

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

- **Tout** : les valeurs de qualité de service (QoS) configurées sur le VLAN voix sont appliquées à toutes les trames entrantes reçues sur l'interface et catégorisées comme VLAN voix.
- **Adresse MAC source de téléphonie** : les valeurs de QoS configurées pour le VLAN voix sont appliquées à toute trame entrante catégorisée comme VLAN voix et contenant un OUI dans l'adresse MAC source qui correspond à un OUI de téléphonie configuré.

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

Pour configurer le mode OUI de téléphonie sur une interface :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **Interface des OUI de téléphonie**.

La page Interface des OUI de téléphonie contient les paramètres OUI du VLAN voix pour toutes les interfaces.

ÉTAPE 2 Pour configurer une interface en tant que port candidat du VLAN voix basé sur les OUI de téléphonie, cliquez sur **Modifier**.

ÉTAPE 3 Entrez les valeurs des champs suivants :

- **Interface** : sélectionnez une interface.
- **Adhésion VLAN OUI de téléphonie** : si cette option est activée, l'interface est un port candidat du VLAN voix basé sur les OUI de téléphonie. Lorsque des paquets correspondant à l'un des OUI de téléphonie configurés sont reçus, le port est ajouté au VLAN voix.

- **Mode de QoS VLAN voix (Mode de QoS OUI de téléphonie** sur la page principale**)** : sélectionnez l'une des options suivantes :
  - *Tous* : les attributs QoS sont appliqués à tous les paquets catégorisés comme VLAN voix.
  - *Adresse MAC source de téléphonie* : les attributs QoS sont uniquement appliqués aux paquets provenant de téléphones IP.

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

Accès VLAN TV port de multidestination

Les VLAN TV de multidiffusion permettent les transmissions de multidiffusion vers les abonnés qui ne se trouvent pas sur le même VLAN données (couche 2 isolée), sans réplication des trames de transmission de multidiffusion pour chaque VLAN d'abonné.

Les abonnés qui ne se trouvent pas sur le même VLAN de données (couche 2 isolée) et qui sont connectés au périphérique à l'aide d'un ID de VLAN différent peuvent partager le même flux de multidiffusion en joignant les ports sur le même ID de VLAN de multidiffusion.

Le port réseau, connecté au serveur de multidiffusion, est configuré statiquement en tant que membre dans l'ID de VLAN de multidiffusion.

Les ports réseau, par le biais desquels les abonnés communiquent avec le serveur de multidiffusion (grâce à l'envoi de messages IGMP), reçoivent les flux de multidiffusion à partir du serveur de multidiffusion, tout en incluant le VLAN TV de multidiffusion dans l'en-tête de paquet de multidiffusion. Pour ces raisons, les ports réseau doivent être configurés de manière statique, comme suit :

- Type de port Liaison ou Général (voir Paramètres d'interface)
- Membre du VLAN TV multidiffusion

Les ports récepteurs de l'abonné ne peuvent être associés au VLAN TV multidiffusion que s'ils sont définis en tant que ports d'accès :

Il est possible d'associer un ou plusieurs groupes d'adresses de multidiffusion IP au même VLAN TV de multidiffusion.

Tout VLAN peut être configuré en tant que VLAN TV de multidiffusion. Un port affecté à un VLAN TV de multidiffusion :

- Rejoint le VLAN TV de multidiffusion.
- Les paquets traversant les ports de sortie dans le VLAN TV de multidiffusion ne sont pas balisés.
- Le paramètre Type de trame du port est défini sur **Tout admettre**, autorisant ainsi les paquets non balisés (voir Paramètres d'interface).

La configuration du VLAN TV de multidiffusion est définie pour chaque port. Les ports client sont configurés pour être membres des VLAN TV multidiffusion à l'aide de la page **Appartenance VLAN du port multidiffusion**.

Surveillance IGMP

Un VLAN TV multidiffusion s'appuie sur la surveillance IGMP, configurée sur le port :

- Les abonnés utilisent des messages IGMP pour rejoindre ou quitter un groupe de multidiffusion.
- Le périphérique effectue la surveillance IGMP et configure le port d'accès conformément à son appartenance de multidiffusion sur le VLAN TV de multidiffusion.

Pour chaque paquet IGMP reçu sur un port d'accès, le périphérique décide de l'associer au VLAN d'accès ou au VLAN TV de multidiffusion, conformément aux règles suivantes :

- Si un message IGMP est reçu sur un port d'accès, avec l'adresse IP de multidiffusion de destination associée au VLAN TV de multidiffusion du port, le logiciel associe le paquet IGMP au VLAN TV de multidiffusion.
- Sinon, le message IGMP est associé au VLAN d'accès et transmis uniquement au sein de ce VLAN.
- Le message IGMP est abandonné si :
  - L'état STP/RSTP sur le port d'accès est **Abandonner**.
  - L'état MSTP du VLAN d'accès est **Abandonner**.
  - L'état MSTP du VLAN TV de multidiffusion est **Abandonner** et le message IGMP est associé à ce VLAN TV de multidiffusion.

Différences entre VLAN standard et VLAN TV de multidiffusion

Tableau 1 Caractéristiques des VLAN normaux et des VLAN TV de multidiffusion

	VLAN standard	VLAN TV multidestination
Appartenance VLAN	La source et tous les ports récepteurs doivent être des membres statiques du même VLAN données.	La source et les ports récepteurs ne peuvent pas être membres du même VLAN données.
Enregistrement de groupes	L'enregistrement des groupes de multidiffusion est dynamique.	Les groupes doivent être associés à un VLAN de multidiffusion de manière statique, mais l'enregistrement réel de la station est dynamique.
Ports récepteurs	Un VLAN peut être utilisé à la fois pour l'envoi et la réception de trafic (aussi bien multidiffusion que monodiffusion).	Un VLAN de multidiffusion ne peut être utilisé que pour la réception de trafic par les stations sur le port (multidiffusion uniquement).
Sécurité et isolation	Les récepteurs du même flux de multidiffusion se trouvent sur le même VLAN données et peuvent communiquer entre eux.	Les récepteurs du même flux de multidiffusion se trouvent sur des VLAN d'accès différents et sont isolés les uns des autres.

Configuration

Configurez un VLAN TV selon les étapes suivantes :

1. Définissez un VLAN TV en associant un ou plusieurs groupes de multidiffusion, ou des plages de groupes, à un VLAN (à l'aide de la page Groupe de multidiffusion aux VLAN).
2. Spécifiez les ports d'accès dans chaque VLAN de multidiffusion (à l'aide de la page Appartenance VLAN du port multidiffusion).

Groupe de multidiffusion aux VLAN

Vous pouvez ajouter un maximum de 256 plages d'adresses IPv4 à un VLAN TV multidiffusion. Dans chacune d'elles, vous pouvez configurer toute l'étendue des adresses de multidiffusion.

Pour définir la configuration d'un VLAN TV de multidiffusion :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Accès VLAN TV port multidiffusion > Groupe de multidestination aux VLAN**.

Les champs suivants s'affichent :

- **VLAN TV de multidiffusion** : VLAN auquel les paquets de multidiffusion sont affectés.
- **Début du groupe de multidiffusion** : première adresse IPv4 du groupe de multidestination.
- **Fin du groupe** : dernière adresse IPv4 de la plage de groupes de multidiffusion.
- **Taille du groupe** : nombre d'adresses dans la première plage de groupes de multidiffusion.

ÉTAPE 2 Cliquez sur **Ajouter** pour associer un groupe de multidiffusion à un VLAN. Vous pouvez sélectionner n'importe quel VLAN.

Renseignez les champs suivants :

- **VLAN TV de multidiffusion** : VLAN auquel les paquets de multidiffusion sont affectés. Un VLAN sélectionné ici devient un VLAN TV multidiffusion.
- **Début du groupe de multidestination** : première adresse IPv4 de la plage de groupes de multidestination.
- **Définition du groupe** : sélectionnez l'une des options de plage suivantes :
  - *Par taille de groupe* : indiquez le nombre d'adresses de multidiffusion dans la plage de groupes.
  - *Par plage* : indiquez une adresse de multidiffusion IPv4 supérieure à celle qui figure dans le champ **Début du groupe de multidiffusion**. Il s'agira de la dernière adresse de la plage.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres VLAN TV de multidiffusion sont modifiés et écrits dans le fichier de Configuration d'exécution.

Appartenance VLAN du port multidiffusion

Pour définir la configuration d'un VLAN TV de multidiffusion :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Accès VLAN TV port multidiffusion > Appartenance VLAN du port multidiffusion**.

ÉTAPE 2 Sélectionnez un VLAN dans **VLAN TV de multidiffusion**.

ÉTAPE 3 Sélectionnez une interface dans **Type d'interface**.

ÉTAPE 4 La liste **Ports d'accès candidats** contient tous les ports d'accès configurés sur le périphérique. Déplacez les ports requis vers le champ **Ports d'accès membres**.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres VLAN TV de multidiffusion sont modifiés et écrits dans le fichier de Configuration d'exécution.

VLAN TV port client multidiffusion

Un service triple play offre trois services de connexion haut débit sur une seule connexion haut débit :

- Accès Internet haut débit
- Vidéo
- Voice (voix)

Le service triple play est offert aux abonnés au fournisseur de services, tout en maintenant une isolation de type couche 2 entre eux.

Chaque abonné possède une boîte CPE MUX. Le MUX possède plusieurs ports d'accès connectés aux périphériques de l'abonné (PC, téléphone, etc.) ainsi qu'un port réseau connecté au périphérique d'accès.

La boîte transfère les paquets depuis le port réseau vers les périphériques de l'abonné, sur la base de la balise VLAN du paquet. Chaque VLAN est mappé à l'un des ports d'accès du MUX.

Les paquets issus des abonnés vers le réseau du fournisseur de services sont transférés en guise de trames VLAN balisées, afin de distinguer les différents types de services, ce qui signifie qu'il y a un ID de VLAN unique dans la boîte CPE pour chaque type de service.

Tous les paquets allant de l'abonné au réseau du fournisseur de services sont encapsulés par le périphérique d'accès avec le VLAN de l'abonné configuré en tant que VLAN client (balise externe ou S-VID), à l'exception des messages de surveillance IGMP issus des récepteurs TV, qui sont associés au VLAN TV de multidiffusion. Les informations de vidéo à la demande (VOD) qui sont également issues des récepteurs TV sont envoyées comme tout autre type de trafic.

Les paquets issus du réseau du fournisseur de services qui sont reçus sur le port réseau de l'abonné sont envoyés sur le réseau du fournisseur de services en tant que paquets à double balise, la balise externe (balise de service ou S-Tag) représentant l'un des deux types de VLAN comme suit :

- VLAN d'abonné (y compris Internet et téléphones IP)
- VLAN TV multidestination

Le VLAN interne (C-Tag) est la balise qui détermine la destination dans le réseau de l'abonné (via la boîte CPE MUX).

Flux de travail

1. Configurez un port d'accès en tant que port client (à l'aide de la page Paramètres d'interface). Pour plus d'informations, reportez-vous à la section QinQ.
2. Configurez le port réseau en tant que port Liaison ou Général avec abonné et VLAN TV de multidiffusion en guise de VLAN balisés (à l'aide de la page Paramètres d'interface).
3. Créez un VLAN TV de multidiffusion comportant jusqu'à 4094 VLAN différents. (La création de VLAN s'effectue par le biais de la configuration de la gestion des VLAN standard.)
4. Associez le port client à un VLAN TV de multidiffusion à l'aide de la page Appartenance VLAN du port multidiffusion.
5. Mappez le VLAN CPE (C-TAG) au VLAN TV de multidiffusion (S-Tag) à l'aide de la page VLAN CPE à VLAN.

VLAN CPE à VLAN

Pour assurer la prise en charge de la boîte CPE MUX auprès des VLAN d'abonné, il se peut que les abonnés aient besoin de plusieurs fournisseurs vidéo, chaque fournisseur étant affecté à un VLAN externe différent.

Les VLAN CPE de multidiffusion (internes) doivent être mappés aux VLAN (externes) des fournisseurs de multidiffusion.

Lorsqu'un VLAN CPE est mappé à un VLAN de multidiffusion, il peut participer à la surveillance IGMP.

Pour mapper des VLAN CPE :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN TV port client multidiffusion > VLAN CPE à VLAN**.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants :

- **VLAN CPE** : saisissez le VLAN défini sur la boîte CPE.
- **VLAN TV de multidiffusion** : sélectionnez le VLAN TV de multidiffusion qui est mappé au VLAN CPE.

ÉTAPE 4 Cliquez sur **Appliquer**. Le mappage de VLAN CPE est modifié et écrit dans le fichier de Configuration d'exécution.

Appartenance VLAN du port multidiffusion

Les ports associés aux VLAN de multidiffusion doivent être configurés en tant que ports clients (voir Paramètres d'interface).

Pour mapper des ports aux VLAN TV de multidiffusion :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN TV port client multidiffusion > Appartenance VLAN du port multidiffusion**.

ÉTAPE 2 Sélectionnez un VLAN dans **VLAN TV de multidiffusion**.

ÉTAPE 3 Sélectionnez une interface dans **Type d'interface**.

ÉTAPE 4 La liste **Ports client candidats** contient tous les ports d'accès configurés sur le périphérique. Déplacez les ports requis vers le champ **Ports client membres**.

ÉTAPE 5 Cliquez sur **Appliquer**. Les nouveaux paramètres sont modifiés et écrits dans le fichier de configuration d'exécution.

13

Arbre recouvrant

Cette section décrit le protocole STP (Spanning Tree Protocol) (IEEE802.1D et IEEE802.1Q) et couvre les rubriques suivantes :

- Types de STP
- État STP et paramètres globaux
- Paramètres d'interface STP
- Paramètres d'interface RSTP
- Présentation du protocole MST (Multiple Spanning Tree)
- Propriétés MSTP
- VLAN vers instance MSTP
- Paramètres d'instance MSTP
- Paramètres d'interface MSTP

Types de STP

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

Des boucles se produisent lorsque des chemins alternatifs existent entre les hôtes. Les boucles peuvent utiliser des commutateurs pour relayer les mêmes paquets indéfiniment, ce qui peut empêcher les paquets d'arriver à leur destination, mais également entraîner des tempêtes de diffusion/multidiffusion et réduire l'efficacité du réseau.

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

Le périphérique prend en charge les versions de protocole STP suivantes :

- Le STP classique fournit un chemin d'accès unique entre deux stations d'arrivée afin d'empêcher et d'éliminer les boucles.
- Le STP rapide (RSTP) détecte les topologies de réseau afin de fournir une convergence du Spanning Tree plus rapide. Ce protocole est plus efficace lorsque la topologie du réseau est naturellement structurée en arborescence et permet une convergence plus rapide. RSTP est activé par défaut.
- STP multiple (MSTP) : MSTP est basé sur RSTP. Il détecte les boucles de couche 2 (Layer 2) et tente de les réduire en empêchant le port impliqué de transférer le trafic. Étant donné que les boucles existent au niveau d'un domaine de couche 2, il peut arriver qu'un port soit bloqué pour éliminer une boucle STP. Le trafic est transféré vers le port qui n'est pas bloqué et le port bloqué ne reçoit aucun trafic. Ce protocole ne permet pas d'utiliser la bande passante de manière efficace, car le port bloqué reste inutilisé.
- MSTP résout ce problème en activant plusieurs instances STP afin de détecter et de réduire séparément les boucles pour chaque instance. Il est donc possible de bloquer un port pour une ou plusieurs instances STP, mais de le laisser actif pour d'autres instances STP. Si différents VLAN sont associés à différentes instances STP, leur trafic est relayé en fonction de l'état du port STP de leurs instances MST associées. Cela permet de mieux utiliser la bande passante.

État STP et paramètres globaux

La page État STP et paramètres globaux contient les paramètres permettant d'activer STP, RSTP ou MSTP.

Utilisez respectivement la page Paramètres d'interface STP, Paramètres d'interface RSTP et Propriétés MSTP pour configurer chaque mode.

Pour définir l'état et les paramètres globaux STP :

ÉTAPE 1 Cliquez sur **Arbre recouvrant** > **État STP et paramètres globaux**.

ÉTAPE 2 Saisissez les paramètres.

Paramètres globaux :

- **État Spanning Tree** : sélectionnez cette option pour l'activer sur le périphérique.
- **Protection de bouclage STP** : sélectionnez cette option pour activer la protection de bouclage sur le périphérique.

- **Mode de fonctionnement STP** : sélectionnez un mode STP.
- **Gestion BPDU** : définissez la façon dont les paquets BPDU sont gérés lorsque le protocole STP est désactivé sur le port ou le périphérique. Les BPDU servent à transmettre des informations du protocole STP.
  - *Filtrage* : filtre les paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
  - *Inondation* : inonde de paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
- **Valeurs par défaut du coût de chemin** : sélectionne la méthode utilisée pour assigner des coûts de chemin par défaut aux ports STP. Le coût de chemin par défaut assigné à une interface varie selon la méthode sélectionnée.
  - *Court* : spécifie la plage de 1 à 65 535 pour les coûts de chemin des ports.
  - *Long* : spécifie la plage de 1 à 200 000 000 pour les coûts de chemin des ports.

Paramètres des ponts :

- **Priorité** : définit la valeur de priorité du pont. Après l'échange de BPDU, le périphérique de priorité moindre devient le pont racine. Si tous les ponts utilisent la même priorité, leurs adresses MAC sont alors utilisées pour déterminer le pont racine. La valeur de priorité du pont est fournie par incréments de 4096. Par exemple, 4096, 8192, 12288, etc.
- **Délai Hello** : définissez le temps d'attente en secondes d'un pont racine entre deux messages de configuration.
- **Âge maximum** : définissez la durée d'attente maximale (en secondes) du périphérique avant qu'il ne tente de redéfinir sa propre configuration lorsqu'il ne reçoit pas de message de configuration.
- **Délai de transfert** : définissez la durée en secondes pendant laquelle le pont reste en mode d'apprentissage avant de transférer des paquets. Pour plus d’informations, reportez-vous à la section Paramètres d'interface STP.

Racine désignée :

- **ID du pont** : priorité du pont concaténée avec l'adresse MAC du périphérique.
- **ID du pont racine** : priorité du pont racine concaténée avec l'adresse MAC du pont racine.
- **Port racine** : port offrant le chemin de moindre coût entre ce pont et le pont racine. (Cette information est importante lorsque le pont n'est pas le pont racine.)

- **Coût du chemin racine** : coût du chemin entre ce pont et la racine.
- **Topology Changes Counts** : nombre total des changements de topologie STP effectués.
- **Dernier changement de topologie** : temps écoulé depuis le dernier changement de topologie. Cette durée s'affiche au format jours/heures/minutes/secondes.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres globaux STP sont écrits dans le fichier de Configuration d'exécution.

Paramètres d'interface STP

La page Paramètres d'interface STP vous permet de configurer le protocole STP port par port et d'afficher les informations apprises par le protocole, comme le pont désigné.

La configuration définie est valide pour toutes les variantes du protocole STP.

Pour configurer STP sur une interface :

ÉTAPE 1 Cliquez sur **Arbre recouvrant** > **Paramètres d'interface STP**.

Les interfaces s'affichent. Les champs sont décrits sur la page Modifier, à l'exception du champ suivant qui est uniquement affiché sur cette page :

- **Rôle du port** : affiche le rôle du port ou du LAG, par port ou LAG par instance, affecté par l'algorithme MSTP afin de fournir le chemin STP.
  - *Racine* : le transfert des paquets via cette interface fournit le chemin de moindre coût pour transférer les paquets vers le périphérique racine.
  - *Désigné* : interface via laquelle le pont est connecté au LAN et qui fournit le chemin de moindre coût du LAN au pont racine pour l'instance MST.
  - *Autre* : l'interface fournit un chemin alternatif de l'interface racine au périphérique racine.
  - *Sauvegarde* : l'interface fournit un chemin de secours pour le chemin du port désigné vers les nœuds terminaux du Spanning Tree. Des ports de secours existent lorsque deux ports sont reliés dans une boucle par un lien point à point. Des ports de secours apparaissent également lorsqu'un LAN possède deux ou plusieurs connexions établies à un segment partagé.

- *Désactivé* : l'interface ne participe pas à l'arbre recouvrant.
- *Limite* : le port sur cette instance est un port frontière. Il hérite de son état de l'instance 0 et peut être affiché sur la page Paramètres d'interface STP.

ÉTAPE 2 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez le port ou le LAG sur lequel Spanning Tree est configuré.
- **STP** : active ou désactive STP sur le port.
- **Port de bordure** : active ou désactive Fast Link sur le port. Si le mode Fast Link est activé pour un port, le port est automatiquement placé en mode Transfert lorsque le lien du port est actif. Fast Link optimise la convergence du protocole STP. Les options sont les suivantes :
  - *Activer* : active immédiatement Fast Link.
  - *Auto* : active Fast Link quelques secondes après l'activation de l'interface. Ceci permet à STP de résoudre les problèmes de boucles avant d'activer Fast Link.
  - *Désactiver* : désactive Fast Link.

  REMARQUE Il est recommandé de définir la valeur sur Auto afin que le périphérique place le port en mode Fast Link lorsqu'un hôte y est connecté, ou qu'il le définisse comme étant un port STP normal lorsqu'il est connecté à un autre périphérique. Cela permet d'éviter les boucles.

  Le port de périphérie n'est pas opérationnel en mode MSTP.
- **Protection racine** : active ou désactive la protection racine sur le périphérique. L'option de protection racine offre un moyen d'appliquer le placement du pont racine au sein du réseau.

  La protection racine permet de garantir que le port sur lequel cette fonction est activée est le port désigné. Normalement, tous les ports du pont racine sont des ports désignés, sauf si deux ou plusieurs ports du pont racine sont connectés. Si le pont reçoit des BPDU supérieurs sur un port sur lequel la protection racine est activée, celle-ci place ce port dans un état STP incohérent pour la racine. Cet état incohérent pour la racine est en fait équivalent à un état d'écoute. Aucun trafic n'est acheminé par ce port. De cette manière, la protection racine applique la position du pont racine.

- **Protection BPDU** : active ou désactive la fonction de protection BPDU (Bridge Protocol Data Unit) sur le port.

  La protection BPDU permet d'appliquer les frontières du domaine STP et de maintenir la topologie active prévisible. Les périphériques situés derrière les ports pour lesquels la protection BPDU est activée ne peuvent pas influencer la topologie STP. Lors de la réception de BPDU, l'opération de protection BPDU désactive le port pour lequel la protection BPDU est configurée. Dans ce cas, un message BPDU est reçu et une interception SNMP est générée.

- **Gestion BPDU** : définissez la façon dont les paquets BPDU sont gérés lorsque le protocole STP est désactivé sur le port ou le périphérique. Les BPDU servent à transmettre des informations du protocole STP.

  - *Use Global Settings* (Utiliser les paramètres globaux) : sélectionnez cette option pour utiliser les paramètres définis sur la page État STP et paramètres globaux.
  - *Filtrage* : filtre les paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
  - *Inondation* : inonde de paquets BPDU lorsque Spanning Tree est désactivé sur une interface.

- **Coût d'acheminement** : définissez la contribution du port au coût du chemin racine ou utilisez le coût par défaut généré par le système.

- **Priorité** : définissez la valeur de priorité du port. La valeur de priorité influence le choix du port lorsqu'un pont dispose de deux ports connectés au sein d'une boucle. La priorité est une valeur comprise entre 0 et 240 ; il doit s'agir d'un multiple de 16.

- **État du port** : affiche l'état STP actuel d'un port.

  - *Désactivé* : le protocole STP est actuellement désactivé sur le port. Le port transfère le trafic tout en apprenant les adresses MAC.
  - *Blocage* : le port est actuellement bloqué et ne peut ni transférer le trafic (à l'exception des données BPDU) ni apprendre les adresses MAC.
  - *Écoute* : le port est en mode Écoute. Il ne peut ni transférer le trafic ni connaître les adresses MAC.
  - *Apprentissage* : le port est en mode Apprentissage. Il ne peut pas transférer le trafic mais il peut prendre connaissance de nouvelles adresses MAC.
  - *Transfert* : le port est en mode Transfert. Il peut réacheminer du trafic et apprendre de nouvelles adresses MAC.

- **ID du pont désigné** : affiche la priorité du pont et l'adresse MAC du pont désigné.

- **ID du port désigné** : affiche la priorité et l'interface du port sélectionné.

- **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.
- **Transitions de transfert** : affiche le nombre de fois où le port est passé de l'état **Blocage** à l'état **Transfert**.
- **Vitesse** : affiche la vitesse du port.
- **LAG** : affiche le LAG auquel appartient le port. Si un port est membre d'un LAG, les paramètres du LAG remplacent ceux du port.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres d'interface sont écrits dans le fichier de Configuration d'exécution.

Paramètres d'interface RSTP

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

La page Paramètres d'interface RSTP vous permet de configurer le protocole RSTP par port. Toute configuration effectuée sur cette page est active lorsque le mode STP global est défini sur RSTP ou MSTP.

Pour entrer les paramètres RSTP :

ÉTAPE 1 Cliquez sur **Arbre recouvrant** > **État STP et paramètres globaux**.

ÉTAPE 2 Activez **RSTP**.

ÉTAPE 3 Cliquez sur **Arbre recouvrant** > **Paramètres d'interface RSTP**. La page Paramètres d'interface RSTP s'ouvre.

ÉTAPE 4 Sélectionnez un port.

REMARQUE Activer la migration des protocoles est uniquement disponible après avoir sélectionné le port connecté au pont associé en cours de test.

ÉTAPE 5 Si un partenaire de lien est détecté via STP, cliquez sur **Activer la migration des protocoles** pour effectuer un test de migration des protocoles. Cette opération détecte si le lien associé utilisant STP existe toujours et s'il a migré ou non vers RSTP ou MSTP. S'il existe toujours en tant que lien STP, le périphérique continue de communiquer avec lui via STP. Sinon, s'il a migré vers RSTP ou MSTP, il communique avec lui respectivement via RSTP ou MSTP.

ÉTAPE 6 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 7 Configurez les paramètres suivants :

- **Interface** : définissez l'interface et précisez le port ou LAG où RSTP doit être configuré.
- **État administratif point à point** : définissez l'état de la liaison point à point. Les ports définis en tant que Full Duplex sont considérés comme liens de port point à point.
  - *Activé* : ce port devient un port de bordure RSTP lorsque cette option est activée et il est placé rapidement en mode Transfert (généralement en 2 secondes).
  - *Désactivé* : le port n'est pas considéré comme port point à point pour le protocole RSTP ; par conséquent, STP fonctionne sur ce port à vitesse normale et non à haute vitesse.
  - *Automatique* : détermine automatiquement l'état du périphérique en utilisant les unités BPDU RSTP.
- **État opérationnel point à point** : affiche l'état opérationnel point à point si l'**État administratif point à point** est défini sur Auto.
- **Rôle** : affiche le rôle du port qui a été assigné par STP pour fournir des chemins STP. Les rôles possibles sont :
  - *Racine* : chemin de moindre coût pour transférer des paquets vers le pont racine.
  - *Désigné* : interface via laquelle le pont est connecté au LAN et qui fournit le chemin de moindre coût du LAN au pont racine.
  - *Alternate* (Alternatif) : fournit un chemin alternatif de l'interface racine au port racine.
  - *Sauvegarde* : fournit un chemin de secours pour le chemin du port désigné vers les nœuds terminaux STP. Cela fournit une configuration dans laquelle deux ports sont reliés dans une boucle par un lien point à point. Des ports de secours sont également utilisés lorsqu'un LAN possède deux ou plusieurs connexions établies à un segment partagé.
  - *Désactivé* : le port ne participe pas au Spanning Tree.
- **Mode** : affiche le mode Spanning Tree actuel : RSTP ou STP classique.
- **État opérationnel Fast Link** : indique si Fast Link (port de bordure) est activé, désactivé ou automatique pour l'interface. Les valeurs disponibles sont les suivantes :
  - *Activé* : Fast Link est activé.
  - *Désactivé* : Fast Link est désactivé.
  - *Auto* : Fast Link s'active quelques secondes après l'activation de l'interface.

- **État du port** : affiche l'état RSTP sur le port spécifique.
  - *Désactivé* : le protocole STP est actuellement désactivé sur le port.
  - *Blocage* : le port est actuellement bloqué et ne peut ni transférer le trafic ni apprendre les adresses MAC.
  - *Écoute* : le port est en mode Écoute. Il ne peut ni transférer le trafic ni connaître les adresses MAC.
  - *Apprentissage* : le port est en mode Apprentissage. Il ne peut pas transférer le trafic mais il peut prendre connaissance des nouvelles adresses MAC.
  - *Transfert* : le port est en mode Transfert. Il peut réacheminer du trafic et apprendre de nouvelles adresses MAC.

ÉTAPE 8 Cliquez sur **Appliquer**. Le fichier de configuration d'exécution est mis à jour.

Présentation du protocole MST (Multiple Spanning Tree)

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. La page Propriétés MSTP permet de définir les paramètres MSTP globaux.

Pour configurer MSTP :

ÉTAPE 1 Définissez le mode de fonctionnement STP sur MSTP, comme décrit à la page État STP et paramètres globaux .

ÉTAPE 2 Définissez les instances MSTP. Chaque instance MSTP calcule et établit une topologie sans boucles pour transmettre les paquets à partir des VLAN qui mappent à l'instance. Reportez-vous à la section VLAN vers instance MSTP.

ÉTAPE 3 Décidez quelle instance MSTP est active dans quel VLAN et associez ces instances MSTP aux VLAN en conséquence.

ÉTAPE 4 Pour configurer les attributs MSTP :

- *Propriétés MSTP*
- Paramètres d'instance MSTP
- *VLAN vers instance MSTP*

Propriétés MSTP

Le protocole MSTP global configure un Spanning Tree distinct pour chaque groupe VLAN et bloque tous les chemins alternatifs possibles sauf un, et ce, dans chaque instance Spanning Tree. MSTP permet la formation de régions MST pouvant exécuter des instances MST multiples (MSTI). Des régions multiples et d'autres ponts STP sont interconnectés à l'aide d'un 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 posséder les mêmes VLAN mappés sur une instance MST, le même numéro de révision de la configuration ainsi que le même nom de région.

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

Ce mappage peut être effectué sur la page VLAN vers instance MSTP.

Utilisez cette page si le système fonctionne en mode MSTP.

Pour définir MSTP :

ÉTAPE 1 Cliquez sur **Arbre recouvrant** > **État STP et paramètres globaux**.

ÉTAPE 2 Activez MSTP.

ÉTAPE 3 Cliquez sur **Arbre recouvrant** > **Propriétés MSTP**.

ÉTAPE 4 Saisissez les paramètres.

- **Nom de région** : définissez un nom de région MSTP.
- **Révision** : définissez un nombre non signé sur 16 bits qui identifie la révision de la configuration MST actuelle. La valeur de ce champ est comprise entre 0 et 65535.
- **Sauts max.** : définissez le nombre total de sauts se produisant dans une région spécifique avant la désactivation de l'unité BPDU. Lorsque le BPDU est désactivé, les informations du port sont obsolètes. La valeur de ce champ est comprise entre 1 et 40.
- **Maître IST** : affiche le maître de la région.

ÉTAPE 5 Cliquez sur **Appliquer**. Les propriétés MSTP sont définies et le fichier de configuration d'exécution est mis à jour.

VLAN vers instance MSTP

La page VLAN vers instance MSTP vous permet de mapper chaque réseau VLAN sur une instance MSTI (Multiple Spanning Tree Instance). Pour que les périphériques soient dans la même région, le mappage des VLAN aux MSTI doit être identique.

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

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

Il est possible de définir jusqu'à 16 instances MST en plus de l'instance zéro.

Le périphérique mappe automatiquement à l'instance CIST (Core and Internal Spanning Tree) les VLAN qui ne sont pas explicitement mappés à l'une des instances MST. L'instance CIST est l'instance MST 0.

Pour relier des VLAN à des instances MST :

ÉTAPE 1 Cliquez sur **Arbre recouvrant** > **VLAN vers instance MSTP**.

La page VLAN vers instance MSTP contient les champs suivants :

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

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

ÉTAPE 3 Configurez les paramètres suivants :

- **ID d'instance MSTP** : sélectionnez l'instance MSTP.
- **VLAN** : définissez les VLAN à mapper à cette instance MST.
- **Action** : choisissez d'**Ajouter** (mapper) le VLAN à l'instance MST ou de le **Supprimer** de celle-ci.

ÉTAPE 4 Cliquez sur **Appliquer**. Les mappages MSTP VLAN sont définis et le fichier de Configuration d'exécution est mis à jour.

Paramètres d'instance MSTP

La page Paramètres d'instance MSTP vous permet de configurer et d'afficher les paramètres par instance MST. Il s'agit de l'équivalent par instance de la *Configuration de l'état et des paramètres globaux STP*.

Pour entrer les paramètres de l'instance MSTP :

ÉTAPE 1 Cliquez sur **Arbre recouvrant** > **Paramètres d'instance MSTP**.

ÉTAPE 2 Saisissez les paramètres.

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

ÉTAPE 3 Cliquez sur **Appliquer**. La configuration de l'instance MST est terminée et le fichier de configuration d'exécution est mis à jour.

Paramètres d'interface MSTP

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

Pour configurer les ports dans une instance MST :

ÉTAPE 1 Cliquez sur **Arbre recouvrant** > **Paramètres d'interface MSTP**.

ÉTAPE 2 Saisissez les paramètres.

- **Instance égale à** : sélectionnez l'instance MSTP à configurer.
- **Type d'interface égal à** : choisissez d'afficher la liste des ports ou des LAG.

ÉTAPE 3 Cliquez sur **Go**. Les paramètres MSTP pour les interfaces de l'instance s'affichent.

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

ÉTAPE 5 Saisissez les paramètres.

- **ID d'instance** : sélectionnez l'instance MST à configurer.
- **Interface** : sélectionnez l'interface pour laquelle les paramètres MSTI doivent être définis.
- **Priorité d'interface** : définissez la priorité du port pour l'interface et l'instance MST spécifiées.
- **Coût de chemin** : entrez la contribution du port au coût du chemin racine dans la zone **Défini par l'utilisateur** ou sélectionnez **Valeurs par défaut** pour utiliser la valeur par défaut.
- **État du port** : affiche l'état MSTP du port spécifique sur une instance MST spécifique. Les paramètres sont définis comme suit :
  - *Désactivé* : STP est actuellement désactivé.
  - *Blocage* : le port sur cette instance est actuellement bloqué et ne peut ni transférer le trafic (à l'exception des données BPDU) ni apprendre les adresses MAC.
  - *Écoute* : le port sur cette instance est en mode Écoute. Il ne peut ni transférer le trafic ni connaître les adresses MAC.
  - *Apprentissage* : le port sur cette instance est en mode Apprentissage. Il ne peut pas transférer le trafic mais il peut prendre connaissance de nouvelles adresses MAC.

- *Transfert* : le port sur cette instance est en mode Transfert. Il peut réacheminer du trafic et apprendre de nouvelles adresses MAC.
- *Limite* : le port sur cette instance est un port frontière. Il hérite de son état de l'instance 0 et peut être affiché sur la page Paramètres d'interface STP.

- **Rôle du port** : affiche le rôle du port ou du LAG, par port ou LAG par instance, assigné par l'algorithme MSTP afin de fournir les chemins STP :
  - *Racine* : le transfert des paquets via cette interface fournit le chemin de moindre coût pour transférer les paquets vers le périphérique racine.
  - *Port désigné* : interface via laquelle le pont est connecté au réseau local (LAN) et qui fournit le chemin de moindre coût du réseau local (LAN) au pont racine pour l'instance MST.
  - *Alternate* (Alternatif) : l'interface fournit un chemin alternatif entre le pont racine et le port racine.
  - *Sauvegarde* : l'interface fournit un chemin de secours pour le chemin du port désigné vers les nœuds terminaux du Spanning Tree. Des ports de secours existent lorsque deux ports sont reliés dans une boucle par un lien point à point. Des ports de secours apparaissent également lorsqu'un LAN possède deux ou plusieurs connexions établies à un segment partagé.
  - *Désactivé* : l'interface ne participe pas au Spanning Tree.
  - *Limite* : le port sur cette instance est un port frontière. Il hérite de son état de l'instance 0 et peut être affiché sur la page Paramètres d'interface STP.
- **Mode** : affiche le mode Spanning Tree actuel de l'interface.
  - Si le partenaire de liaison utilise MSTP ou RSTP, le mode de port affiché est RSTP.
  - Si le partenaire de liaison utilise STP, le mode de port affiché est STP.
- **Type** : affiche le type MST du port.
  - *Limite* : un port frontière relie les ponts MST à un réseau LAN dans une région distante. 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.
- **ID de pont désigné** : affiche l'ID du pont qui connecte la liaison ou le LAN partagé à la racine.
- **ID de port désigné** : affiche l'ID du port sur le pont désigné qui connecte la liaison 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.
- **Sauts restants** : affiche le nombre de sauts restant jusqu'à la prochaine destination.
- **Transitions de transfert** : affiche le nombre de fois où le port est passé du mode Transfert au mode Blocage.

ÉTAPE 6 Cliquez sur **Appliquer**. Le fichier de configuration d'exécution est mis à jour.

14

Gestion des tables d'adresses MAC

Cette section explique comment ajouter des adresses MAC au système. Elle couvre les sujets suivants :

- Adresses statiques
- Adresses dynamiques
- Adresses MAC réservées

Il existe deux types d'adresses MAC : statiques et dynamiques. Selon leur type, les adresses MAC sont stockées dans la *table des adresses statiques* ou dans la *table des adresses dynamiques* avec les informations relatives aux VLAN et aux ports.

Les adresses statiques sont configurées par l'utilisateur, par conséquent elles n'expirent jamais.

Une nouvelle adresse MAC source qui apparaît dans une trame reçue par le périphérique est ajoutée à la table des adresses dynamiques. Cette adresse MAC est conservée pendant une période que vous pouvez configurer. Si aucune autre trame disposant de la même adresse MAC source n'apparaît sur le périphérique avant l'expiration de ce délai, l'entrée MAC est supprimée (expirée) de la table.

Lorsqu'une trame arrive au niveau du périphérique, celui-ci recherche une adresse MAC de destination correspondant à une entrée de la table des adresses statiques ou dynamiques. En cas de correspondance, la trame est marquée en sortie sur un port spécifique de la table. Les trames adressées à une adresse MAC n'ayant pas été trouvée dans les tables sont diffusées/transmises à tous les ports du VLAN approprié. Ces trames sont appelées trames de destination unique inconnue.

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

Adresses statiques

Les adresses MAC statiques sont affectées à une interface physique et à un VLAN spécifiques sur le périphérique. Si une adresse MAC est détectée sur une autre interface, elle est ignorée et n'est pas consignée dans la table des adresses.

Pour définir une adresse statique :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC > Adresses statiques**.

La page Adresses statiques affiche les adresses statiques actuellement définies.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez les paramètres.

- **ID VLAN** : sélectionnez l'ID VLAN du port.
- **Adresse MAC** : saisissez l'adresse MAC de l'interface.
- **Interface** : sélectionnez une interface (unité/logement, port ou LAG) pour l'entrée.
- **État** : sélectionnez le mode de traitement de l'entrée. Les options sont les suivantes :
  - *Permanent* : le système ne supprime jamais cette adresse MAC. Si l'adresse MAC statique est enregistrée dans la Configuration de démarrage, elle est conservée après redémarrage.
  - *Suppr. à la réinitialisation* : l'adresse MAC statique est supprimée lorsque le périphérique est réinitialisé.
  - *Supprimer à l'expiration* : l'adresse MAC est supprimée à expiration du délai.
  - *Sécurisé* : l'adresse MAC est sécurisée lorsque l'interface est en mode verrouillé classique (voir Sécurité des ports).

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

Adresses dynamiques

La table des adresses dynamiques (table de pontage) contient les adresses MAC obtenues en surveillant les adresses source des trames entrant dans le périphérique.

Pour éviter le débordement de cette table et garder de l'espace pour de nouvelles adresses MAC, une adresse est supprimée si elle ne reçoit aucun trafic pendant une période appelée délai d'expiration.

Paramètres des adresses dynamiques

Pour configurer le délai d'expiration des adresses dynamiques :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC > Paramètres des adresses dynamiques**.

ÉTAPE 2 Saisissez le **Délai d'expiration**. Le délai d'expiration est une valeur comprise entre la valeur configurée par l'utilisateur et deux fois cette valeur moins 1. Par exemple, si vous avez saisi une valeur de 300 secondes, le délai d'expiration est compris entre 300 et 599 secondes.

ÉTAPE 3 Cliquez sur **Appliquer**. Le délai d'expiration est mis à jour.

Adresses dynamiques

Pour interroger la table des adresses dynamiques :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC > Adresses dynamiques**.

ÉTAPE 2 Dans le bloc *Filtre*, vous pouvez saisir les critères d'interrogation suivants :

- **ID VLAN** : saisissez l'ID du VLAN pour lequel la table est interrogée.
- **Adresse MAC** : saisissez l'adresse MAC pour laquelle la table est interrogée.
- **Interface** : sélectionnez l'interface au sujet de laquelle la table est interrogée. L'interrogation peut également rechercher des unités/logements, ports ou LAG spécifiques.

ÉTAPE 3 Cliquez sur **Go**. La Table des adresses MAC dynamiques est interrogée et les résultats s'affichent.

ÉTAPE 4 Cliquez sur **Effacer la table** pour supprimer toutes les adresses MAC dynamiques.

Adresses MAC réservées

Lorsque le périphérique reçoit une trame utilisant une adresse MAC de destination qui appartient à une plage réservée (conformément à la norme IEEE), cette trame peut être éliminée ou pontée. L'entrée dans la table des adresses MAC réservées peut spécifier l'adresse MAC réservée ou l'adresse MAC réservée et un type de trame :

Pour ajouter une entrée pour une adresse MAC réservée :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC > Adresses MAC réservées**.

Les adresses MAC s'affichent. Ces champs sont décrits sur la page Ajouter, excepté le champ suivant :

Protocole : affiche le protocole pris en charge sur l'appareil (appelé homologue).

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Entrez les valeurs des champs suivants :

- **Adresse MAC** : sélectionnez l'adresse MAC à réserver.
- **Type de trame** : sélectionnez un type de trame en fonction des critères suivants :
  - *Ethernet V2* : s'applique aux paquets Ethernet V2 avec l'adresse MAC spécifique.
  - *LLC* : s'applique aux paquets LLC (Logical Link Control) avec l'adresse MAC spécifique.
  - *LLC-SNAP* : s'applique aux paquets LLC-SNAP (Logical Link Control/Sub-Network Access Protocol) avec l'adresse MAC spécifique.
  - *Tout* : s'applique à tous les paquets avec l'adresse MAC spécifique.
- **Action** : sélectionnez l'une des actions suivantes qui sera appliquée au paquet entrant correspondant aux critères sélectionnés :
  - *Pont* : transfère le paquet à tous les membres du VLAN.
  - *Abandonner* : supprime le paquet.

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

15

Multidestination

Cette section décrit la fonction de transfert de multidiffusion et couvre les rubriques suivantes :

- Présentation du réacheminement multidestination
- Propriétés
- Adresse MAC de groupe
- Adresse de groupe de multidestination IP
- Configuration de la multidestination IPv4
- Configuration de la multidestination IPv6
- Groupe de multidestination IP de surveillance IGMP/MLD
- Port de routeur multidestination
- Tout transférer
- Multidestination non enregistrée

Présentation du réacheminement multidestination

Le transfert de multidiffusion permet la transmission d'informations en mode 1-à-n. Les applications de multidiffusion sont particulièrement utiles pour transmettre des informations à plusieurs clients lorsque ces clients n'ont pas besoin de l'intégralité du contenu. Ceci est par exemple le cas dans le cadre d'une application de TV par câble où les clients peuvent contacter une chaîne au milieu d'une transmission et interrompre la connexion avant la fin.

Les données sont uniquement envoyées aux ports pertinents. Le fait de ne réacheminer les données que vers les ports pertinents permet d'économiser de la bande passante et des ressources d'hôte sur les liaisons.

Par défaut, toutes les trames de multidiffusion sont envoyées à tous les ports du VLAN. Il est possible de transférer les données de façon sélective uniquement vers les ports concernés et de filtrer (éliminer) le flux de multidiffusion sur les autres ports en activant l'état du filtrage multidiffusion par ponts sur la page Propriétés.

Si le filtrage est activé, les trames de multidiffusion sont transférées vers un sous-ensemble des ports sur le VLAN concerné, comme défini dans la base de données de transfert de multidiffusion (MFDB, Multicast Forwarding Data Base). Le filtrage multidiffusion s'exerce sur l'ensemble du trafic.

L'une des méthodes couramment utilisées de représentation des membres de multidiffusion est la notation (S,G), où S représente la source (unique) qui envoie un flux de données de multidiffusion et G représente l'adresse IPv4 ou IPv6 de groupe. Si un client Multicast peut recevoir du trafic de multidiffusion à partir de n'importe quelle source d'un groupe de multidiffusion donné, celui-ci est enregistré sous (*,G).

Vous pouvez configurer l'un des modes suivants de transfert des trames de multidiffusion :

- **Adresse MAC de groupe** : basée sur l'adresse MAC de destination dans la trame Ethernet.

  REMARQUE Il est possible de mapper une ou plusieurs adresses IP de groupe de multidiffusion à une seule adresse MAC de groupe. Le transfert basé sur une adresse MAC de groupe peut provoquer le transfert d'un flux de multidiffusion IP vers des ports qui ne possèdent aucun récepteur pour ce flux.

- **Adresse IP de groupe** : basée sur l'adresse IP de destination du paquet IP (*,G).
- **Adresse du groupe IP spécifique source** : basée à la fois sur l'adresse IP de destination et l'adresse IP source du paquet IP (S,G).

(S,G) est pris en charge par IGMPv3 et MLDv2 alors qu'IGMPv1/2 et MLDv1 ne prennent en charge que (*.G), qui inclut uniquement l'ID de groupe.

Le périphérique peut prendre en charge jusqu'à 256 adresses de groupe de multidiffusion statiques et dynamiques.

Vous ne pouvez configurer qu'une seule option de filtrage par VLAN.

Configuration de multidiffusion typique

Alors que les routeurs de multidiffusion routent les paquets de multidiffusion d'un sous-réseau IP à un autre, les commutateurs de couche 2 compatibles avec la multidiffusion transfèrent les paquets de multidiffusion vers les nœuds enregistrés au sein d'un LAN ou d'un VLAN.

La configuration type inclut un routeur qui transfère les flux de multidiffusion entre des réseaux IP privés et/ou publics, un périphérique doté de fonctions de surveillance IGMP/MLD et un client de multidiffusion qui souhaite recevoir un flux de multidiffusion. Dans cette configuration, le routeur envoie périodiquement des requêtes IGMP/MLD.

Fonctionnement de la multidiffusion

Dans un service de multidiffusion Couche 2, un commutateur Couche 2 reçoit une seule trame, adressée à une adresse de multidiffusion spécifique. Il crée des copies de la trame pour les transmettre à chacun des ports concernés.

Lorsque la surveillance IGMP/MLD est activée sur le périphérique et que celui-ci reçoit une trame du flux de multidiffusion, il la transfère à tous les ports enregistrés pour recevoir le flux de multidiffusion à l'aide de messages d'adhésion IGMP/MLD.

Le système gère des listes de groupes de multidestination pour chaque VLAN, lesquelles permettent de gérer les informations de multidestination que chaque port doit recevoir. Les groupes de multidiffusion et les ports destinataires associés peuvent être configurés de manière statique ou appris de manière dynamique via la surveillance des protocoles IGMP ou MLD.

Enregistrement multidestination (surveillance IGMP/MLD)

L'enregistrement de multidiffusion 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 la surveillance IGMP/MLD est activée sur un périphérique d'un VLAN, ce dernier analyse les paquets IGMP/MLD que le périphérique reçoit du VLAN et de tous les routeurs multidestination du réseau.

Lorsqu'un périphérique apprend qu'un hôte demande à recevoir un flux de multidiffusion à l'aide de messages IGMP/MLD, éventuellement à partir d'une source spécifique, ce périphérique ajoute cet hôte à sa base MFDB.

Les versions suivantes sont prises en charge :

- IGMP v1/v2/ v3
- MLD v1/v2

REMARQUE Le périphérique ne prend en charge la surveillance IGMP/MLD que sur les VLAN statiques. Il ne prend pas en charge la surveillance IGMP/MLD sur les VLAN dynamiques.

Lorsque vous activez la surveillance IGMP/MLD, globalement ou sur un VLAN, tous les paquets IGMP/MLD sont transmis au processeur. Le processeur analyse les paquets entrants et détermine ce qui suit :

- les ports qui demandent à rejoindre tel ou tel groupe de multidiffusion sur un VLAN spécifique ;
- les ports connectés aux routeurs de multidiffusion (Mrouters) qui génèrent des requêtes IGMP/MLD ;
- les ports qui reçoivent les protocoles de requête PIM, DVMRP ou IGMP/MLD.

Ces VLAN sont affichés sur la page Groupe de multidestination IP de surveillance IGMP/MLD.

Les ports demandant à rejoindre un groupe de multidiffusion spécifique envoient un rapport IGMP/MLD qui spécifie le ou les groupes que l'hôte concerné souhaite rejoindre. Cela provoque la création d'une entrée de transfert dans la base de données de transfert de multidiffusion.

Table de surveillance IGMP

L'émetteur de requêtes de surveillance IGMP sert à prendre en charge un domaine de multidiffusion de couche 2 de commutateurs de surveillance, en l'absence d'un routeur de multidiffusion. Par exemple, lorsqu'un serveur local fournit un contenu multidiffusion et que le routeur (s'il en existe un) de ce réseau ne prend pas en charge la multidiffusion.

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

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

La vitesse de fonctionnement de l'émetteur de requêtes IGMP/MLD doit s'aligner sur celle des commutateurs ayant la surveillance IGMP/MLD activée. Les requêtes doivent être envoyées à un rythme qui corresponde à la durée de vie des entrées dans la table de traçage. Si les requêtes sont envoyées à un rythme inférieur à la durée de vie, l'abonné ne peut pas recevoir les paquets de multidiffusion. Ceci s'effectue sur la page Groupe de multidestination IP de surveillance IGMP/MLD.

Si le mécanisme de choix de l'émetteur de requêtes IGMP/MLD est désactivé, l'émetteur de requêtes de surveillance IGMP/MLD retarde l'envoi des messages de requête générale pendant 60 secondes après son activation. S'il n'y a aucun autre demandeur, il commence à envoyer les messages de requête générale. Il arrête d'envoyer les messages de requête générale s'il détecte un autre demandeur.

L'émetteur de requêtes de surveillance IGMP/MLD reprend l'envoi des messages de requête générale s'il détecte un autre demandeur pendant l'intervalle suivant :

Intervalle passif de requête = Robustesse * Intervalle de requête + 0,5 * Intervalle de réponse aux requêtes.

REMARQUE Il est recommandé de désactiver le mécanisme de choix de l'émetteur de requêtes IGMP/MLD s'il y a un routeur de multidiffusion IPM sur le réseau VLAN.

Propriétés des adresses multidestination

Les adresses de multidiffusion possèdent les propriétés suivantes :

- Chaque adresse de multidiffusion IPv4 se trouve dans la plage d'adresses 224.0.0.0 à 239.255.255.255.
- L'adresse de multidiffusion IPv6 est FF00:/8.
- Pour mapper une adresse IP de groupe de multidiffusion à une adresse de multidiffusion de couche 2 :
  - Pour IPv4, le mappage s'effectue en prenant les 23 bits de poids faible de l'adresse IPv4 et en les ajoutant au préfixe 01:00:5e. Normalement, les 9 bits de poids fort de l'adresse IP sont ignorés et toutes les adresses IP qui diffèrent uniquement par ces bits de poids fort sont mappées à la même adresse de couche 2 puisque les 23 bits de poids faible sont identiques. Par exemple, 234.129.2.3 est mappé à l'adresse de groupe de multidestination MAC 01:00:5e:01:02:03. Il est possible de mapper jusqu'à 32 adresses de groupe de multidestination IP à la même adresse de couche 2.
  - Pour IPv6, le mappage s'effectue en prenant les 32 bits de poids faible de l'adresse multidestination et en y ajoutant le préfixe 33:33. Par exemple, l'adresse multidestination IPv6 FF00:1122:3344 est mappée à l'adresse multidestination de couche 2 33:33:11:22:33:44.

Proxy IGMP/MLD

Le Proxy IGMP/MLD est un protocole simple de multidiffusion IP.

L'utilisation du Proxy IGMP/MLD pour répliquer le trafic de multidiffusion sur des périphériques, tels que « edge box », peut grandement simplifier la conception et la mise en œuvre de ces périphériques. Le fait de ne pas prendre en charge des protocoles de routage de multidiffusion plus compliqués, tels que la multidiffusion indépendante du protocole (PIM) ou le protocole de routage multidiffusion distance-vecteur (DVMRP), réduit non seulement le coût des périphériques, mais aussi les frais de fonctionnement. Un autre avantage est que cela rend les périphériques proxy indépendants du protocole de routage de multidiffusion utilisé par les routeurs de base du réseau. Par conséquent, les périphériques proxy sont facilement déployables dans un réseau de multidiffusion.

Arborescence Proxy IGMP/MLD

Le Proxy IGMP/MLD fonctionne dans une topologie arborescente simple dans laquelle il n'est pas nécessaire d'exécuter un protocole de routage de multidiffusion robuste (par exemple, PIM). Il suffit d'utiliser un protocole simple de routage IPM basé sur l'apprentissage des informations concernant l'appartenance à un groupe ou l'appartenance à un groupe proxy et de transférer les paquets de multidiffusion en fonction de ces informations.

L'arborescence doit être configurée manuellement en désignant les interfaces amont et aval sur chaque périphérique proxy. En outre, le système d'adressage IP appliqué à la topologie arborescente proxy doit être configuré de manière à assurer qu'un périphérique proxy peut gagner l'élection du demandeur IGMP/MLD pour être en mesure de transférer le trafic de multidiffusion. Il ne doit pas y avoir d'autres routeurs de multidiffusion dans l'arborescence hormis les périphériques proxy, et la racine de l'arborescence doit être connectée à une infrastructure de multidiffusion plus large.

Un périphérique proxy effectuant le transfert basé sur IGMP/MLD a une seule interface amont et une ou plusieurs interfaces aval. Ces désignations sont configurées de façon explicite ; il n'y a pas de protocole pour déterminer le type de chaque interface. Un périphérique proxy effectue la partie routeur d'IGMP/MLD sur ses interfaces aval, et la partie hôte d'IGMP/MLD sur son interface amont.

Une seule arborescence est prise en charge.

Règles de transfert et émetteur de requêtes

Les règles suivantes sont appliquées :

- Un paquet de multidestination reçu sur l'interface amont est transmis :
  - sur l'interface amont ;
  - sur toutes les interfaces aval demandant le paquet, uniquement si le périphérique proxy est l'émetteur de requêtes sur les interfaces.
- Un périphérique proxy supprime les paquets de multidiffusion reçus sur une interface aval s'il n'est pas le demandeur sur l'interface.
- Un paquet de multidiffusion reçu sur une interface aval pour laquelle le périphérique proxy est le demandeur est transmis sur l'interface amont et sur toutes les interfaces aval demandant le paquet uniquement si le périphérique proxy est le demandeur sur les interfaces.

Protection d'interface aval

Par défaut, le trafic de multidiffusion IP arrivant sur une interface de l'arborescence IGMP/MLD est transmis. Vous pouvez désactiver le transfert du trafic de multidiffusion IP arrivant sur les interfaces aval. Cela peut être fait globalement ou sur une interface aval donnée.

Propriétés

Pour activer le filtrage multidiffusion et sélectionner la méthode de transfert :

ÉTAPE 1 Cliquez sur **Multidestination > Propriétés**.

ÉTAPE 2 Saisissez les paramètres.

- **État du filtrage multidiffusion par ponts** : sélectionnez cette option pour activer le filtrage.
- **ID VLAN** : sélectionnez l'ID du VLAN dont définir la méthode de transfert.
- **Méthode de transfert pour IPv6** : choisissez l'une des méthodes de transfert suivantes pour les adresses IPv6 :
  - *Adresse de groupe MAC* : transfère les paquets en fonction de l'adresse MAC du groupe de multidestination.
  - *Adresse de groupe IP* : transfère les paquets en fonction de l'adresse IPv6 du groupe de multidestination.

- *Adresse du groupe IP spécifique source* : transfère les paquets en fonction de l'adresse IPv6 source et de l'adresse IPv6 du groupe de multidestination. Si une adresse IPv6 est configurée sur le VLAN, la méthode de réacheminement opérationnelle pour la multidestination IPv6 sera Adresse du groupe IP.

REMARQUE Pour les modes Adresse de groupe IP IPv6 et Adresse du groupe IP spécifique source, le périphérique recherche uniquement une correspondance pour 4 octets avec l'adresse multidestination de destination et pour l'adresse source. Dans le cas de l'adresse multidestination de destination, la correspondance est établie avec les 4 derniers octets de l'ID du groupe. Dans le cas de l'adresse source, la correspondance est établie avec les 3 derniers octets + le cinquième octet en partant de la fin.

- **Méthode de transfert pour IPv4** : choisissez l'une des méthodes de transfert suivantes pour les adresses IPv4 :
  - *Adresse de groupe MAC* : transfère les paquets en fonction de l'adresse MAC du groupe de multidestination.
  - *Adresse de groupe IP* : transfère les paquets en fonction de l'adresse IPv4 du groupe de multidestination.
  - *Adresse du groupe IP spécifique source* : transfère les paquets en fonction de l'adresse IPv4 source et de l'adresse IPv4 du groupe de multidestination. Si une adresse IPv4 est configurée sur le VLAN, la méthode de réacheminement opérationnelle pour la multidestination IPv4 sera Adresse du groupe IP.

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

Adresse MAC de groupe

La page Adresse de groupe MAC offre les fonctions suivantes :

- Interrogation et affichage d'informations tirées de la base de données de transfert de multidiffusion (MFDB, Multicast Forwarding Data Base) concernant un ID de VLAN spécifique ou un groupe spécifique d'adresses MAC. Ces données sont acquises de manière dynamique par traçage IGMP/MLD Snooping ou de manière statique par saisie manuelle.
- Ajout ou suppression d'entrées statiques dans la base MFDB, qui fournissent les informations de transfert statiques basées sur les adresses MAC de destination.
- Affichage de la liste de tous les ports/LAG membres de chaque ID de VLAN ou adresse MAC de groupe, et indication précisant si le trafic doit ou non être transféré vers cette destination.

Pour définir et afficher des groupes de multidiffusion MAC :

ÉTAPE 1 Cliquez sur **Multidestination > Adresse MAC de groupe**.

ÉTAPE 2 Saisissez les paramètres de filtre.

- **ID VLAN est égal à** : saisissez l'ID de VLAN du groupe à afficher.
- **Adresse MAC de groupe égale à** : définissez l'adresse MAC du groupe de multidiffusion à afficher. Si aucune adresse MAC de groupe n'est indiquée, la page contient toutes les adresses MAC de groupe du VLAN sélectionné.

ÉTAPE 3 Cliquez sur **OK**. Les adresses MAC de groupe de multidiffusion sont affichées dans le bloc inférieur.

Les entrées créées sur cette page et sur la page Adresse de groupe de multidestination IP s'affichent. Pour celles qui ont été créées sur la page Adresse de groupe de multidestination IP, les adresses IP sont converties en adresses MAC.

ÉTAPE 4 Cliquez sur **Ajouter** pour ajouter une adresse MAC de groupe statique.

ÉTAPE 5 Saisissez les paramètres.

- **ID VLAN** : définit l'ID de VLAN du nouveau groupe de multidiffusion.
- **Adresse MAC de groupe** : définit l'adresse MAC du nouveau groupe de multidiffusion.

ÉTAPE 6 Cliquez sur **Appliquer** et l'adresse MAC du groupe de multidiffusion est enregistrée dans le fichier de configuration d'exécution.

Pour configurer et afficher l'enregistrement des interfaces au sein du groupe, sélectionnez une adresse et cliquez sur **Détails**.

La page affiche les éléments suivants :

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

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

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

ÉTAPE 9 Sélectionnez la façon dont chaque interface est associée au groupe de multidiffusion :

- **Statique** : rattache l'interface au groupe de multidiffusion en tant que membre statique.
- **Dynamique** : indique que l'interface a été ajoutée au groupe de multidiffusion via la surveillance IGMP/MLD.

- **Interdit** : spécifie que ce port n'est pas autorisé à rejoindre ce groupe de multidiffusion sur ce VLAN.
- **Aucun** : spécifie que le port n'est actuellement pas membre de ce groupe de multidiffusion sur ce VLAN.

ÉTAPE 10 Cliquez sur **Appliquer** ; le fichier de Configuration d'exécution est mis à jour.

REMARQUE Les entrées créées sur la page Adresse de groupe de multidestination IP ne peuvent pas être supprimées sur cette page (même si elles sont sélectionnées).

Adresse de groupe de multidestination IP

La page *Adresse IP de groupe de multidiffusion* est similaire à la page *Adresse de groupe MAC*, à la seule différence que les groupes de multidiffusion y sont identifiés par leurs adresses IP.

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

Pour définir et afficher des groupes de multidiffusion IP :

ÉTAPE 1 Cliquez sur **Multidestination >Adresse de groupe de multidestination IP**.

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

ÉTAPE 2 Saisissez les paramètres nécessaires pour le filtrage.

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

ÉTAPE 3 Cliquez sur **Go**. Les résultats s'affichent dans le bloc inférieur.

ÉTAPE 4 Cliquez sur **Ajouter** pour ajouter une adresse de groupe de multidestination IP statique.

ÉTAPE 5 Saisissez les paramètres.

- **ID VLAN** : définit l'ID de VLAN du groupe à ajouter.
- **Version IP** : sélectionnez le type d'adresse IP.
- **Adresse IP de groupe de multidiffusion** : définit l'adresse IP du nouveau groupe de multidiffusion.
- **Propre à la source** : indique que l'entrée contient une source spécifique et ajoute l'adresse correspondante dans le champ Adresse IP source. Dans le cas contraire, l'entrée est ajoutée sous la forme (*,G), c'est-à-dire une adresse IP de groupe associée à toutes les sources IP.
- **Adresse IP source** : définit l'adresse source à inclure.

ÉTAPE 6 Cliquez sur **Appliquer**. L'IP de multidiffusion du groupe est ajouté et le périphérique est mis à jour.

ÉTAPE 7 Pour configurer et afficher l'enregistrement d'une adresse IP de groupe, sélectionnez une adresse puis cliquez sur **Détails**.

Les ID de VLAN, Version IP, Adresse IP de groupe de multidiffusion et Adresse IP source sélectionnés s'affichent en lecture seule en haut de la fenêtre. Vous pouvez sélectionner le type de filtre :

- **Type d'interface est égal à** : choisissez d'afficher les ports ou les LAG.

ÉTAPE 8 Sélectionnez le type d'association de chaque interface. Les options disponibles sont les suivantes :

- **Statique** : rattache l'interface au groupe de multidiffusion en tant que membre statique.
- **Dynamique** : rattache l'interface au groupe de multidiffusion en tant que membre dynamique.
- **Interdit** : spécifie que ce port n'est pas autorisé à rejoindre ce groupe sur ce VLAN.
- **Aucun** : indique que le port n'est actuellement pas membre de ce groupe de multidiffusion sur ce VLAN. Cette option est définie par défaut tant que l'option Statique ou Interdit n'est pas sélectionnée.

ÉTAPE 9 Cliquez sur **Appliquer**. Le fichier de configuration d'exécution est mis à jour.

Configuration de la multidestination IPv4

Les pages suivantes décrivent la configuration de la multidiffusion IPv4 :

- Surveillance IGMP
- Paramètres d'interface IGMP
- Paramètres de VLAN IGMP
- Proxy IGMP

Surveillance IGMP

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

Pour activer le traçage IGMP Snooping et identifier le périphérique en tant qu'émetteur de requêtes de traçage IGMP Snooping sur un VLAN :

ÉTAPE 1 Cliquez sur **Multidestination** > **Configuration de la multidestination IPv4 > Surveillance IGMP**.

Lorsque la surveillance IGMP est activée globalement, le périphérique qui surveille le trafic réseau peut détecter les hôtes qui ont demandé à recevoir le trafic de multidiffusion. Le périphérique n'exécute la surveillance IGMP que si vous avez activé à la fois la surveillance IGMP et le filtrage multidiffusion par ponts.

Le tableau de surveillance IGMP s'affiche. Les champs affichés sont décrits ci-dessous sur la page Modifier. Les champs suivants sont par ailleurs affichés :

- **IGMP Snooping Status** (État de la surveillance IGMP) : indique si la fonction de surveillance IGMP a été activée (**Administrative** [Administratif]) et si elle est en cours d'exécution sur le VLAN (**Operational** [Opérationnel]).
- **État du demandeur IGMP**—Indique si le demandeur IGMP a été activé (**Administratif**) et s'il s'exécute effectivement sur le VLAN (**Operationnel**).

Activez ou désactivez les fonctionnalités suivantes :

- **État de surveillance IGMP** : sélectionnez cette option pour activer la surveillance IGMP globalement sur toutes les interfaces.
- **État du demandeur IGMP** : sélectionnez cette option pour activer la surveillance IGMP globalement sur toutes les interfaces.

ÉTAPE 2 Pour configurer IGMP sur une interface, sélectionnez un VLAN statique et cliquez ensuite sur **Modifier**. Renseignez les champs suivants :

- **État de surveillance IGMP** : sélectionnez cette option pour activer la surveillance IGMP sur le VLAN. Le périphérique surveille le trafic réseau pour déterminer les hôtes qui ont demandé à recevoir du trafic de multidiffusion. Le périphérique n'exécute la surveillance IGMP que si la surveillance IGMP et le filtrage multidiffusion par ponts sont tous deux activés.
- **Apprentissage automatique des ports MRouter** : sélectionnez cette option pour activer l'apprentissage automatique du routeur de multidiffusion.
- **Sortie immédiate** : sélectionnez cette option pour autoriser le commutateur à supprimer une interface qui envoie un message de sortie de la table de transfert sans envoyer au préalable à l'interface des requêtes générales basées sur MAC. Lorsqu'un message de sortie de groupe IGMP est reçu de la part d'un hôte, le système supprime le port hôte de l'entrée de la table. Après avoir transmis les requêtes IGMP en provenance du routeur de multidiffusion, il supprime les entrées périodiquement s'il ne reçoit aucun rapport d'appartenance IGMP de la part des clients de multidiffusion. Lorsqu'elle est activée, cette fonction réduit le temps nécessaire au blocage du trafic IGMP inutile envoyé à un port du périphérique.
- **Nombre de requêtes du dernier membre** : nombre de requêtes propres au groupe MLD envoyées avant que le périphérique considère qu'il n'existe pas d'autre membre dans le groupe, dans la mesure où ce périphérique est le demandeur choisi.
  - *Utiliser la robustesse des requêtes (x)* : cette valeur est définie sur la page Paramètres de l'interface MLD. Le nombre entre parenthèses correspond à la valeur actuelle de la robustesse des consultations.
  - *Défini par l'utilisateur* : saisissez une valeur définie par l'utilisateur.
- **État de l'émetteur de requêtes IGMP** : sélectionnez cette option pour activer cette fonction. Cette fonction est requise s'il n'y a pas de routeur de multidiffusion.
- **IGMP Querier Election (Choix du demandeur IGMP)** : indique si le choix du demandeur IGMP est activé ou désactivé. Si le mécanisme de choix du demandeur IGMP est activé, le demandeur de surveillance IGPM prend en charge le mécanisme standard de choix du demandeur IGMP, spécifié dans la norme RFC3810.

  Si le mécanisme de choix du demandeur IGMP est désactivé, le demandeur de surveillance IGPM retarde l'envoi des messages de requête générale pendant 60 secondes après son activation, et s'il n'y a pas d'autre demandeur, commence à envoyer les messages de requête générale. Il arrête d'envoyer les messages de requête générale s'il détecte un autre demandeur. Le demandeur de surveillance IGMP reprend l'envoi des messages de requête générale s'il ne détecte aucun autre demandeur pendant un intervalle passif de requête égal à : Robustesse * (Intervalle de requête) + 0,5 * Intervalle de réponse de requête.

- **Version du demandeur IGMP** : sélectionnez la version IGMP utilisée si le périphérique devient le demandeur choisi. Sélectionnez IGMPv3 s'il existe des commutateurs et/ou des routeurs multidestination dans le VLAN qui réalisent le réacheminement de multidestination IP propre à la source. Sinon, sélectionnez IGMPv2.
- **Adresse IP source du demandeur** : sélectionnez l'interface source du périphérique à utiliser dans les messages envoyés. Avec MLD, cette adresse est sélectionnée automatiquement par le système.

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

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

REMARQUE Changements dans la configuration des temporisations de surveillance IGMP, tels que : Robustesse des requêtes, Intervalle de requête, etc. ne prennent pas effet sur les temporisations déjà créées.

Paramètres d'interface IGMP

Une interface qui est définie comme port de routeur de multidiffusion reçoit tous les paquets IGMP (rapports et requêtes) ainsi que toutes les données de multidiffusion.

Pour définir le protocole IGMP sur une interface :

ÉTAPE 1 Cliquez sur **Multidestination** > **Configuration de la multidestination IPv4 > Paramètres d'interface IGMP**.

Les champs suivants sont affichés pour chaque interface sur laquelle IGMP est activé :

- **Nom de l'interface** : interface sur laquelle la surveillance IGMP est définie.
- **Version IGMP du routeur** : version IGMP.
- **Robustesse des requêtes** : entrez le nombre de pertes de paquets prévues sur une liaison.
- **Intervalle de requête (s)** : intervalle à appliquer entre deux requêtes générales si ce périphérique est le demandeur choisi.
- **Intervalle de réponse max aux requêtes (s)** : délai utilisé pour calculer le code de réponse maximum inséré dans les requêtes générales périodiques.

- **Intervalle de requête du dernier membre (ms)** : délai maximal de réponse à utiliser si le périphérique ne peut pas lire cette valeur dans les requêtes propres au groupe envoyées par le demandeur choisi.
- **Multicast TTL Threshold (Seuil TTL de multidiffusion)** : entrez le seuil de temps de vie (TTL, Time-to-Live) des paquets transférés sur une interface.

  Les paquets de multidestination avec une valeur TTL inférieure au seuil ne sont pas réacheminés sur l'interface.

  La valeur par défaut de 0 signifie que tous les paquets de multidiffusion sont transférés sur l'interface.

  La valeur 256 signifie qu'aucun paquet de multidiffusion n'est transféré sur l'interface.

  Configurez le seuil TTL uniquement sur les routeurs de bordure. Inversement, les routeurs sur lesquels vous configurez une valeur de seuil TTL deviennent automatiquement des routeurs de bordure.

ÉTAPE 2 Sélectionnez une interface et cliquez sur **Edit**. Renseignez les valeurs des champs décrits ci-dessus.

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

Paramètres de VLAN IGMP

Pour configurer le protocole IGMP sur un VLAN spécifique :

ÉTAPE 1 Cliquez sur **Multidestination** > **Configuration de la multidestination IPv4 > Paramètres de VLAN IGMP**.

Les champs suivants sont affichés pour chaque VLAN sur lequel IGMP est activé :

- **Nom de l'interface** : .
- **Version IGMP du routeur** : version de la surveillance IGMP.
- **Robustesse des requêtes** : entrez le nombre de pertes de paquets prévues sur une liaison.
- **Intervalle de requête (s)** : intervalle à appliquer entre deux requêtes générales si ce périphérique est le demandeur choisi.
- **Intervalle de réponse max aux requêtes (s)** : délai utilisé pour calculer le code de réponse maximum inséré dans les requêtes générales périodiques.

- **Intervalle de requête du dernier membre (ms)** : saisissez le délai maximal de réponse à utiliser si le périphérique ne le reconnaît pas à partir des requêtes propres au groupe envoyées par l'émetteur de requêtes choisi.
- **Seuil TTL de multidestination** : saisissez la limite de durée de vie (TTL, Time-to-Live) des paquets réacheminés sur une interface.

  Les paquets de multidestination avec une valeur TTL inférieure au seuil ne sont pas réacheminés sur l'interface.

  La valeur par défaut de 0 signifie que tous les paquets de multidiffusion sont transférés sur l'interface.

  La valeur 256 signifie qu'aucun paquet de multidiffusion n'est transféré sur l'interface.

  Configurez le seuil TTL uniquement sur les routeurs de bordure. Inversement, les routeurs sur lesquels vous configurez une valeur de seuil TTL deviennent automatiquement des routeurs de bordure.

ÉTAPE 2 Sélectionnez une interface et cliquez sur **Edit**. Renseignez les valeurs des champs décrits ci-dessus.

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

Proxy IGMP

Pour configurer le proxy IGMP :

ÉTAPE 1 Cliquez sur **Multidestination** > **Configuration de la multidestination IPv4 > Proxy IGMP**.

ÉTAPE 2 Renseignez les champs généraux suivants :

- **Routage de multidiffusion IGMP** : sélectionnez cette option pour activer le routage de multidiffusion IPv4.
- **Downstream Protection (Protection aval)** : sélectionnez cette option pour ignorer les paquets aval non requis par le périphérique.
- **Multidiffusion spécifique à la source** : sélectionnez cette option pour activer la livraison des paquets de multidiffusion provenant d'une adresse source spécifique définie dans le champ suivant.

- **SSM IPv4 Access List (Liste d'accès IPv6 SSM)** : définissez la liste contenant les adresses sources des paquets de multidiffusion :
  - *Liste par défaut* : définit la plage d'accès SSM à 232.0.0.0/8.
  - *Liste d'accès définie par l'utilisateur* : sélectionnez le nom de la liste d'accès IPv4 standard définissant la plage SSM. Ces listes d'accès sont définies dans Liste d'accès.

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

ÉTAPE 4 Pour ajouter une protection à un VLAN, cliquez sur **Ajouter** et renseignez les champs suivants :

- **Upstream Interface (Interface amont)** : sélectionnez l'interface amont. Comme il n'y a qu'une seule interface amont, si une interface a déjà été sélectionnée, ce champ est grisé.
- **Downstream Interface (Interface aval)** : sélectionnez l'interface aval. Il peut y avoir plusieurs interfaces aval.
- **Downstream Protection (Protection aval)** : sélectionnez l'une des options suivantes :
  - *Use Global (Utiliser le paramètre global)* : utilisez l'état défini dans le bloc global.
  - *Désactiver* : désactive le transfert du trafic de multidiffusion IPv4 provenant des interfaces aval.
  - *Activer* : active le transfert du trafic provenant des interfaces aval.

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

Les champs suivants s'affichent pour chaque route de multidiffusion IPv4 :

- **Adresse source** : adresse IPv4 source de monodiffusion.
- **Adresse de groupe** : adresse IPv4 de destination de multidiffusion.
- **Interface entrante** : interface prévue pour un paquet de multidiffusion provenant de la source. Si le paquet n'est pas reçu sur cette interface, il est ignoré.
- **Interfaces sortantes** : interfaces via lesquelles les paquets seront transmis.
- **Uptime (Temps utilisation)** : durée en heures, minutes et secondes pendant laquelle l'entrée a été dans la table de routage de multidiffusion IP.
- **Délai d'expiration** : durée en heures, minutes et secondes avant la suppression de l'entrée dans la table de routage de multidiffusion IP.

Configuration de la multidestination IPv6

Les pages suivantes décrivent la configuration de la multidiffusion IPv6 :

- Surveillance MLD
- Paramètres de l'interface MLD
- Paramètres de VLAN MLD
- Proxy MLD

Surveillance MLD

Pour prendre en charge le transfert sélectif de la multidiffusion IPv6, vous devez activer le filtrage multidiffusion par ponts (sur la page Propriétés). Vous devez aussi activer la surveillance MLD globalement ainsi que pour chacun des VLAN concernés, sur les pages MLD Snooping (Surveillance MLD).

Pour activer la surveillance MLD et la configurer sur un VLAN :

ÉTAPE 1 Cliquez sur **Multidestination** > **Configuration de la multidestination IPv6 > Surveillance MLD**.

Lorsque le traçage MLD Snooping est activé au niveau global, le périphérique qui surveille le trafic réseau peut détecter les hôtes qui ont demandé à recevoir le trafic de multidiffusion. Le périphérique exécute uniquement le traçage MLD Snooping si vous avez activé à la fois MLD Snooping et le filtrage multidiffusion par ponts.

Le tableau de surveillance MLD s'affiche. Les champs affichés sont décrits ci-dessous sur la page Edit (Modifier). Les champs suivants sont par ailleurs affichés :

- **MLD Snooping Status** (État de la surveillance MLD) : indique si la fonction de surveillance MLD a été activée (**Administrative** [Administratif]) et si elle est en cours d'exécution sur le VLAN (**Operational** [Opérationnel]).
- **État du demandeur MLD**—Indique si le demandeur IGMP a été activé (**Administratif**) et s'il s'exécute effectivement sur le VLAN (**Operationnel**).

ÉTAPE 2 Activez ou désactivez les fonctionnalités suivantes :

- **État de surveillance MLD** : sélectionnez cette option pour activer la surveillance MLD globalement sur toutes les interfaces.
- **État du demandeur MLD** : sélectionnez cette option pour activer le demandeur MLD globalement sur toutes les interfaces.

ÉTAPE 3 Pour configurer le proxy MLD sur une interface, sélectionnez un VLAN statique et cliquez ensuite sur **Modifier**. Renseignez les champs suivants :

- **État de surveillance MLD** : sélectionnez cette option pour activer la surveillance MLD sur le VLAN. Le périphérique surveille le trafic réseau pour déterminer les hôtes qui ont demandé à recevoir du trafic de multidiffusion. Le périphérique n'exécute la surveillance MLD que si la surveillance MLD et le filtrage multidiffusion par ponts sont tous deux activés.
- **Apprentissage automatique des ports MRouter** : sélectionnez cette option pour activer l'apprentissage automatique du routeur de multidiffusion.
- **Sortie immédiate** : sélectionnez cette option pour autoriser le commutateur à supprimer une interface qui envoie un message de sortie de la table de transfert sans envoyer au préalable à l'interface des requêtes générales basées sur MAC. Lorsqu'un message de sortie de groupe MLD est reçu de la part d'un hôte, le système supprime le port hôte de l'entrée de la table. Après avoir transmis les requêtes MLD en provenance du routeur de multidiffusion, il supprime les entrées périodiquement s'il ne reçoit aucun rapport d'appartenance MLD de la part des clients de multidiffusion. Lorsqu'elle est activée, cette fonction réduit le temps nécessaire au blocage du trafic MLD inutile envoyé à un port du périphérique.
- **Nombre de requêtes du dernier membre** : nombre de requêtes propres au groupe MLD envoyées avant que le périphérique considère qu'il n'existe pas d'autre membre dans le groupe, dans la mesure où ce périphérique est le demandeur choisi.
  - *Utiliser la robustesse des requêtes (x)* : cette valeur est définie sur la page Paramètres de l'interface MLD. Le nombre entre parenthèses correspond à la valeur actuelle de la robustesse des consultations.
  - *Défini par l'utilisateur* : saisissez une valeur définie par l'utilisateur.
- **État de l'émetteur de requêtes MLD** : sélectionnez cette option pour activer cette fonction. Cette fonction est requise s'il n'y a pas de routeur de multidiffusion.
- **Choix du demandeur MLD** : indique si le choix du demandeur MLD est activé ou désactivé. Si le mécanisme de choix du demandeur MLD est activé, le demandeur de surveillance MLD prend en charge le mécanisme standard de choix du demandeur MLD, spécifié dans la norme RFC3810.

  Si le mécanisme de choix du demandeur MLD est désactivé, le demandeur de surveillance MLD retarde l'envoi des messages de requête générale pendant 60 secondes après son activation, et s'il n'y a pas d'autre demandeur, commence à envoyer les messages de requête générale. Il arrête d'envoyer les messages de requête générale s'il détecte un autre demandeur. Le demandeur de surveillance MLD reprend l'envoi des messages de requête générale s'il ne détecte aucun autre demandeur pendant un intervalle passif de requête égal à : Robustesse * (Intervalle de requête) + 0,5 * Intervalle de réponse de requête.

- **Version du demandeur MLD** : sélectionnez la version MLD utilisée si le périphérique devient le demandeur choisi. Sélectionnez MLDv2 s'il existe des commutateurs et/ou des routeurs multidestination dans le VLAN qui réalisent le réacheminement de multidestination IP propre à la source. Sinon, sélectionnez MLDv1.

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

REMARQUE Changements dans la configuration des temporisations de surveillance MLD, tels que : Robustesse des requêtes, Intervalle de requête, etc. ne prennent pas effet sur les temporisations déjà créées.

Paramètres de l'interface MLD

Une interface qui est définie comme port de routeur de multidiffusion reçoit tous les paquets MLD (rapports et requêtes) ainsi que toutes les données de multidiffusion.

Pour configurer une interface comme interface de routeur de multidiffusion :

ÉTAPE 1 Cliquez sur **Multidestination** > **Configuration de la multidestination IPv6 > Paramètres d'interface MLD**.

Les champs suivants sont affichés pour chaque interface sur laquelle MLD est activé :

- **Version du routeur MLD** : version MLD du routeur de multidiffusion.
- **Robustesse des requêtes** : entrez le nombre de pertes de paquets prévues sur une liaison.
- **Intervalle de requête (s)** : intervalle à appliquer entre deux requêtes générales si ce périphérique est le demandeur choisi.
- **Intervalle de réponse max aux requêtes (s)** : délai utilisé pour calculer le code de réponse maximum inséré dans les requêtes générales périodiques.
- **Intervalle de requête du dernier membre (ms)** : délai maximal de réponse à utiliser si le périphérique ne peut pas lire cette valeur dans les requêtes propres au groupe envoyées par le demandeur choisi.
- **Multicast TTL Threshold (Seuil TTL de multidiffusion)** : entrez le seuil de temps de vie (TTL, Time-to-Live) des paquets transférés sur une interface.

  Les paquets de multidestination avec une valeur TTL inférieure au seuil ne sont pas réacheminés sur l'interface.

La valeur par défaut de 0 signifie que tous les paquets de multidiffusion sont transférés sur l'interface.

La valeur 256 signifie qu'aucun paquet de multidiffusion n'est transféré sur l'interface.

Configurez le seuil TTL uniquement sur les routeurs de bordure. Inversement, les routeurs sur lesquels vous configurez une valeur de seuil TTL deviennent automatiquement des routeurs de bordure.

ÉTAPE 2 Pour configurer une interface, sélectionnez-la et cliquez sur **Modifier**. Renseignez les champs décrits ci-dessus.

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

Paramètres de VLAN MLD

Pour configurer le protocole MLD sur un VLAN spécifique :

ÉTAPE 1 Cliquez sur **Multidestination** > **Configuration de la multidestination IPv6 > Paramètres de VLAN MLD**.

Les champs suivants sont affichés pour chaque VLAN sur lequel MLD est activé :

- **Nom de l'interface** : VLAN pour lequel afficher les informations MLD.
- **Version du routeur MLD** : version du routeur MLD.
- **Robustesse des requêtes** : entrez le nombre de pertes de paquets prévues sur une liaison.
- **Intervalle de requête (s)** : intervalle à appliquer entre deux requêtes générales si ce périphérique est le demandeur choisi.
- **Intervalle de réponse max aux requêtes (s)** : délai utilisé pour calculer le code de réponse maximum inséré dans les requêtes générales périodiques.
- **Intervalle de requête du dernier membre (ms)** : saisissez le délai maximal de réponse à utiliser si le périphérique ne le reconnaît pas à partir des requêtes propres au groupe envoyées par l'émetteur de requêtes choisi.
- **Seuil TTL de multidestination** : saisissez la limite de durée de vie (TTL, Time-to-Live) des paquets réacheminés sur une interface.

  Les paquets de multidestination avec une valeur TTL inférieure au seuil ne sont pas réacheminés sur l'interface.

La valeur par défaut de 0 signifie que tous les paquets de multidiffusion sont transférés sur l'interface.

La valeur 256 signifie qu'aucun paquet de multidiffusion n'est transféré sur l'interface.

Configurez le seuil TTL uniquement sur les routeurs de bordure. Inversement, les routeurs sur lesquels vous configurez une valeur de seuil TTL deviennent automatiquement des routeurs de bordure.

ÉTAPE 2 Pour configurer un VLAN, sélectionnez-le et cliquez sur **Modifier**. Renseignez les champs décrits ci-dessus.

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

Proxy MLD

ÉTAPE 4 Pour configurer Proxy MLD :

ÉTAPE 1 Cliquez sur **Multidestination** > **Configuration de la multidestination IPv6 > Proxy MLD**.

ÉTAPE 2 Renseignez les champs suivants :

- **Routage de multidiffusion MLD** : sélectionnez cette option pour activer le routage de multidiffusion IPv6.
- **Downstream Protection (Protection aval)** : sélectionnez cette option pour ignorer les paquets aval non requis par le périphérique.
- **Multidiffusion spécifique à la source** : sélectionnez cette option pour activer la livraison des paquets de multidiffusion provenant d'une adresse source spécifique définie dans le champ suivant.
- **SSM IPv6 Access List (Liste d'accès IPv6 SSM)** : définissez la liste contenant les adresses sources des paquets de multidiffusion :
  - *Default list* (Liste par défaut) : définit la liste de plages d'accès SSM sur FF3E::/32.
  - *User defined access list* (Liste d'accès définie par l'utilisateur) : sélectionnez le nom de la liste d'accès IPv6 standard définissant la plage SSM. Ces listes d'accès sont définies dans Liste d'accès.

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

ÉTAPE 4 Pour ajouter une protection à un VLAN, cliquez sur **Ajouter** et renseignez les champs suivants :

- **Upstream Interface (Interface amont)** : sélectionnez l'interface de sortie.
- **Downstream Interface (Interface aval)** : sélectionnez l'interface d'entrée.
- **Downstream Protection (Protection aval)** : sélectionnez l'une des options suivantes :
  - *Use Global (Utiliser le paramètre global)* : utilisez l'état défini dans le bloc global.
  - *Désactiver* : désactive le transfert du trafic de multidiffusion IPv6 provenant des interfaces aval.
  - *Activer* : active le transfert du trafic provenant des interfaces aval.

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

Les champs suivants s'affichent pour chaque route de multidiffusion IP :

- **Adresse source** : adresse IPv4 source de monodiffusion.
- **Adresse de groupe** : adresse IPv4 de destination de multidiffusion.
- **Interface entrante** : interface prévue pour un paquet de multidiffusion provenant de la source. Si le paquet n'est pas reçu sur cette interface, il est ignoré.
- **Interfaces sortantes** : interfaces via lesquelles les paquets seront transmis.
- **Uptime (Temps utilisation)** : durée en heures, minutes et secondes pendant laquelle l'entrée a été dans la table de routage de multidiffusion IP.
- **Délai d'expiration** : durée en heures, minutes et secondes avant la suppression de l'entrée dans la table de routage de multidiffusion IP.

Groupe de multidestination IP de surveillance IGMP/MLD

La page Groupe de multidiffusion IP de surveillance IGMP/MLD affiche les adresses de groupes IPv4 et IPv6 apprises à partir des messages IGMP/MLD.

Il peut y avoir une différence entre les informations affichées sur cette page et celles affichées sur la page Adresse de groupe MAC. Voici un exemple : supposons que le système effectue un filtrage selon les groupes basés sur MAC et un port demandé pour rejoindre les groupes de multidestination 224.1.1.1 et 225.1.1.1, et que tous deux soient mappés à la même adresse MAC multidestination 01:00:5e:01:01:01. Dans ce cas, la page Multidestination MAC contient une seule entrée, tandis que cette page en comporte deux.

Pour émettre une requête de recherche d'un groupe de multidiffusion IP :

ÉTAPE 1 Cliquez sur **Multidestination** > **Groupe de multidestination IP de surveillance IGMP/MLD**.

ÉTAPE 2 Définissez le type de groupe de traçage (Snooping) à rechercher : IGMP ou MLD.

ÉTAPE 3 Saisissez tout ou partie des critères de filtrage des requêtes suivants :

- **Adresse de groupe est égale à** : définit l'adresse MAC ou IP du groupe de multidiffusion à interroger.
- **Adresse source est égale à** : définit l'adresse de l'expéditeur à interroger.
- **ID VLAN est égal à** : définit l'ID de VLAN à interroger.

ÉTAPE 4 Cliquez sur **Go**. Les champs suivants s'affichent pour chaque groupe de multidiffusion :

- **VLAN** : ID du VLAN.
- **Adresse de groupe** : adresse MAC ou IP du groupe de multidiffusion.
- **Adresse source** : adresse de l'expéditeur pour tous les ports du groupe spécifié.
- **Ports inclus** : liste des ports de destination pour le flux de multidiffusion.
- **Ports exclus** : liste des ports non membres du groupe.
- **Mode de compatibilité** : version d'enregistrement IGMP/MLD la plus ancienne que le périphérique reçoit des hôtes à l'adresse IP du groupe.

Port de routeur multidestination

Un port de routeur de multidiffusion (Mrouter) est un port qui se connecte à un routeur de multidiffusion. Le périphérique inclut le ou les numéros de ports de routeur de multidiffusion lorsqu'il transfère les flux de multidiffusion et les messages d'enregistrement IGMP/MLD. Cela est indispensable pour que les routeurs de multidiffusion puissent, à leur tour, transférer les flux de multidiffusion et propager les messages d'enregistrement vers d'autres sous-réseaux.

Pour configurer de manière statique les ports qui sont connectés au routeur de multidiffusion, ou afficher ceux dynamiquement détectés :

ÉTAPE 1 Cliquez sur **Multidestination** > **Port de routeur multidestination**.

ÉTAPE 2 Saisissez tout ou partie des critères de filtrage des requêtes suivants :

- **ID VLAN est égal à** : sélectionnez l'ID de VLAN des ports du routeur décrits.
- **Version IP est égale à** : sélectionnez la version IP prise en charge par le routeur de multidiffusion.
- **Type d'interface est égal à** : choisissez d'afficher les ports ou les LAG.

ÉTAPE 3 Cliquez sur **Go**. Les interfaces répondant aux critères de requête s'affichent.

ÉTAPE 4 Sélectionnez le type d'association de chaque port ou LAG. Les options disponibles sont les suivantes :

- **Statique** : le port est configuré de manière statique en tant que port de routeur de multidiffusion.
- **Dynamique** : (affichage uniquement) le port est configuré de manière dynamique en tant que port de routeur de multidiffusion par une requête MLD/IGMP. Pour activer l'apprentissage dynamique des ports de routeurs de multidiffusion, accédez à la page Surveillance IGMP ou à la page Surveillance MLD.
- **Interdit** : ce port ne doit pas être configuré en tant que port de routeur de multidiffusion, même s'il reçoit des requêtes IGMP ou MLD. Si l'option Interdit est activée sur un port, l'apprentissage des ports MRouter n'a pas lieu sur ce port (ce qui signifie que l'option Apprentissage automatique des ports MRouter n'est pas activée sur ce port).
- **Aucun** : le port n'est actuellement pas un port de routeur de multidiffusion.

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

Tout transférer

Lorsque le filtrage de multidiffusion du pont est activé, les paquets de multidiffusion sur les groupes de multidiffusion enregistrés sont transférés aux ports basés sur la surveillance IGMP et la surveillance MLD. Si le filtrage de multidiffusion du pont est désactivé, tous les paquets de multidiffusion inondent le VLAN correspondant.

La page Forward All (Tout transférer) configure les ports et/ou les LAG qui doivent recevoir des flux de multidiffusion en provenance d'un VLAN spécifique. Cette fonction exige que vous activiez le filtrage multidiffusion par ponts sur la page Propriétés des adresses multidestination. Si cette fonction est désactivée, tout le trafic de multidiffusion est envoyé aux ports du périphérique.

Vous pouvez configurer (manuellement) un port en mode Tout transférer de manière statique si les périphériques qui se connectent à ce port ne prennent pas en charge IGMP et/ou MLD.

Les paquets de multidiffusion, à l'exception des messages IGMP et MLD, sont toujours transférés aux ports définis sur Forward All (Tout transférer). Cette configuration concerne uniquement les ports membres du VLAN sélectionné.

Pour définir la multidiffusion Tout transférer :

ÉTAPE 1 Cliquez sur **Multidestination** > **Tout transférer**.

ÉTAPE 2 Définissez les éléments suivants :

- **ID VLAN est égal à** : ID du VLAN dont afficher les ports/LAG.
- **Type d'interface est égal à** : choisissez d'afficher les ports ou les LAG.

ÉTAPE 3 Cliquez sur **Go**. L'état de tous les ports/LAG est affiché.

ÉTAPE 4 Sélectionnez le port/LAG à définir en mode Tout transférer à l'aide des méthodes suivantes :

- **Statique** : le port reçoit tous les flux de multidiffusion.
- **Interdit** : le port ne peut pas recevoir de flux de multidiffusion, même si la surveillance IGMP/MLD l'a désigné pour rejoindre un groupe de multidiffusion.
- **Aucun** : le port n'est actuellement pas un port en mode Tout transférer.

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

Multidestination non enregistrée

Cette fonction permet de garantir que le client reçoit uniquement les groupes de multidiffusion demandés (enregistrés) et non d'autres groupes éventuellement transmis sur le réseau (non enregistrés).

En général, les trames de multidiffusion non enregistrées sont transférées vers tous les ports du VLAN.

Vous pouvez sélectionner un port pour qu'il reçoive ou refuse (filtre) les flux de multidiffusion non enregistrés. Cette configuration est valide pour tout VLAN dont le port est (ou sera) membre.

Pour définir des paramètres de multidiffusion non enregistrée :

ÉTAPE 1 Cliquez sur **Multidestination** > **Multidestination non enregistrée**.

ÉTAPE 2 Sélectionnez **Type d'interface est égal à** : pour afficher les ports ou les LAG.

ÉTAPE 3 Cliquez sur **Go**.

ÉTAPE 4 Définissez les éléments suivants :

- **Port/LAG** : affiche l'ID du port ou du LAG.
- Affiche l'état de transfert de l'interface sélectionnée. Ce champ peut prendre les valeurs suivantes :
  - *Transfert* : active le transfert des trames de multidiffusion non enregistrée vers l'interface sélectionnée.
  - *Filtrage* : active le filtrage (rejet) des trames de multidiffusion non enregistrée sur l'interface sélectionnée.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres sont enregistrés et le fichier de Configuration d'exécution est mis à jour.

16

Configuration IP

Les adresses d'interface IP peuvent être configurées manuellement par l'utilisateur ou automatiquement via un serveur DHCP. Cette section fournit des informations sur la définition des adresses IP du périphérique, soit manuellement soit en faisant du périphérique un client DHCP.

Cette section couvre les sujets suivants :

Présentation

Si les trames géantes sont désactivées, la MTU pour le trafic L3 est limitée à 1 518 octets.

Si les trames géantes sont activées, la MTU pour le trafic L3 est limitée à 9 000 octets.

Le paramètre d'interface IPv4 par défaut du VLAN par défaut est *DHCPv4*. Cela signifie que le périphérique joue le rôle de client DHCPv4 et envoie une demande DHCPv4 lors de l'amorçage.

Si le périphérique reçoit une réponse DHCPv4 du serveur DHCPv4 (contenant une adresse IPv4), il envoie des paquets ARP (Address Resolution Protocol, protocole de résolution d'adresse) pour vérifier que cette adresse IP est unique. Si la réponse ARP indique que l'adresse IPv4 est déjà utilisée, le périphérique envoie le message DHCPDECLINE (Refus DHCP) au serveur DHCP répondu. Il envoie ensuite un nouveau paquet DHCPDISCOVER (Détection DHCP) pour relancer le processus.

Si le périphérique n'a reçu aucune réponse DHCPv4 au bout de 60 secondes, il continue à lancer des requêtes DHCPDISCOVER et utilise l'adresse IPv4 : 192.168.1.254/24.

Des collisions d'adresse IP se produisent lorsqu'une même adresse IP est utilisée par plusieurs périphériques sur un même sous-réseau IP. Les collisions d'adresse nécessitent une action de la part de l'administrateur sur le serveur DHCP et/ou sur les périphériques en conflit avec le périphérique.

Les règles d'affectation d'adresse IP pour le VLAN par défaut sont les suivantes :

- Si le périphérique est configuré avec une adresse IPv4 statique, il émet des requêtes DHCPv4 jusqu'à ce qu'il reçoive une réponse d'un serveur DHCPv4.
- Si l'adresse IP du périphérique change, ce dernier envoie des paquets ARP gratuits au VLAN correspondant pour rechercher les éventuelles collisions d'adresse IP. Cette règle s'applique également lorsque l'appareil revient à l'adresse IP par défaut.
- Le voyant d'état du système s'allume en vert lorsque le serveur DHCP envoie une nouvelle adresse IP unique. Si une adresse IP statique a été définie, la LED d'état du système s'allume également en vert. Ce voyant clignote pendant que l'appareil 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.

Le périphérique peut disposer de plusieurs adresses IP. Chaque adresse IP peut être affectée aux ports, LAG ou VLAN spécifiés. Ces adresses IP sont configurées sur les pages Interfaces IPv4 et Interfaces IPv6. Il est possible d'accéder au périphérique via toutes ses adresses IP à partir des interfaces correspondantes.

Aucune route prédéfinie par défaut n'est fournie. Vous devez définir un acheminement par défaut pour gérer le périphérique à distance. Toutes les passerelles par défaut affectées par DHCP sont stockées en tant que routes par défaut. De plus, vous pouvez définir manuellement des acheminements par défaut. Vous utilisez pour ce faire les pages Routes IPv4 statiques et Routes IPv6.

Dans ce guide, toutes les adresses IP configurées sur le périphérique ou qui lui sont affectées sont également appelées « adresses IP de gestion ».

Interface de bouclage

Présentation

L'interface de bouclage est une interface virtuelle dont l'état opérationnel est toujours actif. Si l'adresse IP qui est configurée sur cette interface virtuelle est utilisée comme adresse locale lors de la communication avec les applications IP distantes, la communication ne sera pas interrompue même si la route vers l'application distante a été modifiée.

L'état opérationnel de l'interface de bouclage est toujours actif. Définissez une adresse IP (IPv4 ou IPv6) sur celle-ci et utilisez cette adresse IP comme adresse IP locale pour la communication IP avec les applications IP distantes. La communication est maintenue tant que les applications distantes restent joignables à partir de n'importe quelle interface IP (sans bouclage) active du commutateur. En revanche, si l'adresse IP d'une interface IP est utilisée pour la communication avec des applications distantes, la communication est interrompue lorsque l'interface IP est arrêtée.

Une interface de bouclage ne prend pas en charge le pontage ; elle ne peut pas être membre d'un VLAN et aucun protocole Couche 2 ne peut être activé sur celui-ci.

L'identifiant de l'interface de liaison locale IPv6 est 1.

Configuration d'une interface de bouclage

Pour configurer une interface de bouclage IPv4, il suffit d'en ajouter une dans Interfaces IPv4.

Pour configurer une interface de bouclage IPv6, il suffit d'en ajouter une dans Adresses IPv6.

Interfaces et gestion IPv4

Cette section couvre les sujets suivants :

- Interfaces IPv4
- Routes IPv4 statiques
- Table des adresses IPv4
- Access Lists
- VRRP
- ARP
- Proxy ARP

- Relais UDP/Assistance IP
- Fureteur/Relais DHCP
- Serveur DHCP

Interfaces IPv4

Pour que vous puissiez gérer le périphérique à l'aide de l'utilitaire de configuration Web, vous devez définir et connaître l'adresse de gestion IPv4 du périphérique. L'adresse IP de l'appareil peut être configurée manuellement ou reçue automatiquement depuis un serveur DHCP.

La page Interface IPv4 permet de configurer les adresses IP pour la gestion des appareils. Cette adresse IP peut être configurée sur une interface de port, de LAG, de VLAN, de bouclage ou hors bande.

REMARQUE Le logiciel de l'appareil utilise un seul ID de VLAN (VID) pour chaque adresse IP configurée sur un port ou un LAG. Le périphérique utilise le premier VID non encore utilisé, à partir de 4 094.

Pour configurer des adresses IPv4 :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4** > **Interface IPv4**.

Pour activer le routage IPv4, cochez la case **Enable** (Activer).

ÉTAPE 2 Cliquez sur **Appliquer**. Le paramètre est enregistré dans le fichier Configuration d'exécution.

Les champs suivants sont affichés dans la table des interfaces IPv4 :

- **Interface** : unité/interface pour laquelle l'adresse IP est définie. Il peut également s'agir du port OOB.
- **IP Address Type** (Type d'adresse IP) – les options disponibles sont les suivantes :
  - *DHCP* : déterminée par le serveur DHCP.
  - *Statique* : saisie manuellement. Les interfaces statiques sont des interfaces non DHCP qui ont été créées par l'utilisateur.
  - *Default* (Par défaut) : adresse par défaut existant sur le périphérique par défaut avant toute configuration.
- **Adresse IP** : adresse IP configurée pour l'interface.
- **Masque** : masque d'adresse IP configuré.

- **État** : résultats de la vérification d'unicité de l'adresse IP.
  - *Tentative* : aucun résultat final pour la vérification d'unicité de l'adresse IP.
  - *Valide* : contrôle de collision d'adresse IP terminé ; aucune collision détectée.
  - *Dupliqué valide* : contrôle de collision d'adresse IP terminé ; une adresse IP en double a été détectée.
  - *Dupliqué* : doublon d'adresse IP détecté pour l'adresse IP par défaut.
  - *Retardé* : l'attribution de l'adresse IP est retardée de 60 secondes si le client DHCP est activé au démarrage afin de lui donner le temps de découvrir l'adresse DHCP.
  - *Non reçu* : concerne l'adresse DHCP. Lorsqu'un client DCHP démarre un processus de découverte, il attribue l'adresse IP factice 0.0.0.0 avant l'obtention de l'adresse réelle. Cette adresse factice a l'état « Non reçu ».

ÉTAPE 3 Cliquez sur **Ajouter**.

ÉTAPE 4 Sélectionnez l'un des champs suivants :

- **Interface** : sélectionnez le port, le port OOB, le LAG, le bouclage ou le VLAN comme interface associée à cette configuration IP, puis choisissez une interface dans la liste.
- **Type d'adresse IP** : sélectionnez l'une des options suivantes :
  - *Adresse IP dynamique* : recevez l'adresse IP depuis un serveur DHCP.
  - *Adresse IP statique* : saisissez l'adresse IP.

ÉTAPE 5 Si vous avez sélectionné **Adresse IP statique**, renseignez le champ **Masque** :

- **IP Address** (Adresse IP) : saisissez l'adresse IP de l'interface.
- **Masque de réseau** : masque IP pour cette adresse.
- **Longueur du préfixe** : longueur du préfixe IPv4.

ÉTAPE 6 Cliquez sur **Appliquer**. Les paramètres d'adresse IPv4 sont modifiés et écrits dans le fichier de Configuration d'exécution.

PRÉCAUTION Lorsque le système se trouve dans l'un des modes pile et comporte une unité principale de sauvegarde, Cisco recommande de configurer l'adresse IP en tant qu'adresse statique afin d'éviter toute déconnexion du réseau lors d'un basculement de l'unité principale de la pile. La raison est que lorsque l'unité principale/de sauvegarde prend le contrôle de la pile, en cas d'utilisation de DHCP, il se peut qu'elle reçoive une adresse IP différente de celle qui a été reçue par l'unité principale d'origine de la pile.

Routes IPv4 statiques

Cette page permet de configurer et d'afficher les routes IPv4 statiques sur le périphérique. Lors du routage du trafic, le saut suivant est déterminé à l'aide de l'algorithme LPM (Longest Prefix Match, correspondance avec le préfixe le plus long). L'adresse IPv4 d'une destination peut correspondre à plusieurs routes dans la table des routes IPv4 statiques. Le périphérique utilise l'acheminement qui correspond au masque de sous-réseau le plus élevé, c'est-à-dire au préfixe le plus long. Si plusieurs passerelles par défaut sont définies avec la même valeur métrique, c'est l'adresse IPv4 la plus basse parmi les passerelles par défaut configurées qui est utilisée.

Pour définir une route IP statique :

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

La table de routes IPv4 statiques s'affiche. Les champs suivants sont affichés pour chaque entrée :

- **Préfixe IP de destination** : préfixe de l'adresse IP de destination.
- **Longueur du préfixe** : longueur du préfixe de route IP pour l'adresse IP de destination.
- **Type de route** : indique s'il s'agit d'une route locale, de rejet ou distante.
- **Adresse IP du routeur de saut suivant** : adresse IP ou alias IP du saut suivant sur la route.
- **Paramètre** : coût de ce saut (valeur inférieure préférable).
- **Interface sortante** : interface sortante utilisée pour cette route.
- ID d'objet de suivi : (pris en charge uniquement par les appareils de la gamme 550) ID d'élément suivi IP SLA (Accord de niveau de service IP Cisco) associé à cette entrée. Ce champ et le suivant ne s'affichent qu'en présence d'un accord de niveau de service.
- **État du suivi** : (pris en charge uniquement par les appareils de la gamme 550) état de l'élément suivi : Actif ou Inactif.

REMARQUE La définition d'un ID d'élément suivi IP SLA pour une entrée de routage permet de vérifier la connectivité à un réseau distant via un saut suivant spécifique. En l'absence de connectivité, l'état de l'élément suivi sera Inactif et le routeur sera supprimé de la table de réacheminement (pour plus d'informations, consultez la section Configuration IP : SLA).

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les valeurs appropriées dans les champs suivants :

- **Préfixe IP de destination** : saisissez le préfixe d'adresse IP de la destination.
- **Masque** : sélectionnez l'un des éléments suivants, puis renseignez la valeur requise :
  - **Masque de réseau** : préfixe de la route IP pour l'IP de destination sous forme de masque (nombre de bits alloués à la route dans l'adresse réseau).
  - **Longueur du préfixe** : longueur du préfixe de la route IP pour l'IP de destination sous forme d'adresse IP.
- **Type d'acheminement** : sélectionnez le type d'acheminement approprié.
  - *Rejeter* : rejette l'acheminement indiqué et stoppe tout routage vers le réseau de destination via toutes les passerelles. Cela garantit l'élimination de toutes les trames qui arrivent avec l'IP de destination de cet acheminement. La sélection de cette valeur désactive les commandes suivantes : Adresse IP de saut suivant, Métrique et Suivi IP SLA.
  - *Distant* : indique que l'acheminement est un chemin distant.
- **Adresse IP du routeur de saut suivant** : saisissez l'adresse ou l'alias IP du saut suivant sur l'acheminement.

  REMARQUE Vous ne pouvez pas configurer d'acheminement statique via un sous-réseau IP à connexion directe dans lequel le périphérique obtient son adresse IP d'un serveur DHCP.
- **Métrique** : saisissez la distance administrative jusqu'au saut suivant. La plage est comprise entre 1 et 255.
- **Suivi IP SLA** : (uniquement pour les appareils de la gamme 550) sélectionnez cette option pour activer l'association de cette entrée avec élément suivi IP SLA. Ce champ et le suivant ne s'affichent qu'en présence d'un accord de niveau de service.
- **ID d'élément suivi** : (uniquement pour les appareils de la gamme 550) saisissez l'ID de l'élément. Ce champ et le suivant ne s'affichent qu'en présence d'un accord de niveau de service.

ÉTAPE 4 Cliquez sur **Appliquer**. La route IP statique est enregistrée dans le fichier de Configuration d'exécution.

Table des adresses IPv4

Voici comment afficher la table de réacheminement IPv4 :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4** > **Table de réacheminement IPv4**.

La table de réacheminement IPv4 s'affiche. Les champs suivants sont affichés pour chaque entrée :

- **Préfixe IP de destination** : préfixe de l'adresse IP de destination.
- **Longueur du préfixe** : préfixe de route IP pour la longueur de l'adresse IP de destination.
- **Type de route** : indique s'il s'agit d'une route locale, de rejet ou distante.
- **Adresse IP du routeur de saut suivant** : adresse IP du saut suivant.
- **Propriétaire de route** : il peut s'agir de l'une des options suivantes :
  - *Par défaut* : la route a été configurée par la configuration système par défaut.
  - *Statique* : la route a été créée manuellement.
  - *Dynamique* : la route a été créée par un protocole de routage IP.
  - *DHCP* : la route a été reçue d'un serveur DHCP.
  - *Directement connecté* : l'acheminement est un sous-réseau auquel l'appareil est connecté.
- **Paramètre** : coût de ce saut (valeur inférieure préférable).
- **Distance administrative** : distance administrative jusqu'au saut suivant (valeur inférieure préférable). Cette option ne concerne pas les routes statiques.
- **Interface sortante** : interface sortante utilisée pour cette route.

RIPv2

Reportez-vous à la section Configuration IP : RIPv2.

VRRP

Reportez-vous à la section Configuration IP : VRRP.

ARP

Le périphérique gère une table ARP (Address Resolution Protocol, protocole de résolution d'adresse) pour tous les périphériques connus résidant sur ses sous-réseaux IP à connexion directe. Un sous-réseau IP à connexion directe désigne un sous-réseau auquel une interface IPv4 du périphérique est connectée. Lorsque le périphérique doit envoyer/acheminer un paquet vers un périphérique local, il effectue une recherche dans la table ARP pour obtenir l'adresse MAC du périphérique en question. La table ARP contient à la fois des adresses statiques et des adresses dynamiques. Les adresses statiques sont configurées manuellement et n'ont pas de limite de validité. Le périphérique crée des adresses dynamiques à partir des paquets ARP qu'il reçoit. Les adresses dynamiques ont une durée de vie limitée, que vous configurez.

REMARQUE Les informations de mappage sont utilisées pour le routage, ainsi que pour le réacheminement du trafic généré.

Pour définir les tables ARP :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4** > **ARP**.

ÉTAPE 2 Saisissez les paramètres.

- **Délai d'expiration des entrées ARP** : saisissez la durée en secondes pendant laquelle les adresses dynamiques peuvent rester dans la table ARP. Les adresses dynamiques ne sont valides dans la table que pour la durée définie par Délai d'expiration des entrées ARP. Lorsqu'une adresse dynamique arrive à expiration, elle est supprimée de la table et doit être réapprise pour figurer à nouveau dans cette table.
- **Effacer les entrées de la table ARP** : sélectionnez le type des entrées ARP à effacer du système.
  - *Tout* : supprime immédiatement toutes les adresses statiques et dynamiques.
  - *Dynamique* : supprime immédiatement toutes les adresses dynamiques.
  - *Statique* : supprime immédiatement toutes les adresses statiques.
  - *Délai d'expiration normal* : supprime les adresses dynamiques en fonction de la durée de vie configurée pour les entrées ARP.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres globaux ARP sont écrits dans le fichier de Configuration d'exécution.

La table ARP contient les champs suivants :

- **Interface** : interface IPv4 du sous-réseau IP à connexion directe où réside le périphérique IP.
- **Adresse IP** : adresse IP du périphérique IP.

- **Adresse MAC** : adresse MAC du périphérique IP.
- **État** : indique si l'entrée a été saisie manuellement ou apprise de manière dynamique.

ÉTAPE 4 Cliquez sur **Ajouter**.

ÉTAPE 5 Configurez les paramètres suivants :

- **Version IP** : format d'adresse IP pris en charge par l'hôte. Seul IPv4 est pris en charge.
- **Interface** : vous pouvez configurer une interface IPv4 sur un port, un LAG ou un VLAN. Sélectionnez l'interface voulue dans la liste des interfaces IPv4 configurées sur le périphérique.
- **Adresse IP** : saisissez l'adresse IP du périphérique local.
- **Adresse MAC** : saisissez l'adresse MAC du périphérique local.

ÉTAPE 6 Cliquez sur **Appliquer**. L'entrée ARP est enregistrée dans le fichier de Configuration d'exécution.

Proxy ARP

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

REMARQUE La fonction de proxy ARP n'est disponible que lorsque le périphérique est en mode L3.

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

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

Pour activer le proxy ARP sur toutes les interfaces IP :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4** > **Proxy ARP**.

ÉTAPE 2 Sélectionnez **Proxy ARP** pour permettre au périphérique de répondre aux requêtes ARP concernant des nœuds distants avec l'adresse MAC du périphérique.

ÉTAPE 3 Cliquez sur **Appliquer**. Le proxy ARP est activé et le fichier de Configuration d'exécution est mis à jour.

Relais UDP/Assistance IP

En général, les commutateurs ne routent pas les paquets de diffusion IP d'un sous-réseau IP à un autre. Toutefois, cette fonction permet au périphérique de relayer des paquets de diffusion UDP spécifiques reçus de ses interfaces IPv4 vers des adresses IP de destination spécifiques.

Pour configurer le relais des paquets UDP reçus d'une interface IPv4 donnée vers un port UDP de destination particulier, ajoutez un relais UDP :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4** > **Relais UDP/Assistance IP**.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Sélectionnez l'**Interface IP source** vers laquelle le périphérique doit relayer les paquets de diffusion UDP sur la base du port de destination UDP configuré. L'interface choisie doit être l'une des interfaces IPv4 configurées sur le périphérique.

ÉTAPE 4 Saisissez le numéro du **port UDP de destination** des paquets que le périphérique doit relayer. Sélectionnez un port connu dans la liste déroulante ou cliquez sur la case d'option du port pour entrer le numéro manuellement.

ÉTAPE 5 Saisissez l'**adresse IP de destination** qui doit recevoir les paquets UDP relayés. Si ce champ contient 0.0.0.0, les paquets UDP sont éliminés. Si ce champ contient 255.255.255.255, des paquets UDP sont envoyés à toutes les interfaces IP.

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

Fureteur/Relais DHCP

Cette section couvre les sujets suivants :

- Présentation
- Propriétés
- Paramètres d'interface
- Interfaces validées de surveillance DHCP
- Base de données de liaison de surveillance DHCP

Présentation

Présentation de la surveillance DHCPv4

La surveillance DHCP est une méthode de sécurité qui empêche la réception de mauvais paquets de réponses DHCP et qui consigne les adresses DHCP. Pour ce faire, elle effectue une distinction entre les ports sécurisés ou non sécurisés du périphérique.

Un port sécurisé est un port qui est connecté à un serveur DHCP et qui est autorisé à attribuer des adresses DHCP. Les messages DHCP reçus sur des ports sécurisés peuvent transiter par le périphérique.

Un port non sécurisé est un port qui ne peut pas attribuer d'adresses DHCP. Par défaut, tous les ports sont considérés comme étant non sécurisés jusqu'à ce que vous déclariez le contraire (sur la page Paramètres d'interface).

Présentation du relais DHCPv4

Le relais DHCP relaye les paquets DHCP vers le serveur DHCP.

Le périphérique peut relayer les messages DHCP reçus de la part des VLAN ne disposant pas d'adresses IP. Dès que le relais DHCP est activé sur un VLAN sans adresse IP, l'option 82 est insérée automatiquement. Cette insertion se trouve dans le VLAN en question et n'influence pas la gestion globale de l'insertion de l'option 82.

Relais DHCP transparent

Si vous utilisez un relais DHCP transparent et un agent de relais DHCP externe, procédez comme suit :

- Activez la surveillance DHCP.
- Activez l'insertion de l'option 82.
- Désactivez le relais DHCP.

Dans le cas d'un relais DHCP standard :

- Activez le relais DHCP.
- Vous n'avez pas besoin d'activer l'insertion de l'option 82.

Option 82

L'option 82 (Option des informations sur l'agent de relais DHCP) transfère des informations sur le port et l'agent à un serveur DHCP central, en indiquant où une adresse IP attribuée se connecte physiquement au réseau.

L'objectif global de l'option 82 est d'aider le serveur DHCP à choisir le meilleur sous-réseau IP (groupe de réseaux) pour l'obtention d'une adresse IP.

Les options suivantes sont disponibles au niveau du périphérique :

- **Insertion DHCP :** ajoute des informations sur l'option 82 aux paquets qui ne disposent pas d'informations étrangères sur l'option 82.
- **Intercommunication DHCP :** transfère ou rejette des paquets DHCP qui contiennent des informations sur l'option 82 et qui proviennent de ports non sécurisés. Sur les ports sécurisés, les paquets DHCP contenant des informations sur l'option 82 sont toujours transférés.

La table suivante affiche le flux de paquets passant par le relais DHCP, la surveillance DHCP et les modules Option 82 :

Les cas suivants peuvent se présenter :

- Le client DHCP et le serveur DHCP sont connectés au même VLAN. Dans ce cas, un pontage standard transmet les messages DHCP entre le client et le serveur DHCP.
- Le client DHCP et le serveur DHCP sont connectés à des VLAN différents. Dans ce cas, seul le relais DHCP est en mesure de diffuser les messages DHCP entre le client et le serveur DHCP. Les messages DHCP de monodiffusion sont transmis par des routeurs standard. Par conséquent, si l'option DHCP Relay (Relais DHCP) est activée sur un VLAN sans adresse IP, un routeur externe est nécessaire.

Seul le relais DHCP relaye des messages DHCP vers un serveur DHCP.

Interactions entre la surveillance DHCPv4, le relais DHCPv4 et l'option 82

Les tableaux suivants décrivent le comportement du périphérique en fonction des différentes combinaisons entre surveillance DHCP, relais DHCP et option 82.

Vous découvrirez comment les paquets de requêtes DHCP sont traités quand la surveillance DHCP n'est pas activée et que le relais DHCP l'est.

	Relais DHCP VLAN avec adresse IP		Relais DHCP VLAN sans adresse IP	
	Le paquet arrive sans l'option 82	Le paquet arrive avec l'option 82	Le paquet arrive sans l'option 82	Le paquet arrive avec l'option 82
Insertion de l'option 82 désactivée	Le paquet est envoyé sans l'option 82	Le paquet est envoyé avec l'option 82 d'origine	Relais : insère l'option 82 Pont : l'option 82 n'est pas insérée	Relais : ignore le paquet Pont : le paquet est envoyé avec l'option 82 d'origine
Insertion de l'option 82 activée	Relais : le paquet est envoyé avec l'option 82 Pont : l'option 82 n'est pas envoyée	Le paquet est envoyé avec l'option 82 d'origine	Relais : le paquet est envoyé avec l'option 82 Pont : l'option 82 n'est pas envoyée	Relais : ignore le paquet Pont : le paquet est envoyé avec l'option 82 d'origine

Voici comment les paquets de requêtes DHCP sont traités quand la surveillance DHCP et le relais DHCP sont activés :

	Relais DHCP VLAN avec adresse IP		Relais DHCP VLAN sans adresse IP	
	Le paquet arrive sans l'option 82	Le paquet arrive avec l'option 82	Le paquet arrive sans l'option 82	Le paquet arrive avec l'option 82
Insertion de l'option 82 désactivée	Le paquet est envoyé sans l'option 82	Le paquet est envoyé avec l'option 82 d'origine	Relais : insère l'option 82 Pont : l'option 82 n'est pas insérée	Relais : ignore le paquet Pont : le paquet est envoyé avec l'option 82 d'origine

	Relais DHCP VLAN avec adresse IP		Relais DHCP VLAN sans adresse IP	
Insertion de l'option 82 activée	Relais : le paquet est envoyé avec l'option 82 Pont : l'option 82 est ajoutée (si le port est sécurisé, se comporte comme si la surveillance DHCP n'était pas activée)	Le paquet est envoyé avec l'option 82 d'origine	Relais : le paquet est envoyé avec l'option 82 Pont : l'option 82 est insérée (si le port est sécurisé, se comporte comme si la surveillance DHCP n'était pas activée)	Relais : ignore le paquet Pont : le paquet est envoyé avec l'option 82 d'origine

Voici comment les paquets de réponses DHCP sont traités quand la surveillance DHCP est désactivée :

	Relais DHCP VLAN avec adresse IP		Relais DHCP VLAN sans adresse IP	
	Le paquet arrive sans l'option 82	Le paquet arrive avec l'option 82	Le paquet arrive sans l'option 82	Le paquet arrive avec l'option 82
Insertion de l'option 82 désactivée	Le paquet est envoyé sans l'option 82	Le paquet est envoyé avec l'option 82 d'origine	Relais : ignore l'option 82 Pont : le paquet est envoyé sans l'option 82	Relais : 1. Si la réponse provient du périphérique, le paquet est envoyé sans l'option 82 2. Si la réponse ne provient pas du périphérique, le paquet est ignoré Pont : le paquet est envoyé avec l'option 82 d'origine
Insertion de l'option 82 activée	Le paquet est envoyé sans l'option 82	Relais : le paquet est envoyé sans l'option 82 Pont : le paquet est envoyé avec l'option 82	Relais : ignore l'option 82 Pont : le paquet est envoyé sans l'option 82	Relais : le paquet est envoyé sans l'option 82 Pont : le paquet est envoyé avec l'option 82

Voici comment les paquets de réponses DHCP sont traités quand la surveillance DHCP et le relais DHCP sont activés :

	Relais DHCP VLAN avec adresse IP		Relais DHCP VLAN sans adresse IP	
	Le paquet arrive sans l'option 82	Le paquet arrive avec l'option 82	Le paquet arrive sans l'option 82	Le paquet arrive avec l'option 82
Insertion de l'option 82 désactivée	Le paquet est envoyé sans l'option 82	Le paquet est envoyé avec l'option 82 d'origine	Relais : ignore l'option 82 Pont : le paquet est envoyé sans l'option 82	Relais 1. Si la réponse provient du périphérique, le paquet est envoyé sans l'option 82 2. Si la réponse ne provient pas du périphérique, le paquet est ignoré Pont : le paquet est envoyé avec l'option 82 d'origine
Insertion de l'option 82 activée	Le paquet est envoyé sans l'option 82	Le paquet est envoyé sans l'option 82	Relais : ignore l'option 82 Pont : le paquet est envoyé sans l'option 82	Le paquet est envoyé sans l'option 82

Base de données de liaison de surveillance DHCP

La surveillance DHCP crée une base de données (appelée base de données de liaison de surveillance DHCP) à partir des informations provenant des paquets DHCP entrant dans le périphérique via des ports sécurisés.

La base de données de liaison de surveillance DHCP contient les données suivantes : port d'entrée, VLAN d'entrée, adresse MAC du client et adresse IP du client le cas échéant.

La base de données de liaison de surveillance DHCP est également utilisée par les fonctionnalités de protection de la source IP et d'inspection ARP dynamique pour déterminer les sources légitimes des paquets.

Ports sécurisés DHCP

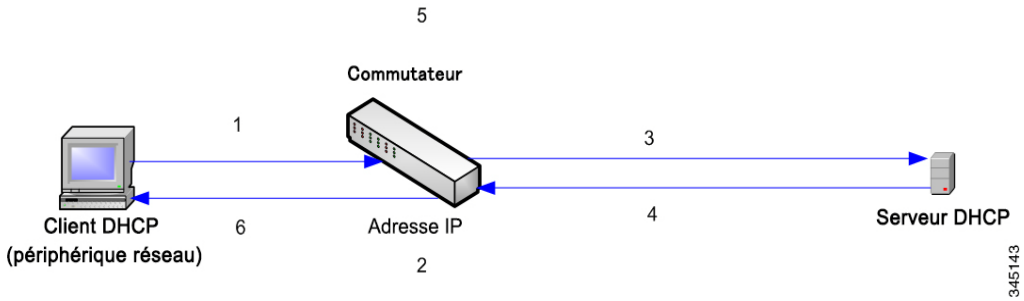
Les ports DHCP peuvent être sécurisés ou non sécurisés. Par défaut, tous les ports sont non sécurisés. Pour créer un port sécurisé, utilisez la page Paramètres d'interface. Les paquets transitant par ces ports sont automatiquement transférés. Les paquets passant par des ports sécurisés sont utilisés pour créer la base de données de liaison et sont gérés comme décrit ci-dessous.

Si la surveillance DHCP n'est pas activée, tous les ports sont sécurisés par défaut.

Création de la base de données de liaison de surveillance DHCP

Vous verrez ici comment le périphérique gère les paquets DHCP lorsque le client et le serveur DHCP sont sécurisés. La base de données de liaison de surveillance DHCP est créée dans le cadre de ce processus.

Traitement du paquet sécurisé DHCP



Voici la liste des actions entreprises :

ÉTAPE 1 Le périphérique envoie DHCPDISCOVER pour demander une adresse IP ou DHCPREQUEST pour accepter une adresse IP et la louer.

ÉTAPE 2 Le périphérique surveille le paquet et ajoute des informations IP-MAC à la base de données de liaison de surveillance DHCP.

ÉTAPE 3 Le périphérique transfère les paquets DHCPDISCOVER ou DHCPREQUEST.

ÉTAPE 4 Le serveur DHCP envoie un paquet DHCPOFFER pour proposer une adresse IP, DHCPACK pour en affecter une ou DHCPNAK pour rejeter la demande d'adresse.

ÉTAPE 5 Le périphérique surveille le paquet. Si une entrée correspondant au paquet existe dans la table de liaison de surveillance DHCP, le périphérique la remplace par la liaison IP-MAC à la réception de DHCPACK.

ÉTAPE 6 Le périphérique transfère DHCPOFFER, DHCPACK ou DHCPNAK.

Voici ci-dessous comment les paquets DHCP sont traités au niveau des ports sécurisés et non sécurisés. La base de données de liaison de surveillance DHCP est stockée dans la mémoire non volatile.

Traitement des paquets de surveillance DHCP

Type de paquet	Arrivée via une interface d'entrée non sécurisée	Arrivée via une interface d'entrée sécurisée
DHCPDISCOVER	Transfert vers des interfaces sécurisées uniquement.	Transfert vers des interfaces sécurisées uniquement.
DHCPOFFER	Filtre	Transfert du paquet en fonction des informations DHCP. Si l'adresse de destination est inconnue, le paquet est filtré.
DHCPREQUEST	Transfert vers des interfaces sécurisées uniquement.	Transfert vers des interfaces sécurisées uniquement.
DHCPACK	Filtre	Identique à DHCPOFFER et une entrée est ajoutée à la base de données de liaison de surveillance DHCP.
DHCPNAK	Filtre	Identique à DHCPOFFER Suppression de l'entrée le cas échéant.
DHCPDECLINE	Confirmation de la présence des informations dans la base de données. Si les informations existent et ne correspondent pas à l'interface sur laquelle le message a été reçu, le paquet est filtré. Sinon, le paquet est transmis aux interfaces sécurisées uniquement et l'entrée est supprimée de la base de données.	Transfert vers des interfaces sécurisées uniquement.

Type de paquet	Arrivée via une interface d'entrée non sécurisée	Arrivée via une interface d'entrée sécurisée
DHCPRELEASE	Identique à DHCPDECLINE	Identique à DHCPDECLINE
DHCPINFORM	Transfert vers des interfaces sécurisées uniquement.	Transfert vers des interfaces sécurisées uniquement.
DHCPLEASEQUERY	Filtre	Transfert

Surveillance DHCP avec relais DHCP

Si la surveillance et le relais DHCP sont activés globalement, alors si la surveillance DHCP est active sur le VLAN du client, les règles de surveillance DHCP stockées dans la base de données de liaison de surveillance DHCP sont appliquées et cette base de données est mise à jour sur le VLAN du serveur DHCP et du client pour les paquets relayés.

Configuration DHCP par défaut

Vous découvrirez ici les options par défaut de la surveillance et du relais DHCP.

Option	État par défaut
Surveillance DHCP	Désactivée
Insertion de l'option 82	Désactivée
Intercommunication de l'option 82	Désactivée
Vérifier l'adresse MAC	Activé
Base de données de liaison de surveillance DHCP de secours	Désactivée
Relais DHCP	Désactivé

Configuration du workflow DHCP

Pour configurer le relais et la surveillance DHCP :

ÉTAPE 1 Activez l'option DHCP Snooping (Surveillance DHCP) et/ou l'option DHCP Relay (Relais DHCP) sur la page Propriétés.

ÉTAPE 2 Définissez les interfaces sur lesquelles la surveillance DHCP est activée sur la page Paramètres d'interface.

ÉTAPE 3 Configurez les interfaces comme étant sécurisées ou non sécurisées sur la page *Interfaces validées de surveillance DHCP*.

ÉTAPE 4 Facultatif. Ajoutez des entrées à la base de données de liaison de surveillance DHCP sur la page Base de données de liaison de surveillance DHCP.

Propriétés

Pour configurer le relais DHCP, la surveillance DHCP et l'option 82 :

ÉTAPE 1 Cliquez sur **Configuration IP > Interfaces et gestion IPv4 > Surveillance/Relais DHCP > Propriétés**.

Renseignez les champs suivants :

- **Option 82**—Sélectionnez **Option 82** pour insérer des informations sur cette option dans les paquets.
- **Relais DHCP** : sélectionnez cette option pour activer le relais DHCP.
- **État de la surveillance DHCP** : sélectionnez cette option pour activer la surveillance DHCP.
- **Option 82 Pass Through** : sélectionnez cette option pour conserver les informations étrangères sur l'option82 lors du transfert de paquets.
- **Vérifier l'adresse MAC** : sélectionnez cette option pour vérifier que l'adresse MAC source de l'en-tête de couche 2 correspond à l'adresse matérielle du client telle qu'elle apparaît dans l'en-tête DHCP (partie de la capacité utile) sur les ports DHCP non sécurisés.
- **Base de données de secours** : sélectionnez cette option pour sauvegarder la base de données de liaison de surveillance DHCP sur la mémoire Flash du périphérique.

ÉTAPE 2 Cliquez sur **Appliquer**. Les paramètres sont consignés dans le fichier de Configuration d'exécution.

ÉTAPE 3 Pour définir un serveur DHCP, cliquez sur **Ajouter**.

ÉTAPE 4 Saisissez l'adresse IP du serveur DHCP et cliquez sur **Appliquer**. Les paramètres sont consignés dans le fichier de Configuration d'exécution.

Paramètres d'interface

Le relais et la surveillance DHCP peuvent être activés sur toutes les interfaces et sur tous les VLAN. Pour qu'un relais DHCP soit fonctionnel, une adresse IP doit être configurée sur le VLAN ou sur une interface.

Pour activer la surveillanceou le relais DHCP sur des interfaces spécifiques :

ÉTAPE 1 Cliquez sur **Configuration IP > Interfaces et gestion IPv4 > Surveillance/Relais DHCP > Paramètres d'interface.**

ÉTAPE 2 Pour activer le relais ou la surveillance DHCP sur une interface, cliquez sur **Ajouter**.

ÉTAPE 3 Sélectionnez l'interface et les fonctionnalités à activer : **Relais DHCP** ou **Surveillance** ou les deux.

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

Interfaces validées de surveillance DHCP

Les paquets provenant de ports ou LAG non sécurisés sont contrôlés par rapport à la base de données de liaison de surveillance DHCP (reportez-vous à la page Base de données de liaison de surveillance DHCP).

Par défaut, les interfaces sont sécurisées.

Pour désigner une interface non sécurisée :

ÉTAPE 1 Cliquez sur **Configuration IP > Interfaces et gestion IPv4 > Surveillance/Relais DHCP > Interfaces validées de surveillance DHCP**.

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

ÉTAPE 3 Sélectionnez **Interface sécurisée** (**Oui** ou **Non**).

ÉTAPE 4 Cliquez sur **Appliquer** pour enregistrer les paramètres dans le fichier de configuration de fonctionnement.

Base de données de liaison de surveillance DHCP

Consultez la section Création de la base de données de liaison de surveillance DHCP pour savoir comment les entrées dynamiques sont ajoutées à la base de données de liaison de surveillance DHCP.

Veuillez noter les points suivants au sujet de la maintenance de la base de données de liaison de surveillance DHCP :

- Le périphérique ne met pas à jour la base de données de liaison de surveillance DHCP lorsqu'une station est déplacée vers une autre interface.
- Si un port est en panne, les entrées de ce port ne sont pas supprimées.
- Lorsque la surveillance DHCP est désactivée pour un VLAN, les entrées de liaison recueillies pour ce VLAN sont supprimées.
- Si la base de données est pleine, la surveillance DHCP continue de transférer des paquets, mais aucune nouvelle entrée n'est créée. Notez que si la protection de la source IP et/ou l'inspection ARP sont activées, les clients qui ne sont pas inscrits dans la base de données de liaison de surveillance DHCP ne peuvent pas se connecter au réseau.

Pour ajouter des entrées à la base de données de liaison de surveillance DHCP :

ÉTAPE 1 Cliquez sur **Configuration IP > Interfaces et gestion IPv4** > **Surveillance/Relais DHCP > Base de données de liaison de surveillance DHCP**.

Pour afficher un sous-ensemble des entrées de la base de données de liaison de surveillance DHCP, saisissez les critères de recherche appropriés dans le filtre et cliquez sur **OK**.

Les champs de la base de données de liaison de surveillance DHCP sont affichés. Ils sont décrits sur la page **Add** (Ajouter), à l'exception du champ **IP Source Guard** (Protection de la source IP) :

- **Statut :**
  - *Actif* : la fonction Protection de la source IP est active sur le périphérique.
  - *Inactif* : la fonction Protection de la source IP n'est pas active sur le périphérique.
- **Motif :**
  - *Sans problème*
  - *Sans ressource*
  - *Sans VLAN de surveillance*
  - *Confiance de port*

ÉTAPE 2 Pour ajouter une entrée, cliquez sur **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants :

- **ID du VLAN** : VLAN sur lequel le paquet est attendu.
- **Adresse MAC** : adresse MAC du paquet.
- **Adresse IP** : adresse IP du paquet.
- **Interface** : l'unité/le logement/l'interface qui doit réceptionner le paquet.
- **Type** : ce champ peut prendre les valeurs suivantes :
  - *Dynamique* : l'entrée a une durée de bail limitée.
  - *Statique* : l'entrée a été configurée pour être statique.
- **Durée de bail** : si l'entrée est dynamique, saisissez la durée pendant laquelle l'entrée doit être active dans la base de données DHCP. (S'il n'y a pas de durée de bail, choisissez Infini.)

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

Serveur DHCP

Cette section couvre les sujets suivants :

Présentation

La fonction du serveur DHCPv4 vous permet de configurer le périphérique en tant que serveur DHCPv4. Un serveur DHCPv4 sert à attribuer une adresse IPv4 et d'autres informations à un autre périphérique (client DHCP).

Le serveur DHCPv4 attribue des adresses IPv4 à partir d'un groupe d'adresses IPv4 défini par l'utilisateur.

Les modes suivants sont possibles :

- **Static Allocation (Allocation statique)** : l'adresse matérielle ou l'identifiant client d'un hôte est mappée manuellement sur une adresse IP. Cette opération s'effectue sur la page Hôtes statiques.
- **Dynamic Allocation (Allocation dynamique)** : un client obtient une adresse IP allouée pour une certaine durée (qui peut être illimitée). Si le client DHCP ne renouvelle pas l'adresse IP allouée, cette adresse IP expire à la fin de cette durée et le client doit faire une nouvelle demande d'adresse IP. Cela s'effectue sur la page Groupe de réseaux.

Dépendances entre les fonctions

- Il est impossible de configurer à la fois un serveur DHCP et un client DHCP sur le système : si une interface est activée en tant que client DHCP, vous ne pourrez pas activer un serveur DHCP global.
- Lorsque le relais DHCPv4 est activé, il est impossible de configurer le périphérique en tant que serveur DHCP.

Configurations et paramètres par défaut

- Le périphérique n'est pas configuré comme serveur DHCPv4 par défaut.
- Lorsque le périphérique est activé comme serveur DHCPv4, aucun groupe d'adresses réseau n'est défini par défaut.

Flux de travail d'activation de la fonction serveur DHCP

Pour configurer le périphérique en tant que serveur DHCPv4 :

ÉTAPE 1 Activez le périphérique comme serveur DHCP via la page Propriétés.

ÉTAPE 2 Si vous ne souhaitez pas affecter certaines adresses IP, configurez-les à l'aide de la page Excluded Addresses (Adresses exclues).

ÉTAPE 3 Définissez jusqu'à 16 groupes d'adresses IP réseau à l'aide de la page Groupe de réseaux.

ÉTAPE 4 Configurez les clients auxquels attribuer une adresse IP permanente à l'aide de la page Static Hosts (Hôtes statiques).

ÉTAPE 5 Configurez les options DHCP requises sur la page Options DHCP. Vous pouvez y définir les valeurs à renvoyer pour chaque option DHCP appropriée.

ÉTAPE 6 Ajoutez une interface IP dans la plage de l'un des groupes DHCP sur la page Groupe de réseaux. Le périphérique répond aux requêtes DHCP depuis cette interface IP. Par exemple, si la plage du groupe est 1.1.1.1 -1.1.1.254, ajoutez une adresse IP contenue dans cette plage pour que les clients directement connectés reçoivent une adresse IP du groupe configuré.

Effectuez cette opération sur la page Interfaces IPv4.

ÉTAPE 7 Affichez les adresses IP attribuées à l'aide de la page Address Binding (Liaison d'adresses). Les adresses IP peuvent être supprimées sur cette page.

Propriétés

Pour configurer le périphérique en tant que serveur DHCPv4 :

ÉTAPE 1 Cliquez sur **Configuration IP** >**Interfaces et gestion IPv4** > **Serveur DHCP > Propriétés** pour afficher la page Propriétés.

ÉTAPE 2 Sélectionnez **Activer** pour configurer le périphérique comme serveur DHCP.

ÉTAPE 3 Cliquez sur **Appliquer**. Le périphérique fonctionne immédiatement en tant que serveur DHCP. Toutefois, il n'attribue les adresses IP aux clients qu'une fois un groupe créé.

Groupe de réseaux

Lorsqu'un périphérique est utilisé comme serveur DHCP, il faut définir un ou plusieurs groupes d'adresses IP à partir desquels le périphérique attribuera les adresses IP aux clients DHCP. Chaque groupe de réseaux comporte une plage d'adresses appartenant à un sous-réseau spécifique. Ces adresses sont attribuées à différents clients dans ce sous-réseau.

Lorsqu'un client demande une adresse IP, le périphérique utilisé en tant que serveur DHCP attribue une adresse IP selon les éléments suivants :

- **Directly-attached Client** (Client à connexion directe) : le périphérique attribue une adresse du groupe de réseaux dont le sous-réseau correspond à celui configuré sur l'interface IP du périphérique à partir duquel la demande DHCP a été reçue.

  Si le message est arrivé directement (et non via le relais DHCP), le groupe est un groupe local qui appartient à l'un des sous-réseaux IP définis sur l'interface d'entrée de couche 2. Dans ce cas, le masque IP du groupe équivaut au masque IP de l'interface IP et les adresses IP minimum et maximum du groupe appartiennent au sous-réseau IP.

- **Remote Client** (Client distant) : le périphérique prend une adresse IP du groupe de réseaux avec le sous-réseau IP correspondant à l'adresse IP de l'agent de relais DHCP.

  Si le message est arrivé via le relais DHCP, l'adresse utilisée appartient au sous-réseau IP spécifié par l'adresse IP minimum et le masque IP du groupe. Il s'agit alors d'un groupe distant.

Vous pouvez définir jusqu'à 16 groupes de réseaux.

Pour créer un groupe d'adresses IP et définir leurs durées de bail :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4** > **Serveur DHCP** > **Groupes de réseaux**.

Les groupes réseau précédemment définis s'affichent. Ces champs sont décrits ci-dessous sur la page **Ajouter**. Le champ suivant est affiché (mais pas décrit sur la page **Ajouter**) :

- **Nombre d'adresses louées** : nombre d'adresses du groupe qui ont été attribuées (louées).

ÉTAPE 2 Cliquez sur **Ajouter** pour définir un nouveau groupe réseau. Remarque : vous pouvez renseigner soit les champs Subnet IP Address (Adresse IP de sous-réseau) et Masque soit les champs Masque, Address Pool Start (Début de groupe d'adresses) et Address Pool End (Fin de groupe d'adresses).

ÉTAPE 3 Renseignez les champs suivants :

- **Pool Name (Nom du groupe)** : saisissez le nom du groupe.
- **Subnet IP Address (Adresse IP de sous-réseau)** : saisissez le sous-réseau où réside le groupe réseau.
- **Masque** : saisissez l'une des informations suivantes :
  - *Masque réseau* : vérifiez et saisissez le masque réseau du groupe.
  - *Longueur du préfixe* : vérifiez et saisissez le nombre de bits compris dans le préfixe de l'adresse.
- **Address Pool Start (Début de groupe d'adresses)** : saisissez la première adresse IP dans la plage du groupe de réseaux.
- **Address Pool End (Fin de groupe d'adresses)** : saisissez la dernière adresse IP dans la plage du groupe réseau.
- **Durée de bail** : saisissez sur quelle durée un client DHCP peut utiliser l'adresse IP de ce groupe. Vous pouvez configurer une durée de bail jusqu'à 49 710 jours ou une durée illimitée.
  - *Infini* : la durée du bail n'est pas limitée.
  - *Jours* : durée du bail en jours. Ce délai doit être compris entre 0 et 49 710 jours.
  - *Heures* : durée du bail en heures. Vous devez tout d'abord remplir le champ Jours avant de pouvoir renseigner les heures.
  - *Minutes* : durée du bail en minutes. Vous devez tout d'abord remplir les champs Jours et Heures avant de pouvoir renseigner les minutes.

- **Adresse IP de routeur par défaut (option 3)** : saisissez le routeur par défaut pour le client DHCP.
- **Adresse IP de serveur de noms de domaines (option 6)** : sélectionnez l'un des serveurs DNS du périphérique (s'il est déjà configuré) ou sélectionnez **Autre** etsaisissez l'adresse IP du serveur DNS accessible au client DHCP.
- **Nom de domaine (option 15)** : saisissez le nom de domaine pour un client DHCP.
- **Adresse IP de serveur NetBIOS WINS (option 44)** : saisissez le serveur de nom NetBIOS WINS disponible pour un client DHCP.
- **Type de nœud NetBIOS (option 46)** : sélectionnez la façon de résoudre le nom NetBIOS. Les types de nœud suivants sont valides :
  - *Hybride* : une combinaison hybride de nœud frontière et de nœud périphérique est utilisée. Lorsque vous configurez l'utilisation du nœud hybride, un ordinateur tente toujours le nœud périphérique d'abord puis ensuite le nœud frontière, si le nœud périphérique échoue. Il s'agit de la valeur par défaut.
  - *Mixte* : une combinaison de communications de nœud frontière et de nœud périphérique est utilisée pour enregistrer et résoudre les noms NetBIOS. Le nœud mixte utilise d'abord le nœud frontière puis ensuite, si nécessaire, le nœud périphérique. Il est préférable de ne pas choisir le nœud mixte pour des réseaux plus grands car sa préférence pour les diffusions de nœud frontière augmente le trafic réseau.
  - *Peer-to-Peer (Homologue)* : les communications point à point avec le serveur de nom NetBIOS sont utilisées pour enregistrer et traduire les noms d'ordinateur en adresses IP.
  - *Broadcast (Diffusion)* : les messages de diffusion IP Broadcast sont utilisés pour enregistrer et traduire les noms NetBIOS en adresses IP.
- **Adresse IP du serveur SNTP (option 4)** : sélectionnez l'un des serveurs DNS du périphérique (s'il est déjà configuré) ou sélectionnez **Autre** et saisissez l'adresse IP du serveur de temps pour le client DHCP.
- **Adresse IP du serveur de fichiers (siaddr)** : saisissez l'adresse IP du serveur TFTP/SCP à partir duquel le fichier de configuration est téléchargé.
- **Nom d'hôte du serveur de fichier (sname/option 66)** : saisissez le nom du serveur TFTP/SCP.
- **Nom du fichier de configuration (fichier/option 67)** : saisissez le nom du fichier utilisé comme fichier de configuration.

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

Adresses exclues

Par défaut, le serveur DHCP suppose que toutes les adresses du groupe peuvent être attribuées aux clients. Il est possible d'exclure une seule adresse IP ou une plage d'adresses IP. Les adresses exclues sont exclues de tous les groupes DHCP.

Pour définir une plage d'adresses exclues :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4** > **Serveur DHCP** > **Adresses exclues**.

Les adresses IP précédemment définies s'affichent.

ÉTAPE 2 Pour ajouter une plage d'adresses IP à exclure, cliquez sur **Ajouter** et renseignez les champs :

- **Adresse IP de début** : première adresse IP dans la plage des adresses IP exclues.
- **End IP Address (Adresse IP de fin)** : dernière adresse IP dans la plage des adresses IP exclues.

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

Hôtes statiques

Vous souhaitez peut-être allouer une adresse IP permanente qui ne change jamais à certains clients DHCP. Le client est alors connu en tant qu'hôte statique.

Vous pouvez définir un maximum de 120 hôtes statiques.

Pour attribuer manuellement une adresse IP permanente à un client spécifique :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4** > **Serveur DHCP** > **Hôtes statiques**.

Les hôtes statiques s'affichent. Les champs affichés sont décrits dans la page Ajouter, sauf celui-ci :

- **Identifiant de client/d'adresse MAC**.

ÉTAPE 2 Pour ajouter un hôte statique, cliquez sur **Ajouter**, puis renseignez les champs suivants :

- **Adresse IP** : saisissez l'adresse IP qui a été attribuée de façon statique à l'hôte.
- **Nom d'hôte** : saisissez le nom de l'hôte qui peut être une chaîne de symboles et un entier.

- **Masque** : saisissez le masque de réseau de l'hôte statique.
  - *Masque réseau* : vérifiez et saisissez le masque réseau de l'hôte statique.
  - *Longueur du préfixe* : vérifiez et saisissez le nombre de bits compris dans le préfixe de l'adresse.
- **Type d'identifiant** : saisissez comment identifier l'hôte statique spécifique.
  - *Identifiant de client* : saisissez une identification unique du client spécifié dans une notation hexadécimale, comme : 01b60819681172.

ou :

  - *Adresse MAC* : saisissez l'adresse MAC du client.

  Saisissez l'identifiant de client ou l'adresse MAC, en fonction du type sélectionné.
- **Nom du client** : saisissez le nom de l'hôte statique à l'aide d'un jeu de caractères ASCII standard. Le nom du client ne doit pas contenir le nom de domaine.
- **Adresse IP de routeur par défaut (option 3)** : saisissez le routeur par défaut pour l'hôte statique.
- **Adresse IP de serveur de noms de domaines (option 6)** : sélectionnez l'un des serveurs DNS du dispositif (s'il est déjà configuré) ou sélectionnez **Autre** etsaisissez l'adresse IP du serveur DNS accessible au client DHCP.
- **Nom de domaine Option 15** : saisissez le nom de domaine pour l'hôte statique.
- **Adresse IP de serveur NetBIOS WINS (option 44)** : saisissez le serveur de nom NetBIOS WINS disponible pour l'hôte statique.
- **Type de nœud NetBIOS (option 46)** : sélectionnez la façon de résoudre le nom NetBIOS. Les types de nœud suivants sont valides :
  - *Hybride* : une combinaison hybride de nœud frontière et de nœud périphérique est utilisée. Lorsque vous configurez l'utilisation du nœud hybride, un ordinateur tente toujours le nœud périphérique d'abord puis ensuite le nœud frontière, si le nœud périphérique échoue. Il s'agit de la valeur par défaut.
  - *Mixte* : une combinaison de communications de nœud frontière et de nœud périphérique est utilisée pour enregistrer et résoudre les noms NetBIOS. Le nœud mixte utilise d'abord le nœud frontière puis ensuite, si nécessaire, le nœud périphérique. Il est préférable de ne pas choisir le nœud mixte pour des réseaux plus grands car sa préférence pour les diffusions de nœud frontière augmente le trafic réseau.

- *Peer-to-Peer (Homologue)* : les communications point à point avec le serveur de nom NetBIOS sont utilisées pour enregistrer et traduire les noms d'ordinateur en adresses IP.
- *Broadcast (Diffusion)* : les messages de diffusion IP Broadcast sont utilisés pour enregistrer et traduire les noms NetBIOS en adresses IP.

- **Adresse IP du serveur SNTP (option 4)** : sélectionnez l'un des serveurs DNS du périphérique (s'il est déjà configuré) ou sélectionnez **Autre** et saisissez l'adresse IP du serveur de temps pour le client DHCP.
- **Adresse IP du serveur de fichiers (siaddr)** : saisissez l'adresse IP du serveur TFTP/SCP à partir duquel le fichier de configuration est téléchargé.
- **Nom d'hôte du serveur de fichier (sname/option 66)** : saisissez le nom du serveur TFTP/SCP.
- **Nom du fichier de configuration (fichier/option 67)** : saisissez le nom du fichier utilisé comme fichier de configuration.

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

Options DHCP

Lorsque le périphérique fonctionne en tant que serveur DHCP, les options DHCP peuvent être configurées par l'intermédiaire de l'option HEX. Une description de ces options est disponible dans RFC2131.

La configuration de ces options détermine la réponse envoyée aux clients DHCP dont les paquets incluent une demande (via l'option 55) pour les options DHCP configurées.

Exemple : l'option DHCP 66 est configurée avec le nom d'un serveur TFTP sur la page Options DHCP. Lorsqu'un paquet DHCP du client est reçu et qu'il contient l'option 66, le serveur TFTP est renvoyé en tant que valeur de l'option 66.

Pour configurer une ou plusieurs options DHCP :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4** > **Serveur DHCP** > **Options DHCP**.

Les options DHCP précédemment configurées sont affichées.

ÉTAPE 2 Pour configurer une option qui n'a pas encore été configurée, renseignez le champ :

- **Nom de groupe de serveurs DHCP égal à** : sélectionnez l'un des groupes d'adresses réseau définis sur la page Groupe de réseaux.

ÉTAPE 3 Cliquez sur **Ajouter** et renseignez les champs :

- **Nom du groupe** : affiche le nom du groupe pour lequel le code est en cours de définition.
- **Code** : saisissez le code d'option DHCP.
- **Type** : les cases d'option de ce champ changent en fonction du type du paramètre d'options DHCP. Sélectionnez l'un des codes suivants, puis entrez la valeur du paramètre d'options DHCP :
  - *Hex* : sélectionnez cet élément si vous souhaitez saisir la valeur hexadécimale du paramètre pour l'option DHCP. Une valeur hexadécimale peut être fournie à la place de tout autre type de valeur. Par exemple, vous pouvez spécifier une valeur hexadécimale d'une adresse IP au lieu de l'adresse IP elle-même.

    Aucune validation de la valeur hexadécimale n'est effectuée. Par conséquent, si vous entrez une valeur hexadécimale qui représente une valeur incorrecte, aucune erreur n'est fournie et le client est susceptible de ne pas pouvoir traiter le paquet DHCP à partir du serveur.
  - *IP* : sélectionnez cette option pour saisir une adresse IP si elle est adaptée à l'option DHCP sélectionnée.
  - *Liste IP* : saisissez la liste des adresses IP en les séparant par une virgule.
  - *Entier* : sélectionnez cette option afin de saisir une valeur entière du paramètre pour l'option DHCP sélectionnée.
  - *Booléen* : sélectionnez cette option si le paramètre de l'option DHCP sélectionnée est Booléen.
- **Valeur booléenne** : si le type est Booléen, sélectionnez la valeur à renvoyer : **True** ou **False**.
- **Valeur** : si le type n'est pas Booléen, saisissez la valeur à envoyer pour ce code.
- **Description** : saisissez une description à des fins de documentation.

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

Liaison d'adresse

Utilisez la page Address Binding (Liaison d'adresses) pour afficher et supprimer les adresses IP attribuées par le périphérique ainsi que leurs adresses MAC correspondantes.

Pour afficher et/ou supprimer les liaisons d'adresses :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4** > **Serveur DHCP** > **Liaison d'adresse**.

Les champs suivants pour les liaisons d'adresses s'affichent :

- **Adresse IP** : adresses IP des clients DHCP.
- **Type d'adresse** : indique si l'adresse du client DHCP apparaît comme une adresse MAC ou à l'aide de l'identificateur de client.
- **Adresse MAC/Identificateur de clients** : identification unique du client spécifiée comme adresse MAC ou dans une notation hexadécimale ; par exemple : 01b60819681172.
- **Lease Expiration (Expiration du bail)** : date et heure d'expiration du bail de l'adresse IP de l'hôte ou Infini si la durée du bail a été définie ainsi.
- **Type** : manière dont l'adresse IP a été attribuée au client. Les options possibles sont les suivantes :
  - *Statique* : l'adresse matérielle de l'hôte a été mappée sur une adresse IP.
  - *Dynamique* : l'adresse IP obtenue de façon dynamique du périphérique appartient au client pour une durée spécifiée. L'adresse IP expire à la fin de cette durée et le client doit demander une autre adresse IP.
- **État** : les options disponibles sont les suivantes :
  - *Allocated (Attribuée)* : l'adresse IP a été attribuée. Lorsqu'un hôte statique est configuré, son état est attribué.
  - *Declined (Refusée)* : l'adresse IP a été fournie mais pas acceptée. Elle n'est donc pas attribuée.
  - *Expired (Expirée)* : le bail de l'adresse IP a expiré.
  - *Pre-Allocated (Préattribuée)* : une entrée a l'état Préattribuée entre le moment où elle est fournie et le moment où le ACK (accusé de réception) DHCP est envoyé par le client. Elle devient alors attribuée.

ÉTAPE 2 Cliquez sur **Supprimer**. Le fichier de configuration d'exécution est mis à jour.

Interfaces et gestion IPv6

Cette section couvre les sujets suivants :

Présentation

Internet Protocol version 6 (IPv6) est un protocole de couche réseau utilisé dans les communications entre réseaux à commutation de paquets. IPv6 a été conçu pour remplacer IPv4, le protocole Internet le plus souvent déployé.

IPv6 apporte davantage de souplesse dans l'affectation des adresses IP car la taille des adresses passe de 32 à 128 bits. Les adresses IPv6 sont constituées de huit groupes de quatre chiffres hexadécimaux, par exemple FE80:0000:0000:0000:0000:9C00:876A:130B. La forme abrégée, dans laquelle un groupe de zéros peut être ignoré et remplacé par « :: », est également admise. Exemple : ::FE80::9C00:876A:130B.

Les nœuds IPv6 nécessitent un mécanisme de mappage intermédiaire pour communiquer avec d'autres nœuds IPv6 sur un réseau uniquement IPv4. Ce mécanisme, appelé tunnel, permet à des hôtes uniquement IPv6 de contacter des services IPv4, ainsi qu'à des hôtes et réseaux IPv6 isolés de contacter un nœud IPv6 sur une infrastructure IPv4.

La fonction de tunneling utilise un mécanisme ISATAP ou manuel (reportez-vous à la section Tunnel IPv6). La fonction Tunneling considère le réseau IPv4 comme une liaison locale IPv6 virtuelle, avec des mappages entre chaque adresse IPv4 et une adresse IPv6 de liaison locale.

Le périphérique détecte les trames IPv6 d'après le type IPv6 Ethertype.

Comme lors du routage IPv4, les trames adressées à l'adresse MAC du périphérique mais à une adresse IPv6 non connue du périphérique sont transférées au périphérique de saut suivant. Ce périphérique peut être la station finale cible ou un routeur plus près de la destination. Le mécanisme de transfert s'appuie sur la nouvelle création d'une trame L2 autour du paquet L3 reçu (essentiellement) inchangé avec l'adresse MAC du périphérique de saut suivant comme adresse MAC de destination.

Le système utilise les messages de routage statique et de découverte des voisins (similaires aux messages ARP IPv4) pour créer les tables de transferts et les adresses de saut suivant appropriées.

Un acheminement définit le chemin entre deux périphériques en réseau. Les entrées de routage ajoutées par l'utilisateur sont statiques et sont utilisées par le système jusqu'à ce qu'elles soient supprimées par l'utilisateur. Elles ne sont pas affectées par les protocoles de routage. Si les routes statiques doivent être actualisées, cette procédure doit être effectuée explicitement par l'utilisateur. La responsabilité d'empêcher les boucles de routage dans le réseau incombe à l'utilisateur.

Les acheminements IPv6 statiques peuvent être soit :

- À connexion directe : la destination est directement connectée à une interface sur le périphérique et la destination de paquets (l'interface) est ainsi utilisée comme adresse de saut suivant.
- Récursifs : où uniquement le saut suivant est spécifié et l'interface sortante est dérivée du saut suivant.

De la même manière, les adresses MAC des périphériques de saut suivant (y compris les systèmes finaux à connexion directe) sont automatiquement dérivées à l'aide de la découverte du réseau. Cependant, l'utilisateur peut remplacer et compléter cela en ajoutant manuellement les entrées à la table des voisins.

Configuration globale IPv6

Pour définir des paramètres IPv6 globaux et les paramètres de client DHCPv6 :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv6** > **Configuration globale IPv6**.

ÉTAPE 2 Saisissez les valeurs appropriées dans les champs suivants :

- **Routage IPv6** : sélectionnez cette option pour activer le routage IPv6. Lorsque cette option n'est pas activée, le périphérique agit comme hôte (et non comme routeur) ; il peut ainsi recevoir des paquets de gestion mais il ne peut pas les transférer. Lorsque le routage est activé, le périphérique peut transférer les paquets IPv6.

  Si vous activez le routage IPv6, les adresses précédemment attribuées à l'interface de l'appareil via la configuration automatique seront supprimées de l'annonce envoyée par un routeur sur le réseau.

- **Intervalle de limites de débit ICMPv6** : saisissez la fréquence à laquelle les messages d'erreur ICMP sont générés.

- **Taille des cases de limite de débit ICMPv6** : saisissez le nombre maximal de messages d'erreur ICMP que le périphérique peut envoyer dans chaque intervalle.

- **Limite de saut IPv6** : saisissez le nombre maximal de routeurs intermédiaires qu'un paquet peut traverser pour atteindre sa destination finale. Chaque fois qu'un paquet est transféré à un autre routeur, la limite de saut est réduite. Lorsque la limite de saut devient zéro, le paquet est ignoré. Cela empêche un transfert infini des paquets.

- **Paramètres de client DHCPv6**

  - *Unique Identifier (DUID) Format (Format de l'identificateur unique (DUID))* : il s'agit de l'identificateur du client DHCP utilisé par le serveur DHCP pour localiser le client. Les formats suivants sont disponibles :

    Link-Couche (Couche de liaison) : (par défaut). Si vous sélectionnez cette option, l'adresse MAC du périphérique est utilisée.

    Enterprise Number (Numéro d'entreprise) : lorsque vous sélectionnez cette option, renseignez les champs suivants.

  - *Enterprise Number (Numéro d'entreprise)* : numéro d'entreprise privé enregistré par les fournisseurs comme géré par IANA.

  - *Identifier (Identificateur)* : chaîne hexadécimale définie par le fournisseur (jusqu'à 64 caractères hexadécimaux). Si le nombre de caractères est impair, un zéro est ajouté à droite. Vous pouvez ajouter un point ou une virgule tous les deux caractères hexadécimaux pour les séparer.

- **DHCPv6 Unique Identifier (DUID) (Identificateur unique DHCPv6 (DUID))** : affiche l'identificateur sélectionné.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres globaux IPv6 et les paramètres de client DHCPv6 sont mis à jour.

Interfaces IPv6

Vous pouvez configurer l'interface IPv6 sur un port, un LAG, un VLAN, une interface de bouclage ou un tunnel.

Contrairement aux autres types d'interfaces, une interface de tunnel est d'abord créée sur la page Tunnel IPv6, puis l'interface IPv6 est configurée sur le tunnel sur cette page.

Pour définir une interface IPv6 :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv6** > **Interfaces IPv6**.

ÉTAPE 2 Saisissez les paramètres.

- **IPv6 Link Local Default Zone** (Zone de liaison locale IPv6 par défaut) : sélectionnez cette option pour activer une zone par défaut. Il s'agit d'une interface à utiliser pour sortir un paquet de liaison locale arrivant sans interface spécifiée ou avec sa zone 0 par défaut.
- **IPv6 Link Local Default Zone Interface** (Interface de la zone de liaison locale IPv6 par défaut) : sélectionnez une interface à utiliser comme zone par défaut. Il peut s'agir d'un tunnel précédemment défini ou d'une autre interface.

ÉTAPE 3 Cliquez sur **Appliquer** pour configurer la zone par défaut.

La Table des interfaces IPv6 est affichée en plus du champ suivant :

- **Type de tunnel** : manuel, 6 vers 4 et ISATAP.

ÉTAPE 4 Cliquez sur **Ajouter** pour ajouter une nouvelle interface sur laquelle IPv6 est activé.

ÉTAPE 5 Renseignez les champs suivants :

- **Interface IPv6** : sélectionnez une unité, un port, un LAG, une interface de bouclage ou un VLAN spécifique pour l'adresse IPv6.

ÉTAPE 6 Pour configurer l'interface comme client DHCPv6, ce qui signifie activer l'interface pour recevoir des informations depuis le serveur DHCPv6, comme la configuration SNTP et des informations DNS, renseignez les champs **Client DHCPv6** :

- **Client DHCPv6** : sélectionnez cette option pour activer le client DHCPv6 sur l'interface (avec ou sans état).
- **Commentaire rapide** : sélectionnez cette option pour activer l'utilisation du système d'échange à deux messages pour l'allocation d'adresse et la configuration d'autres paramètres. Si cette option est activée, le client inclut l'option d'envoi rapide dans un message de sollicitation.
- **Minimum Information Refresh Time (Intervalle minimal d'actualisation des informations)** : cette valeur est utilisée pour mettre une limite sur la valeur de l'intervalle d'actualisation. Lorsque le serveur envoie une option d'intervalle d'actualisation inférieure à cette valeur, cette valeur est utilisée en substitution. Sélectionnez **Infini** (aucune actualisation sauf si le serveur envoie cette option) ou **Défini par l'utilisateur** pour définir une valeur.
- **Information Refresh Time (Intervalle d'actualisation des informations)** : cette valeur indique la fréquence d'actualisation par le périphérique des informations reçues du serveur DHCPv6. Si cette option n'est pas reçue du serveur, la valeur entrée ici est utilisée. Sélectionnez **Infini** (aucune actualisation sauf si le serveur envoie cette option) ou **Défini par l'utilisateur** pour définir une valeur.

ÉTAPE 7 Pour configurer des paramètres IPv6 supplémentaires, renseignez les champs suivants :

- **Configuration automatique d'adresses IPv6** : sélectionne la configuration automatique des adresses à partir des annonces de routeur envoyées par des voisins.
- **Nombre de tentatives DAD** : saisissez le nombre de messages de sollicitation des voisins consécutifs à envoyer lors du processus DAD (Duplicate Address Detection, détection des adresses en double) sur les adresses IPv6 Unicast de l'interface. DAD vérifie l'unicité d'une nouvelle adresse IPv6 Unicast avant de l'attribuer. Les nouvelles adresses restent à l'état provisoire pendant la vérification DAD. Saisissez **0** dans ce champ pour désactiver le traitement de détection des adresses en double sur l'interface indiquée. Saisissez **1** dans ce champ pour indiquer une transmission unique, sans transmission de suivi.
- **Envoyer des messages ICMPv6** : active la génération de messages concernant les destinations injoignables.
- **Version MLD** : version MLD IPv6.
- **Redirections IPv6** : sélectionnez cette option pour activer l'envoi des messages de redirection ICMP IPv6. Ces messages permettent d'informer les autres périphériques de ne pas envoyer du trafic à ce périphérique, mais plutôt à un autre périphérique.

ÉTAPE 8 Cliquez sur **Appliquer** pour activer le traitement IPv6 sur l'interface sélectionnée. Pour les interfaces IPv6 standard, les adresses suivantes sont configurées automatiquement :

- Adresse de liaison locale, à l'aide de l'ID d'interface au format EUI-64, sur la base de l'adresse MAC d'un périphérique
- Toutes les adresses de multidiffusion de liaison locale des nœuds (FF02::1)
- Adresse multidestination du nœud sollicité (au format FF02::1:FFXX:XXXX)

ÉTAPE 9 Appuyez sur le bouton **Restart (Redémarrer)** pour lancer l'actualisation des informations sans état reçues du serveur DHCPv6.

ÉTAPE 10 Cliquez sur **Table des adresses IPv6** pour affecter manuellement des adresses IPv6 à l'interface, si nécessaire. Cette page est décrite à la section Adresses IPv6.

ÉTAPE 11 Pour ajouter un tunnel, sélectionnez une interface (définie en tant que tunnel sur la page Interfaces IPv6) dans la table des tunnels IPv6 et cliquez sur **Table de tunnels IPv6**. Reportez-vous à la section Tunnel IPv6.

Détails du client DHCPv6

Le bouton **Détails** affiche les informations reçues sur l'interface à partir d'un serveur DHCPv6.

Cette option est activée lorsque l'interface sélectionnée est définie comme client DHCPv6 sans état.

Lorsque vous appuyez sur ce bouton, les champs suivants s'affichent (pour les informations reçues du serveur DHCP) :

- **DHCP Operational Mode** (Mode de fonctionnement DHCP) : permet d'afficher Enabled (Activé) lorsque les conditions suivantes sont remplies :
  - L'interface est active.
  - IPv6 y est activé.
  - Le client DHCPv6 y est activé.
- **État de service avec état** : précise si le client reçoit des informations de configuration avec état d'un serveur DHCP.
- **État de service sans état** : précise si le client reçoit des informations de configuration sans état depuis un serveur DHCP.
- **Adresse IPv6 IA NA** : l'ID IA a une valeur de balise C/IANAID, T1-C/T1, T2, - C/T2,. T1 et T2 sont disponibles lorsqu'au moins une adresse est reçue sur l'interface.

- **Adresse du serveur DHCP** : adresse du serveur DHCPv6.
- **DUID du serveur DHCP** : identificateur unique du serveur DHCPv6.
- **DHCP Server Preference** (Préférence du serveur DHCP) : priorité de ce serveur DHCPv6.
- **Intervalle minimal d'actualisation des informations** : voir ci-dessus.
- **Intervalle d'actualisation des informations** : voir ci-dessus.
- **Received Information Refresh Time (Intervalle reçu pour l'actualisation des informations)** : intervalle d'actualisation reçu du serveur DHCPv6.
- **Remaining Information Refresh Time (Intervalle restant avant l'actualisation des informations)** : temps restant jusqu'à la prochaine actualisation.
- **DNS Servers (Serveurs DNS)** : liste des serveurs DNS reçue du serveur DHCPv6.
- **DNS Domain Search List (Liste de recherche de domaines DNS)** : liste des domaines reçue du serveur DHCPv6.
- **SNTP Servers (Serveurs SNTP)** : liste des serveurs SNTP reçue du serveur DHCPv6.
- **POSIX Timezone String (Chaîne de fuseau horaire POSIX)** : fuseau horaire reçu du serveur DHCPv6.
- **Configuration Server (Serveur de configuration)** : serveur contenant un fichier de configuration reçu du serveur DHCPv6.
- **Configuration Path Name (Nom du chemin de configuration)** : chemin vers le fichier de configuration sur le serveur de configuration reçu du serveur DHCPv6.

Tunnel IPv6

Les tunnels permettent la transmission des paquets IPv6 sur des réseaux IPv4. Chaque tunnel a une adresse IPv4 source et s'il s'agit d'un tunnel manuel, il dispose également d'une adresse IPv4 de destination. Le paquet IPv6 est encapsulé entre ces adresses.

Tunnels ISATAP

le dispositif prend en charge un seul tunnel ISATAP (Intra-Site Automatic Tunnel Addressing Protocol).

Un tunnel ISATAP est un tunnel point-multipoint. L'adresse source est l'adresse IPv4 (ou l'une des adresses IPv4) du périphérique.

Lors de la configuration d'un tunnel ISATAP, l'adresse IPv4 de destination est fournie par le routeur. Remarque :

- Une adresse IPv6 de liaison locale est affectée à l'interface ISATAP. L'adresse IP initiale est affectée à l'interface, qui est alors activée.
- Si une interface ISATAP est active, l'adresse IPv4 du routeur ISATAP est résolue via DNS à l'aide d'un mappage ISATAP-à-IPv4. Si l'enregistrement DNS ISATAP n'est pas résolu, le mappage nom d'hôte-à-adresse ISATAP est recherché dans la table de mappage des hôtes.
- S'il est impossible de résoudre l'adresse IPv4 du routeur ISATAP à l'aide du processus DNS, l'interface IP ISATAP reste active. Le système ne comportera un routeur par défaut pour le trafic ISATAP qu'après résolution du processus DNS.

Types de tunnels supplémentaires

Vous pouvez configurer les types de tunnels ci-dessous sur l'appareil :

- **Tunnel manuel**
  - Une adresse IPv6 de liaison locale est affectée à l'interface ISATAP. L'adresse IP initiale est affectée à l'interface, qui est alors activée.
  - Si une interface ISATAP est active, l'adresse IPv4 du routeur ISATAP est résolue via DNS à l'aide d'un mappage ISATAP-à-IPv4. Si l'enregistrement DNS ISATAP n'est pas résolu, le mappage nom d'hôte-à-adresse ISATAP est recherché dans la table de mappage des hôtes.
  - S'il est impossible de résoudre l'adresse IPv4 du routeur ISATAP à l'aide du processus DNS, l'interface IP ISATAP reste active. Le système ne comportera un routeur par défaut pour le trafic ISATAP qu'après résolution du processus DNS.

  Il s'agit d'une définition point à point. Lors de la création d'un tunnel manuel, vous pouvez saisir l'adresse IP source (l'une des adresses IP du périphérique) et l'adresse IPv4 de destination.
- **Tunnel 6to4**

  Le type 6to4 est un mécanisme de tunnellisation automatique qui utilise le réseau IPv4 sous-jacent comme couche de liaison multi-accès hors diffusion pour IPv6. Un seul tunnel 6to4 est pris en charge sur un dispositif.

  Le tunnel 6to4 est seulement pris en charge lorsque le réacheminement IPv6 est pris en charge.

  La multidiffusion IPv6 n'est pas prise en charge sur l'interface de tunnel 6to4.

Le commutateur crée automatiquement un préfixe lié 2002::/16 sur le tunnel 6to4. La route 2002::/16 connectée sur le tunnel est ajoutée à la table de routage suite à la création du préfixe lié.

Lorsque le mode tunnel passe de 6to4 à un autre mode, le préfixe lié et les routes connectées sont supprimés.

Si l'interface sortante du saut suivant est le tunnel 6to4, l'adresse IPv4 du nœud de saut suivant est extraite du préfixe 2002:WWXX:YYZZ::/48 de l'adresse IPv6 du saut suivant IPv6, s'il s'agit d'une adresse globale, et des 32 derniers bits de l'identifiant d'interface de l'adresse IPv6 du saut suivant IPv6, s'il s'agit d'une adresse de liaison locale.

Ce tableau indique les tunnels compatibles avec les différents périphériques :

Type du tunnel	Sx350	SG350x	SG350XG	SG550X	SG550XG
ISATAP	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge
Manuel	Non pris en charge	Non pris en charge	Mode natif Pris en charge – jusqu'à 16 tunnels Non pris en charge avec une pile hybride.	Jusqu'à 16 tunnels (au total)	Jusqu'à 16 tunnels (au total)
Tunnel 6to4 automatique	Non pris en charge	Non pris en charge	Mode natif 1 tunnel 4 vers 6 (avec jusqu'à 16 tunnels au total) Pile Hybride : Non pris en charge.	1 tunnel 4 vers 6 (avec jusqu'à 16 tunnels au total)	1 tunnel 4 vers 6 (avec jusqu'à 16 tunnels au total)

Configuration des tunnels

Pour configurer un tunnel IPv6 :

ÉTAPE 1 Cliquez sur **Configuration IP > Interfaces et gestion IPv6 > Tunnel IPv6**.

ÉTAPE 2 Saisissez les paramètres ISATAP.

- **Intervalle de sollicitation ISATAP** : nombre de secondes entre deux messages de sollicitation de routeur ISATAP, si aucun routeur ISATAP actif n'a été détecté. Il peut s'agir de la **Valeur par défaut** ou d'un intervalle **Défini par l'utilisateur**.
- **Robustesse ISATAP** : permet de calculer l'intervalle des requêtes de sollicitation de routeur. Plus la valeur est élevée, plus les requêtes sont fréquentes. Il peut s'agir de la **Valeur par défaut** ou d'un intervalle **Défini par l'utilisateur**.

REMARQUE Le tunnel ISATAP ne sera pas opérationnel si l'interface IPv4 sous-jacente n'est pas active.

REMARQUE Les tunnels manuels 6 vers 4 sont réservés au dispositif SG350XG et à la gamme Sx 550. Pour ces dispositifs, la page affiche la **Table de tunnels IPv6** qui présente et permet de créer et de configurer des tunnels IPv6 tunnels (voir les étapes ci-dessous).

Le Sx350 et le Sx350X prennent uniquement en charge les tunnels ISATAP. Pour ces appareils, le tunnel ISATAP est configuré en cliquant sur le bouton **Créer un tunnel ISATAP** et en saisissant les informations pour les champs **Adresse IPv4 source** et **Nom du routeur ISATAP**. Consultez les explications suivantes pour ces champs.

ÉTAPE 3 Renseignez les champs suivants :

- **Nom du tunnel** : sélectionnez un numéro de tunnel.
- **Tunnel Type** (Type du tunnel) : sélectionnez un type de tunnel : Manuel, 6 vers 4 et ISATAP.
- **État du tunnel (appelé État sur la page principale)** : sélectionnez cette option pour activer le tunnel. Si ce tunnel est fermé ultérieurement, cette indication figure dans ce champ.
- **Interceptions SNMP d'état de lien** : sélectionnez cette option pour activer la génération d'une interception lorsque l'état de la liaison d'un port a été changé. Si vous ne souhaitez pas recevoir d'interceptions (traps) sur des ports spécifiques (par exemple, ISP nécessite seulement des interceptions sur les ports connectés à son infrastructure et ne requiert aucune interception pour les ports connectés à l'équipement de l'utilisateur), cette fonction peut être désactivée.
- **Source (appelé Type de source sur la page principale)** : affiche l'une des options suivantes :
  - *Auto* : sélectionne automatiquement l'adresse IPv4 la plus basse parmi toutes ses interfaces IPv4 configurées comme adresse source pour les paquets envoyés sur l'interface de tunnel.

    Si cette adresse IPv4 la plus basse est supprimée de l'interface (effacée ou déplacée vers une autre interface), l'adresse IPv4 minimale suivante est sélectionnée comme adresse IPv4 locale.
  - *Adresse IPv4* : saisissez l'adresse IPv4 de l'interface utilisée comme adresse source pour le tunnel.
  - *Interface* : sélectionnez l'interface dont l'adresse IPv4 est utilisée comme adresse source du tunnel.

    La page principale contient une colonne nommée Adresse source. Voici l'adresse IP sélectionnée compte tenu de la sélection effectuée ci-dessus.

- **Destination** : (pour le tunnel manuel uniquement) sélectionnez l'une des options suivantes pour spécifier l'adresse de destination du tunnel :
  - *Nom d'hôte* : nom DNS de l'hôte distant.
  - *Adresse IPv4* : adresse IPv4 de l'hôte distant.
- **Nom de routeur ISATAP** : (pour les tunnels ISATAP uniquement) sélectionnez l'une des options suivantes pour configurer une chaîne globale qui représente un nom de domaine de routeur de tunnel automatique spécifique.
  - *Valeurs par défaut* : il s'agit toujours d'ISATAP.
  - *Défini par l'utilisateur* : saisissez le nom de domaine du routeur.

ÉTAPE 4 Cliquez sur **Appliquer**. Le tunnel est enregistré dans le fichier de Configuration d'exécution.

REMARQUE Avec les appareils des gammes 350XG et 550, pour arrêter un tunnel, cliquez sur **Modifier** et décochez l'option **État du tunnel**. Pour désactiver les interceptions, cliquez sur **Modifier** et décochez l'option **Interceptions SNMP d'état de liaison**.

Adresses IPv6

Pour affecter une adresse IPv6 à une interface IPv6 :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv6** > **Adresses IPv6**.

ÉTAPE 2 Pour filtrer la table, sélectionnez un nom d'interface et cliquez sur **OK**. L'interface s'affiche dans la table des adresses IPv6. Ces champs sont définis sur la page Ajouter, excepté les champs suivants :

- **Source de l'adresse** : affiche l'un des types de sources d'adresse suivants : DHCP, Système ou Statique.
- **État DAD** : indique l'état DAD et précise si l'option Détection d'accès en double est activée ou non.
- **Durée de vie souhaitée** : affiche l'entrée Durée de vie souhaitée.
- **Durée de vie valide** : affiche l'entrée Durée de vie valide.
- **Délai d'expiration** : affiche le délai d'expiration.

ÉTAPE 3 Cliquez sur **Ajouter**.

ÉTAPE 4 Saisissez les valeurs des champs.

- **Interface IPv6** : affiche l'interface sur laquelle l'adresse IPv6 doit être définie. Si un astérisque (*) s'affiche, cela signifie que l'interface IPv6 n'est pas activée mais a été configurée.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 à ajouter.
  - *Liaison locale* : une adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : une adresse IPv6 qui est de type global IPV6 monodiffusion, visible et joignable à partir d'autres réseaux.
  - *Pluridiffusion* : l'adresse IPv6 est une adresse de pluridiffusion. Il s'agit d'une adresse attribuée à un ensemble d'interfaces appartenant généralement à des nœuds différents. Un paquet envoyé à une adresse pluridiffusion est délivré à l'interface la plus proche (comme défini par les protocoles de routage utilisés) identifiée par l'adresse pluridiffusion.

  REMARQUE La pluridiffusion ne peut pas être utilisée si l'adresse IPv6 se trouve sur une interface ISATAP.
- **Adresse IPv6**outre les adresses de liaison locale et de multidiffusion par défaut, le périphérique ajoute aussi automatiquement des adresses globales à l'interface en fonction des annonces de routeur qu'il reçoit. Le périphérique prend en charge un maximum de 128 adresses sur l'interface. Chaque adresse doit correspondre à une adresse IPv6 valide, spécifiée au format hexadécimal au moyen de valeurs de 16 bits séparées par le signe deux-points.

  Vous pouvez ajouter les types d'adresses suivants aux différents types de tunnels :
  - *Tunnels manuels* : adresse globale ou de pluridiffusion
  - *Tunnels ISATAP* : adresse globale avec EUI-6
  - *Tunnels 6to4* : aucun
- **Longueur du préfixe** : la longueur du préfixe IPv6 global est une valeur comprise entre 0 et 128 qui indique le nombre de bits contigus les plus significatifs de l'adresse dont est composé le préfixe (la partie réseau de l'adresse).
- **EUI-64** : sélectionnez cette option pour employer le paramètre EUI-64 afin d'identifier la portion de l'adresse IPv6 globale correspondant à l'ID d'interface en utilisant le format EUI-64 sur la base de l'adresse MAC d'un périphérique.

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

Configuration du routeur IPv6

Les sections suivantes décrivent comment configurer les routeurs IPv6. Il couvre les sujets suivants :

- Annonce de routeur
- Préfixes IPv6

Annonce de routeur

Les routeurs IPv6 peuvent annoncer leur préfixes aux périphériques voisins. Cette fonction peut être activée ou supprimée par interface, comme suit :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv6** > **Configuration du routeur IPv6 > Annonce de routeur**.

ÉTAPE 2 Pour configurer une interface présente dans la table des annonces du routeur, sélectionnez l'interface souhaitée et cliquez sur **Modifier**.

ÉTAPE 3 Renseignez les champs suivants :

- **Suppress Router Advertisement (Supprimer l'annonce du routeur)** : sélectionnez **Oui** pour supprimer les transmissions des annonces du routeur IPv6 sur l'interface. Si cette fonction n'est pas supprimée, saisissez les champs suivants :
- **Préférence de routeur** : sélectionnez **Faible**, **Moyenne** ou **Élevée** comme valeur de préférence pour le routeur. Les messages d'annonce du routeur sont envoyés avec la préférence configurée dans ce champ. Si aucune préférence n'est configurée, ils sont envoyés avec une préférence moyenne.

L'association d'une préférence avec un routeur est utile lorsque, par exemple, deux routeurs sur une liaison fournissent un routage équivalent mais à des coûts différents et que la politique prévoit que les hôtes doivent préférer l'un des routeurs.

- **Include Advertisement Interval Option (Inclure l'option d'intervalle d'annonce)** : permet d'indiquer qu'une option d'annonce est utilisée par le système. Cette option indique à un nœud mobile en visite l'intervalle dans lequel il peut s'attendre à recevoir des annonces de routeur. Le nœud peut utiliser ces informations dans son algorithme de détection de mouvement.
- **Hop Limit (Limite de saut)** : valeur annoncée par le routeur. Si la valeur n'est pas de zéro, elle est utilisée comme limite de saut par l'hôte.
- **Managed Address Configuration Flag (Indication de configuration d'adresses gérées)** : cette indication permet d'indiquer aux hôtes connectés qu'ils doivent utiliser la configuration automatique avec conservation d'état pour obtenir des adresses. Les hôtes peuvent utiliser simultanément la configuration automatique avec et sans conservation d'état.

- **Other Stateful Configuration Flag (Indication de configuration d'autres informations avec conservation d'état)** : cette indication permet d'indiquer aux hôtes connectés qu'ils doivent utiliser la configuration automatique avec conservation d'état pour obtenir d'autres informations (outre l'adresse).

  REMARQUE Si Managed Address Configuration Flag (Indication de configuration d'adresses gérées) est définie, un hôte connecté peut utiliser la configuration automatique avec conservation d'état pour obtenir les autres informations (outre l'adresse), indépendamment de la définition de cette indication.

- **Neighbor Solicitation Retransmissions Interval (Intervalle de retransmission de sollicitations de voisinage)** : spécifiez cet intervalle pour déterminer le temps entre les retransmissions des messages de sollicitation de voisinage lorsque vous traduisez l'adresse ou sondez l'accessibilité d'un voisin.

- **Maximum Router Advertisement Interval (Intervalle d'annonce maximal de routeur)** : saisissez le temps maximal qui peut s'écouler entre deux annonces de routeur.

L'intervalle entre deux transmissions doit être inférieur ou égal à la durée de vie de l'annonce de routeur IPv6 si vous configurez l'acheminement en tant que routeur par défaut à l'aide de cette commande. Afin d'éviter la synchronisation avec d'autres nœuds IPv6, l'intervalle réel utilisé est sélectionné de manière aléatoire parmi les valeurs comprises entre les valeurs minimale et maximale.

- **Minimum Router Advertisement Interval (Intervalle d'annonce minimal de routeur)** : saisissez le temps minimal qui peut s'écouler entre deux annonces de routeur (**Défini par l'utilisateur**) ou sélectionnez **Valeurs par défaut** afin d'utiliser la valeur par défaut du système.

  REMARQUE L'intervalle minimal d'annonce de routeur ne peut jamais excéder 75 % de l'intervalle maximal d'annonce de routeur et ne peut pas être inférieur à 3 secondes.

- **Router Advertisement Lifetime (Durée de vie d'annonce de routeur)** : saisissez le temps restant, en secondes, durant lequel ce routeur continue à fonctionner en tant que routeur par défaut. La valeur zéro signifie que le routeur ne fonctionne plus en tant que routeur par défaut.

- **Délai d'accessibilité** : saisissez le temps pendant lequel le nœud IPv6 distant est considéré comme joignable (en millisecondes) (**Défini par l'utilisateur**) ou sélectionnez l'option **Valeurs par défaut** afin d'utiliser la valeur par défaut du système.

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

Préfixes IPv6

Pour définir des préfixes à annoncer sur les interfaces du périphérique :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv6** > **Configuration du routeur IPv6 > Préfixes IPv6**.

ÉTAPE 2 Si nécessaire, activez le champ **Filtre** et cliquez sur **OK**. Le groupe d'interfaces correspondant au filtre s'affiche.

ÉTAPE 3 Pour ajouter une interface, cliquez sur **Ajouter**.

ÉTAPE 4 Sélectionnez l'interface IPv6 requise sur laquelle un préfixe doit être ajouté.

ÉTAPE 5 Renseignez les champs suivants :

- **Prefix Address (Adresse de préfixe)** : réseau IPv6. La forme de cet argument doit être celle indiquée dans RFC 4293 où l'adresse est composée de caractères hexadécimaux, utilisant des valeurs de 16 bits entre les caractères deux-points.
- **Prefix Length** (Longueur du préfixe) : longueur du préfixe IPv6. Une valeur décimale qui indique le nombre de bits contigus les plus significatifs de l'adresse dont se compose le préfixe (la partie réseau de l'adresse). Une barre oblique doit précéder la valeur décimale.
- **Annonce de préfixe** : sélectionnez cette option pour annoncer ce préfixe.
- **Valid Lifetime (Durée de vie valide)** : durée restante, en secondes, de validité de ce préfixe, elle correspond au temps qui précède son annulation. L'adresse générée à partir d'un préfixe annulé ne doit pas apparaître en tant qu'adresse de source ou de destination d'un paquet.
  - *Infini* : sélectionnez cette valeur pour renseigner ce champ avec la valeur 4 294 967 295, qui représente l'infini.
  - *Défini par l'utilisateur* : saisissez une valeur.
- **Durée de vie préférée** : la durée restante, en secondes, durant laquelle ce préfixe continue à être prioritaire. Une fois ce temps écoulé, le préfixe ne doit plus être utilisé en tant qu'adresse source dans une nouvelle communication mais, les paquets reçus sur cette interface sont traités comme prévu. La durée de vie préférée ne doit pas être supérieure à la durée de vie valide.
  - *Infini* : sélectionnez cette valeur pour renseigner ce champ avec la valeur 4 294 967 295, qui représente l'infini.
  - *Défini par l'utilisateur* : saisissez une valeur.

- **Configuration automatique** : cette option permet d'activer la configuration automatique des adresses IPv6 à l'aide de la configuration automatique sans conservation d'état sur une interface et d'activer le traitement IPv6 sur cette interface. Les adresses sont configurées en fonction des préfixes reçus dans les messages Annonce de routeur.
- **Prefix Status (État de préfixe)** : sélectionnez l'une des options suivantes :
  - *On-link* : cette option permet de configurer le préfixe spécifié en tant que On-link. Les nœuds qui envoient du trafic aux adresses contenant le préfixe spécifié considèrent la destination comme localement joignable sur la liaison. Un préfixe On-link est inséré dans la table de routage en tant que préfixe connecté (défini par un bit L).
  - *No Onlink* (Non On-link) : cette option permet de configurer le préfixe spécifié en tant que Non On-link. Un préfixe Non On-link est inséré dans la table de routage en tant que préfixe connecté mais annoncé avec un bit L vide.
  - *Offlink (Off-link)* : cette option permet de configurer le préfixe spécifié en tant que Off-link. Le préfixe est annoncé avec un bit L vide. Le préfixe n'est pas inséré dans la table de routage en tant que préfixe connecté. Si le préfixe existe déjà dans la table de routage en tant que préfixe connecté (par exemple, parce que le préfixe a aussi été configuré en ajoutant une adresse IPv6), il est supprimé.

ÉTAPE 6 Cliquez sur **Appliquer** pour enregistrer la configuration dans le fichier de Configuration d'exécution.

Liste des routeurs IPv6 par défaut

La page Liste des routeurs par défaut IPv6 vous permet de configurer et d'afficher les adresses de routeur IPv6 par défaut. Cette liste contient les routeurs susceptibles de devenir le routeur par défaut du périphérique pour le trafic non local (elle peut être vide). Le périphérique sélectionne un routeur au hasard dans la liste. Le périphérique prend en charge un seul routeur IPv6 statique par défaut. Les routeurs dynamiques par défaut sont des routeurs qui ont envoyé des annonces de routeur à l'interface IPv6 du périphérique.

Lorsque vous ajoutez ou supprimez des adresses IP, les événements suivants se produisent :

- Lorsque vous supprimez une interface IP, toutes les adresses IP de routeur par défaut sont supprimées. Il est impossible de supprimer des adresses IP dynamiques.
- Un message d'alerte apparaît lorsque vous tentez d'insérer plusieurs adresses définies par l'utilisateur.
- Un message d'alerte apparaît lorsque vous tentez d'insérer une adresse d'un type autre qu'une liaison locale « fe80: ».

Pour définir un routeur par défaut :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv6** > **Liste des routeurs IPv6 par défaut**.

Cette page affiche les champs suivants pour chaque routeur par défaut :

- **Interface sortante** : interface IPv6 sortante où réside le routeur par défaut.
- **Adresse IPv6 du routeur par défaut** : adresse IP de liaison locale du routeur par défaut.
- **Type** : configuration du routeur par défaut qui inclut les options suivantes :
  - *Statique* : le routeur par défaut a été ajouté manuellement à cette table à l'aide du bouton **Ajouter**.
  - *Dynamique* : le routeur par défaut a été configuré de manière dynamique.
- **Métrique** : coût de ce saut.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un routeur par défaut statique.

ÉTAPE 3 Renseignez les champs suivants :

- **Type du prochain saut** : adresse IP de la destination suivante vers laquelle le paquet est envoyé. Vous disposez des possibilités suivantes :
  - *Global* : une adresse IPv6 qui est de type global IPV6 monodiffusion, visible et joignable à partir d'autres réseaux.
  - *Liaison locale* : une interface IPv6 et une adresse IPv6 qui identifient uniquement des hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Point à point* : un tunnel point à point. Pris en charge si les tunnelsde routage IPv6 sont pris en charge.
- **Interface sortante** : affiche l'interface Liaison locale sortante.
- **Adresse IPv6 du routeur par défaut** : adresse IP du routeur statique par défaut.
- **Métrique** : saisissez les coûts de ce saut.

ÉTAPE 4 Cliquez sur **Appliquer**. Le routeur par défaut est enregistré dans le fichier de Configuration d'exécution.

Voisins IPv6

La page Voisins IPv6 vous permet de configurer et d'afficher la liste des voisins IPv6 sur l'interface IPv6. La table Voisins IPv6, également appelée Cache de détection du voisinage IPv6, affiche les adresses MAC des voisins IPv6 qui font partie du même sous-réseau IPv6 que le périphérique. C'est l'équivalent IPv6 de la table ARP IPv4. Lorsque le périphérique a besoin de communiquer avec ses voisins, il utilise la table de voisinage IPv6 pour déterminer les adresses MAC à partir de leurs adresses IPv6.

Cette page affiche les voisins détectés automatiquement ou configurés manuellement. Chaque entrée indique l'interface à laquelle le voisin est connecté, les adresses IPv6 et MAC de ce voisin, son type de configuration (statique ou dynamique) et l'état du voisin.

Pour définir des voisins IPv6 :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv6** > **Voisins IPv6**.

Vous pouvez sélectionner une option **Effacer la table** afin d'effacer certaines adresses IPv6 (ou toutes) de la table des voisins IPv6.

- **Statique uniquement** : supprime les entrées d'adresse IPv6 statiques.
- **Dynamique uniquement** : supprime les entrées d'adresse IPv6 dynamiques.
- **Dynamique et statique** : supprime les entrées d'adresse IPv6 statiques et dynamiques.

Les champs suivants sont affichés pour les interfaces de voisinage :

- **Interface** : type d'interface de voisinage IPv6.
- **Adresse IPv6** : adresse IPv6 d'un voisin.
- **Adresse MAC** : adresse MAC mappée sur l'adresse IPv6 spécifiée.
- **Type** : type de saisie des informations de cache de découverte des voisins (statique ou dynamique).
- **État** : indique l'état du voisin IPv6. Les valeurs disponibles sont les suivantes :
  - *Incomplet* : résolution d'adresse en cours. Le voisin n'a pas encore répondu.
  - *Atteignable* : le voisin est reconnu comme étant accessible.
  - *Périmé* : un voisin précédemment connu est inaccessible. Aucune action n'est entreprise pour vérifier son accessibilité tant qu'il n'est pas nécessaire de lui envoyer du trafic.
  - *Retard* : un voisin précédemment connu est inaccessible. L'interface reste à l'état Retard pour la durée prédéfinie indiquée par Délai de retard. Si aucune confirmation d'accessibilité n'est reçue, l'état passe à Sonde.

- *Sonde* : le voisin n'est plus reconnu comme inaccessible et des sondes UNS (Unicast Neighbor Solicitation, sollicitation de voisinage Unicast) sont envoyées pour vérifier son accessibilité.

- **Routeur** : spécifie si le voisin est un routeur (**Oui** ou **Non**).

ÉTAPE 2 Pour ajouter un voisin à la table, cliquez sur **Ajouter**.

ÉTAPE 3 Les champs suivants s'affichent :

- **Interface** : affiche l'interface de voisinage IPv6 à ajouter.
- **Adresse IPv6** : saisissez l'adresse réseau IPv6 affectée à l'interface. Cette adresse doit être une adresse IPv6 valide.
- **Adresse MAC** : saisissez l'adresse MAC mappée sur l'adresse IPv6 spécifiée.

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

ÉTAPE 5 Pour passer le type d'adresse IP de **Statique à Dynamique**, sélectionnez l'adresse, cliquez sur **Modifier** et utilisez la page Modifier les voisins IPv6.

Liste de préfixes IPv6

Lorsque la fonction Sécurité du premier saut est configurée, il est possible de définir des règles de filtrage basées sur les préfixes IPv6. Vous pouvez définir ces listes sur la page Liste de préfixes IPv6.

Les listes de préfixes sont configurées avec les mots clés **autoriser** ou **refuser** afin d'autoriser ou de refuser un préfixe sur la base d'une condition correspondante. Un refus implicite s'applique au trafic qui ne correspond à aucune entrée de liste de préfixes.

Une entrée de liste de préfixes se compose d'une adresse IP et d'un masque de bits. L'adresse IP peut être destinée à la route d'un réseau classful, d'un sous-réseau ou d'un seul hôte. Le masque de bits est un nombre compris entre 1 et 32.

Les listes de préfixes sont configurées pour filtrer le trafic à partir d'une correspondance de longueur de préfixe exacte ou d'une correspondance au sein d'une plage lorsque les mots clés ge et le sont utilisés.

Les paramètres **Supérieur à** et **Inférieur à** permettent de spécifier une plage de longueurs de préfixe et d'offrir une configuration plus souple que si vous utilisiez seulement l'argument réseau/longueur. Une liste de préfixes est traitée par le biais d'une correspondance exacte lorsque ni le paramètre **Supérieur à** ni le paramètre **Inférieur à** n'est spécifié. Si seul le paramètre **Supérieur à** est spécifié, la plage va de la valeur saisie pour **Supérieur à** à une

longueur 32 bits complète. Si seul le paramètre **Inférieur à** est spécifié, la plage va de la valeur saisie pour l'argument réseau/longueur à la valeur **Inférieur à**. Si les arguments **Inférieur à** et **Supérieur à** sont tous les deux renseignés, la plage est comprise entre les valeurs utilisées pour **Inférieur à** et **Supérieur à**.

Procédure de création d'une liste de préfixes :

ÉTAPE 1 Cliquez sur **Configuration IP > Interfaces et gestion IPv6 > Liste de préfixes IPv6**.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants :

- **Nom de la liste** : sélectionnez l'une des options suivantes :
  - *Utiliser la liste existante* : sélectionnez une liste précédemment définie pour lui ajouter un préfixe.
  - *Créer une nouvelle liste* : saisissez un nom pour créer une nouvelle liste.
- **Numéro de séquence** : spécifie l'emplacement du préfixe dans la liste de préfixes. Sélectionnez l'une des options suivantes :
  - *Numérotation automatique* : place le nouveau préfixe IPV6 après la dernière entrée de la liste de préfixes. Le numéro de séquence équivaut au dernier numéro de séquence plus 5. Si la liste est vide, la première entrée de la liste de préfixes se voit attribuer le numéro 5 et les entrées suivantes de la liste de préfixes sont incrémentées par 5.
  - *Défini par l'utilisateur* : insère le nouveau préfixe IPV6 à l'emplacement spécifié par le paramètre. S'il y a une entrée avec ce numéro, elle est remplacée par la nouvelle.
- **Type de la règle** : entrez la règle pour la liste de préfixes.
  - *Autoriser* : autorise les réseaux qui respectent la condition.
  - *Refuser* : refuse les réseaux qui ne respectent pas la condition.
  - *Description* : texte.
- **Préfixe IPv6** : préfixe de route IP.
- **Longueur du préfixe** : longueur du préfixe de route IP.

- **Supérieur à** : longueur minimale du préfixe devant être utilisée pour la correspondance. Sélectionnez l'une des options suivantes :
  - *Aucune limite* : aucune longueur minimale du préfixe ne doit être utilisée pour la correspondance.
  - *Défini par l'utilisateur* : longueur minimale du préfixe devant être respectée.
- **Inférieur à** : longueur maximale du préfixe devant être utilisée pour la correspondance. Sélectionnez l'une des options suivantes :
  - *Aucune limite* : aucune longueur maximale du préfixe ne doit être utilisée pour la correspondance.
  - *Défini par l'utilisateur* : longueur maximale du préfixe devant être respectée.
- **Description** : entrez une description de la liste de préfixes.

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

Listes d'accès IPv6

La liste d'accès IPv6 peut être utilisée sur la page Proxy MLD > Paramètres globaux du proxy MLD > Liste d'accès IPv6 SSM.

Pour créer une liste d'accès :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv6 > Liste d'accès IPv6**.

ÉTAPE 2 Pour ajouter une nouvelle liste d'accès, cliquez sur **Ajouter**, puis renseignez les champs suivants :

- **Nom de la liste d'accès** : sélectionnez l'une des options suivantes :
  - *Utiliser la liste existante* : sélectionnez une liste d'accès existante.
  - *Créer une nouvelle liste* : saisissez le nom d'une nouvelle liste d'accès.
- **Source IPv6 Address** (Adresse IPv6 source) : entrez l'adresse IPv6 source. Les options suivantes sont disponibles :
  - *Tous* : toutes les adresses IP sont incluses.
  - *Défini par l'utilisateur* : saisissez une adresse IP.

- **Prefix length** (Longueur du préfixe) : saisissez la longueur du préfixe IPv6 source :
- **Action** : sélectionnez une action pour la liste d'accès. Les options suivantes sont disponibles :
  - *Autoriser* : permet d'autoriser l'entrée des paquets à partir des adresses IP contenues dans la liste d'accès.
  - *Refuser* : permet de refuser l'entrée des paquets à partir des adresses IP contenues dans la liste d'accès.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres sont consignés dans le fichier de Configuration d'exécution.

Routes IPv6

L'IPv6 Forwarding Table (Table de redirection IPv6) contient les différents acheminements qui ont été configurés. L'un de ces acheminements est un acheminement par défaut (adresse IPv6:0), qui utilise le routeur par défaut sélectionné dans la liste des routeurs par défaut IPv6 afin d'envoyer des paquets aux périphériques de destination qui ne font pas partie du même sous-réseau IPv6 que le périphérique. Outre l'acheminement par défaut, la table contient aussi des acheminements dynamiques, qui sont des acheminements de redirection ICMP reçues des routeurs IPv6 via des messages de redirection ICMP. Cela peut se produire lorsque le routeur par défaut que le périphérique utilise n'est pas celui défini pour le trafic des sous-réseaux IPv6 avec lesquels le périphérique veut communiquer.

Pour visualiser les acheminements IPv6 :

Cliquez sur **Configuration IP** > **Interfaces et gestion IPv6** > **Routes IPv6**.

Cette rubrique affiche les champs suivants :

- **Préfixe IPv6** : préfixe de l'adresse de la route IP pour l'adresse de sous-réseau IPv6 de destination.
- **Longueur du préfixe** : longueur du préfixe d'acheminement IP pour l'adresse de sous-réseau IPv6 de destination. Il est précédé d'une barre oblique.
- **Interface sortante** : interface utilisée pour réacheminer le paquet.
- **Saut suivant** : type d'adresse vers laquelle le paquet est transféré. En général, il s'agit de l'adresse d'un routeur du voisinage. Les types suivants sont disponibles :
  - *Liaison locale* : une interface IPv6 et une adresse IPv6 qui identifient uniquement des hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le

préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.

- *Global* : une adresse IPv6 qui est de type global IPV6 monodiffusion, visible et joignable à partir d'autres réseaux.
- *Point-to-Point (Point à point)* : un tunnel point à point.

- **Métrique** : valeur utilisée pour comparer cet acheminement à d'autres acheminements vers la même destination dans la table des routeurs IPv6. Tous les acheminements par défaut ont la même valeur.
- **Durée de vie** : laps de temps durant lequel le paquet peut être envoyé et renvoyé, avant sa suppression.
- **Type d'acheminement** : mode de rattachement de la destination et méthode utilisée pour obtenir l'entrée. Les valeurs sont les suivantes :
  - *S (Statique)* : l'entrée a été configurée manuellement par un utilisateur.
  - *I (Redirection ICMP)* : l'entrée est un acheminement dynamique de redirection ICMP reçu d'un routeur IPv6 via des messages de redirection ICMP.
  - *ND (Annonce de routeur)* : l'entrée est récupérée dans un message d'annonce de routeur.

ÉTAPE 1 Pour ajouter un nouvel acheminement, cliquez sur **Ajouter**, puis renseignez les champs décrits ci-dessus. Renseignez également le champ suivant :

- **Adresse IPv6** : ajoutez l'adresse IPv6 du nouvel acheminement.

ÉTAPE 2 Cliquez sur **Appliquer** pour enregistrer les modifications.

Relais DHCPv6

Cette section couvre les sujets suivants :

- Destinations globales
- Paramètres d'interface

Le relais DHCPv6 est utilisé pour transférer des messages DHCPv6 vers des serveurs DHCPv6. Il est défini dans RFC 3315.

Lorsque le client DHCPv6 n'est pas directement connecté au serveur DHCPv6, un agent de relais DHCPv6 (le périphérique) auquel ce client DHCPv6 est directement connecté encapsule les messages reçus du client DHCPv6 directement connecté et les transfère au serveur DHCPv6.

Dans le sens inverse, l'agent de relais décapsule les paquets reçus du serveur DHCPv6 et les transfère au client DHCPv6.

L'utilisateur doit configurer la liste des serveurs DHCP vers lesquels des paquets sont transférés. Vous pouvez configurer deux groupes de serveurs DHCPv6 :

- **Destinations globales** : les paquets sont toujours relayés vers ces serveurs DHCPv6.
- **Interface List (Liste d'interfaces)** : il s'agit d'une liste de serveurs DHCPv6 par interface. Lorsqu'un paquet DHCPv6 est reçu sur une interface, le paquet est relayé vers les serveurs de la liste d'interfaces (si existante) et les serveurs de la liste de destinations globales.

Dépendances envers les autres fonctions

Les fonctions de client DHCPv6 et de relais DHCPv6 s'excluent mutuellement sur une interface.

Destinations globales

Pour configurer une liste de serveurs DHCPv6 vers laquelle tous les paquets DHCPv6 sont relayés :

ÉTAPE 1 Cliquez sur **Configuration IP > Interfaces et gestion IPv6 > Relais DHCPv6 > Destinations globales**.

ÉTAPE 2 Pour ajouter un serveur DHCPv6 par défaut, cliquez sur **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants :

- **Type d'adresse IPv6** : saisissez le type de l'adresse de destination vers laquelle les messages client sont transférés. Le type d'adresse peut être **Liaison locale**, **Global** ou **Multidiffusion** (All_DHCP_Relay_Agents_and_Servers).
- **DHCPv6 Server IP Address (Adresse IP serveur DHCPv6)** : saisissez l'adresse du serveur DHCPv6 vers lequel les paquets sont transférés.
- **IPv6 Interface** (Interface IPv6) : saisissez l'interface de destination sur laquelle les paquets sont transmis lorsque le type d'adresse du serveur DHCPv6 est **Link Local** (Liaison locale) ou **Multicast** (Multidiffusion). Il peut s'agir d'un LAG, d'un VLAN ou d'un tunnel.

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

Paramètres d'interface

Pour activer la fonction de relais DHCPv6 sur une interface et pour configurer une liste de serveurs DHCPv6 vers lesquels les paquets DHCPv6 sont relayés, lorsque ceux-ci sont reçus sur cette interface.

ÉTAPE 1 Cliquez sur **Configuration IP > Interfaces et gestion IPv6 > Relais DHCPv6 > Paramètres d'interface**.

ÉTAPE 2 Pour activer DHCPv6 sur une interface et ajouter en option un serveur DHCPv6 pour une interface, cliquez sur **Ajouter**.

Renseignez les champs suivants :

- **Interface source** : sélectionnez l'interface (port, LAG, VLAN ou tunnel) pour laquelle le relais DHCPv6 est activé.
- **Use Global Destinations Only (Utiliser seulement des destinations globales)** : sélectionnez cette option pour transférer des paquets uniquement vers les serveurs de destinations globales DHCPv6.
- **Type d'adresse IPv6** : saisissez le type de l'adresse de destination vers laquelle les messages client sont transférés. Le type d'adresse peut être **Liaison locale**, **Global** ou **Multidiffusion** (All_DHCP_Relay_Agents_and_Servers).
- **DHCPv6 Server IP Address (Adresse IP serveur DHCPv6)** : saisissez l'adresse du serveur DHCPv6 vers lequel les paquets sont transférés.
- **Destination IPv6 Interface** (Interface IPv6 de destination) : saisissez l'interface sur laquelle les paquets sont transmis lorsque le type d'adresse du serveur DHCPv6 est **Link Local** (Liaison locale) ou **Multicast** (Multidiffusion).

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

Routage basé sur une stratégie

Le routage en fonction de la stratégie (PBR) permet d'acheminer les paquets sélectionnés vers une adresse de saut suivant en fonction des champs des paquets et en utilisant des ACL pour la classification. Ce type de routage permet de moins dépendre de routes définies à partir de protocoles de routage.

Mappage de route

Le mappage de route permet de configurer le routage en fonction de la stratégie.

Pour ajouter un mappage de route :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Routage en fonction de la stratégie** > **Mappage de route**.

ÉTAPE 2 Cliquez sur **Ajouter**, puis renseignez les paramètres suivants :

- **Nom du mappage de route** : sélectionnez l'une des options ci-dessous pour définir un mappage de route :
  - *Utiliser un mappage existant* : sélectionnez un mappage de route prédéfini pour y ajouter une nouvelle règle.
  - *Créer un nouveau mappage* : saisissez le nom du nouveau mappage de route.
- **Numéro de séquence** : numéro indiquant la position ou la priorité des règles dans un mappage de route spécifié. Si un mappage de route contient plus d'une règle (ACL) définie dans le cadre de ce mappage, le numéro de séquence détermine l'ordre suivant lequel les paquets seront associés aux ACL (du nombre le plus bas au plus élevé).
- **Type d'IP du mappage de route** : sélectionnez IPv6 ou IPv4 selon le type d'adresse IP du saut suivant.
- **Correspondance ACL** : sélectionnez une ACL préalablement définie. Les paquets seront associés à cette ACL.
- **Type de saut suivant IPv6** : si l'adresse de saut suivant est une adresse IPv6, sélectionnez l'une des options suivantes :
  - *Global* : une adresse IPv6 qui est de type global IPV6 monodiffusion, visible et joignable à partir d'autres réseaux.
  - *Liaison locale* : une interface IPv6 et une adresse IPv6 qui identifient uniquement des hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local.
  - *Point à point* : un tunnel point à point.
- **Interface** : affiche l'interface Liaison locale sortante.
- **Saut suivant** : adresse IP du routeur du saut suivant.

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

Liaison d'un mappage de route

Tous les paquets arrivant sur une interface liée à un mappage de route et correspondant à une règle de mappage de route sont acheminés vers le saut suivant défini dans cette règle.

Pour lier une interface à un mappage de route :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Routage en fonction de la stratégie** > **Liaison d'un mappage de route**.

ÉTAPE 2 Cliquez sur **Ajouter**, puis renseignez les paramètres suivants :

- **Interface** : sélectionnez une interface (avec une adresse IP).
- **Mappage de route IPv4 lié** : sélectionnez un mappage de route IPv4 pour le lier à l'interface.
- **Mappage de route IPv6 lié** : sélectionnez un mappage de route IPv6 pour le lier à l'interface.

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

Routes basées sur une stratégie

Pour afficher les mappages de route définis :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Routage en fonction de la stratégie** > **Routes basées sur une stratégie**.

ÉTAPE 2 Les mappages de route préalablement définis s'affichent :

- **Nom de l'interface** : interface à laquelle le mappage de route est lié.
- **Nom du mappage de route** : nom du mappage de route.
- État du mappage de route : état de l'interface.
  - *Actif* : l'interface est activée.
  - *Interface inactive* : l'interface est désactivée.
- **Nom de l'ACL** : ACL associée au mappage de route.
- **Saut suivant** : destination vers laquelle les paquets correspondant au mappage de route seront acheminés.

- **État du saut suivant** : accessibilité du saut suivant :
  - *Actif* : l'adresse IP du saut suivant est accessible.
  - *Inaccessible* : l'état n'est pas actif, car l'adresse IP du saut suivant est inaccessible.
  - *Non direct* : l'état n'est pas actif, car l'adresse IP du saut suivant n'est pas connectée directement au sous-réseau d'un périphérique.

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 périphérique convertit les noms de domaine en adresses IP via un ou plusieurs serveurs DNS configurés.

Paramètres DNS

Utilisez la page Paramètres DNS pour activer la fonction DNS, configurer les serveurs DNS et définir le domaine par défaut utilisé par le périphérique.

ÉTAPE 1 Cliquez sur **Configuration IP** > **Système de noms de domaine** > **Paramètres DNS**.

ÉTAPE 2 En mode de base, définissez les paramètres suivants :

- **Server Definition** (Définition du serveur) : sélectionnez l'une des options ci-dessous pour définir le serveur DNS :
  - *Par adresse IP* : l'adresse IP est saisie pour le serveur DNS.
  - *Disabled* (Désactivé) : aucun serveur DNS n'est défini.
- **Server IP Address** (Adresse IP du serveur) : si vous avez sélectionné By IP Address (Par adresse IP) ci-dessus, saisissez l'adresse IP du serveur DNS.
- **Nom de domaine par défaut** : saisissez le nom de domaine DNS utilisé pour compléter des noms d'hôte incomplets. Le périphérique ajoute ces informations à tous les noms de domaine incomplets (NFQDN), afin de les convertir en noms de domaine complets (FQDN).

  REMARQUE N'incluez pas le point initial qui sépare un nom incomplet du nom de domaine (comme cisco.com).

ÉTAPE 3 En mode avancé, définissez les paramètres suivants :

- **DNS** : sélectionnez cette option pour désigner le périphérique comme client DNS et lui permettre de convertir les noms DNS en adresses IP via un ou plusieurs serveurs DNS configurés.
- **Polling Retries (Tentatives d'interrogation)** : saisissez le nombre de fois où le périphérique peut envoyer une requête DNS à un serveur DNS avant de conclure que ce serveur DNS n'existe pas.
- **Polling Timeout (Délai de l'interrogation)** : saisissez la durée en secondes pendant laquelle le périphérique attend une réponse à une requête DNS.
- **Intervalle d'interrogation** : saisissez la fréquence (en secondes) à laquelle le périphérique envoie des paquets de requête DNS lorsque le nombre maximal de tentatives a été atteint.
  - *Valeurs par défaut* : cette option permet d'utiliser la valeur par défaut.

    Cette valeur = 2*(Polling Retries (Tentatives d'interrogation) + 1)* Polling Timeout (Délai de l'interrogation)
  - *Défini par l'utilisateur* : cette option permet de saisir une valeur définie par l'utilisateur.
- **Paramètres par défaut** : saisissez les paramètres par défaut suivants :
  - *Nom de domaine par défaut* : saisissez le nom de domaine DNS utilisé pour compléter des noms d'hôte incomplets. Le périphérique ajoute ces informations à tous les noms de domaine incomplets (NFQDN), afin de les convertir en noms de domaine complets (FQDN).

    REMARQUE N'incluez pas le point initial qui sépare un nom incomplet du nom de domaine (comme cisco.com).
  - *Liste de recherche de domaine DHCP* : cliquez sur **Détails** pour afficher la liste des serveurs DNS configurés sur le périphérique.

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

La **table de serveur DNS** affiche les informations suivantes pour chaque serveur DNS configuré :

- **Serveur DNS** : adresse IP du serveur DNS.
- **Préférence** : chaque serveur dispose d'une valeur de préférence ; une valeur plus petite signifie une plus grande probabilité d'être utilisée.
- **Source** : source de l'adresse IP du serveur (statique ou DHCPv4 ou DHCPv6).
- **Interface** : interface de l'adresse IP du serveur.

ÉTAPE 5 Vous pouvez définir jusqu'à huit serveurs DNS. Pour ajouter un serveur DNS, cliquez sur **Ajouter**.

ÉTAPE 6 Saisissez les paramètres.

- **Version IP** : sélectionnez Version 6 pour IPv6 ou Version 4 pour IPv4.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, sélectionnez l'interface de réception.
- **Adresse IP du serveur DNS** : saisissez l'adresse IP du serveur DNS.
- **Préférence** : sélectionnez une valeur déterminant l'ordre dans lequel les domaines sont utilisés (du bas vers le haut). Cette option détermine efficacement l'ordre dans lequel les noms incomplets sont complétés au cours des requêtes DNS.

ÉTAPE 7 Cliquez sur **Appliquer**. Le serveur DNS est enregistré dans le fichier de Configuration d'exécution.

Liste de recherche

La liste de recherche peut contenir une entrée statique définie par l'utilisateur sur la page Paramètres DNS et des entrées dynamiques reçues des serveurs DHCPv4 et DHCPv6.

Pour afficher les noms de domaine configurés sur le périphérique, cliquez sur **Configuration IP** > **Système de noms de domaine** > **Liste de recherche**.

Les champs suivants sont affichés pour chaque serveur DNS configuré sur le périphérique :

- **Nom de domaine** : nom de domaine qui peut être utilisé sur le périphérique.
- **Source** : source de l'adresse IP du serveur (statique ou DHCPv4 ou DHCPv6) pour ce domaine.
- **Interface** : interface de l'adresse IP du serveur pour ce domaine.

- **Préférence** : ordre dans lequel les domaines sont utilisés (du bas vers le haut). Cette option détermine efficacement l'ordre dans lequel les noms incomplets sont complétés au cours des requêtes DNS.

Mappage d'hôtes

Les mappages Nom d'hôte/Adresse IP sont enregistrés dans la zone Table de mappage d'hôtes (cache DNS).

Ce cache peut contenir les types d'entrée suivants :

- **Entrées statiques** : paires de mappage qui ont été manuellement ajoutées au cache. Un maximum de 64 entrées statiques est possible.
- **Entrées dynamiques** : paires de mappage qui ont été ajoutées par le système suite à une utilisation par l'utilisateur ou une entrée pour chaque adresse IP configurée sur le périphérique par DHCP. Un maximum de 256 entrées dynamiques est possible.

La résolution des noms commence toujours par la vérification des entrées statiques, se poursuit par la vérification des entrées dynamiques et se termine par l'envoi de demandes au serveur DNS externe.

Vous pouvez associer huit adresses IP à chaque serveur DNS pour chaque nom d'hôte.

Pour ajouter un nom d'hôte et son adresse IP :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Système de noms de domaine** > **Mappage d'hôtes**.

ÉTAPE 2 Si nécessaire, sélectionnez l'option **Effacer la table** afin d'effacer certaines entrées ou toutes les entrées de la Table de mappage d'hôtes.

- **Statique uniquement** : supprime les hôtes statiques.
- **Dynamique uniquement** : supprime les hôtes dynamiques.
- **Dynamique et statique** : supprime les hôtes statiques et dynamiques.

La Table de mappage d'hôtes contient les champs suivants :

- **Nom d'hôte** : nom d'hôte défini par l'utilisateur ou nom complet.
- **IP Address** : adresse IP d'hôte.
- **IP Version** : version IP de l'adresse IP de l'hôte.
- **Type** : une entrée **dynamique** ou **statique** dans le cache.
- **État** : affiche les résultats des tentatives d'accéder à l'hôte.

- *OK* : tentative réussie.
- *Negative Cache (Cache négatif)* : tentative échouée, ne réessayez pas.
- *Pas de réponse* : pas de réponse mais le système peut effectuer ultérieurement une nouvelle tentative.

- **TTL (s)** : s'il s'agit d'une entrée dynamique, cette option indique sa durée de conservation dans le cache.
- **TTL restant (s)** : s'il s'agit d'une entrée dynamique, cette option indique combien de temps encore elle va rester dans le cache.

ÉTAPE 3 Pour ajouter un mappage d'hôtes, cliquez sur **Ajouter**.

ÉTAPE 4 Saisissez les paramètres.

- **Version IP** : sélectionnez **Version 6** pour IPv6 ou **Version 4** pour IPv4.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, sélectionnez l'interface de réception.
- **Host Name** : saisissez un nom d'hôte défini par l'utilisateur ou un nom complet. Les noms d'hôte sont limités aux lettres ASCII de A à Z (avec distinction majuscules/minuscules), les chiffres de 0 à 9, le caractère souligné et le tiret. Le point (.) est utilisé pour séparer les étiquettes.
- **Adresse IP** : saisissez une seule adresse ou jusqu'à huit adresses IP associées (IPv4 ou IPv6).

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres sont enregistrés dans le fichier Configuration d'exécution.

17

Configuration IP : RIPv2

Cette section décrit la fonctionnalité RIP (Routing Information Protocol), version 2.

REMARQUE Cette fonctionnalité n'est prise en charge que sur les appareils de la gamme 550.

Elle couvre les sujets suivants :

- Vue d'ensemble
- Fonctionnement de RIP sur le périphérique
- Configuration de RIP
- Liste d'accès

Vue d'ensemble

Routing Information Protocol (RIP) est une implémentation d'un protocole de vecteur de distance pour les réseaux locaux et étendus. Elle définit les routeurs comme *actifs* ou *passifs* (silencieux). Les routeurs actifs annoncent leurs routes aux autres ; les routeurs passifs écoutent et mettent à jour leurs routes en fonction des annonces, mais ils n'annoncent rien. Généralement, les routeurs exécutent RIP en mode actif, alors que les hôtes utilisent le mode passif.

La passerelle par défaut est une route statique et est annoncée par RIP de la même façon que tous les autres routeurs statiques, si elle est activée par la configuration.

Lorsque le routage IP est activé, RIP fonctionne intégralement. Lorsque le routage IP est désactivé, RIP fonctionne en mode passif, à savoir qu'elle n'apprend que les routes à partir des messages RIP reçus et ne les envoie pas.

REMARQUE Pour activer le routage IP, accédez à la page Interfaces IPv4.

L'appareil prend en charge RIP version 2, qui est basé sur les normes suivantes :

- RFC2453 RIP Version 2, Novembre 1998
- RFC2082 RIP-2 MD5 Authentication, Janvier 1997
- RFC1724 RIP Version 2 MIB Extension

Les paquets RIPv1 reçus sont supprimés.

Fonctionnement de RIP sur le périphérique

La section suivante décrit l'activation, la configuration du décalage, le mode passif, l'authentification, les compteurs de statistiques et la base de données des homologues de RIP.

Activation de RIP

- La fonction RIP doit être activée globalement et par interface.
- RIP peut uniquement être configurée si elle est activée.
- La désactivation globale de RIP supprime la configuration de RIP sur le système.
- La désactivation de RIP sur une interface supprime la configuration de RIP sur l'interface spécifiée.
- Si le routage IP est désactivé, les messages RIP ne sont pas envoyés, mais en cas de réception de messages RIP, ils sont utilisés pour mettre à jour les informations de table de routage.

REMARQUE La fonction RIP peut uniquement être définie sur les interfaces IP configurées manuellement. Cela signifie que la fonction RIP ne peut pas être définie sur une interface dont l'adresse IP a été reçue à partir d'un serveur DHCP ou dont l'adresse IP est l'adresse IP par défaut.

Configuration du décalage

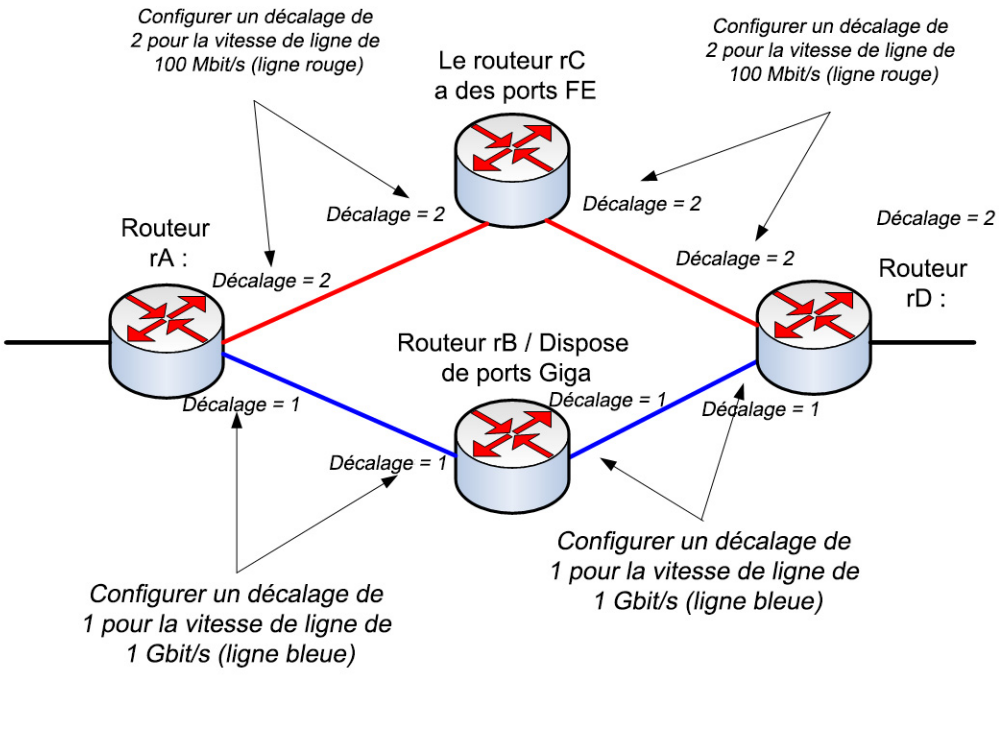
Un message RIP inclut une métrique (nombre de sauts) pour chaque route.

Un décalage est un numéro supplémentaire qui est ajouté à une métrique pour affecter le coût des chemins. Le décalage est défini par interface et peut, par exemple, refléter la vitesse, le délai et toute autre qualité de cette interface spécifique. De cette façon, vous pouvez ajuster le coût relatif des interfaces comme vous le souhaitez.

Il est de votre responsabilité de définir le décalage pour chaque interface (1 par défaut).

L'illustration suivante présente la configuration du décalage de métrique pour diverses interfaces, en fonction de la vitesse de port.

Configuration du décalage (en fonction de la vitesse de port)



Le routeur rD peut envoyer les données à rA via rB ou rC. Puisque rC prend uniquement en charge les ports Fast Ethernet (FE) et que rB prend en charge les ports Gigabit Ethernet (GE), le coût du chemin du routeur rD au routeur rA est supérieur via le routeur rC (plus 4 au coût du chemin) par rapport au chemin via le routeur rB (plus 2 au coût du chemin). Par conséquent, il est préférable de transférer le trafic via le routeur rB. Pour ce faire, vous devez configurer un décalage différent (valeur de métrique) sur chaque interface en fonction de sa vitesse de ligne.

Pour plus d'informations, reportez-vous à la section Configuration du décalage.

Mode passif

Il est possible de désactiver la transmission des messages de mise à jour du routage via une interface IP spécifique. Dans ce cas, le routeur est passif et ne reçoit que les informations RIP mises à jour sur cette interface. Par défaut, la transmission des mises à jour du routage sur une interface IP est activée.

Pour plus d'informations, reportez-vous à la section Paramètres RIPv2.

Filtrage des mises à jour du routage

Vous pouvez filtrer les routes entrantes et sortantes pour une interface IP donnée à l'aide de deux listes d'accès standard : une pour les entrées et l'autre pour les sorties.

La liste d'accès standard est une liste nommée et ordonnée de paires constituées d'un préfixe IP (adresse IP et longueur du masque IP) et d'une action. L'action peut être « refuser » ou « autoriser ».

Si une liste d'accès est définie, chaque route depuis le message RIP est comparée à la liste, en commençant par la première paire : si elle correspond à la première paire et que l'action est « autoriser », la route est transmise ; si l'action est « refuser », la route n'est pas transmise. Si la route ne correspond pas, la paire suivante est analysée.

Si la route ne correspond à aucune paire, l'action « refuser » est appliquée.

Annonce des entrées de route par défaut sur les interfaces IP

L'adresse spéciale 0.0.0.0 est utilisée pour décrire une route par défaut. L'utilisation d'une route par défaut évite de devoir répertorier chaque réseau possible dans les mises à jour du routage lorsqu'un ou plusieurs routeurs étroitement connectés dans le système sont préparés à transférer le trafic aux réseaux qui ne sont pas explicitement répertoriés. Ces routeurs créent des entrées RIP pour l'adresse 0.0.0.0, comme s'ils étaient connectés à un réseau.

Vous pouvez activer l'annonce de route par défaut et la configurer avec une métrique donnée.

Fonctionnalité de redistribution

Voici une liste des types de routes pouvant être distribuées par RIP :

- **Connectée** : routes RIP pour lesquelles le protocole RIP n'est pas activé (définition locale) sur les interfaces IP définies correspondantes. La table de routage RIP répertorie uniquement par défaut les routes pour lesquelles le protocole RIP est activé sur les interfaces IP correspondantes.
- **Statique** : routes (distantes) définies manuellement.

Pour indiquer si oui ou non les routes statiques ou connectées doivent être redistribuées par RIP, configurez la fonctionnalité Redistribution de la route statique ou la fonctionnalité Redistribution de la route connectée, respectivement.

Ces deux fonctionnalités sont désactivées par défaut et peuvent être activées globalement.

Lorsque ces fonctionnalités sont activées, les routes refusées sont annoncées par les routes ayant une métrique de 16.

La configuration de route peut être propagée par l'intermédiaire de l'une des options suivantes :

- **Paramètre par défaut**

  Si cette option est sélectionnée, RIP utilise la valeur de métrique par défaut prédéfinie pour la configuration de route propagée.

- Transparent (par défaut)

  Si cette option est sélectionnée, RIP utilise la métrique de table de routage comme métrique RIP pour la configuration de route propagée.

  Il en résulte le comportement suivant :

  - Si la valeur de métrique d'une route est égale ou inférieure à 15, cette valeur est utilisée dans le protocole RIP lors de l'annonce de cette route.
  - Si la valeur de métrique d'une route est supérieure à 15, la route n'est pas annoncée aux autres routeurs via RIP.

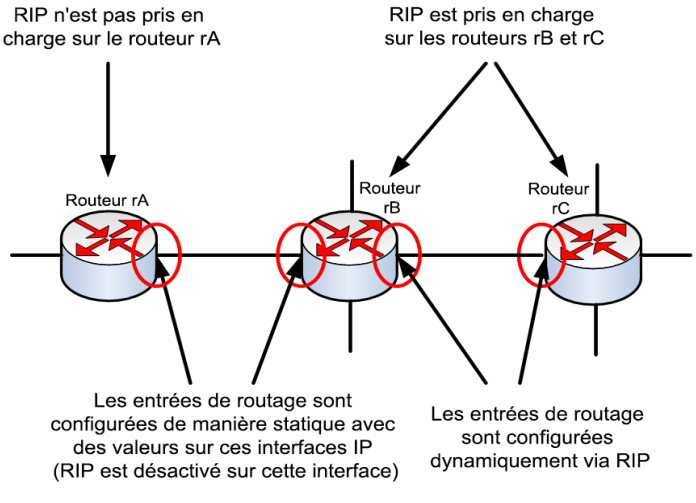
- **Paramètre défini par l'utilisateur**

  Si cette option est sélectionnée, RIP utilise la valeur de métrique saisie par l'utilisateur.

Utilisation de la fonction RIP dans un réseau dont les périphériques ne sont pas de type RIP

La configuration de route statique et les interfaces connectées doivent être prises en compte lorsque la fonction RIP est utilisée. Consultez à ce sujet l'illustration suivante, qui présente un réseau dans lequel certains routeurs prennent en charge RIP et d'autres pas.

Réseau comportant des routeurs RIP et non RIP



Le routeur rA ne prend pas en charge RIP. Les entrées de routage pourvues d'une métrique appropriée sont donc configurées comme statiques sur ce routeur, alors que sur le routeur rB, la route vers le routeur rA est considérée comme connectée. À l'inverse, les routeurs rB et rC reçoivent et distribuent leurs entrées de routage via RIP.

La configuration de route connectée du routeur rB peut être propagée au routeur rC via la métrique par défaut ou le système transparent. Une route statique/connectée est *redistribuée* soit avec la métrique de la route statique (métrique transparente), soit avec la métrique définie par la commande de métrique par défaut.

Pour plus d'informations, reportez-vous à la section Fonctionnalité de redistribution.

Authentification RIP

Vous pouvez désactiver l'authentification des messages RIP par interface IP ou activer l'un des types suivants d'authentification :

- **Texte en clair ou mot de passe** : utilise un mot de passe de clé (chaîne) qui est envoyé avec la route à un autre routeur. Le routeur de destination compare cette clé avec sa propre clé configurée. Si elles sont identiques, il accepte la route.
- MD5 : utilise l'authentification Digest MD5. Chaque routeur est configuré avec un ensemble de clés secrètes. On appelle cet ensemble une **chaîne de clé**. Chaque chaîne de clé comprend une ou plusieurs clés. Chaque clé a un numéro d'identification (**identifiant de la clé**), une **chaîne de clé** et éventuellement une valeur **send-lifetime** et **accept-lifetime**. La valeur send-lifetime est la période pendant laquelle une clé d'authentification appartenant à une chaîne de clé peut être envoyée ; la valeur accept-lifetime est la période pendant laquelle une clé d'authentification appartenant à une chaîne de clé peut être reçue.

  Chaque message RIP transmis contient le Digest MD5 calculé du message (contenant la chaîne de clé), plus l'identifiant de clé de la chaîne de clé utilisée. La chaîne de clé est également configurée sur le récepteur. L'identifiant de clé est utilisé par le récepteur afin de sélectionner la clé pour valider le Digest MD5.

Compteurs de statistiques RIP

Vous pouvez contrôler le fonctionnement de RIP en consultant les compteurs de statistiques par interface IP. Pour obtenir une description de ces compteurs, reportez-vous à la section Statistiques RIPv2.

Base de données des homologues RIP

Vous pouvez contrôler la base de données des homologues RIP par interface IP. Pour obtenir une description de ces compteurs, reportez-vous à la section Base de données d'homologues RIPv2.

Configuration de RIP

Les actions suivantes peuvent être effectuées :

- Actions obligatoires :
  - Activez/désactivez globalement le protocole RIP, à l'aide de la page Propriétés RIPv2.
  - Activez/désactivez le protocole RIP sur une interface IP, à l'aide de la page Paramètres RIPv2.
- Actions facultatives (si elles ne sont pas effectuées, les valeurs par défaut sont utilisées par le système).
  - Activez/désactivez RIP pour annoncer les routes statiques ou connectées et sa métrique sur l'interface IP, à l'aide de la page Propriétés RIPv2.
  - Configurez le décalage ajouté à la métrique pour les routes entrantes sur une interface IP, à l'aide de la page Paramètres RIPv2.
  - Activez le mode passif sur une interface IP, à l'aide de la page Paramètres RIPv2.
  - Sachez quelles routes sont traitées dans les mises à jour du routage entrant/sortant en spécifiant une liste d'adresses IP sur l'interface IP (reportez-vous à la section Liste d'accès).
  - Annoncez les entrées de route par défaut sur l'interface IP, à l'aide de la page Paramètres RIPv2.
  - Activez l'authentification RIP sur une interface IP, à l'aide de la page Paramètres RIPv2.

Les pages suivantes sont décrites :

- Propriétés RIPv2
- Paramètres RIPv2
- Statistiques RIPv2
- Base de données d'homologues RIPv2

Propriétés RIPv2

REMARQUE Cette fonctionnalité n'est prise en charge que sur les périphériques Sx550X/SG550XG.

Pour activer/désactiver RIP sur l'appareil.

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4** > **RIPv2 > Propriétés RIPv2**.

ÉTAPE 2 Sélectionnez les options suivantes selon vos besoins :

- **RIP** : les options ci-après sont disponibles :
  - *Activer* : activez RIP.
  - *Désactiver* : désactivez RIP. La désactivation de RIP supprime la configuration de RIP sur le système.
  - *Fermer* : définissez l'état global de RIP sur « fermer ».
- **Annonce RIP** : permet d'activer l'envoi de mises à jour de routage à toutes le interfaces IP RIP.
- **Annonce de route par défaut** : permet d'activer l'envoi de la route par défaut au domaine RIP. Cette route sera utilisée comme routeur par défaut.
- **Mesure par défaut** : saisissez la valeur de la métrique par défaut (reportez-vous à la section Fonctionnalité de redistribution).

ÉTAPE 3 **Redistribution de la route statique** : sélectionnez cette fonction pour l'activer (décrite à la section Fonctionnalité de redistribution).

ÉTAPE 4 Si la fonction **Redistribute Static Route** (Redistribution de la route statique) est activée, sélectionnez une option pour le champ **Redistribute Static Metric** (Redistribution de la mesure statique). Les options suivantes sont disponibles :

- **Mesure par défaut** : si cette option est sélectionnée, RIP utilise la valeur de métrique par défaut pour la configuration de route statique propagée (reportez-vous à la section Fonctionnalité de redistribution).
- **Transparent** : si cette option est sélectionnée, RIP utilise la métrique de table de routage comme métrique RIP pour la configuration de route statique propagée. Il en résulte le comportement suivant :
  - Si la valeur de métrique d'une route statique est égale ou inférieure à 15, cette valeur est utilisée dans le protocole RIP lors de l'annonce de cette route statique.
  - Si la valeur de métrique d'une route statique est supérieure à 15, la route statique n'est pas annoncée aux autres routeurs via RIP.
- **Métrique définie par l'utilisateur** : saisissez la valeur de la métrique.

ÉTAPE 5 **Redistribution de la route connectée** : sélectionnez cette fonction pour l'activer (décrite à la section Redistribution de la configuration de route statique).

ÉTAPE 6 Si la fonction **Redistribute Connected Route** (Redistribution de la route connectée) est activée, sélectionnez une option pour le champ **Redistribute Connected Metric** (Redistribuer le paramètre connecté). Les options suivantes sont disponibles :

- **Mesure par défaut** : si cette option est sélectionnée, RIP utilise la valeur de métrique par défaut pour la configuration de route statique propagée (reportez-vous à la section Fonctionnalité de redistribution).
- **Transparent** : si cette option est sélectionnée, RIP utilise la métrique de table de routage comme métrique RIP pour la configuration de route statique propagée. Il en résulte le comportement suivant :
  - Si la valeur de métrique d'une route statique est égale ou inférieure à 15, cette valeur est utilisée dans le protocole RIP lors de l'annonce de cette route statique.
  - Si la valeur de métrique d'une route statique est supérieure à 15, la route statique n'est pas annoncée aux autres routeurs via RIP.
- **Métrique définie par l'utilisateur** : saisissez la valeur de la métrique.

ÉTAPE 7 Cliquez sur **Appliquer**. Les paramètres sont consignés dans le fichier de Configuration d'exécution.

Paramètres RIPv2

Pour configurer RIP sur une interface IP :

ÉTAPE 1 Cliquez sur **Configuration IP** > **RIPv2 > Paramètres RIPv2**.

ÉTAPE 2 Les paramètres RIP s'affichent par interface IP. Pour ajouter une nouvelle interface IP, cliquez sur **Add** (Ajouter), puis renseignez les champs suivants :

- **Adresse IP** : sélectionnez une interface IP définie sur l'interface Couche 2.
- **Fermer** : conserve la configuration RIP sur l'interface, mais définit l'interface sur inactive.
- **Passif** : indique si l'envoi des messages de mise à jour de route RIP est autorisé sur l'interface IP spécifiée. Si ce champ n'est pas activé, les mises à jour RIP ne sont pas envoyées (passives).

- **Décalage** : indique le numéro métrique de l'interface IP spécifiée. Il reflète le coût supplémentaire d'utilisation de cette interface, en fonction de la vitesse de celle-ci.
- **Default Route Advertisement** (Annonce de route par défaut) : cette option est définie de manière globale sur la page Propriétés RIPv2. Vous pouvez utiliser la définition globale ou définir ce champ pour cette interface spécifique. Les options suivantes sont disponibles :
  - *Global* : permet d'utiliser les paramètres globaux définis sur l'écran **Propriétés RIPv2**.
  - *Activer* : permet d'activer l'annonce de route par défaut sur cette interface RIP.
  - *Désactiver* : permet de désactiver l'annonce de route par défaut sur cette interface RIP.
- **Mesure d'annonce de route par défaut** : permet d'indiquer la métrique de la route par défaut pour cette interface.
- **Mode d'authentification** : état d'authentification de RIP (activer/désactiver) sur une interface IP spécifiée. Les options suivantes sont disponibles :
  - *Aucun* : aucune authentification n'est effectuée.
  - *Texte* : le mot de passe de clé entré dessous est utilisé pour l'authentification.
  - *MD5* : le Digest MD5 de la chaîne de clé sélectionnée ci-dessous est utilisé pour l'authentification.
- **Mot de passe de la clé** : si le type d'authentification Texte a été sélectionné, saisissez le mot de passe à utiliser.
- **Chaîne de la clé** : si le mode d'authentification MD5 a été sélectionné, saisissez la chaîne de clé à assimiler. Cette chaîne de clé est créée comme indiqué à la section Gestion des clés.
- **Liste de distribution entrante** : permet de configurer le filtrage sur les routes RIP entrantes pour la ou les adresses IP spécifiées dans le Nom de la liste d'accès. Si ce champ est activé, sélectionnez le Nom de la liste d'accès ci-dessous.
- **Nom de la liste d'accès** : permet d'indiquer le nom de la liste d'accès (qui inclut une liste d'adresses IP) du filtrage des routes entrantes RIP pour une interface IP spécifiée. Pour obtenir une description des listes d'accès, reportez-vous à la section Paramètres de la liste d'accès.
- **Liste de distribution sortante** : permet de configurer le filtrage sur les routes RIP sortantes pour la ou les adresses IP spécifiées dans le Nom de la liste d'accès. Si ce champ est activé, sélectionnez le Nom de la liste d'accès ci-dessous.

- **Nom de la liste d'accès** : permet d'indiquer le Nom de la liste d'accès (qui inclut une liste d'adresses IP) du filtrage des routes sortantes RIP pour une interface IP spécifiée. Pour obtenir une description des listes d'accès, reportez-vous à la section Paramètres de la liste d'accès.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres sont consignés dans le fichier de Configuration d'exécution.

Statistiques RIPv2

Pour afficher les compteurs de statistiques RIP de chaque adresse IP :

ÉTAPE 1 Cliquez sur **Configuration IP** > **RIPv2 > Statistiques RIPv2**.

Les champs suivants sont affichés :

- **Interface IP** : interface IP définie sur l'interface de couche 2.
- **Paquets incorrects reçus** : spécifie le nombre de paquets incorrects identifiés par RIP sur l'interface IP.
- **Routes incorrectes reçues** : spécifie le nombre de routes incorrectes reçues et identifiées par RIP sur l'interface IP. Les routes incorrectes sont des routes dont les paramètres de route sont incorrects. Par exemple, la destination IP est une adresse de diffusion, ou la métrique est 0 ou supérieure à 16.
- **Mise à jour envoyée** : indique le nombre de paquets envoyés par RIP sur l'interface IP.

ÉTAPE 2 Pour effacer tous les compteurs de l'interface, cliquez sur **Effacer tous les compteurs de l'interface**.

Base de données d'homologues RIPv2

Pour afficher la base de données des homologues RIP (voisins) :

ÉTAPE 1 Cliquez sur **Configuration IP** > **RIPv2 > Base de données de routeur homologue RIPv2**.

Les champs suivants sont affichés pour la base de données de routeur homologue :

- **Adresse IP du routeur** : interface IP définie sur l'interface de couche 2.

- **Paquets incorrects reçus** : spécifie le nombre de paquets incorrects identifiés par RIP sur l'interface IP.
- **Routes incorrectes reçues** : spécifie le nombre de routes incorrectes reçues et identifiées par RIP sur l'interface IP. Les routes incorrectes sont des routes dont les paramètres de route sont incorrects. Par exemple, la destination IP est une adresse de diffusion, ou la métrique est 0 ou supérieure à 16.
- **Date de dernière màj** : indique quand RIP a reçu pour la dernière fois des routes RIP depuis l'adresse IP distante.

ÉTAPE 2 Pour effacer tous les compteurs, cliquez sur **Effacer tous les compteurs de l'interface**.

Liste d'accès

Pour obtenir une description des listes d'accès, reportez-vous à la section Filtrage des mises à jour du routage.

Pour créer des listes d'accès, procédez comme suit :

1. Créez une liste d'accès avec une seule adresse IP, à l'aide de la page Liste d'accès.
2. Au besoin, ajoutez des adresses IP supplémentaires via la page Liste d'accès IPv4 source.

Paramètres de la liste d'accès

Pour définir la configuration globale d'une liste d'accès.

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4 > Liste d'accès** > **Paramètres de la liste d'accès**.

ÉTAPE 2 Afin d'ajouter une nouvelle liste d'accès, cliquez sur **Ajouter** pour ouvrir la page Ajouter une liste d'accès, puis renseignez les champs suivants :

- **Nom** : définissez un nom pour la liste d'accès.
- **Source IPv4 Address** (Adresse IPv4 source) : entrez l'adresse IPv6 source. Les options suivantes sont disponibles :
  - *Tous* : toutes les adresses IP sont incluses.
  - *Défini par l'utilisateur* : saisissez une adresse IP.

- **Masque de la source IPv4** : entrez le type et la valeur du masque d'adresse IPv4 source. Les options suivantes sont disponibles :
  - *Masque de réseau* : saisissez le masque de réseau.
  - *Longueur du préfixe* : saisissez la longueur du préfixe.
- **Action** : sélectionnez une action pour la liste d'accès. Les options suivantes sont disponibles :
  - *Autoriser* : permet d'autoriser l'entrée des paquets à partir des adresses IP contenues dans la liste d'accès.
  - *Refuser* : permet de refuser l'entrée des paquets à partir des adresses IP contenues dans la liste d'accès.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres sont consignés dans le fichier de Configuration d'exécution.

Liste d'accès IPv4 source

Pour peupler une liste d'accès avec des adresses IP.

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4 > Liste d'accès** > **Liste d'adresses IPv4 source**.

ÉTAPE 2 Pour modifier les paramètres d'une liste d'accès, cliquez sur **Add** (Ajouter) et modifiez l'un des champs suivants :

- **Nom de la liste d'accès** : nom de la liste d'accès.
- **Adresse IPv4 source** : adresse IPv4 source. Les options suivantes sont disponibles :
  - *Tous* : toutes les adresses IP sont incluses.
  - *Défini par l'utilisateur* : saisissez une adresse IP.
- **Masque de la source IPv4** : type et valeur du masque d'adresse IPv4 source. Les options suivantes sont disponibles :
  - *Masque de réseau* : saisissez le masque de réseau (par exemple, 255.255.0.0).
  - *Longueur du préfixe* : saisissez la longueur du préfixe.

- **Action** : action pour la liste d'accès. Les options suivantes sont disponibles :
  - *Autoriser* : permet d'autoriser l'entrée des paquets à partir des adresses IP contenues dans la liste d'accès.
  - *Refuser* : permet de refuser l'entrée des paquets à partir des adresses IP contenues dans la liste d'accès.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres sont consignés dans le fichier de Configuration d'exécution.

18

Configuration IP : VRRP

REMARQUE Cette fonctionnalité n'est prise en charge que sur les commutateurs de la gamme 550.

Ce chapitre décrit le fonctionnement du protocole VRRP (Virtual Router Redundancy Protocol) et la configuration des routeurs virtuels exécutant VRRP via une interface utilisateur graphique Web.

Elle couvre les sujets suivants :

Vue d'ensemble

VRRP est un protocole d'élection et de redondance qui attribue dynamiquement la responsabilité d'un routeur virtuel à l'un des routeurs physiques d'un LAN. Cette méthode joue en faveur de la disponibilité et de la fiabilité des voies de routage du réseau.

Avec VRRP, un routeur physique d'un routeur virtuel est désigné comme unité principale, tandis qu'un autre routeur physique du même routeur virtuel prend le relais si le routeur principal rencontre un problème. Les routeurs physiques sont appelés des routeurs VRRP.

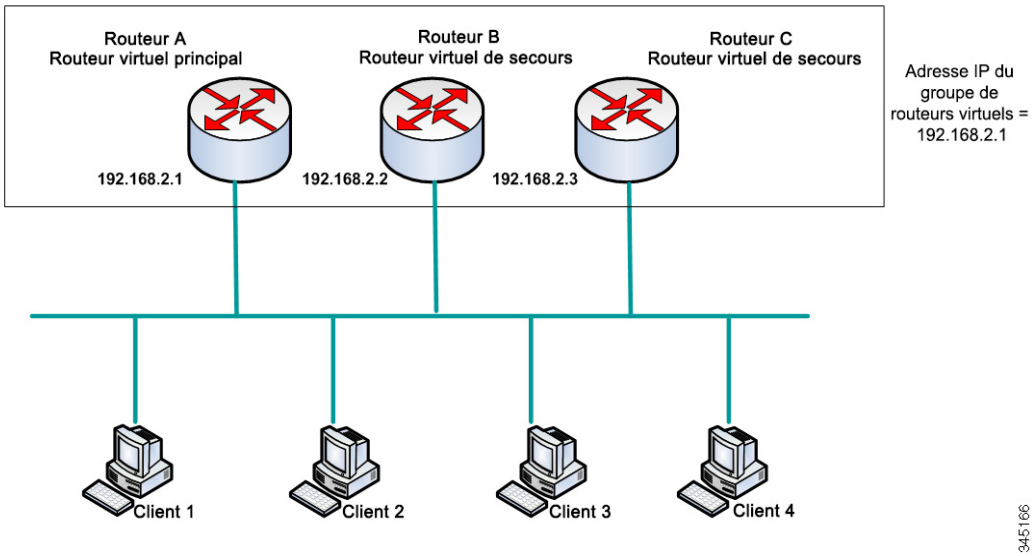
La passerelle par défaut d'un hôte participant est attribuée au routeur virtuel, et non à un routeur physique. Si le routeur physique qui procède au routage des paquets au nom du routeur virtuel est défaillant, un autre routeur physique est choisi automatiquement pour le remplacer. Le routeur physique qui transfère des paquets à tout moment est appelé le routeur principal.

Le protocole VRRP permet également de répartir la charge du trafic. Il est possible de partager équitablement le trafic entre les routeurs disponibles en configurant VRRP de sorte à ce que plusieurs routeurs se partagent le trafic vers et depuis des clients LAN.

Topologie VRRP

Vous allez découvrir la topologie d'un LAN sur lequel VRRP est configuré. Dans cet exemple, les routeurs A, B et C sont des routeurs VRRP et englobent un routeur virtuel. L'adresse IP du routeur virtuel est la même que celle configurée pour l'interface Ethernet du routeur A (198.168.2.1).

Topologie VRRP de base



Le routeur virtuel utilise l'adresse IP de l'interface Ethernet physique du routeur A, ce dernier joue donc le rôle de routeur virtuel principal et est également propriétaire de l'adresse IP. En tant que routeur virtuel principal, le routeur A contrôle l'adresse IP du routeur virtuel et se charge d'acheminer les paquets au nom du routeur virtuel. Les clients 1 à 3 sont configurés avec l'adresse IP de la passerelle par défaut : 198.168.2.1. Le client 4 est configuré avec l'adresse IP de la passerelle par défaut : 198.168.2.2.

REMARQUE Le routeur VRRP, propriétaire de l'adresse IP, répond/traite les paquets à destination de l'adresse IP. Le routeur VRRP, routeur virtuel principal, mais pas propriétaire de l'adresse IP, ne répond/traite pas ces paquets.

Les routeurs B et C font office de routeurs virtuels de secours. Si le routeur virtuel principal est défaillant, le routeur affichant la priorité la plus élevée prend sa place et propose ses services aux hôtes LAN tout en minimisant les interruptions.

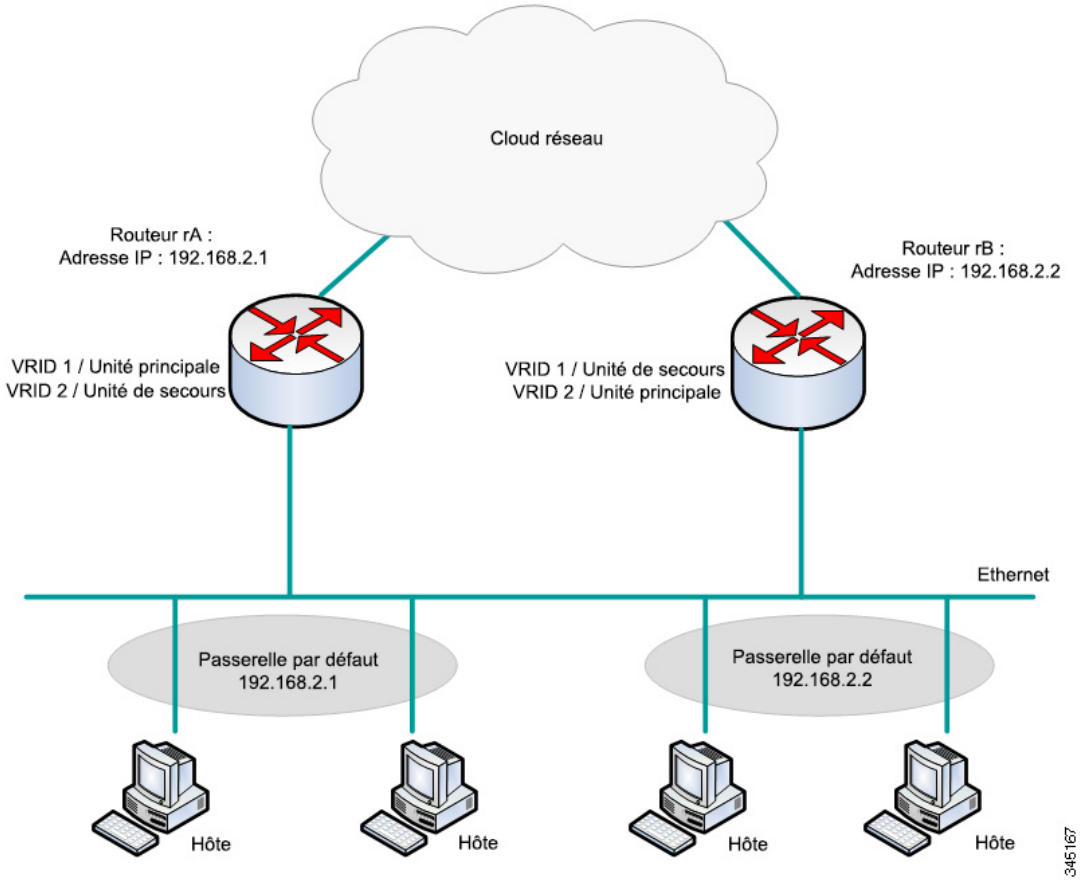
REMARQUE La priorité du routeur VRRP dépend des éléments suivants : si le routeur VRRP est le propriétaire, sa priorité est de 255 (la plus élevée) ; s'il n'est pas propriétaire, sa priorité est configurée manuellement (toujours inférieure à 255).

Lorsque le routeur A est à nouveau opérationnel, il reprend son rôle de routeur virtuel principal. Pendant toute la durée de l'indisponibilité, les deux routeurs principaux transfèrent des paquets, ce qui peut engendrer certains doublons (comportement normal), mais aucune interruption.

Pour en savoir plus sur les rôles joués par les routeurs VRRP et sur les conséquences d'une défaillance du routeur virtuel principal, consultez la section Priorité et devancement du routeur VRRP.

Vous allez découvrir la topologie d'un LAN sur lequel VRRP est configuré. Les routeurs A et B se partagent le trafic vers et depuis les clients 1 à 4. Ces routeurs sont les routeurs virtuels de secours l'un de l'autre en cas de panne.

Topologie VRRP du partage de charge



Dans cette topologie, deux routeurs virtuels sont configurés. Pour le routeur virtuel 1, rA est le propriétaire de l'adresse IP 192.168.2.1 et joue le rôle de routeur virtuel principal, et rB est le routeur virtuel de secours de rA. Les clients 1 et 2 sont configurés avec l'adresse IP de la passerelle par défaut : 198.168.2.1.

Pour le routeur virtuel 2, rB est le propriétaire de l'adresse IP 192.168.2.2 et joue le rôle de routeur virtuel principal, et rA est le routeur virtuel de secours de rB. Les clients 3 et 4 sont configurés avec l'adresse IP de la passerelle par défaut : 198.168.2.2.

Éléments configurables de VRRP

Chaque routeur virtuel du même LAN doit posséder un identifiant unique de routeur virtuel (VRID). Tous les routeurs VRRP prenant en charge le même routeur virtuel doivent être configurés à l'aide de toutes les informations relatives au routeur virtuel, y compris son VRID. Les routeurs virtuels doivent être activés sur le périphérique seulement si le routage IP est également activé.

Vous pouvez configurer un routeur VRRP de sorte à ce qu'il fasse partie d'un ou plusieurs routeurs virtuels, en utilisant soit l'interface de ligne de commande, soit l'interface utilisateur graphique Web, comme décrit dans la section Configuration de VRRP.

Pour configurer un routeur virtuel, vous renseignez toutes les informations utiles, telles que l'ID et les adresses IP du routeur virtuel, sur chaque routeur VRRP qui prend en charge le routeur virtuel. Vous pouvez configurer et personnaliser les éléments suivants.

Identification du routeur virtuel

Le routeur virtuel doit se voir attribuer un identifiant (VRID) et éventuellement une description. Les sections suivantes décrivent les différents attributs du routeur virtuel.

VRRP prend en charge jusqu'à 255 routeurs virtuels (groupes VRRP).

Versions VRRP

Le périphérique prend en charge les types de versions VRRP suivants :

- VRRPv3 IPv4 basé sur RFC5798. Des messages VRRPv3 sont envoyés.
- VRRPv3 et VRRPv2 IPv4 basés sur RFC5798. Des messages VRRPv3 et VRRPv2 sont envoyés.
- VRRPv2 IPv4 basé sur RC3768. Des messages VRRPv2 sont envoyés.

La version VRRP est configurée sur chaque routeur virtuel. VRRPv2 est la version par défaut.

Vous pouvez être confronté aux situations suivantes lors de la configuration d'un routeur virtuel :

- Tous les routeurs VRRP existants du routeur virtuel sont exécutés en mode VRRPv3. Dans ce cas, choisissez également VRRPv3 pour votre nouveau routeur VRRP.
- Tous les routeurs VRRP existants du routeur virtuel sont exécutés en mode VRRPv2. Dans ce cas, choisissez également VRRPv2 pour votre nouveau routeur VRRP.
- Si au moins un routeur VRRP du routeur virtuel est exécuté en mode VRRPv2 et VRRPv3. Dans ce cas, choisissez VRRPv3 pour votre routeur VRRP, même si VRRPv2 est également compatible.

  REMARQUE Si le routeur virtuel comporte des routeurs uniquement compatibles avec VRRPv2 et d'autres uniquement compatibles avec VRRPv3, vous devez configurer au moins un routeur VRRPv2 et VRRPv3.

REMARQUE Lorsque les modes VRRPv2 et VRRPv3 sont activés sur un routeur VRRP, ce dernier transmet des paquets VRRPv2 et VRRPv3. Conformément aux normes VRRPv3, l'activation des modes VRRPv2 et VRRPv3 doit être réalisée lors de la mise à niveau depuis v2 vers v3. Vous pouvez disposer des deux versions uniquement de manière temporaire. Veuillez consulter la norme VRRPv3 pour en savoir plus sur l'interconnexion entre VRRPv2 et VRRPv3.

Adresses IP du routeur virtuel

Chaque routeur virtuel se voit attribuer une ou plusieurs adresses IP dont le routeur principal actuel est en charge.

Un routeur VRRP prenant en charge un routeur virtuel doit posséder une interface IP sur le même sous-réseau IP incluant les adresses IP configurées sur le routeur virtuel.

Vous devez respecter les règles suivantes lorsque vous attribuez des adresses IP à un routeur virtuel :

- Tous les routeurs VRRP prenant en charge le routeur virtuel doivent être configurés avec les mêmes adresses IP que celles du routeur virtuel.
- Vous ne pouvez pas utiliser l'une des adresses IP pour un autre routeur virtuel ou pour des routeurs VRRP qui ne prennent pas en charge le routeur virtuel.
- L'un des routeurs VRRP prenant en charge le routeur virtuel doit être propriétaire de toutes les adresses IP du routeur virtuel. Un routeur VRRP est le propriétaire des adresses IP si ces dernières sont de véritables adresses configurées sur son interface IP.

- Si un routeur VRRP (le routeur physique) est propriétaire des adresses IP du routeur virtuel, l'adresse IP du routeur virtuel doit être configurée manuellement sur le routeur VRRP ; elle ne doit pas être attribuée via DHCP.
- Si un routeur VRRP n'est pas propriétaire des adresses IP du routeur virtuel :
  - Les routeurs VRRP non propriétaires doivent être configurés à l'aide d'une interface IP sur le même sous-réseau IP que les adresses IP du routeur virtuel.
  - Les sous-réseaux IP correspondants doivent être configurés manuellement au niveau du routeur VRRP ; ils ne doivent pas être attribués via DHCP.

Tous les routeurs VRRP prenant en charge le même routeur virtuel doivent être configurés de manière identique. Si les configurations sont différentes, la configuration du routeur principal sera utilisée. Un routeur VRRP de secours envoie un message SYSLOG lorsque sa configuration est différente de celle du routeur principal.

Adresse IP source d'un routeur VRRP

Chaque routeur VRRP prenant en charge un routeur virtuel utilise sa propre adresse IP comme adresse IP source dans ses messages VRRP sortants pour le routeur virtuel. Les routeurs VRRP du même routeur virtuel communiquent les uns avec les autres via des messages VRRP. Si un routeur VRRP est propriétaire de l'adresse IP du routeur virtuel, alors l'adresse IP correspond à l'une des adresses IP du routeur virtuel. Si un routeur VRRP n'est pas propriétaire de l'adresse IP du routeur virtuel, alors l'adresse IP correspond à l'adresse IP de l'interface du routeur VRRP sur le même sous-réseau IP que le routeur virtuel.

Si l'adresse IP source a été configurée manuellement, la configuration est supprimée et l'adresse IP source par défaut est utilisée (l'adresse IP la plus faible du routeur VRRP définie sur l'interface). Si l'adresse IP source correspond à celle par défaut, une nouvelle adresse IP source par défaut est utilisée.

Priorité et devancement du routeur VRRP

Un aspect essentiel du schéma de redondance VRRP consiste à attribuer une priorité VRRP à chaque routeur VRRP. Cette priorité VRRP doit faire référence à l'efficacité démontrée par un routeur VRRP qui remplacerait un routeur virtuel défini dans le routeur VRRP. Si plusieurs routeurs VRRP de secours se tiennent à disposition du routeur virtuel, la priorité détermine celui qui remplacera le routeur principal actuel en cas de défaillance.

Si un routeur virtuel est propriétaire de l'adresse IP, sa priorité VRRP est automatiquement attribuée par le système (255) et le routeur VRRP (sur lequel ce routeur virtuel est attribué) est automatiquement exécuté comme routeur virtuel principal s'il est actif.

Dans la figure «Topologie VRRP de base», si le routeur A, étant le routeur virtuel principal, est en panne, un processus de sélection est lancé pour déterminer si les routeurs de secours B ou C doivent le remplacer. Si les routeurs B et C disposent des priorités 101 et 100, respectivement, le routeur B deviendra le routeur virtuel principal en raison de sa priorité plus élevée. Si les deux routeurs ont la même priorité, celui affichant l'adresse IP la plus élevée sera choisi pour remplacer le routeur virtuel principal.

Par défaut, une fonction de devancement est activée, qui fonctionne comme suit :

- Activé : quand un routeur VRRP ayant une priorité plus élevée que le routeur principal actuel est actif, il remplace le routeur principal actuel.
- Désactivé : même si un routeur VRRP ayant une priorité plus élevée que le routeur principal actuel est actif, il ne remplace pas le routeur principal actuel. Seul le routeur principal d'origine (lorsqu'il est disponible) remplace le routeur de secours.

Annonces VRRP

Le routeur virtuel principal envoie des annonces VRRP aux routeurs du même groupe (disposant de la même identification de routeur virtuel).

Ces annonces sont encapsulées dans des paquets IP et envoyées à l'adresse IPv4 de multidiffusion attribuée au groupe VRRP. Les annonces sont envoyées chaque seconde par défaut ; vous pouvez définir l'intervalle d'annonce.

Cet intervalle est exprimé en ms (plage : 50 à 40950, valeur par défaut : 1 000). Une non-valeur n'est pas valide.

- Dans la version 3 du VRRP, l'intervalle d'annonce opérationnel est arrondi aux 10 ms inférieures les plus proches.
- Dans la version 2 du VRRP, l'intervalle d'annonce opérationnel est arrondi à la seconde inférieure la plus proche. La valeur opérationnelle minimale est de 1 s.

Configuration de VRRP

Routeurs virtuels

Les propriétés VRRP peuvent être configurées et personnalisées sur la page Routeurs virtuels VRRP.

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4 > VRRP > Routeurs virtuels**.

Les routeurs virtuels sont affichés. Les champs sont décrits sur la page **Ajouter**, sauf les champs suivants générés par le système :

- **État de l'unité principale/de secours** : indique si le routeur virtuel est une unité principale, une unité de secours ou aucune des deux.
- **Adresse principale de l'unité principale** : affiche l'adresse IP du routeur principal.
- **Mode devancement** : indique si le mode devancement est activé ou désactivé.

ÉTAPE 2 Pour ajouter un routeur virtuel, cliquez sur **AJOUTER**.

ÉTAPE 3 Renseignez les champs suivants :

- **Interface** : interface sur laquelle le routeur virtuel est défini.
- **Identifiant du routeur virtuel** : numéro défini par l'utilisateur identifiant le routeur virtuel.
- **Description** : chaîne définie par l'utilisateur identifiant le routeur virtuel.
- **État** : sélectionnez cette option pour activer VRRP sur le périphérique.
- **Version** : sélectionnez la version de VRRP à utiliser sur ce routeur.
- **Propriétaire de l'adresse IP** : si **Oui** est sélectionné, vous savez que l'adresse IP du périphérique correspond à l'adresse IP du routeur virtuel. Sélectionnez les adresses IP propriétaires dans la liste **Adresse IP disponible** et déplacez-les vers la liste **Adresse IP propriétaire**.

  Si vous sélectionnez **No** (Non), vous devez saisir la ou les adresses du routeur virtuel dans le champ **Virtual Router IP Addresses** (Adresses IP du routeur virtuel). Si vous ajoutez plusieurs adresses IP, séparez-les comme suit : 1.1.1.1, 2.2.2.2.
- **Adresse IP source** : sélectionnez l'adresse IP à utiliser dans les messages VRRP. L'adresse IP source par défaut est l'adresse IP la plus faible définie sur l'interface.
- **Priorité** : si ce périphérique est le propriétaire, ce champ indique la valeur 255 et vous ne pouvez pas la modifier. Dans le cas contraire, saisissez la priorité de ce périphérique en fonction de sa capacité à remplacer le routeur principal. 100 est la valeur par défaut d'un périphérique non propriétaire.
- **Mode devancement** : sélectionnez l'une des options suivantes :
  - *Vrai* : quand un routeur VRRP ayant une priorité plus élevée que le routeur principal actuel est actif, il remplace le routeur principal actuel.
  - *Faux* : même si un routeur VRRP ayant une priorité plus élevée que le routeur principal actuel est actif, il ne remplace pas le routeur principal actuel. Seul le routeur principal d'origine (lorsqu'il est disponible) remplace le routeur de secours.

- **Mode de contrôle d'acceptation** : sélectionnez l'une des options suivantes :
  - *Accepter* : le routeur virtuel dans l'état Maître acceptera les paquets à destination de l'adresse IP du routeur virtuel comme étant la sienne, même s'il n'en est pas le propriétaire.
  - *Abandonner* : le routeur virtuel dans l'état Maître supprimera les paquets à destination de l'adresse IP du routeur virtuel s'il n'en est pas le propriétaire.
- **Suivi IP SLA** : sélectionnez cette option pour activer le suivi de connexion entre le routeur et le saut suivant de la route par défaut.
- **Objet de suivi** : entrez le numéro du suivi SLA qui vérifie la connexion. Cette valeur a été saisie sur la page **Suivis SLA**.
- **Réduire** : si l'objet de suivi est dans l'état Inactif, la priorité VRRP du routeur est réduite de cette valeur.
- **Intervalle d'annonce** : indiquez la fréquence d'envoi des paquets d'annonce.

  REMARQUE Si ces paramètres sont modifiés (**Modifier**), le routeur virtuel est modifié et un nouveau message est envoyé en suivant les nouveaux paramètres.

ÉTAPE 4 Pour en savoir plus sur un routeur virtuel, cliquez sur **Détails**.

Les champs suivants sont affichés pour le routeur virtuel sélectionné :

- **Interface** : l'interface Couche 2 (port, LAG ou VLAN) sur laquelle le routeur virtuel est défini.
- **Identifiant du routeur virtuel** : numéro d'identification du routeur virtuel.
- **Adresse MAC du routeur virtuel** : adresse MAC virtuelle du routeur virtuel.
- **Table d'adresse IP du routeur virtuel** : adresses IP associées à ce routeur virtuel.
- **Description** : nom du routeur virtuel.
- **État supplémentaire**
  - *Version* : version du routeur virtuel.
  - *État* : activé pour le protocole VRRP.
  - *Propriétaire de l'adresse IP* : propriétaire de l'adresse IP du routeur virtuel.
  - *Temps de déphasage* : temps utilisé dans le calcul de l'intervalle d'arrêt de l'unité principale.
  - *Intervalle d'inactivité de l'unité principale* : durée d'inactivité de l'unité principale.

- *État de l'unité principale/de secours* : indique si le routeur virtuel est l'unité principale ou l'unité de secours.
- *Mode devancement* : indique si le mode devancement est activé.
- *Mode Accepter/Contrôler* : affiche Abandonner ou Accepter.

- **Paramètres de suivi**
  - *Objet de suivi* : entrez le numéro du suivi SLA qui vérifie la connexion.
  - *Réduire* : si l'objet de suivi est dans l'état Inactif, la priorité VRRP du routeur est réduite de cette valeur.
  - *État* : indique si la route est active ou inactive.
  - *Priorité actuelle* : affiche la priorité du routeur.
- **Mes paramètres (du routeur virtuel sélectionné)**
  - *Priorité* : priorité de ce périphérique de routeur virtuel, selon sa capacité à fonctionner comme unité principale.
  - *Intervalle d'annonce* : intervalle de temps décrit à la section Annonces VRRP.
  - *Adresse IP source* : adresse IP à utiliser dans les messages VRRP.
- **Paramètres principaux**
  - *Priorité* : 255
  - *Intervalle d'annonce* : intervalle de temps décrit à la section Annonces VRRP.
  - *Adresse IP source* : adresse IP à utiliser dans les messages VRRP.

Statistiques VRRP

Pour afficher les statistiques VRRP et effacer les compteurs de l'interface :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4 > VRRP > Statistiques VRRP**.

Les champs suivants sont affichés pour chaque interface sur laquelle VRRP est activé :

- **Interface** : affiche l'interface sur laquelle VRRP est activé.
- **Somme de contrôle non valide** : affiche le nombre de paquets ayant des sommes de contrôle non valides.

- **Longueur de paquet non valide** : affiche le nombre de paquets ayant des longueurs de paquet non valides.
- **TTL incorrect** : affiche le nombre de paquets ayant des valeurs TTL (Time-to-Live) non valides.
- **Type de paquet VRRP non valide** : affiche le nombre de paquets ayant des types de paquet VRRP non valides.
- **ID VRRP non valide** : affiche le nombre de paquets ayant des ID VRRP non valides.
- **Numéro de protocole non valide** : affiche le nombre de paquets ayant des numéros de protocole non valides.
- **Liste IP non valide** : affiche le nombre de paquets ayant des listes IP non valides.
- **Intervalle non valide** : affiche le nombre de paquets ayant des intervalles non valides.
- **Authentification non valide** : affiche le nombre de paquets dont l'authentification a échoué.

ÉTAPE 2 Sélectionnez une Interface.

ÉTAPE 3 Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs de cette interface.

ÉTAPE 4 Cliquez sur **Clear All Interface Counters** (Effacer tous les compteurs de l'interface) pour effacer tous les compteurs.

19

Configuration IP : SLA

REMARQUE Cette fonctionnalité n'est prise en charge que sur les commutateurs de la gamme 550.

Ce chapitre décrit l'utilisation de la fonctionnalité de contrat de niveau de service (SLA).

Il couvre les sujets suivants :

- Vue d'ensemble
- Utilisation du contrat de niveau de service (SLA)

Vue d'ensemble

Suivi IP SLA pour VRRP

VRRP désigne un protocole d'élection qui attribue, de façon dynamique, la responsabilité d'un routeur virtuel à l'un des routeurs physiques du réseau. Le routeur dont la priorité VRRP est la plus élevée est sélectionné comme routeur principal du réseau. Tous les autres routeurs sont des routeurs de secours. En cas de défaillance du routeur principal, le routeur de secours dont la priorité VRRP est la plus élevée prend le relais.

Le protocole VRRP fournit des informations sur l'état du routeur proprement dit, mais pas sur les états des routes utilisées par celui-ci. Par conséquent, lors de l'utilisation d'un routage statique, il se peut que le routeur principal continue de fonctionner comme tel, puisqu'il est fonctionnel, malgré la perte de connectivité entre le routeur et le saut suivant (route par défaut). Le contrat de niveau de service (SLA) IP VRRP fournit un mécanisme de suivi de la connectivité vers le saut suivant de la route par défaut du routeur VRRP. En cas de perte de connectivité vers le saut suivant, la priorité VRRP du routeur principal est réduite, ce qui permet à l'un des routeurs de secours de priorité supérieure (à la valeur décrémentée) de prendre le relais et de devenir le routeur principal. Cela a pour effet d'établir une connexion au saut suivant via le nouveau routeur principal sélectionné. Le contrat de niveau de service (SLA) IP n'est pas nécessaire lors de l'utilisation du protocole RIP ou d'autres protocoles de routage dynamique.

Le suivi des objets avec des contrats de niveau de service (SLA) IP repose sur les opérations IP SLA pour détecter une connexion vers une destination réseau donnée. Une opération de ce type envoie des paquets ICMP à l'adresse définie par l'utilisateur (le saut suivant requis) et surveille la réussite ou l'échec des réponses en provenance de l'hôte. Un objet de suivi est utilisé pour effectuer le suivi des résultats de l'opération et définir l'état sur *actif* ou *inactif* en fonction de la réussite ou de l'échec de la destination ICMP.

Un état d'objet de suivi peut être utilisé par diverses applications dans le cadre de décisions pour lesquelles la connectivité réseau doit être connue. VRRP constitue un parfait exemple de ce type d'application. L'objet de suivi est affecté à un routeur VRRP. Si l'état de suivi est « Inactif », la priorité VRRP du routeur est réduite selon une valeur définie par l'utilisateur. Si l'état de suivi est « Actif », la priorité VRRP d'origine du routeur est conservée.

Suivi IP SLA pour les routes statiques IPv4

Lors de l'utilisation d'un routage statique, il se peut qu'une route statique soit active, mais que le réseau de destination soit inaccessible via le saut suivant spécifié. Par exemple, la route statique en question présente la valeur la plus faible vers le réseau de destination et l'interface sortante vers le saut suivant est active ; cependant la connexion est « interrompue » sur le chemin vers le réseau de destination. Dans ce cas, il se peut que le périphérique utilise la route statique, bien qu'il ne fournisse pas de connexion au réseau de destination. Le suivi des objets IP SLA pour les routes statiques fournit un mécanisme de suivi de la connexion au réseau de destination via le saut suivant spécifié dans la route statique. En cas de perte de la connexion, l'état de la route est défini sur « Inactif » et, le cas échéant, une autre route statique (qui se trouve dans l'état « Actif ») peut être sélectionnée pour le trafic de routage.

À l'instar du suivi IP SLA pour VRRP, le suivi des objets IP SLA pour les routes statiques repose sur des opérations IP SLA pour détecter une connexion vers des réseaux de destination. L'opération IP SLA envoie des paquets ICMP à l'adresse définie par l'utilisateur (un hôte sur le réseau de destination requis) et définit le saut suivant à utiliser pour l'opération ping. Elle vérifie ensuite l'état des réponses en provenance de l'hôte (réussite ou échec). Un objet de suivi est utilisé pour effectuer le suivi des résultats de l'opération et définir l'état sur « Actif » ou « Inactif » en fonction de la réussite ou de l'échec de la destination ICMP. L'opération de suivi est affectée à une route statique. Si l'état du suivi est inactif, l'état de la route statique est défini sur « Inactif ». Si l'état du suivi est actif, l'état de la route statique reste « Actif ».

Vous trouverez, ci-dessous, la description des principaux termes utilisés dans cette section :

- **Opération** : chaque opération IP SLA ICMP Echo envoie une seule demande ICMP Echo à une adresse cible selon une fréquence configurée. Elle attend ensuite une réponse.

- **État de l'objet de suivi** : chaque objet de suivi conserve un état d'opération, à savoir : *Actif* ou *Inactif*. Après la création de l'objet, son état est défini sur *Actif*. Le tableau ci-dessous spécifie la conversion du code de retour de l'opération IP SLA en état d'objet :

Code de retour de l'opération	État de l'opération de suivi
OK	Actif
Erreur	Inactif

REMARQUE Si l'opération IP SLA spécifiée par l'argument de suivi n'est pas configurée ou si sa planification est *en attente*, son état est OK.

REMARQUE Une application liée à un objet de suivi inexistant se verra attribuer l'état *Actif*.

- **État de l'opération SLA** : cet état peut être défini sur **Planifié**, ce qui signifie que l'opération commence immédiatement, ou sur **En attente**, ce qui signifie qu'elle a été créée, mais pas activée.
- **Valeur d'expiration** : indique l'intervalle d'attente du message de réponse ICMP Echo ou d'un message d'erreur ICMP.
- **Code de retour** : une fois l'opération terminée, le code de retour correspondant est défini en fonction des éléments suivants :
  - Une réponse ICMP Echo a été reçue : le code de retour est défini sur **OK**.
  - Une réponse ICMP Error a été reçue : le code de retour est défini sur **erreur**.
  - Aucune réponse ICMP n'a été reçue : le code de retour est défini sur **erreur**.
  - Adresse IP source configurée ou Interface source inaccessible : le code de retour est défini sur erreur.
- **Suivi** : effectue le suivi des résultats des opérations.
- **Retard** : lorsque le résultat d'une opération IP SLA indique que l'état de l'objet de suivi doit passer de Y à X, cet objet effectue les actions suivantes :
  - L'état de l'objet de suivi n'est pas modifié et l'objet de suivi lance le retardateur pour l'intervalle.
  - Si l'état initial (Y) est reçu à nouveau au cours de la période d'activation du retardateur, ce dernier est annulé et l'état reste défini sur Y.
  - En cas d'expiration du retardateur, l'état de l'objet de suivi passe sur X et cet état est transmis aux applications associées.

Utilisation du contrat de niveau de service (SLA)

Opérations ICMP-Echo

Les opérations IP SLA ICMP-Echo peuvent être configurées sur cette page. Ces opérations seront exécutées conformément à la fréquence saisie.

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4 > SLA > Opérations ICMP-Echo**.

Les opérations ICMP-Echo sont affichées (certains champs sont décrits sur la page **Ajouter**) :

- **État** : indique En attente ou Planifié, comme décrit dans la section Vue d'ensemble ci-dessus.
- **Code de retour** : affiche OK ou Erreur, comme décrit dans la section Vue d'ensemble ci-dessus.

ÉTAPE 2 Pour ajouter une nouvelle opération, cliquez sur **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants :

- **Numéro d'opération** : indiquez un numéro inutilisé.
- **État de l'opération** : sélectionnez l'une des options suivantes :
  - *En attente* : l'opération n'est pas activée.
  - *Planifié* : l'opération est activée.

Paramètres ICMP-Echo

- **Cible de l'opération** : sélectionnez la méthode de définition de la cible de l'opération :
  - *Par IP* : entrez l'adresse IP de la cible de l'opération.
  - *Par nom d'hôte* : entrez le nom d'hôte de la cible de l'opération.

  REMARQUE Si l'opération IP SLA concerne la fonctionnalité Routes statiques, la cible de l'opération est l'adresse IP de l'hôte dans le réseau distant défini par la route statique.
- **Définition de la source** : si ce champ n'est pas défini, l'opération sélectionne l'adresse IP source la plus proche de la destination. Pour définir ce champ, sélectionnez l'une des options suivantes :
  - *Auto* : l'interface source est basée sur les informations de la table de redirection.
  - *Par adresse* : indiquez une autre adresse IP source.

- **Adresse IP du saut suivant** : sélectionnez **Aucune** ou **Définie par l'utilisateur**. Si l'option « Définie par l'utilisateur » est sélectionnée, entrez l'adresse IP du saut suivant. Ce paramètre doit être défini uniquement pour les opérations IP SLA utilisées pour les routes statiques.
- **Taille de données de la requête** : indiquez la taille des données du paquet de requêtes pour une opération ICMP Echo. Cette taille correspond à la partie de capacité utile du paquet ICMP, qui correspond à un paquet IP de 64 octets.
- **Fréquence** : indiquez la fréquence à laquelle l'opération SLA est exécutée (envoi de paquets). Cette valeur doit être supérieure à la valeur d'expiration.
- **Expiration** : indiquez la période pendant laquelle une opération IP SLA attend une réponse à son paquet de requêtes. Il est conseillé de baser la valeur de l'argument des millisecondes sur la somme du temps de parcours maximum pour les paquets et du temps de traitement de l'opération IP SLA.

ÉTAPE 4 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Suivis SLA

Les suivis SLA peuvent être configurés sur cette page. Ils permettent d'effectuer le suivi des codes de retour IP SLA et de définir l'état *actif* ou *inactif* en conséquence.

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4 > SLA > Suivis SLA**.

Les objets de suivi SLA sont affichés (certains champs sont décrits sur la page **Ajouter**) :

- **État** : affiche l'une des valeurs suivantes :
  - *Inactif* : aucune connexion à la route (le paquet a renvoyé le code Erreur).
  - *Actif* : connexion à la route (le paquet a renvoyé le code OK).
- **Type d'opération** : peut uniquement afficher **ICMP-Echo**.
- **Intervalle de retard restant (s)** : période de retard restante.

ÉTAPE 2 Pour ajouter un nouvel objet, cliquez sur **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants :

- **Numéro de suivi** : indiquez un numéro inutilisé.
- **Numéro d'opération** : sélectionnez une opération SLA dans la liste.

- **Délai - Actif** : indique le délai, en secondes, à observer pour passer de l'état Inactif à l'état Actif :
  - *Aucun* : l'état du suivi est modifié immédiatement.
  - *Période de retard* : l'état du suivi est modifié au terme de cette période.
- **Délai - Inactif** : indique le délai, en secondes, à observer pour passer de l'état Actif à l'état Inactif :
  - *Aucun* : l'état du suivi est modifié immédiatement.
  - *Période de retard* : l'état du suivi est modifié au terme de cette période.

ÉTAPE 4 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Statistiques ICMP-Echo

Pour afficher les statistiques SLA :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Interfaces et gestion IPv4 > SLA > Statistiques ICMP-Echo**.

ÉTAPE 2 Renseignez les champs suivants :

- **Opération SLA** : sélectionnez l'une des opérations définies précédemment.
- **Fréquence d'actualisation** : sélectionnez la fréquence d'actualisation des statistiques. Les options disponibles sont les suivantes :
  - *No Refresh* : les statistiques ne sont pas actualisées.
  - *15 s* : les statistiques sont actualisées toutes les 15 secondes.
  - *30 s* : les statistiques sont actualisées toutes les 30 secondes.
  - *60 s* : les statistiques sont actualisées toutes les 60 secondes.

ÉTAPE 3 Affichez les champs suivants :

- **Réussites de l'opération** : nombre de fois où l'opération Echo de suivi SLA a réussi.
- **Échecs de l'opération** : nombre de fois où l'opération Echo de suivi SLA a échoué.
- **Requêtes ICMP-Echo** : nombre de paquets de requêtes envoyés.
- **Réponses ICMP-Echo** : nombre de paquets de réponses reçus.
- **Erreurs ICMP-Echo** : nombre de paquets d'erreurs reçus.

Pour actualiser ces compteurs, cliquez sur :

- **Effacer les compteurs** : efface les compteurs de l'opération sélectionnée.
- **Effacer les compteurs de toutes les opérations** : efface les compteurs de toutes les opérations.
- **Actualiser** : actualise les compteurs.

20

Sécurité

Cette section décrit le contrôle d'accès et la sécurité du périphérique. Le système gère différents types de sécurité.

La liste de rubriques suivante décrit les différents types de fonctions de sécurité présentées dans cette section. Certaines fonctionnalités sont utilisées pour plusieurs types de sécurité ou de contrôle et s'affichent donc à plusieurs reprises dans la liste des rubriques présentée ci-dessous.

L'autorisation d'administrer le périphérique est décrite dans les sections suivantes :

- Configuration de TACACS+
- Sécurité du mot de passe
- Méthode d'accès de gestion
- Authentification de l'accès de gestion
- Gestion des clés
- Gestion sécurisée des données sensibles
- Serveur SSL
- Serveur SSH
- Client SSH

La protection contre les attaques visant le processeur du périphérique est décrite dans les sections suivantes :

- Services TCP/UDP
- Contrôle des tempêtes
- Contrôle d'accès

Le contrôle d'accès au réseau des utilisateurs finaux par l'intermédiaire du périphérique est décrit dans les sections suivantes :

- Méthode d'accès de gestion
- Configuration de TACACS+
- RADIUS
- Sécurité des ports
- Authentification 802.1X

La protection contre les autres utilisateurs du réseau est décrite dans les sections suivantes. Il s'agit d'attaques qui transitent par le périphérique, mais qui ne sont pas dirigées vers ce dernier.

- Prévention du déni de service
- Serveur SSL
- Contrôle des tempêtes
- Sécurité des ports
- Protection de la source IP
- Inspection ARP
- Contrôle d'accès
- Sécurité du premier saut

Configuration de 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 périphérique peut servir de client TACACS+ utilisant le serveur TACACS+ pour les services suivants :

- **Authentification** : assure l'authentification des utilisateurs se connectant au périphérique en utilisant des noms d'utilisateur et des mots de passe définis par l'utilisateur.

- **Autorisation** : effectuée au moment de la connexion. Une fois la session d'authentification terminée, une session d'autorisation commence en utilisant le nom d'utilisateur authentifié. Le serveur TACACS+ vérifie ensuite les privilèges de l'utilisateur.
- **Comptabilité** : activez la gestion de comptes des sessions de connexion à l'aide du serveur TACACS+. Cela permet à l'administrateur système de générer des rapports de gestion de comptes depuis le serveur TACACS+.

Outre le fait de fournir des services d'authentification et d'autorisation, le protocole TACACS+ permet de garantir la protection du message TACACS grâce à un corps de message TACACS chiffré.

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 en charge cette fonction, l'appareil revient à des connexions multiples.

Gestion de comptes utilisant un serveur TACACS+

L'utilisateur peut activer la gestion de comptes des sessions de connexion à l'aide d'un serveur RADIUS ou TACACS+.

Le port TCP configurable par l'utilisateur utilisé pour la gestion de comptes du serveur TACACS+ est le même port TCP utilisé pour l'authentification et l'autorisation du serveur TACACS+.

Les informations suivantes sont envoyées au serveur TACACS+ par le périphérique lorsque l'utilisateur se connecte ou se déconnecte :

Table 1:

Argument	Description	Dans le message de démarrage	Dans le message d'arrêt
task_id	Identificateur unique de session de gestion de comptes.	Oui	Oui
utilisateur	Nom d'utilisateur saisi pour l'authentification de la connexion.	Oui	Oui
rem-addr	Adresse IP de l'utilisateur.	Oui	Oui
elapsed-time	Indique la durée de connexion de l'utilisateur.	Non	Oui
reason	Rapports indiquant la raison de l'arrêt de la session.	Non	Oui

Valeurs par défaut

Les valeurs par défaut suivantes concernent cette fonction :

- Aucun serveur TACACS+ n'est défini par défaut.
- Si vous configurez un serveur TACACS+, la fonction de gestion de comptes est désactivée par défaut.

Interactions avec les autres fonctions

Vous ne pouvez pas activer la gestion de comptes sur un serveur RADIUS et un serveur TACACS+.

Flux de travail

Pour utiliser un serveur TACACS+, procédez comme suit :

ÉTAPE 1 Ouvrez un compte utilisateur sur le serveur TACACS+.

ÉTAPE 2 Configurez ce serveur et définissez les autres paramètres sur les pages Client TACACS+.

ÉTAPE 3 Sélectionnez **TACACS+** sur la page Gestion de l'authentification d'accès. Ainsi, lorsqu'un utilisateur se connecte au périphérique, l'authentification est effectuée sur le serveur TACACS+ au lieu de sur la base de données locale.

REMARQUE Si plusieurs serveurs TACACS+ ont été configurés, le périphérique utilise les priorités configurées des serveurs TACACS+ disponibles pour sélectionner le serveur TACACS+ à utiliser par le périphérique.

Client TACACS+

La page TACACS+ permet de configurer les serveurs TACACS+.

Seuls les utilisateurs qui ont le niveau de privilèges 15 sur le serveur TACACS+ peuvent administrer le périphérique. Le niveau de privilèges 15 est attribué à un utilisateur ou à un groupe d'utilisateurs sur le serveur TACACS+ par le biais de la chaîne suivante dans la définition de l'utilisateur ou du groupe :

```
service = exec {
priv-lvl = 15
}
```

Pour configurer les paramètres du serveur TACACS+ :

ÉTAPE 1 Cliquez sur **Sécurité** > **TACACS+**.

ÉTAPE 2 Activez **Gestion de comptes TACACS+** si nécessaire. Consultez l'explication fournie à la section Gestion de comptes utilisant un serveur TACACS+.

ÉTAPE 3 Configurez les paramètres par défaut suivants :

- **Chaîne de clé** : entrez la **Chaîne de clé** par défaut utilisée pour la communication avec tous les serveurs TACACS+ en mode **Chiffré** ou **Texte en clair**. Le périphérique peut être configuré pour utiliser cette clé ou pour utiliser une clé saisie pour un serveur spécifique (saisie sur la page Ajouter un serveur TACACS+).

  Si vous n'entrez pas de chaîne de clé dans ce champ, la clé de serveur saisie sur la page Ajouter un serveur TACACS+ doit correspondre à la clé de cryptage utilisée par le serveur TACACS+.

  Si vous entrez ici une chaîne de clé et une chaîne de clé pour un seul serveur TACACS+, la chaîne de clé configurée pour le serveur TACACS+ est prioritaire.

- **Délai de réponse** : saisissez la durée qui s'écoule avant l'expiration de la connexion entre le périphérique et le serveur TACACS+. Si aucune valeur n'est entrée sur la page Ajouter un serveur TACACS+ pour un serveur spécifique, la valeur appliquée est celle figurant dans ce champ.

- **Interface IPv4 source** : sélectionnez l'interface source IPv4 du périphérique à utiliser dans les messages envoyés pour les communications avec le serveur TACACS+.

- **Interface IPv6 source** : sélectionnez l'interface source IPv6 du périphérique à utiliser dans les messages envoyés pour les communications avec le serveur TACACS+.

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

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres TACACS+ par défaut sont ajoutés au fichier de Configuration d'exécution. Ces paramètres sont utilisés si les paramètres équivalents ne sont pas définis sur la page Ajouter.

Les informations relatives à chaque serveur TACACS sont affichées dans la Table des serveurs TACACS+. Les champs de cette table sont renseignés sur la page **Ajouter**, sauf le champ **État**. Ces champs indiquent si le serveur est connecté ou pas à l'appareil.

ÉTAPE 5 Pour ajouter un serveur TACACS+, cliquez sur **Ajouter**.

ÉTAPE 6 Saisissez les paramètres.

- **Définition du serveur** : sélectionnez l'une des méthodes d'identification du serveur TACACS+ ci-après :
  - *Par adresse IP* : si vous avez sélectionné cette option, entrez l'adresse IP du serveur dans le champ **Nom/Adresse IP du serveur**.
  - *Par nom* : si vous avez sélectionné cette option, entrez le nom du serveur dans le champ **Nom/Adresse IP du serveur**.
- **Version IP** : sélectionnez la version IP prise en charge pour l'adresse source : IPv6 ou IPv4.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée).
- **Nom/Adresse IP du serveur** : saisissez l'adresse IP ou le nom du serveur TACACS+.
- **Priorité** : saisissez l'ordre dans lequel ce serveur TACACS+ est utilisé. Zéro correspond au serveur TACACS disposant de la priorité la plus élevée : il s'agit du serveur qui sera utilisé en premier. Si le périphérique ne parvient pas à établir de session avec le serveur possédant la priorité la plus élevée, il essaie avec le serveur disposant du niveau de priorité suivant.
- **Chaîne de clé** : saisissez la chaîne de clé par défaut utilisée pour l'authentification et le cryptage entre le périphérique et le serveur TACACS+. La clé doit correspondre à celle configurée sur le serveur TACACS+.

  Une chaîne de clé est utilisée pour crypter les communications à l'aide de MD5. Vous pouvez sélectionner la clé par défaut du périphérique ou saisir une clé dans le formulaire **Crypté** ou **Texte en clair**. Si vous ne disposez pas de chaîne de clé cryptée (à partir d'un autre périphérique), saisissez la chaîne de clé en texte en clair et cliquez sur **Apply**. La chaîne de clé cryptée est générée et affichée.

  Si vous entrez une clé, la chaîne de clé par défaut est remplacée si une autre chaîne de clé est définie pour le périphérique sur la page principale.

- **Délai de réponse** : sélectionnez **Défini par l'utilisateur** et saisissez le laps de temps qui s'écoule avant l'expiration de la connexion entre le périphérique et le serveur TACACS+. Sélectionnez **Valeurs par défaut** pour utiliser la valeur par défaut affichée sur la page.
- **Port IP d'authentification** : saisissez le numéro de port via lequel s'opère la session TACACS+.
- **Connexion unique** : sélectionnez cette option afin de permettre la réception de toutes les informations à l'aide d'une seule connexion. Si le serveur TACACS+ ne prend pas en charge cette fonction, l'appareil revient à des connexions multiples.

ÉTAPE 7 Cliquez sur **Appliquer**. Le serveur TACACS+ est ajouté au fichier de Configuration d'exécution du périphérique.

ÉTAPE 8 Pour afficher les données sensibles sous forme de texte en clair sur cette page, cliquez sur **Afficher les données sensibles sous forme de texte clair**.

RADIUS

Les serveurs RADIUS (Remote Authorization Dial-In User Service) offrent un contrôle d'accès réseau basé sur MAC ou 802.1X centralisé.

Le périphérique peut être configuré en tant que client RADIUS pouvant utiliser un serveur RADIUS pour fournir une sécurité centralisée, et en tant que serveur RADIUS.

Client RADIUS

Une société peut utiliser le périphérique pour établir un serveur RADIUS (Remote Authorization Dial-In User Service, service d'authentification à distance des utilisateurs) afin de fournir un contrôle d'accès réseau basé sur MAC ou 802.1X centralisé à tous ses périphériques. Ainsi, les stratégies d'authentification et d'autorisation peuvent être traitées sur un seul serveur pour tous les périphériques de l'entreprise.

Lorsque le périphérique est configuré comme client RADIUS, il peut utiliser le serveur RADIUS pour les services suivants :

- **Authentification** : assure l'authentification des utilisateurs normaux et 802.1X se connectant au périphérique en utilisant des noms d'utilisateur et des mots de passe définis par l'utilisateur.

- **Autorisation** : effectuée au moment de la connexion. Une fois la session d'authentification terminée, une session d'autorisation commence en utilisant le nom d'utilisateur authentifié. Le serveur RADIUS vérifie ensuite les privilèges de l'utilisateur.

Comptabilité : activez la gestion de comptes des sessions de connexion à l'aide du serveur RADIUS. Cela permet à l'administrateur système de générer des rapports de gestion de comptes depuis le serveur RADIUS. Le port TCP configurable par l'utilisateur utilisé pour la gestion de comptes du serveur RADIUS est le même port TCP utilisé pour l'authentification et l'autorisation du serveur RADIUS.

Valeurs par défaut

Les valeurs par défaut suivantes concernent cette fonction :

- Aucun serveur RADIUS n'est défini par défaut.
- Si vous configurez un serveur RADIUS, la fonction de gestion de comptes est désactivée par défaut.

Interactions avec les autres fonctions

Vous ne pouvez pas activer la gestion de comptes à la fois sur un serveur RADIUS et sur un serveur TACACS+.

Flux de travail du serveur RADIUS

Pour utiliser un serveur RADIUS, procédez comme suit :

ÉTAPE 1 Ouvrez un compte pour le périphérique sur le serveur RADIUS.

ÉTAPE 2 Configurez ce serveur et les autres paramètres sur les pages RADIUS et Ajouter un serveur RADIUS.

REMARQUE Si plusieurs serveurs RADIUS ont été configurés, le périphérique utilise les priorités configurées des serveurs RADIUS disponibles pour sélectionner le serveur RADIUS à utiliser par le périphérique.

Pour définir les paramètres du serveur RADIUS :

ÉTAPE 1 Cliquez sur **Sécurité** > **Client RADIUS**.

ÉTAPE 2 Saisissez l'option Gestion de comptes RADIUS. Les options suivantes sont disponibles :

- **Contrôle d'accès basé sur les ports (802.1X, MAC, Authentification Web)** : spécifie que le serveur RADIUS est utilisé pour la gestion de comptes des ports 802.1x.

- **Accès de gestion** : spécifie que le serveur RADIUS est utilisé pour la gestion de comptes des connexions utilisateur.
- **Contrôle d'accès basé sur les ports et accès de gestion** : spécifie que le serveur RADIUS est utilisé à la fois pour la gestion de comptes des connexions utilisateur et la gestion de comptes des ports 802.1x.
- **Aucun** : spécifie que le serveur RADIUS n'est pas utilisé pour la gestion de comptes.

ÉTAPE 3 Saisissez les paramètres RADIUS par défaut, si nécessaire. Les valeurs entrées dans les Paramètres par défaut sont appliquées à tous les serveurs. Si une valeur n'est pas entrée pour un serveur spécifique (sur la page Ajouter un serveur RADIUS), le périphérique utilise les valeurs contenues dans ces champs.

- **Retries** : saisissez le nombre de demandes transmises qui sont envoyées au serveur RADIUS avant que le système considère qu'une défaillance s'est produite.
- **Délai de réponse** : saisissez le nombre de secondes pendant lesquelles le périphérique attend une réponse du serveur RADIUS avant de relancer la demande ou de passer au serveur suivant.
- **Délai d'inactivité** : saisissez le nombre de minutes qui s'écoulent avant qu'un serveur RADIUS non réactif soit contourné pour les demandes de services. Si la valeur est égale à 0, le serveur n'est pas contourné.
- **Chaîne de clé** : saisissez la chaîne de clé par défaut utilisée pour l'authentification et le cryptage entre le périphérique et le serveur RADIUS. Cette clé doit correspondre à la clé configurée sur le serveur RADIUS. Une chaîne de clé est utilisée pour crypter les communications à l'aide de MD5. Vous pouvez saisir la clé en mode **Chiffré** ou **Texte en clair**. Si vous ne disposez pas de chaîne de clé cryptée (à partir d'un autre périphérique), saisissez la chaîne de clé en texte en clair et cliquez sur **Apply**. La chaîne de clé cryptée est générée et affichée.

  Cette clé remplace la chaîne de clé par défaut, si une telle clé a été définie.

- **Interface IPv4 source** : sélectionnez l'interface source IPv4 du périphérique à utiliser dans les messages pour les communications avec le serveur RADIUS.
- **Interface IPv6 source** : sélectionnez l'interface IPv6 source du dispositif à utiliser dans les messages pour les communications avec le serveur RADIUS.

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

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres RADIUS par défaut du périphérique sont mis à jour dans le fichier de Configuration d'exécution.

Pour ajouter un serveur RADIUS, cliquez sur **Ajouter**.

ÉTAPE 5 Entrez les valeurs dans les champs pour chaque serveur RADIUS. Pour utiliser les valeurs par défaut entrées sur la page RADIUS, sélectionnez **Valeurs par défaut**.

- **Définition de serveur** : indiquez si vous souhaitez spécifier le serveur RADIUS par son adresse IP ou son nom.
- **Version IP** : sélectionnez la version de l'adresse IP du serveur RADIUS.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée).
- **Nom/Adresse IP du serveur** : spécifiez le serveur RADIUS par son adresse IP ou son nom.
- **Priority** : saisissez la priorité du serveur. La priorité détermine l'ordre dans lequel le périphérique essaie de contacter les serveurs pour authentifier un utilisateur. Le périphérique commence par le serveur RADIUS ayant la priorité la plus élevée (priorité zéro).
- **Chaîne de clé** : saisissez la chaîne de clé utilisée pour l'authentification et le cryptage des communications entre le périphérique et le serveur RADIUS. Cette clé doit correspondre à la clé configurée sur le serveur RADIUS. Vous pouvez la saisir en mode **Chiffré** ou **Texte en clair**. Si l'option **Valeurs par défaut** est sélectionnée, le périphérique essaie de s'authentifier sur le serveur RADIUS en utilisant la chaîne de clé par défaut.
- **Délai de réponse** : sélectionnez **Défini par l'utilisateur** et saisissez le nombre de secondes pendant lesquelles le périphérique attend une réponse du serveur RADIUS avant de relancer la demande ou de passer au serveur suivant si le nombre maximal de tentatives a été atteint. Si l'option **Valeurs par défaut** est sélectionnée, le périphérique utilise la valeur de délai par défaut.
- **Port d'authentification** : saisissez le numéro de port UDP du port du serveur RADIUS pour les demandes d'authentification.

- **Port de gestion de comptes** : saisissez le numéro de port UDP du port du serveur RADIUS pour les demandes de gestion de comptes.
- **Tentatives** : sélectionnez **Défini par l'utilisateur** et entrez le nombre de demandes envoyées au serveur RADIUS avant que l'on considère qu'une défaillance est survenue. Si l'option **Valeurs par défaut** est sélectionnée, le périphérique utilise la valeur par défaut du nombre de tentatives.
- **Délai d'inactivité** : sélectionnez **Défini par l'utilisateur** et saisissez le nombre de minutes qui doivent s'écouler avant qu'un serveur RADIUS non réactif soit contourné pour les demandes de services. Si l'option **Valeurs par défaut** est sélectionnée, le périphérique utilise la valeur par défaut du délai d'inactivité. Si vous saisissez 0 minute, aucun délai d'inactivité ne sera appliqué.
- **Type d'utilisation** : saisissez le type d'authentification du serveur RADIUS. Les options sont les suivantes :
  - *Connexion* : le serveur RADIUS est utilisé pour l'authentification des utilisateurs qui demandent à administrer le périphérique.
  - *802.1X* : le serveur RADIUS est utilisé pour l'authentification 802.1x.
  - *Tous* : le serveur RADIUS est utilisé pour l'authentification des utilisateurs qui demandent à administrer le périphérique et pour l'authentification 802.1X.

ÉTAPE 6 Cliquez sur **Appliquer**. La définition du serveur RADIUS est ajoutée au fichier de Configuration d'exécution du périphérique.

ÉTAPE 7 Pour afficher les données sensibles sous forme de texte en clair sur la page, cliquez sur **Afficher les données sensibles sous forme de texte clair**.

Serveur RADIUS

Le périphérique peut être configuré comme serveur RADIUS. Pour ce faire, utilisez les pages de l'interface utilisateur décrites ci-dessous.

Paramètres globaux du serveur RADIUS

Pour définir les paramètres globaux du serveur RADIUS :

ÉTAPE 1 Cliquez sur **Sécurité** > **Serveur RADIUS > Paramètres globaux du serveur RADIUS**.

ÉTAPE 2 Saisissez les paramètres suivants :

- **État du serveur RADIUS** : cochez cette case pour activer l'état de la fonctionnalité du serveur RADIUS.

- **Port d'authentification** : saisissez le numéro de port UDP du port du serveur RADIUS pour les demandes d'authentification.
- **Port de gestion de comptes** : saisissez le numéro de port UDP du port du serveur RADIUS pour les demandes de gestion de comptes.

Paramètres de filtre

- **Filtres de gestion de comptes RADIUS** : cochez cette case pour générer des filtres pour les événements de gestion de comptes RADIUS.
- **Filtres d'échec d'authentification RADIUS** : cochez cette case pour générer des filtres pour les tentatives de connexion qui ont échoué.
- **Filtres de réussite d'authentification RADIUS** : cochez cette case pour générer des filtres pour les connexions qui ont réussi.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres RADIUS par défaut du périphérique sont mis à jour dans le fichier de Configuration d'exécution.

Clés de serveur RADIUS

Pour définir les clés de serveur RADIUS :

ÉTAPE 1 Cliquez sur **Sécurité** > **Serveur RADIUS > Clés de serveur RADIUS**.

ÉTAPE 2 Saisissez les clés RADIUS par défaut, si nécessaire. Les valeurs saisies dans le champ Clé par défaut sont appliquées à tous les serveurs configurés (sur la page Ajouter un serveur RADIUS) afin d'utiliser la clé par défaut.

- **Clé par défaut** : saisissez la chaîne de clé par défaut utilisée pour l'authentification et le cryptage entre le périphérique et le client RADIUS. Sélectionnez l'une des options suivantes :
  - *Conserver la clé par défaut existante* : pour les serveurs spécifiés, le périphérique tente d'authentifier le client RADIUS en utilisant la chaîne de clé par défaut.
  - *Crypté* : pour crypter les communications en utilisant MD5, saisissez la clé sous forme cryptée.
  - *Texte en clair* : saisissez la chaîne de clé au format texte en clair.
- **Digest MD5** : affiche le Digest MD5 du mot de passe saisi par l'utilisateur.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres RADIUS par défaut du périphérique sont mis à jour dans le fichier de Configuration d'exécution.

ÉTAPE 4 Pour ajouter une clé secrète, cliquez sur **Ajouter** et renseignez les champs suivants :

- **Adresse NAS** : adresse du commutateur où réside le client RADIUS.
- **Clé secrète** : adresse du commutateur où réside le client RADIUS.
  - *Utiliser la clé par défaut* : pour les serveurs spécifiés, le périphérique tente d'authentifier le client RADIUS en utilisant la chaîne de clé par défaut existante.
  - *Crypté* : pour crypter les communications en utilisant MD5, saisissez la clé sous forme cryptée.
  - *Texte en clair* : saisissez la chaîne de clé au format texte en clair.

ÉTAPE 5 Cliquez sur **Appliquer**. La clé du périphérique est mise à jour dans le fichier de configuration d'exécution.

Groupes de serveurs RADIUS

Pour configurer un groupe d'utilisateurs qui se serviront du périphérique comme serveur RADIUS :

ÉTAPE 1 Cliquez sur **Sécurité** > **Serveur RADIUS > Groupes de serveurs RADIUS**.

ÉTAPE 2 Cliquez sur **Ajouter**, puis renseignez les champs suivants :

- **Nom du groupe** : saisissez le nom du groupe.
- **Niveau de privilège** : saisissez le niveau de privilège d'accès de gestion du groupe.
- **Période** : cochez cette case pour permettre l'application d'une période à ce groupe.
- **Nom de période** : si l'option Période est sélectionnée, choisissez la période à utiliser. Cliquez sur **Modifier** pour définir une période dans la section Plage horaire. Ce champ n'est affiché que si vous avez créé une période auparavant.
- **VLAN** : sélectionnez le VLAN pour les utilisateurs :
  - *Aucun* : aucun ID de VLAN n'est envoyé.
  - *ID de VLAN* : ID de VLAN envoyé.
  - *Nom de VLAN* : nom de VLAN envoyé.

ÉTAPE 3 Cliquez sur **Appliquer**. La définition du groupe RADIUS est ajoutée au fichier de configuration d'exécution du périphérique.

Utilisateurs du serveur RADIUS

Pour ajouter un utilisateur :

ÉTAPE 1 Cliquez sur **Sécurité** > **Serveur RADIUS > Utilisateurs du serveur RADIUS**.

Les utilisateurs actuels sont affichés.

ÉTAPE 2 Cliquez sur **Ajouter**.

- **Nom d'utilisateur** : saisissez le nom d'un utilisateur.
- **Nom du groupe** : sélectionnez un groupe défini précédemment.
- **Mot de passe** : entrez l'une des options suivantes :
  - *Crypté* : une chaîne de clé est utilisée pour crypter les communications à l'aide de MD5. Pour utiliser le cryptage, entrez la clé sous forme cryptée.
  - *Texte en clair* : si vous ne disposez pas de chaîne de clé cryptée (à partir d'un autre périphérique), saisissez la chaîne de clé en texte en clair. La chaîne de clé cryptée est générée et affichée.

ÉTAPE 3 Cliquez sur **Appliquer**. La définition de l'utilisateur est ajoutée au fichier de configuration d'exécution du périphérique.

Gestion de comptes du serveur RADIUS

Le serveur RADIUS enregistre les derniers journaux de gestion de comptes dans un fichier de cycle sur FLASH. Ces journaux peuvent être affichés.

Pour afficher la gestion de comptes du serveur RADIUS :

ÉTAPE 1 Cliquez sur **Sécurité** > **Serveur RADIUS > Gestion de comptes du serveur RADIUS**.

Les événements de gestion de comptes RADIUS sont affichés avec les champs suivants :

- **Nom d'utilisateur** : nom d'un utilisateur.
- **Type d'événement** : une des valeurs suivantes :
  - *Démarrer* : la session a été lancée.
  - *Arrêter* : la session a été arrêtée.
  - *Changement de date/heure* : modification de la date/heure du périphérique.
  - *Réinitialisation* : le périphérique a été réinitialisé à l'heure indiquée.

- **Méthode d'authentification** : méthode d'authentification utilisée. Affiche **S/O** si le type d'événement est Changement de date/heure ou Réinitialisation.
- **Adresse NAS** : adresse du commutateur où réside le client RADIUS. Affiche **S/O** si le type d'événement est Changement de date/heure ou Réinitialisation.
- **Adresse utilisateur** : si l'utilisateur authentifié est l'administrateur réseau, il s'agit de l'adresse IP ; si l'utilisateur est une station, il s'agit de l'adresse MAC. Affiche **S/O** si le type d'événement est Changement de date/heure ou Réinitialisation.
- **Heure d'événement** : heure de l'événement.

ÉTAPE 2 Pour afficher des informations supplémentaires sur un utilisateur/événement, sélectionnez l'élément souhaité, puis cliquez sur **Détails**.

Les champs suivants s'affichent :

REMARQUE Les champs de cette page dépendent du type de compte affiché et des détails reçus pour celui-ci. Tous les champs ne sont pas toujours affichés.

- **Heure d'événement** : voir ci-dessus.
- **Type d'événement** : voir ci-dessus.
- **Nom d'utilisateur** : voir ci-dessus.
- **Méthode d'authentification** : voir ci-dessus.
- **Adresse IPv4 NAS** : voir **Adresse NAS** ci-dessus.
- **Port NAS** : port utilisé sur le commutateur à l'adresse du NAS.
- **Adresse utilisateur** : voir ci-dessus.
- **Durée de session de gestion de comptes** : voir **Heure d'événement** ci-dessus.
- **Motif de fin de session** : affiche le motif de fin de la session ; une demande utilisateur, par exemple.

Utilisateurs rejetés par le serveur RADIUS

Pour afficher les utilisateurs qui ont tenté de s'authentifier à l'aide du serveur RADIUS et qui ont été rejetés :

ÉTAPE 1 Cliquez sur **Sécurité** > **Serveur RADIUS > Utilisateurs rejetés par RADIUS**.

Les utilisateurs rejetés sont affichés avec les champs suivants :

- **Type d'événement** : affiche l'une des options suivantes :
  - *Rejeté* : l'utilisateur a été rejeté.
  - *Changement d'heure* : l'horloge sur le périphérique a été modifiée par l'administrateur.
  - *Réinitialisation* : le périphérique a été réinitialisé par l'administrateur.
- **Nom d'utilisateur** : nom de l'utilisateur rejeté.
- **Type d'utilisateur** : affiche l'une des options d'authentification suivantes relatives à l'utilisateur :
  - *Nom de connexion* : utilisateur ayant accès à la gestion.
  - *802.1x* : utilisateur avec accès réseau 802.1x.
  - *S/O* : pour l'événement de réinitialisation.
- **Motif** : motif de rejet de l'utilisateur.
- **Heure** : heure à laquelle l'utilisateur a été rejeté.

ÉTAPE 2 Pour afficher des informations supplémentaires sur l'utilisateur rejeté, sélectionnez-le, puis cliquez sur **Détails**.

Les champs suivants s'affichent :

REMARQUE Les champs de cette page dépendent du type de compte affiché et des détails reçus pour celui-ci. Tous les champs ne sont pas toujours affichés.

- **Heure d'événement** : voir ci-dessus.
- **Nom d'utilisateur** : voir ci-dessus.
- **Type d'utilisateur** : voir ci-dessus.
- **Motif du rejet** : motif de rejet de l'utilisateur.
- **Adresse IP NAS** : adresse du serveur d'accès réseau (NAS). Le NAS est le commutateur qui exécute le client RADIUS.

Pour effacer le tableau des utilisateurs rejetés, cliquez sur **Effacer**.

Entrées NAS inconnues du serveur RADIUS

Pour afficher les refus d'authentification dus au fait que les serveurs NAS étaient inconnus du serveur RADIUS :

ÉTAPE 1 Cliquez sur **Sécurité** > **Serveur RADIUS > Entrées NAS inconnues du serveur RADIUS**.

Les champs suivants s'affichent :

- **(Journal) Type d'événement**
  - *NAS inconnu* : un événement NAS inconnu s'est produit.
  - *Changement d'heure* : l'horloge sur le périphérique a été modifiée par l'administrateur.
  - *Réinitialisation* : le périphérique a été réinitialisé par l'administrateur.
- **Adresse IP** : adresse IP du serveur NAS inconnu.
- **Heure** : horodatage de l'événement.

Statistiques du serveur RADIUS

Pour afficher les statistiques du serveur RADIUS :

ÉTAPE 1 Cliquez sur **Sécurité** > **Serveur RADIUS > Statistiques du serveur RADIUS**.

Les champs suivants s'affichent :

- **Source des statistiques** :
  - *Global* : statistiques pour tous les utilisateurs.
  - *NAS spécifique* : statistiques d'un NAS spécifique.
- **Fréquence d'actualisation** : sélectionnez la fréquence d'actualisation, autrement dit la durée qui s'écoule avant l'actualisation des statistiques de l'interface.
- **Paquets entrants sur le port d'authentification** : nombre de paquets reçus sur le port d'authentification.
- **Demandes d'accès entrantes depuis des adresses inconnues** : nombre de demandes d'accès entrantes en provenance d'adresses NAS inconnues.
- **Demandes d'accès entrantes en double** : nombre de paquets retransmis qui ont été reçus.

- **Acceptations d'accès envoyées** : nombre d'acceptations d'accès envoyées.
- **Rejets d'accès envoyés** : nombre de rejets d'accès envoyés.
- **Challenges d'accès envoyés** : nombre de challenges d'accès envoyés.
- **Demandes d'accès en entrée de format incorrect** : nombre de demandes d'accès reçues dans un format incorrect.
- **Demandes d'authentification entrantes avec un authentificateur incorrect** : nombre de paquets entrants avec des mots de passe incorrects.
- **Paquets d'authentification entrants avec d'autres erreurs** : nombre de paquets d'authentification entrants reçus avec d'autres erreurs.
- **Paquets d'authentification entrants de type inconnu** : nombre de paquets d'authentification entrants reçus de type inconnu.
- **Paquets entrants sur le port de gestion de comptes** : nombre de paquets entrants sur le port de gestion de comptes.
- **Demandes d'authentification entrantes depuis des adresses inconnues** : nombre de demandes d'authentification entrantes en provenance d'adresses inconnues.
- **Demandes de gestion de comptes entrantes en double** : nombre de demandes de compte en double en entrée.
- **Réponses de gestion de comptes envoyées** : nombre de réponses de gestion de comptes envoyées.
- **Demandes de gestion de comptes entrantes de format incorrect** : nombre de demandes de gestion de comptes de format incorrect.
- **Demandes de gestion de comptes entrantes avec un authentificateur incorrect** : nombre de demandes de gestion de comptes entrantes avec un authentificateur incorrect.
- **Paquets de gestion de comptes entrants avec d'autres erreurs** : nombre de paquets de gestion de comptes entrants avec d'autres erreurs.
- **Demandes de gestion de comptes entrantes non enregistrées** : nombre de demandes de gestion de comptes entrantes qui n'ont pas été enregistrées.
- **Paquets de gestion de comptes entrants de type inconnu** : nombre de paquets de gestion de comptes entrants de type inconnu.

Pour effacer les compteurs, cliquez sur **Effacer les compteurs**.

Pour actualiser les compteurs, cliquez sur **Actualiser**.

Sécurité du mot de passe

Le nom d'utilisateur/mot de passe par défaut est **cisco**/**cisco**. Lors de votre première ouverture de session avec le nom d'utilisateur et le mot de passe par défaut, vous devez saisir un nouveau mot de passe. L'option obligeant à créer des mots de passe complexes est activée par défaut. Si le mot de passe que vous choisissez n'est pas suffisamment complexe (les **Paramètres de complexité du mot de passe** peuvent être activés sur la page Sécurité du mot de passe), le système vous invite à créer un autre mot de passe.

Reportez-vous à la section Comptes d'utilisateur pour plus d'informations sur le mode de création d'un compte utilisateur.

Étant donné que les mots de passe permettent d'authentifier les utilisateurs qui accèdent au périphérique, les mots de passe trop 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.

Pour définir les règles de complexité des mots de passe :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du mot de passe**.

ÉTAPE 2 Saisissez les paramètres d'expiration suivants pour les mots de passe :

- **Expiration du mot de passe** : si cette option est sélectionnée, l'utilisateur sera invité à modifier le mot de passe une fois le **Délai d'expiration du mot de passe** atteint.
- **Délai d'expiration du mot de passe** : saisissez la durée en jours à l'issue de laquelle le système invite l'utilisateur à changer de mot de passe.

  REMARQUE L'expiration du mot de passe s'applique aussi aux mots de passe de longueur nulle (pas de mot de passe).

ÉTAPE 3 Sélectionnez **Paramètres de complexité du mot de passe** afin d'activer les règles de complexité pour les mots de passe.

Si la complexité du mot de passe est activée, les nouveaux mots de passe doivent être conformes aux paramètres par défaut suivants :

- Avoir une longueur minimale de huit caractères.
- Contenir des caractères appartenant à au moins trois classes de caractères (caractères majuscules, minuscules, numériques et spéciaux disponibles sur un clavier standard).
- Être différents du mot de passe actuel.
- Ne pas contenir de caractère répété plus de trois fois consécutivement.

- Ne pas répéter ou inverser le nom d'utilisateur ou toute variante obtenue en changeant la casse des caractères.
- Ne pas répéter ou inverser le nom du fabricant ou toute variante obtenue en changeant la casse des caractères.

ÉTAPE 4 Si les **Paramètres de complexité du mot de passe** sont activés, les paramètres suivants peuvent être configurés :

- **Minimal Password Length** : saisissez le nombre minimum de caractères requis pour les mots de passe.

  REMARQUE Un mot de passe de longueur nulle (pas de mot de passe) est autorisé, et un délai d'expiration du mot de passe peut lui être attribué.
- **Allowed Character Repetition** : saisissez le nombre de fois qu'un caractère peut être répété.
- **Minimal Number of Character Classes** : saisissez le nombre de classes de caractères qui doivent être présentes dans un mot de passe. Les classes de caractères sont minuscules (1), majuscules (2), chiffres (3) et symboles ou caractères spéciaux (4).
- **The New Password Must Be Different than the Current One** : si cette option est sélectionnée, lors de la modification du mot de passe, le nouveau mot de passe ne peut pas être identique au mot de passe actuel.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres de mot de passe sont écrits dans le fichier de Configuration d'exécution.

REMARQUE Il est possible de configurer l'équivalence nom d'utilisateur-mot de passe et l'équivalence fabricant-mot de passe via l'interface de ligne de commande (CLI). Pour des instructions supplémentaires, reportez-vous au *Guide de référence de l'interface de ligne de commande (CLI)*.

Gestion des clés

REMARQUE Cette section s'applique uniquement à la gamme de produits 550.

Cette section vous indique comment configurer des chaînes de clé pour les applications et les protocoles, tels que RIP. Pour obtenir une description de la façon dont RIP utilise une chaîne de clé pour l'authentification, reportez-vous à la section Configuration IP : RIPv2.

Il couvre les sujets suivants :

- Chaîne de clé
- Paramètres de la clé

Chaîne de clé

REMARQUE Cette fonctionnalité n'est prise en charge que sur les périphériques Sx550X/SG550XG.

Procédure de création d'une chaîne de clé :

ÉTAPE 1 Cliquez sur **Sécurité** > **Gestion de la clé** > **Paramètres de chaîne de la clé**.

ÉTAPE 2 Afin d'ajouter une nouvelle chaîne de clé, cliquez sur **Ajouter** pour ouvrir la page Ajouter chaîne de la clé et renseignez les champs suivants :

- **Chaîne de la clé** : nom de la chaîne de clé.
- **Identifiant de la clé** : identifiant entier de la chaîne de clé.
- **Chaîne de clé** : valeur de la chaîne de clé. Entrez l'une des options suivantes :
  - *Défini par l'utilisateur (chiffré)* : saisissez une version sous forme chiffrée.
  - *Défini par l'utilisateur (texte en clair)* : saisissez une version sous forme de texte en clair

  REMARQUE Vous pouvez entrer les valeurs **Accepter la durée de service** et **Envoyer la durée de service**. La valeur Accepter la durée de service indique quand l'identifiant de la clé est valide pour la réception des paquets. La valeur Envoyer la durée de service indique quand l'identifiant de la clé est valide pour l'envoi des paquets.
- **Accepter la durée de service/Envoyer la durée de service** : indique quand les paquets disposant de cette clé sont acceptés. Sélectionnez une des options suivantes :
  - *Toujours valable* : aucune limite de durée de service n'est définie pour l'identifiant de la clé.
  - *Défini par l'utilisateur* : la durée de service de la chaîne de clé est limitée. Si cette option est sélectionnée, renseignez les champs suivants :

  REMARQUE Si vous sélectionnez Défini par l'utilisateur, l'heure système doit être réglée manuellement ou depuis SNTP. Sinon, Accepter la durée de service et Envoyer la durée de service échouent systématiquement.

Les champs suivants sont pertinents pour les champs **Accept Life Time** (Accepter la durée de service) et **Send Life Time** (Envoyer la durée de service) :

- **Date de début** : entrez la date de début de validité de l'identifiant de la clé.
- **Heure de début** : entrez l'heure de début de validité de l'identifiant de la clé à la date de début spécifiée.
- **Heure de fin** : spécifie la date de fin de validité de l'identifiant de la clé. Sélectionnez une des options suivantes :
  - *Infini* : aucune limite de durée de service n'est définie pour l'identifiant de la clé.
  - *Durée* : la durée de service de l'identifiant de la clé est limitée. Si cette option est sélectionnée, renseignez les champs suivants :
- **Durée** : durée de validité de l'identifiant de la clé. Renseignez les champs suivants :
  - *Jours* : nombre de jours pendant lequel l'identifiant de la clé est valide.
  - *Heures* : nombre d'heures pendant lequel l'identifiant de la clé est valide.
  - *Minutes* : nombre de minutes pendant lequel l'identifiant de la clé est valide.
  - *Secondes* : nombre de secondes pendant lequel l'identifiant de la clé est valide.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres sont consignés dans le fichier de Configuration d'exécution.

Paramètres de la clé

Procédure d'ajout d'une clé à une chaîne de clé existante :

ÉTAPE 1 Cliquez sur **Sécurité** > **Gestion de la clé** > **Paramètres de la clé**.

ÉTAPE 2 Pour ajouter une nouvelle chaîne de clé, cliquez sur **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants :

- **Chaîne de la clé** : nom de la chaîne de clé.
- **Identifiant de la clé** : identifiant entier de la chaîne de clé.
- **Chaîne de clé** : valeur de la chaîne de clé. Entrez l'une des options suivantes :
  - *Défini par l'utilisateur (chiffré)* : saisissez une version sous forme chiffrée.
  - *Défini par l'utilisateur (texte en clair)* : saisissez une version sous forme de texte en clair.

REMARQUE Vous pouvez entrer les valeurs **Accepter la durée de service** et **Envoyer la durée de service**. La valeur **Accepter la durée de service** indique quand l'identifiant de la clé est valide pour la réception des paquets. La valeur **Envoyer la durée de service** indique quand l'identifiant de la clé est valide pour l'envoi des paquets. Les champs sont uniquement décrits pour **Accepter la durée de service**. Ils sont identiques pour **Envoyer la durée de service**.

- **Accepter la durée de service** : indique quand les paquets disposant de cette clé sont acceptés. Sélectionnez une des options suivantes :
  - *Toujours valable* : aucune limite de durée de service n'est définie pour l'identifiant de la clé.
  - *Défini par l'utilisateur* : la durée de service de la chaîne de clé est limitée. Si cette option est sélectionnée, renseignez les champs suivants :
- **Date de début** : entrez la date de début de validité de l'identifiant de la clé.
- **Date de fin** : entrez la date de fin de validité de l'identifiant de la clé.
- **Heure de début** : entrez l'heure de début de validité de l'identifiant de la clé à la date de début spécifiée.
- **Heure de fin** : spécifie la date de fin de validité de l'identifiant de la clé. Sélectionnez une des options suivantes :
  - *Infini* : aucune limite de durée de service n'est définie pour l'identifiant de la clé.
  - *Durée* : la durée de service de l'identifiant de la clé est limitée. Si cette option est sélectionnée, renseignez les champs suivants :
- **Durée** : durée de validité de l'identifiant de la clé. Renseignez les champs suivants :
  - *Jours* : nombre de jours pendant lequel l'identifiant de la clé est valide.
  - *Heures* : nombre d'heures pendant lequel l'identifiant de la clé est valide.
  - *Minutes* : nombre de minutes pendant lequel l'identifiant de la clé est valide.
  - *Secondes* : nombre de secondes pendant lequel l'identifiant de la clé est valide.

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

ÉTAPE 5 Pour toujours afficher les données confidentielles sous forme de texte en clair (et non sous forme chiffrée), cliquez sur **Afficher les données sensibles en texte clair**.

Méthode d'accès de gestion

Cette rubrique décrit les règles d'accès correspondant à diverses méthodes de gestion.

Elle couvre les sujets suivants :

- Profil d'accès
- Règles de profils

Les profils d'accès déterminent la façon d'authentifier les utilisateurs et de les autoriser à accéder au périphérique via différentes méthodes d'accès. Les profils d'accès peuvent limiter l'accès de gestion à partir de sources spécifiques.

Seuls les utilisateurs qui passent le profil d'accès actif et les méthodes d'authentification de l'accès de gestion peuvent accéder au périphérique.

Un seul profil d'accès à la fois peut être actif sur le périphérique.

Les profils d'accès contiennent une ou plusieurs règles. Les règles sont exécutées dans l'ordre c'est-à-dire en fonction de leur priorité dans le profil d'accès (de haut en bas).

Les règles sont composées de filtres qui incluent les éléments suivants :

- **Méthodes d'accès** : méthodes permettant l'accès au périphérique et sa gestion :
  - 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** : ports (y compris le port OOB), LAG ou VLAN autorisés à accéder à l'utilitaire de configuration Web ou interdits d'accès à celui-ci.
- **Adresse IP source** : adresses ou sous-réseauxIP. 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 périphérique 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

La page Access Profiles affiche les profils d'accès définis et permet de sélectionner un profil d'accès en tant que profil actif.

Lorsqu'un utilisateur tente d'accéder au périphérique par le biais d'une méthode d'accès, le périphérique vérifie si le profil d'accès actif autorise explicitement l'accès de gestion au périphérique via cette méthode. Si aucune correspondance n'est trouvée, l'accès est refusé.

Lorsqu'une tentative d'accès au périphérique s'effectue en violation du profil d'accès actif, le périphérique génère un message SYSLOG pour en avertir l'administrateur système.

Si un profil d'accès Console uniquement a été activé, la seule façon de le désactiver est d'établir une connexion directe entre la station de gestion et le port de console physique sur le périphérique.

Pour plus d'informations, reportez-vous à la section Règles de profils.

Utilisez la page Access Profiles pour créer un profil d'accès et ajouter sa première règle. Si le profil d'accès ne contient qu'une seule règle, vous avez terminé. Pour ajouter des règles supplémentaires au profil, utilisez la page Profile Rules.

ÉTAPE 1 Cliquez sur **Sécurité** > **Méthode d'accès de gestion** > **Profils d'accès**.

Cette page affiche tous les profils d'accès, qu'ils soient actifs ou non.

ÉTAPE 2 Pour modifier le profil d'accès actif, sélectionnez un profil dans le menu déroulant **Profil d'accès actif** et cliquez sur **Appliquer**. Le profil choisi devient alors le profil d'accès actif.

> REMARQUE Un message d'avertissement s'affiche si vous avez sélectionné Console uniquement. Si vous poursuivez, vous serez immédiatement déconnecté de l'utilitaire de configuration Web et ne pourrez plus accéder au périphérique que via le port console. Cela s'applique uniquement aux types d'appareils qui comportent un port de console.

Si vous sélectionnez un autre profil d'accès, un message s'affiche pour vous avertir que, selon le profil d'accès sélectionné, vous pourriez être déconnecté de l'utilitaire de configuration Web.

ÉTAPE 3 Cliquez sur **OK** pour sélectionner le profil d'accès actif ou sur **Annuler** pour abandonner cette action.

ÉTAPE 4 Cliquez sur **Ajouter** pour ouvrir la page Ajouter un profil d'accès. Cette page vous permet de configurer un nouveau profil ainsi qu'une règle.

ÉTAPE 5 Saisissez le **Nom du profil d'accès**. Ce nom peut comporter jusqu’à 32 caractères.

ÉTAPE 6 Saisissez les paramètres.

- **Rule Priority** : saisissez la priorité des règles. Lorsque le paquet est mis en correspondance avec une règle, les groupes d'utilisateurs se voient accorder ou refuser l'accès au périphérique. La priorité des règles est indispensable pour faire correspondre les paquets aux règles, la correspondance des paquets étant établie sur une base de première correspondance. La priorité la plus élevée est « 1 ».
- **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 périphérique répondant aux critères du profil d'accès Telnet se voient autoriser ou refuser l'accès.
  - *Telnet sécurisé (SSH)* : les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès SSH se voient autoriser ou refuser l'accès.
  - *HTTP* : les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès HTTP se voient autoriser ou refuser l'accès.
  - *HTTP sécurisé (HTTPS)* : les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès HTTPS se voient autoriser ou refuser l'accès.
  - *SNMP* : les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès SNMP se voient autoriser ou refuser l'accès.
- **Action** : sélectionnez l'action rattachée à la règle. Les options sont les suivantes :
  - *Autoriser* : autorise l'accès au périphérique dans la mesure où l'utilisateur correspond aux paramètres du profil.
  - *Refuser* : refuse l'accès au périphérique dans la mesure où l'utilisateur correspond aux paramètres du profil.
- **Applies to Interface** : sélectionnez l'interface rattachée à la règle. Les options sont les suivantes :
  - *All* : s'applique à tous les ports, VLAN et LAG.
  - *Défini par l'utilisateur* : s'applique à l'interface sélectionnée.
- **Interface** : entrez le numéro d'interface si l'option Défini par l'utilisateur a été sélectionnée.

- **Applies to Source IP Address** : sélectionnez le type d'adresse IP source auquel le profil d'accès s'applique. Le champ *Adresse IP source* est valide pour un sous-réseau. Sélectionnez l'une des valeurs suivantes :
  - *Tout* : s'applique à tous les types d'adresses IP.
  - *User Defined* : s'applique uniquement aux types d'adresses IP définis dans les champs.
- **Version IP** : entrez la version de l'adresse IP source : Version 6 ou Version 4.
- **IP Address** : saisissez l'adresse IP source.
- **Mask** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs suivants :
  - *Masque de réseau* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Longueur du préfixe* : sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l'adresse IP source.

ÉTAPE 7 Cliquez sur **Appliquer**. Le profil d'accès est écrit dans le fichier de Configuration d'exécution. Vous pouvez à présent sélectionner ce profil d'accès en tant que profil d'accès actif.

Règles de profils

Les profils d'accès peuvent comporter jusqu'à 128 règles afin de déterminer qui est autorisé à gérer le périphérique ainsi qu'à y accéder et les méthodes d'accès pouvant être utilisées.

Chaque règle d'un profil d'accès comporte une action et des critères (un ou plusieurs paramètres) à faire correspondre. Une priorité est affectée à chaque règle. Les règles ayant la priorité la plus basse sont vérifiées en premier. Si le paquet entrant correspond à une règle, l'action associée à cette dernière est appliquée. Si aucune règle correspondante n'est trouvée dans le profil d'accès actif, le paquet est abandonné.

Par exemple, vous pouvez limiter l'accès au périphérique depuis toutes les adresses IP à l'exception de celles qui sont attribuées au centre de gestion informatique. Le périphérique peut ainsi continuer à être géré tout en bénéficiant d'un autre niveau de sécurité.

Pour ajouter des règles de profil à un profil d'accès :

ÉTAPE 1 Cliquez sur **Sécurité** > **Méthode d'accès de gestion** > **Règles de profil**.

ÉTAPE 2 Sélectionnez le champ Filtre et un profil d'accès. Cliquez sur **Go**.

Le profil d'accès sélectionné apparaît dans la Table des règles de profil.

ÉTAPE 3 Cliquez sur **Ajouter** pour ajouter une règle.

ÉTAPE 4 Saisissez les paramètres.

- **Nom du profil d'accès** : sélectionnez un profil d'accès.
- **Rule Priority** : saisissez la priorité des règles. Lorsque le paquet est mis en correspondance avec une règle, les groupes d'utilisateurs se voient accorder ou refuser l'accès au périphérique. La priorité des règles est indispensable pour faire correspondre les paquets aux règles, la correspondance des paquets étant établie sur une base de première correspondance.
- **Management Method** : sélectionnez la méthode de gestion pour laquelle la règle est définie. Les options sont les suivantes :
  - *All* : affecte toutes les méthodes de gestion à la règle.
  - *Telnet* : les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès Telnet se voient autoriser ou refuser l'accès.
  - *Telnet sécurisé (SSH)*: les utilisateurs demandant l'accès au périphérique 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 périphérique répondant aux critères du profil d'accès HTTP se voient autoriser ou refuser l'accès.
  - *HTTP sécurisé (HTTPS)* : les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès HTTPS se voient autoriser ou refuser l'accès.
  - *SNMP* : les utilisateurs demandant l'accès au périphérique répondant aux critères du profil d'accès SNMP se voient autoriser ou refuser l'accès.
- **Action** : sélectionnez l'une des options suivantes :
  - *Autoriser* : autorise l'accès aux périphériques aux utilisateurs provenant de la source IP et de l'interface définies dans cette règle.
  - *Refuser* : refuse l'accès aux périphériques aux utilisateurs provenant de la source IP et de l'interface définies dans cette règle.

- **Applies to Interface** : sélectionnez l'interface rattachée à la règle. Les options sont les suivantes :
  - *All* : s'applique à tous les ports, VLAN et LAG.
  - *Défini par l'utilisateur* : s'applique uniquement au port, VLAN ou LAG sélectionné.
- **Interface** : entrez le numéro d'interface. Vous pouvez également indiquer le port OOB.
- **Applies to Source IP Address** : sélectionnez le type d'adresse IP source auquel le profil d'accès s'applique. Le champ *Adresse IP source* est valide pour un sous-réseau. Sélectionnez l'une des valeurs suivantes :
  - *Tout* : s'applique à tous les types d'adresses IP.
  - *User Defined* : s'applique uniquement aux types d'adresses IP définis dans les champs.
- **Version IP** : sélectionnez la version IP prise en charge pour l'adresse source : IPv6 ou IPv4.
- **IP Address** : saisissez l'adresse IP source.
- **Masque** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs :
  - *Masque de réseau* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Longueur du préfixe* : sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l'adresse IP source.

ÉTAPE 5 Cliquez sur **Appliquer**. La règle est ajoutée au profil d'accès.

Authentification de l'accès de gestion

Vous pouvez attribuer des modes d'autorisation et d'authentification aux différentes méthodes d'accès de gestion, telles que SSH, console, Telnet, HTTP et HTTPS. L'authentification peut être effectuée localement ou sur un serveur TACACS+ ou RADIUS.

Si l'autorisation est activée, l'identité et les privilèges de lecture/écriture de l'utilisateur font l'objet d'une vérification. Si l'autorisation n'est pas activée, seule l'identité de l'utilisateur est vérifiée.

La méthode d'autorisation/authentification utilisée est déterminée par l'ordre de sélection des méthodes d'authentification. Si la première méthode d'authentification n'est pas disponible, la méthode suivante sera utilisée. Par exemple, si les méthodes d'authentification sélectionnées sont RADIUS et Local, et que tous les serveurs RADIUS configurés sont interrogés en vertu de leur ordre de priorité et qu'ils ne répondent pas, l'utilisateur est autorisé/authentifié au niveau local.

Si l'autorisation est activée et si une méthode d'authentification échoue ou si le niveau de privilège de l'utilisateur est insuffisant, ce dernier se voit refuser l'accès au périphérique. En d'autres termes, si l'authentification échoue pour une méthode d'authentification, le périphérique n'essaie pas d'utiliser la méthode d'authentification suivante et s'arrête.

De la même façon, si l'autorisation n'est pas activée et que l'authentification échoue pour une méthode, le périphérique arrête la tentative d'authentification.

Pour définir les méthodes d'authentification d'une méthode d'accès :

ÉTAPE 1 Cliquez sur **Sécurité** > **Authentification de l'accès de gestion**.

ÉTAPE 2 Renseignez le champ **Application** (type) de la méthode d'accès de gestion.

ÉTAPE 3 Sélectionnez **Autorisation** pour activer l'authentification et l'autorisation de l'utilisateur selon la liste des méthodes décrites ci-dessous. Si vous ne sélectionnez pas le champ, seule l'authentification est exécutée. Si l'autorisation est activée, les privilèges de lecture/écriture des utilisateurs font l'objet d'une vérification. Le niveau de privilège est défini sur la page Comptes d'utilisateur.

ÉTAPE 4 Utilisez les flèches pour déplacer la méthode d'authentification entre la colonne **Méthodes facultatives** et la colonne **Méthodes sélectionnées**. La première méthode sélectionnée correspond à celle qui sera utilisée en premier.

- *RADIUS* : l'utilisateur est autorisé/authentifié sur un serveur RADIUS. Vous devez avoir configuré un ou plusieurs serveurs RADIUS. Pour que le serveur RADIUS accorde l'accès à l'utilitaire de configuration Web, ce serveur doit renvoyer cisco-avpair = shell:priv-lvl=15.
- *TACACS+* : l'utilisateur est autorisé/authentifié sur le serveur TACACS+. Vous devez avoir configuré un ou plusieurs serveurs TACACS+.
- *Aucun* : l'utilisateur est autorisé à accéder au périphérique sans autorisation/authentification.
- *Locale* : le nom d'utilisateur et le mot de passe sont comparés aux données stockées sur le périphérique local. Ces paires de nom d'utilisateur et mot de passe sont définies sur la page Comptes d'utilisateur.

REMARQUE La méthode d'authentification **Local** ou **None** doit toujours être sélectionnée en dernier. Toutes les méthodes d'authentification sélectionnées après **Local** ou **None** sont ignorées.

ÉTAPE 5 Cliquez sur **Appliquer**. Les méthodes d'authentification sélectionnées sont associées à la méthode d'accès.

Gestion sécurisée des données sensibles

Reportez-vous à la section Sécurité : Gestion sécurisée des données sensibles.

Serveur SSL

Cette section décrit la fonctionnalité SSL (Secure Socket Layer).

Elle couvre les sujets suivants :

- Présentation de SSL
- Paramètres d'authentification de serveur SSL

Présentation de SSL

La fonctionnalité SSL (Secure Socket Layer) permet d'ouvrir une session HTTPS sur l'appareil.

Une session HTTPS peut être ouverte avec le certificat par défaut qui est présent sur l'appareil.

Certains navigateurs génèrent des avertissements lors de l'utilisation d'un certificat par défaut, car ce certificat n'est pas signé par une autorité de certification (CA, Certification Authority). Il est recommandé d'utiliser un certificat signé par une CA de confiance.

Pour ouvrir une session HTTPS avec un certificat créé par l'utilisateur, procédez comme suit :

1. Générez un certificat.
2. Demandez que le certificat soit certifié par une CA.
3. Importez le certificat signé dans l'appareil.

Par défaut, le périphérique contient un certificat qui peut être modifié.

HTTPS est activé par défaut.

Paramètres d'authentification de serveur SSL

Il peut être nécessaire de générer un nouveau certificat pour remplacer le certificat par défaut présent sur l'appareil.

Pour créer un certificat :

ÉTAPE 1 Cliquez sur **Sécurité > Serveur SSL > Paramètres d'authentification de serveur SSL**.

Les informations relatives aux **numéros de certificats actifs SSL** 1 et 2 apparaissent dans la Table des clés de serveur SSL. Sélectionnez l'un des champs suivants :

Ces champs sont définis sur la page **Modifier**, excepté pour les champs suivants :

- **Valide du** : spécifie la date à partir de laquelle le certificat est valide.
- **Valide jusqu'au** : spécifie la date jusqu'à laquelle le certificat est valide.
- **Source du certificat** : spécifie si le certificat a été généré par le système (Autogénéré) ou l'utilisateur (Défini par l'utilisateur).

ÉTAPE 2 Sélectionnez un certificat actif.

ÉTAPE 3 Cliquez sur **Générer une demande de certificat**.

ÉTAPE 4 Renseignez les champs suivants :

- **ID de certificat** : sélectionnez le certificat actif.
- **Nom courant** : spécifie l'adresse IP ou l'URL complète de l'appareil. Si elle n'est pas indiquée, le système utilisera l'adresse IP la plus basse de l'appareil (lors de la génération du certificat).
- **Unité organisationnelle** : spécifie l'unité organisationnelle ou le nom du service.
- **Nom de l'organisation** : spécifie le nom de l'organisation.
- **Lieu** : spécifie l'emplacement ou le nom de la ville.
- **État** : spécifie le nom de l'état ou de la province.
- **Pays** : spécifie le nom du pays.
- **Durée** : indiquez la durée de validité du certificat (en jours).
- **Demande de certificat** : affiche la clé créée lorsque vous cliquez sur le bouton **Demande de génération d'un certificat**.

ÉTAPE 5 Cliquez sur **Générer une demande de certificat**. Le système crée alors une clé qui doit être entrée dans l'autorité de certification (Certification Authority, CA). Copiez-la à partir du champ **Demande de certificat**.

Procédure d'importation d'un certificat :

ÉTAPE 1 Cliquez sur **Sécurité > Serveur SSL > Paramètres d'authentification de serveur SSL**.

ÉTAPE 2 Cliquez sur **Importer le certificat**.

ÉTAPE 3 Renseignez les champs suivants :

- **ID de certificat** : sélectionnez le certificat actif.
- **Source du certificat** : indique que le certificat est défini par l'utilisateur.
- **Certificat** : copiez dans le certificat reçu.
- **Importer une paire de clés RSA** : sélectionnez cette option pour autoriser la copie dans la nouvelle paire de clés RSA.
- **Clé publique** : copiez dans la clé publique RSA.
- **Clé privée (chiffrée)** : sélectionnez et copiez dans la clé privée RSA sous forme chiffrée.
- **Clé privée (texte en clair)** : sélectionnez et copiez dans la clé privée RSA sous forme de texte en clair.

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

ÉTAPE 5 Cliquez sur **Afficher les données sensibles sous forme chiffrée** pour afficher cette clé sous forme chiffrée. Une fois que vous avez cliqué sur ce bouton, les clés privées sont écrites dans le fichier de configuration sous forme chiffrée (dès que vous cliquez sur Appliquer). Lorsque le texte s'affiche sous forme chiffrée, le bouton devient **Afficher les données sensibles sous forme de texte clair,** ce qui vous permet de réafficher le texte en clair.

Le bouton **Détails** affiche le certificat et la paire de clés RSA. Cela vous permet de copier le certificat et la paire de clés RSA vers un autre appareil (via la fonction copier/coller). Lorsque vous cliquez sur **Afficher les données sensibles sous forme chiffrée**, les clés privées apparaissent sous forme chiffrée.

Pour modifier un certificat :

ÉTAPE 1 Cliquez sur **Sécurité > Serveur SSL > Paramètres d'authentification de serveur SSL**.

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

ÉTAPE 3 Renseignez les champs suivants :

- **Régénérer la clé RSA** : sélectionnez ce champ pour régénérer la clé RSA.

- **Longueur de clé** : sélectionnez soit **Utiliser la valeur par défaut** soit **Définie par l'utilisateur** et saisissez la longueur.
- **Nom commun** : entrez .
- **Unité organisationnelle** : indiquez l'unité organisationnelle liée au certificat.
- **Emplacement** : saisissez l'emplacement de l'unité d'organisation pour le certificat.
- **État** : saisissez l'état de l'unité d'organisation pour le certificat.
- **Comté** : saisissez le comté de l'unité d'organisation pour le certificat.
- **Durée** : indiquez la durée de validité du certificat.

Serveur SSH

Reportez-vous à la section Sécurité : Serveur SSH.

Client SSH

Reportez-vous à la section Sécurité : Client SSH.

Services TCP/UDP

La page Services TCP/UDP active les services TCP ou UDP sur le périphérique, généralement pour des raisons de sécurité.

Le périphérique fournit les services TCP/UDP suivants :

- **HTTP** : activé par défaut
- **HTTPS** : activé par défaut en usine
- **SNMP** : désactivé par défaut en usine
- **Telnet** : désactivé par défaut en usine
- **SSH** : désactivé par défaut en usine

Les connexions TCP actives sont également affichées dans cette fenêtre.

Pour configurer les services TCP/UDP :

ÉTAPE 1 Cliquez sur **Sécurité** > **Services TCP/UDP**.

ÉTAPE 2 Activez ou désactivez les services TCP/UDP suivants sur les services affichés.

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

ÉTAPE 3 Cliquez sur **Appliquer**. Les services sont écrits dans le fichier de Configuration d'exécution.

La table des services TCP contient les champs suivants pour chaque service :

- **Nom de service** : méthode d'accès utilisée par le périphérique pour fournir le service TCP.
- **Type** : protocole IP utilisé par le service.
- **Adresse IP locale** : adresse IP locale via laquelle le périphérique propose le service.
- **Port local** : port TCP local via lequel le périphérique propose le service.
- **Adresse IP distante** : adresse IP de l'appareil distant qui demande le service.
- **Port distant** : port TCP de l'appareil distant qui demande le service.
- **État** : état du service.

La table des services UDP affiche les informations suivantes :

- **Nom de service** : méthode d'accès utilisée par le périphérique pour fournir le service UDP.
- **Type** : protocole IP utilisé par le service.
- **Adresse IP locale** : adresse IP locale via laquelle le périphérique propose le service.
- **Port local** : port UDP local via lequel le périphérique propose le service.
- **Instance d'application** : instance de service du service UDP. (Par exemple, lorsque deux expéditeurs envoient des données vers la même destination.)

Contrôle des tempêtes

Cette section décrit le contrôle des tempêtes. Elle couvre les sujets suivants :

- Contrôle des tempêtes
- Statistiques de contrôle des tempêtes

Lorsque des trames de Diffusion (Broadcast), Multidiffusion (Multicast) ou Monodiffusion inconnue (Unknown Unicast) sont reçues, elles sont dupliquées et une copie est envoyée à tous les ports de sortie possibles. Cela signifie dans la pratique qu'elles sont envoyées à tous les ports appartenant au VLAN approprié. De cette manière, une seule trame d'entrée est convertie en plusieurs trames, ce qui peut potentiellement occasionner une tempête de trafic.

La protection contre les tempêtes vous permet de limiter le nombre de trames entrant dans le périphérique et de définir les types de trames pris en compte dans le calcul de cette limite.

Lorsque la fréquence d'images de Diffusion, Multidiffusion ou Monodiffusion inconnue est supérieure au seuil défini par l'utilisateur, les images reçues au-delà du seuil sont rejetées.

Contrôle des tempêtes

Pour définir le contrôle des tempêtes :

ÉTAPE 1 Cliquez sur **Sécurité** > **Contrôle des tempêtes** > **Paramètres de contrôle des tempêtes**.

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

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez le port pour lequel activer le contrôle des tempêtes.

Contrôle des tempêtes de monodiffusion inconnue

- **Storm Control State** (État de contrôle des tempêtes) : sélectionnez cette option pour activer le contrôle des tempêtes sur les paquets de monodiffusion.
- **Seuil de débit** : saisissez le débit maximum auquel les paquets inconnus peuvent être transmis. Cette valeur peut être indiquée en **Kbit/s** ou en **pourcentage** de la bande passante totale disponible.
- **Trap on Storm** (Filtre en cas de tempête) : sélectionnez cette option pour appliquer un filtre lorsqu'une tempête se produit sur un port. Si cette option n'est pas sélectionnée, aucun filtre n'est envoyé.

- **Shutdown on Storm** (Arrêt en cas de tempête) : sélectionnez cette option pour arrêter un port lorsqu'une tempête se produit sur celui-ci. Si cette option n'est pas sélectionnée, le trafic supplémentaire est ignoré.

Contrôle des tempêtes de multidiffusion

- **Storm Control State** (État de contrôle des tempêtes) : sélectionnez cette option pour activer le contrôle des tempêtes sur les paquets de multidiffusion.
- **Multicast Type** (Type de multidiffusion) : sélectionnez l'un des types de paquets de multidiffusion suivants sur lequel implémenter le contrôle des tempêtes :
  - *All* (Tous) : le contrôle des tempêtes est implémenté sur tous les paquets de multidiffusion sur le port.
  - *Registered Multicast* (Clients de multidiffusion enregistrés) : le contrôle des tempêtes est implémenté uniquement sur les adresses de multidiffusion enregistrées sur le port.
  - *Unregistered Multicast* (Clients de multidiffusion non enregistrés) : le contrôle des tempêtes est implémenté uniquement sur les adresses de multidiffusion non enregistrées sur le port.
- **Rate Threshold** (Seuil de débit) : saisissez le débit maximum auquel les paquets inconnus peuvent être transmis. Cette valeur peut être indiquée en **Kbit/s** ou en **pourcentage** de la bande passante totale disponible.
- **Trap on Storm** (Filtre en cas de tempête) : sélectionnez cette option pour appliquer un filtre lorsqu'une tempête se produit sur un port. Si cette option n'est pas sélectionnée, aucun filtre n'est envoyé.
- **Shutdown on Storm** (Arrêt en cas de tempête) : sélectionnez cette option pour arrêter un port lorsqu'une tempête se produit sur celui-ci. Si cette option n'est pas sélectionnée, le trafic supplémentaire est ignoré.

Contrôle des tempêtes de diffusion

- **Storm Control State** (État de contrôle des tempêtes) : sélectionnez cette option pour activer le contrôle des tempêtes sur les paquets de diffusion.
- **Rate Threshold** (Seuil de débit) : saisissez le débit maximum auquel les paquets inconnus peuvent être transmis. Cette valeur peut être indiquée en **Kbit/s** ou en **pourcentage** de la bande passante totale disponible.
- **Trap on Storm** (Filtre en cas de tempête) : sélectionnez cette option pour appliquer un filtre lorsqu'une tempête se produit sur un port. Si cette option n'est pas sélectionnée, aucun filtre n'est envoyé.

- **Shutdown on Storm** (Arrêt en cas de tempête) : sélectionnez cette option pour arrêter un port lorsqu'une tempête se produit sur celui-ci. Si cette option n'est pas sélectionnée, le trafic supplémentaire est ignoré.

ÉTAPE 4 Cliquez sur **Appliquer**. Le contrôle des tempêtes est modifié et le fichier de Configuration d'exécution est mis à jour.

Statistiques de contrôle des tempêtes

Procédure d'affichage des statistiques de contrôle des tempêtes :

ÉTAPE 1 Cliquez sur **Sécurité** > **Contrôle des tempêtes > Statistiques de contrôle des tempêtes**.

ÉTAPE 2 Sélectionnez une Interface.

ÉTAPE 3 Indiquez le taux d'actualisation : sélectionnez la fréquence d'actualisation des statistiques. Les options disponibles sont les suivantes :

- **No Refresh** : les statistiques ne sont pas actualisées.
- **15 s** : les statistiques sont actualisées toutes les 15 secondes.
- **30 s** : les statistiques sont actualisées toutes les 30 secondes.
- **60 s** : les statistiques sont actualisées toutes les 60 secondes.

Les statistiques suivantes s'affichent pour le contrôle des tempêtes de diffusion, de multidiffusion et de monodiffusion inconnue :

- **Type de trafic multidiffusion** : (Uniquement pour le trafic multidiffusion) Enregistré ou Non enregistré.
- **Bytes Passed** (Octets transmis) : nombre d'octets reçus.
- **Bytes Dropped** (Octets supprimés) : nombre d'octets supprimés en raison du contrôle des tempêtes.
- **Last Drop Time** (Heure de la dernière suppression) : heure à laquelle le dernier octet a été supprimé.

ÉTAPE 4 Pour effacer tous les compteurs sur toutes les interfaces, cliquez sur **Clear All Interfaces Counters** (Effacer les compteurs de toutes les interfaces). Pour effacer tous les compteurs sur une interface, sélectionnez-la et cliquez sur **Effacer les compteurs de l'interface**.

Sécurité des ports

REMARQUE La sécurité des ports ne peut pas être activée sur les ports sur lesquels 802.1X est activé ou sur les ports qui ont été définis comme destination SPAN.

Vous pouvez accroître la sécurité réseau en limitant l'accès à un port pour des utilisateurs disposant d'adresses MAC spécifiques. Les adresses MAC peuvent être apprises de façon dynamique ou configurées de manière statique.

La sécurité des ports surveille les paquets reçus et appris. L'accès aux ports verrouillés est limité aux utilisateurs disposant d'adresses MAC spécifiques.

La sécurité des ports dispose de quatre modes :

- **Verrouillage classique** : toutes les adresses MAC apprises sur le port sont verrouillées et le port n'apprend aucune nouvelle adresse MAC. Les adresses apprises ne sont pas soumises à un délai d'expiration ni à un réapprentissage.
- **Verrouillage dynamique limité** : le périphérique apprend des adresses MAC jusqu'à la limite configurée des adresses autorisées. Une fois la limite atteinte, le périphérique n'apprend pas d'adresses supplémentaires. Dans ce mode, les adresses sont soumises à un délai d'expiration ainsi qu'à un réapprentissage.
- **Sécurisé en permanence** : conserve les adresses MAC dynamiques actuellement associées au port et apprend au maximum le nombre d'adresses autorisées sur le port (défini par l'option Nombre max. d'adresses autorisées). Les opérations de réapprentissage et de délai d'expiration sont désactivées.
- **Suppression sécur. à la réinitialisation** : supprime les adresses MAC dynamiques actuellement associées au port après la réinitialisation. Les nouvelles adresses MAC peuvent être apprises en tant qu'adresses supprimées à la réinitialisation (Delete-On-Reset) jusqu'au nombre d'adresses autorisées sur le port. Les opérations de réapprentissage et de délai d'expiration sont désactivées.

Lorsqu'une trame d'une nouvelle adresse MAC est détectée sur un port sur lequel elle n'est pas autorisée (le port est verrouillé de façon classique et une nouvelle adresse MAC est détectée ou bien le port est verrouillé de façon dynamique et le nombre maximal des adresses autorisées a été dépassé), il est fait appel au mécanisme de protection et l'une des actions suivantes peut s'appliquer :

- La trame est rejetée.
- La trame est transmise.
- Le port est fermé.

Lorsque l'adresse MAC sécurisée est détectée sur un autre port, la trame est transmise mais l'adresse MAC n'est pas apprise sur ce port.

Outre l'une de ces actions, vous pouvez également générer des interceptions ainsi qu'en limiter la fréquence ou le nombre afin d'éviter de surcharger les appareils.

Pour configurer la sécurité des ports :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité des ports**.

ÉTAPE 2 Sélectionnez une interface à modifier et cliquez sur **Modifier**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez le nom de l'interface.
- **État de l'interface** : sélectionnez l'état de verrouillage du port.
- **Learning Mode** : sélectionnez le type de verrouillage du port. L'État de l'interface doit être déverrouillé pour que ce champ puisse être configuré. Le champ Mode d'apprentissage est uniquement activé si le champ *État de l'interface* est verrouillé. Pour modifier le Mode d'apprentissage, État de l'interface doit être désactivé. Une fois ce mode modifié, vous pouvez rétablir l'état de l'interface. Les options sont les suivantes :
  - *Verrouillage classique* : verrouille immédiatement le port, quel que soit le nombre d'adresses ayant déjà été apprises.
  - *Verrouillage dynamique limité* : verrouille le port en supprimant les adresses MAC dynamiques actuellement associées au port. Le port apprend au maximum le nombre d'adresses autorisées sur le port. Le réapprentissage et le délai d'expiration des adresses MAC sont activés.
  - *Sécurisé en permanence* : conserve les adresses MAC dynamiques actuellement associées au port et apprend au maximum le nombre d'adresses autorisées sur le port (défini par l'option **Nombre max. d'adresses autorisées**). Les opérations de réapprentissage et de délai d'expiration sont activées.
  - *Suppression sécur. à la réinitialisation* : supprime les adresses MAC dynamiques actuellement associées au port après la réinitialisation. Les nouvelles adresses MAC peuvent être apprises en tant qu'adresses supprimées à la réinitialisation (Delete-On-Reset) jusqu'au nombre d'adresses autorisées sur le port. Les opérations de réapprentissage et de délai d'expiration sont désactivées.
- **Nombre max. d'adresses autorisées** : saisissez le nombre maximum d'adresses MAC pouvant être apprises sur le port dans la mesure où le mode d'apprentissage *Verrouillage dynamique limité* est sélectionné. Le chiffre 0 indique que seules les adresses statiques sont prises en charge dans l'interface.

- **Action en cas de violation** : sélectionnez l'action à appliquer aux paquets qui arrivent sur un port verrouillé. Les options sont les suivantes :
  - *Abandonner* : supprime les paquets en provenance d'une source non apprise.
  - *Transférer* : transfère les paquets en provenance d'une source inconnue sans apprendre l'adresse MAC.
  - *Arrêter* : abandonne les paquets en provenance d'une source non apprise et ferme le port. Le port reste fermé jusqu'à ce qu'il soit réactivé ou jusqu'à ce que le périphérique soit réinitialisé.
- **« Trap »** : sélectionnez cette option pour activer les messages « trap » lorsqu'un paquet est reçu sur un port verrouillé. Ceci est approprié pour les violations de verrouillage. Pour le Verrouillage classique, ceci correspondra à toute nouvelle adresse reçue. Pour le Verrouillage dynamique limité, cela correspondra à toute nouvelle adresse qui dépassera le nombre des adresses autorisées.
- **Fréquence du/des message(s) « trap »** : saisissez la durée minimale qui s'écoulera entre deux messages « trap ».

ÉTAPE 4 Cliquez sur **Appliquer**. La sécurité des ports est modifiée et le fichier de Configuration d'exécution est mis à jour.

Authentification 802.1X

Reportez-vous au chapitre Sécurité : Authentification 802.1X pour obtenir de plus amples informations sur l'authentification 802.1x.

Protection de la source IP

La protection de la source IP est une fonction de sécurité qui peut être utilisée pour empêcher les attaques de trafic provoquées lorsqu'un hôte essaie d'utiliser l'adresse IP de son voisin.

Lorsque la protection de la source IP est activée, le périphérique transmet uniquement le trafic IP client vers les adresses IP contenues dans la base de données de liaison de surveillance DHCP. Cela inclut à la fois les adresses ajoutées par la surveillance DHCP et les entrées ajoutées manuellement.

Si le paquet correspond à une entrée contenue dans la base de données, le périphérique le transfère. Sinon, le paquet est supprimé.

Cette section décrit la fonction de protection de la source IP. Elle couvre les sujets suivants :

- Interactions avec les autres fonctions
- Filtrage
- Workflow de la protection de la source IP
- Propriétés
- Paramètres d'interface
- Base de données de liaison

Interactions avec les autres fonctions

Les points suivants sont pertinents pour la protection de la source IP :

- La surveillance DHCP doit être activée au niveau global afin de permettre la protection de la source IP sur une interface.
- La protection de la source IP peut être active sur une interface uniquement si :
  - La surveillance DHCP est activée sur au moins un des VLAN du port.
  - L'interface est non sécurisée DHCP. Tous les paquets présents sur des ports sécurisés sont transférés.
- Si un port est sécurisé DHCP, il est possible de configurer le filtrage des adresses IP statiques, même si la protection de la source IP n'est pas active, à la condition que la protection de la source IP soit activée sur le port.
- Lorsque l'état du port passe de non sécurisé DHCP à sécurisé DHCP, les entrées du filtrage des adresses IP statiques restent dans la base de données de liaison, mais elles deviennent inactives.
- La sécurité des ports ne peut pas être activée si le filtrage des adresses IP et MAC source est configuré sur un port.
- La protection de la source IP utilise des ressources TCAM et ne nécessite qu'une seule règle TCAM par entrée d'adresse de protection de source IP. Si le nombre d'entrées de protection de source IP est supérieur au nombre de règles TCAM disponibles, les adresses supplémentaires sont inactives.

Filtrage

Si la protection de la source IP est activée sur un port :

- Les paquets DHCP autorisés par la surveillance DHCP sont autorisés.
- Si le filtrage des adresses IP sources est activé :
  - Trafic IPv4 : seul le trafic avec une adresse IP source associée au port est autorisé.
  - Trafic non IPv4 : autorisé (y compris les paquets ARP).

Workflow de la protection de la source IP

Pour configurer la protection de la source IP :

ÉTAPE 1 Activez la surveillance DHCP sur la page Propriétés.

ÉTAPE 2 Définissez les VLAN sur lesquels la surveillance DHCP est activée sur la page Paramètres d'interface.

ÉTAPE 3 Configurez les interfaces comme étant sécurisées ou non sécurisées sur la page Paramètres d'interface.

ÉTAPE 4 Activez la protection de la source IP sur la page (Protection de la source IP) Propriétés.

ÉTAPE 5 Activez la protection de la source IP sur les interfaces non sécurisées, comme requis, sur la page (IP Source Guard [Protection de la source IP]) Paramètres d'interface.

ÉTAPE 6 Affichez les entrées de la base de données de liaison sur la page (Protection de la source IP) Base de données de liaison.

Propriétés

Pour activer la protection de la source IP globalement :

ÉTAPE 1 Cliquez sur **Sécurité** > **Protection de la source IP** > **Propriétés**.

ÉTAPE 2 Sélectionnez **Activer** pour activer la protection de la source IP globalement.

ÉTAPE 3 Cliquez sur **Appliquer** pour activer la protection de la source IP.

Paramètres d'interface

Si la protection de la source IP est activée sur un port/LAG non sécurisé, les paquets DHCP autorisés par la surveillance DHCP sont transmis. Si le filtrage des adresses IP sources est activé, la transmission des paquets est autorisée comme suit :

- **Trafic IPv4** : seul le trafic IPv4 avec une adresse IP source associée au port spécifique est autorisé.
- **Trafic non IPv4** : tout le trafic non IPv4 est autorisé.

Reportez-vous à la section Interactions avec les autres fonctions pour plus d'informations sur l'activation de la protection de la source IP sur des interfaces.

Pour configurer la protection de la source IP sur des interfaces :

ÉTAPE 1 Cliquez sur **Sécurité** > **Protection de la source IP** > **Paramètres d'interface**.

ÉTAPE 2 Sélectionnez un port/LAG dans le champ **Filtre** et cliquez sur **OK**. Les ports/LAG de cette unité sont affichés avec les informations suivantes :

- **Protection de la source IP** : indique si la protection de la source IP est activée sur le port.
- **Interface sécurisée de surveillance DHCP** : indique s'il s'agit d'une interface sécurisée DHCP.

ÉTAPE 3 Sélectionnez le port/LAG et cliquez sur **Modifier**. Sélectionnez **Activer** dans le champ **Protection de la source IP** pour activer la protection de la source IP sur l'interface.

ÉTAPE 4 Cliquez sur **Appliquer** pour copier le paramètre dans le fichier de Configuration d'exécution.

Base de données de liaison

La protection de source IP utilise la base de données de liaison de surveillance DHCP pour vérifier les paquets issus de ports non sécurisés. Si le périphérique tente d'écrire un trop grand nombre d'entrées dans la base de données de liaison de surveillance DHCP, les entrées en excès sont maintenues dans un état inactif. Les entrées sont supprimées lors de l'expiration de leur durée de bail, des entrées inactives pouvant alors être rendues actives.

Reportez-vous à la section Fureteur/Relais DHCP.

REMARQUE La page Base de données de liaison n'affiche **que** les entrées de la base de données de liaison de surveillance DHCP qui sont définies sur des ports pour lesquels la protection de source IP est activée.

Pour afficher la base de données de liaison de surveillance DHCP et connaître l'utilisation de TCAM, définissez l'option **Insertion inactive** :

ÉTAPE 1 Cliquez sur **Sécurité** > **Protection de la source IP** > **Base de données de liaison**.

ÉTAPE 2 La base de données de liaison de surveillance DHCP utilise des ressources TCAM pour gérer la base de données. Remplissez le champ **Insertion inactive** pour sélectionner la fréquence à laquelle le périphérique doit tenter d'activer les entrées inactives. Les options suivantes sont disponibles :

- **Fréquence des tentatives** : fréquence à laquelle les ressources TCAM sont vérifiées.
- **Jamais** : il ne faut jamais tenter de réactiver les adresses inactives.

ÉTAPE 3 Cliquez sur **Appliquer** pour enregistrer les modifications ci-dessus dans la Configuration d'exécution et/ou sur **Recommencer maintenant** pour vérifier les ressources TCAM.

Les entrées de la base de données de liaison sont affichées :

- **ID du VLAN** : VLAN sur lequel le paquet est attendu.
- **Adresse MAC** : adresse MAC à mettre en correspondance.
- **Adresse IP** : adresse IP à mettre en correspondance.
- **Interface** : interface sur laquelle le paquet est attendu.
- **État** : indique si l'interface est active.
- **Type** : indique si l'entrée est dynamique ou statique.
- **Motif** : si l'interface n'est pas active, indique le motif. Les motifs suivants sont possibles :
  - *Sans problème* : l'interface est active.
  - *Sans VLAN de surveillance* : la surveillance DHCP n'est pas activée sur le VLAN.
  - *Confiance de port* : le port est maintenant sécurisé.
  - *Sans ressource* : les ressources TCAM sont épuisées.

ÉTAPE 4 Pour afficher un sous-ensemble de ces entrées, saisissez les critères de recherche appropriés et cliquez sur **OK**.

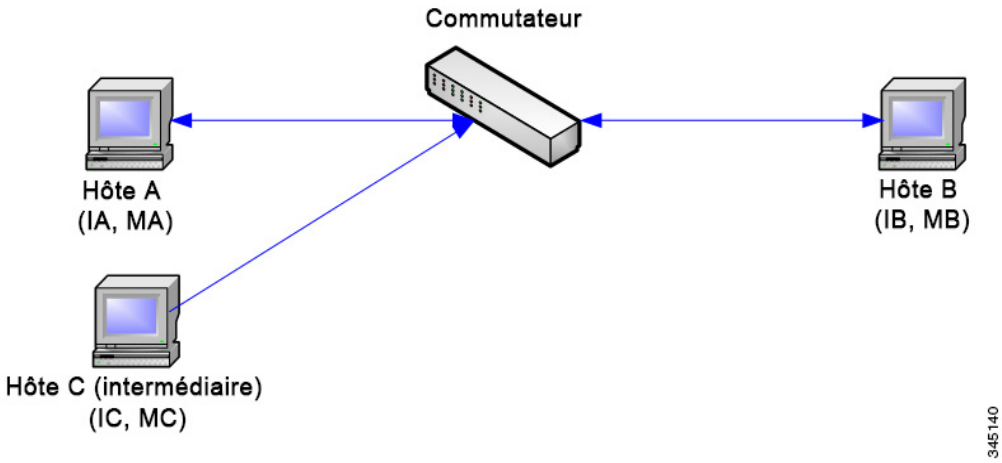
Inspection ARP

ARP permet la communication IP au sein d'un domaine de diffusion de couche 2 (Layer 2) en mappant les adresses IP à des adresses MAC.

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. Cela 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.

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.

Cette rubrique décrit la fonction d'inspection ARP. Elle couvre les sujets suivants :

Comment ARP peut empêcher l'empoisonnement de cache

La fonction d'inspection ARP s'applique aux interfaces sécurisées ou non (reportez-vous à la page Paramètres d'interface).

Les interfaces sont classées par l'utilisateur comme suit :

- **Interfaces sécurisées** : les paquets ne sont pas inspectés.
- **Interfaces non sécurisées** : 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 ; sinon, il ne l'est pas.

- 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, 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 (Validation de paquet ARP) est sélectionnée (page Propriétés), les vérifications de validation supplémentaires suivantes sont effectuées :

- **Adresse MAC source** : 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.
- **Adresse MAC de destination** : 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.
- **Adresses IP** : 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.

Il est possible de définir un maximum de 1 024 entrées dans la table de contrôle d'accès ARP.

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.

Valeurs ARP par défaut

Le tableau suivant décrit les valeurs ARP par défaut :

Option	État par défaut
Inspection ARP dynamique	Non activée
Validation de paquet ARP	Désactivée
Inspection ARP activée sur VLAN	Désactivée
Intervalle du tampon du journal	La génération d'un message SYSLOG pour les paquets supprimés est activée avec un intervalle de 5 secondes.

Workflow de l'inspection ARP

Pour configurer l'inspection ARP :

ÉTAPE 1 Activez l'inspection ARP et définissez diverses options sur la page Propriétés.

ÉTAPE 2 Configurez les interfaces en tant qu'interfaces ARP sécurisées ou non sécurisées sur la page Paramètres d'interface.

ÉTAPE 3 Ajoutez des règles sur les pages Règles de contrôle d'accès ARP.

ÉTAPE 4 Définissez les VLAN sur lesquels l'inspection ARP est activée, ainsi que les règles de contrôle d'accès de chaque VLAN sur la page Paramètres VLAN.

Propriétés

Procédure de configuration des propriétés de l'inspection ARP :

ÉTAPE 1 Cliquez sur **Sécurité** > **Inspection ARP > Propriétés**.

Renseignez les champs suivants :

- **État de l'inspection ARP** : sélectionnez cette option pour activer l'inspection ARP.
- **Validation de paquet ARP** : sélectionnez cette option pour activer les vérifications de validation.

- **Intervalle du tampon du journal** : sélectionnez l'une des options suivantes :
  - *Fréquence des tentatives* : active l'envoi de messages SYSLOG pour les paquets supprimés. Saisissez la fréquence à laquelle les messages sont envoyés.
  - *Jamais* désactive l'envoi de messages SYSLOG pour les paquets supprimés.

ÉTAPE 2 Cliquez sur **Appliquer**. Les paramètres sont définis et le fichier de Configuration d'exécution est mis à jour.

Paramètres d'interface

Les paquets issus des ports/LAG non sécurisés sont vérifiés à l'aide de la table des règles d'accès ARP et de la base de données de liaison de surveillance DHCP si la surveillance DHCP est activée (reportez-vous à la page Base de données de liaison de surveillance DHCP).

Par défaut, les ports/LAG sont non sécurisés en ce qui concerne l'inspection ARP.

Pour modifier l'état sécurisé ARP d'un port/LAG :

ÉTAPE 1 Cliquez sur **Sécurité** > **Inspection ARP** > **Paramètres d'interface**.

Les ports/LAG ainsi que leur état sécurisé / non sécurisé ARP sont affichés.

ÉTAPE 2 Pour définir un port/LAG comme étant non sécurisé, sélectionnez le port/LAG et cliquez sur **Modifier**.

ÉTAPE 3 Sélectionnez **Sécurisé** ou **Non sécurisé** et cliquez sur **Appliquer** pour enregistrer les paramètres dans le fichier de Configuration d'exécution.

Contrôle d'accès ARP

Pour ajouter des entrées à la table d'inspection ARP :

ÉTAPE 1 Cliquez sur **Sécurité** > **Inspection ARP > Contrôle d'accès ARP**.

ÉTAPE 2 Pour ajouter une entrée, cliquez sur **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants :

- **Nom de contrôle d'accès ARP** : saisissez un nom créé par l'utilisateur.
- **Adresse IP** : adresse IP du paquet.
- **Adresse MAC** : adresse MAC du paquet.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres sont définis et le fichier de Configuration d'exécution est mis à jour.

Règles de contrôle d'accès ARP

Pour ajouter des règles supplémentaires à un groupe de contrôle d'accès ARP créé précédemment :

ÉTAPE 1 Cliquez sur **Sécurité** > **Inspection ARP > Règles de contrôle d'accès ARP**.

Les règles d'accès actuellement définies sont affichées.

Pour sélectionner un groupe spécifique, sélectionnez Filtre, choisissez le nom du contrôle, puis cliquez sur **Ok**.

ÉTAPE 2 Pour ajouter des règles supplémentaires à un groupe, cliquez sur **Ajouter**.

ÉTAPE 3 Sélectionnez un **Nom de contrôle d'accès ARP** et renseignez les champs suivants :

- **Adresse IP** : adresse IP du paquet.
- **Adresse MAC** : adresse MAC du paquet.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres sont définis et le fichier de Configuration d'exécution est mis à jour.

Paramètres VLAN

Pour activer l'inspection ARP sur des VLAN et associer des groupes de contrôle d'accès à un VLAN :

ÉTAPE 1 Cliquez sur **Sécurité** > **Inspection ARP > Paramètres VLAN**.

ÉTAPE 2 Pour activer l'inspection ARP sur un VLAN, déplacez le VLAN depuis la liste **VLAN disponibles** vers la liste **VLAN activés**.

ÉTAPE 3 Pour associer un groupe de contrôle d'accès ARP à un VLAN, cliquez sur **Ajouter**. Sélectionnez le numéro du VLAN, ainsi qu'un **nom** de **contrôle d'accès ARP** défini précédemment.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres sont définis et le fichier de Configuration d'exécution est mis à jour.

Sécurité du premier saut

Sécurité : Sécurité du premier saut IPv6

Prévention du déni de service

Le déni de service (DoS) est une tentative de piratage visant à rendre le périphérique indisponible pour les utilisateurs.

Les attaques DoS saturent le périphérique avec des demandes de communication externes, de telle manière que le périphérique ne peut pas répondre au trafic légitime. Ces attaques provoquent souvent la surcharge du processeur du périphérique.

- Adresses martiennes
- Filtrage SYN
- Protection du débit SYN
- Filtrage ICMP
- Filtrage de fragments IP

Secure Core Technology (SCT)

Une méthode pour contrer les dénis de service (DoS) employée par le périphérique est la fonction SCT. La fonction SCT est activée par défaut sur le périphérique et ne peut pas être désactivée.

Le périphérique Cisco est un périphérique avancé qui gère le trafic de gestion, de protocole et de surveillance, outre le trafic de l'utilisateur final (TCP).

La fonction SCT garantit que le périphérique reçoive et traite le trafic de gestion et de protocole, quel qu'il soit le trafic reçu. Ceci est possible en limitant le débit du trafic TCP sur le processeur.

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

La fonction SCT peut être gérée sur la page Paramètres de la suite de sécurité (bouton **Details** [Détails]).

Types d'attaques par déni de service (DoS)

Les types de paquets suivants, ou d'autres stratégies, peuvent être impliqués dans une attaque par déni de service :

- **Paquets TCP SYN** : ces paquets ont souvent été envoyés par une adresse d'expéditeur fausse. Chaque paquet est géré comme une requête de connexion, ce qui provoque une connexion semi-ouverte du serveur en renvoyant un paquet TCP/SYN-ACK (confirmation) et en attendant un paquet de réponse en provenance de l'adresse de l'expéditeur (réponse au paquet ACK). Cependant, étant donné que l'adresse de l'expéditeur est fausse, la réponse n'arrive jamais. Ces connexions semi-ouvertes saturent le nombre de connexions disponibles que le périphérique peut effectuer, l'empêchant ainsi de répondre aux requêtes légitimes.
- **Paquets TCP SYN-FIN** : les paquets SYN sont envoyés pour créer une connexion TCP. Les paquets TCP FIN sont envoyés pour fermer une connexion. Un paquet où les indicateurs SYN et FIN sont définis ne devrait jamais exister. En conséquence, ces paquets peuvent constituer une attaque au périphérique et doivent être bloqués.
- **Adresses martiennes** : les adresses martiennes sont incorrectes du point de vue du protocole IP. Pour plus d'informations, reportez-vous à la section Adresses martiennes.
- **Attaque ICMP** : l'envoi de paquets ICMP mal-formés ou la révélation du nombre de paquets ICMP à la victime risque de provoquer une défaillance système.
- **Fragmentation IP** : des fragments IP endommagés avec des charges utiles surdimensionnées et se chevauchant sont envoyés au périphérique. Ceci risque de provoquer une défaillance dans plusieurs systèmes d'exploitation en raison d'un bogue dans leur code de réassemblage de fragmentation TCP/IP. Les systèmes d'exploitation Windows 3.1x, Windows 95 et Windows NT, ainsi que les versions Linux antérieures aux versions 2.0.32 et 2.1.63 sont vulnérables à ce type d'attaque.
- **Distribution Stacheldraht** : le pirate utilise un programme client pour se connecter aux modules de traitement (des systèmes compromis qui envoient des instructions aux agents zombies), ce qui facilite le déni de service. Les agents sont compromis via les modules de traitement attaqués par le pirate.

Utilisation de routines automatiques pour exploiter des failles dans les programmes qui acceptent des connexions distantes sur le hôtes distants ciblés. Chaque module de traitement peut contrôler jusqu'un millier d'agents.

- **Cheval de Troie Invasor** : un cheval de Troie permet au pirate de télécharger un agent zombie (si le cheval de Troie n'en contient pas un). Les pirates peuvent également entrer dans les systèmes à l'aide d'outils automatiques qui exploitent les failles des programmes écoutant les connexions des hôtes distants. Ce scénario concerne principalement le périphérique lorsqu'il est utilisé comme serveur sur le Web.
- **Cheval de Troie Back Orifice** : ce cheval de Troie est une variante qui utilise le logiciel Back Orifice pour déposer le cheval de Troie.

Défense contre les attaques par déni de service (DoS)

La fonctionnalité Prévention du déni de service (DoS) permet à l'administrateur système de résister à des attaques de ce type en suivant l'une des méthodes ci-dessous :

- Activer la protection TCP SYN. Si cette fonctionnalité est activée, des rapports sont émis lorsqu'une attaque de paquet SYN est identifiée. Le port attaqué peut être temporairement désactivé. Une attaque SYN est identifiée lorsque le nombre de paquets SYN par seconde dépasse le seuil défini par l'utilisateur.
- Bloquer les paquets SYN-FIN.
- Bloquer les paquets contenant des adresses martiennes (page Adresses martiennes).
- Empêcher les connexions TCP à partir d'une interface spécifique (page Filtrage SYN) et fixer un débit maximal pour les paquets (page Protection du débit SYN).
- Configurer le blocage de certains paquets ICMP (page Filtrage ICMP).
- Abandonner les paquets IP fragmentés en provenance d'une interface spécifique (page Filtrage de fragments IP).
- Interdire les attaques de Distribution Stacheldraht, du cheval de Troie Invasor et du cheval de Troie Back Orifice (page Paramètres de la suite de sécurité).

Dépendances entre les fonctions

Les ACL et les stratégies de QoS avancées ne sont pas actives lorsque la protection contre le déni de service est activée sur un port. Un message d'erreur apparaît si vous essayez d'activer la prévention du déni de service (DoS) lorsqu'un ACL est défini sur l'interface ou si vous essayez de définir un ACL sur une interface où la prévention du déni de service (DoS) est activée.

Une attaque SYN ne peut pas être bloquée s'il y a un ACL actif sur une interface.

Configuration par défaut

La fonctionnalité Prévention du déni de service (DoS) est configurée par défaut comme suit :

- La fonctionnalité Prévention du déni de service (DoS) est désactivée par défaut.
- La protection SYN-FIN est activée par défaut (même si la fonctionnalité Prévention du déni de service (DoS) est désactivée).
- Si la protection SYN est activée, le mode de protection par défaut est **Bloquer et rapporter**. Le seuil par défaut est 30 paquets SYN par seconde.
- Toutes les autres fonctionnalités de prévention du déni de service (DoS) sont désactivées par défaut.

Paramètres de la suite de sécurité

REMARQUE Avant d'activer la prévention du déni de service (DoS), vous devez supprimer les liaisons de toutes les listes de contrôle d'accès (ACL, Access Control Lists) et stratégies de QoS avancées qui sont liées à un port. Les ACL et les stratégies de QoS avancées ne sont pas actives lorsque la protection contre le déni de service est activée sur un port.

Pour configurer les paramètres globaux de prévention du déni de service et contrôler la fonction SCT :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Paramètres de suite de sécurité**.

Mécanisme de protection du processeur : Activé indique que la fonction SCT est activée.

ÉTAPE 2 Cliquez sur **Details** (Détails) en regard de **CPU Utilization** (Utilisation du CPU) pour accéder à la page Utilisation du processeur et afficher les informations d'utilisation des ressources du CPU.

ÉTAPE 3 Cliquez sur **Edit** (Modifier) en regard de **TCP SYN Protection** (Protection SYN TCP) pour définir cette fonction.

ÉTAPE 4 Sélectionnez **Protection contre les DoS** pour activer la fonctionnalité.

- **Désactiver** : désactive la fonctionnalité.
- **Protection de niveau système** : active la partie de la fonction qui empêche les attaques de Distribution Stacheldraht, du cheval de Troie Invasor et du cheval de Troie Back Orifice.
- **Protection de niveau système et de niveau interface** : active la partie de la fonction qui empêche les attaques de Distribution Stacheldraht, du cheval de Troie Invasor et du cheval de Troie Back Orifice.

ÉTAPE 5 Si vous sélectionnez la **Protection de niveau système** ou la **Protection de niveau système et de niveau interface**, activez une ou plusieurs des options de Protection contre les DoS suivantes :

- **Distribution Stacheldraht** : abandonne les paquets TCP dont le port TCP source est 16660.
- **Cheval de Troie Invasor** : abandonne les paquets TCP dont le port TCP de destination est 2140 et le port TCP source 1024.
- **Cheval de Troie Back Orifice** : abandonne les paquets UDP dont le port UDP de destination est 31337 et le port UDP source est 1024.

ÉTAPE 6 Cliquez sur les options suivantes selon vos besoins :

- **Martian Addresses** (Adresses martiennes) : cliquez sur **Edit** (Modifier) pour accéder à la page Adresses martiennes.
- **SYN Filtering** (Filtrage SYN) : cliquez sur **Edit** (Modifier) pour accéder à la page Filtrage SYN.
- **Protection du débit SYN** : (couche 2 uniquement) cliquez sur **Modifier** pour accéder à la page Protection du débit SYN.
- **ICMP Filtering** (Filtrage ICMP) : cliquez sur **Edit** (Modifier) pour accéder à la page Filtrage ICMP.
- **IP Fragmented** (IP fragmenté) : cliquez sur **Edit** (Modifier) pour accéder à la page Filtrage de fragments IP.

ÉTAPE 7 Cliquez sur **Appliquer**. Les paramètres de la suite de sécurité de prévention du déni de service sont écrits dans le fichier de Configuration d'exécution.

Protection SYN

Les ports du réseau risquent d'être utilisés par les pirates pour attaquer le périphérique lors d'une attaque SYN, ce qui utilise des ressources TCP (tampons) et de l'énergie du CPU.

Étant donné que le CPU est protégé à l'aide de la fonction SCT, le trafic TCP vers le CPU est limité. Cependant, si un ou plusieurs ports sont attaqués par un grand nombre de paquets SYN, le CPU reçoit uniquement les paquets du pirate, ce qui crée un déni de service.

Lors de l'utilisation de la fonctionnalité de protection SYN, le processeur compte les paquets SYN entrants par seconde par chaque port de réseau vers le processeur.

Si le nombre est supérieur au seuil spécifique 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 la protection SYN :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Protection SYN**.

ÉTAPE 2 Saisissez les paramètres.

- **Bloquer les paquets SYN-FIN** : sélectionnez cette option pour activer la fonctionnalité. Tous les paquets TCP avec les indicateurs SYN et FIN sont rejetés sur tous les ports.
- **Mode de protection SYN** : sélectionnez l'un des trois modes ci-dessous :
  - *Désactiver* : la fonctionnalité est désactivée sur une interface spécifique.
  - *Rapport* : génère un message SYSLOG. L'état du port bascule vers **Attaqué** lorsque le seuil est dépassé.
  - *Bloquer et rapporter* : lorsqu'une attaque TCP SYN est identifiée, les paquets TCP SYN destinés au système sont rejetés et l'état du port bascule vers **Bloqué**.
- **Seuil de protection SYN** : nombre de paquets SYN par seconde avant de bloquer les paquets SYN (un SYN de déni avec une règle « MAC-to-me » sera appliqué sur le port).
- **Période de protection SYN** : temps en secondes avant de débloquer les paquets SYN (le SYN de déni avec la règle « MAC-to-me » est dissocié du port).

ÉTAPE 3 Cliquez sur **Appliquer**. La protection SYN est définie et le fichier de Configuration d'exécution est mis à jour.

La Table des interfaces de protection SYN affiche les champs suivants pour chaque port ou LAG (en fonction des besoins de l'utilisateur).

- **État actuel** : état de l'interface. Ce champ peut prendre les valeurs suivantes :
  - *Normal* : aucune attaque n'a été identifiée sur cette interface.
  - *Bloqué* : le trafic n'est pas transmis sur cette interface.
  - *Attaqué* : une attaque a été identifiée sur cette interface.
- **Dernière attaque** : date de la dernière attaque SYN-FIN identifiée par le système et action du système (**Rapporté** ou **Bloqué et rapporté**).

Adresses martiennes

La page Martian Addresses (Adresses martiennes) permet de saisir les adresses IP qui indiquent une attaque si elles sont détectées sur le réseau. Les paquets provenant de ces adresses sont abandonnés.

Le périphérique prend en charge un ensemble d'adresses martiennes réservées qui sont incorrectes du point de vue du protocole IP. Les adresses martiennes réservées prises en charge regroupent les éléments suivants :

- Les adresses définies comme étant incorrectes sur la page Adresses martiennes.
- Les adresses qui sont incorrectes du point de vue du protocole (comme les adresses de bouclage), et notamment les adresses contenues dans les plages suivantes :
  - **0.0.0.0/8 (à l'exception de 0.0.0.0/32 en tant qu'adresse source)** : les adresses situées dans ce bloc font référence aux hôtes source de ce réseau.
  - **127.0.0.0/8** : utilisée en tant qu'adresse de bouclage d'hôte Internet.
  - **192.0.2.0/24** : utilisée en tant que réseau de test TEST-NET dans la documentation et les exemples de codes.
  - **224.0.0.0/4 (en tant qu'adresse IP source)** : utilisée dans les affectations d'adresses de multidiffusion IPv4, anciennement connue sous le nom d'espace d'adressage de classe D.
  - **240.0.0.0/4 (à l'exception de 255.255.255.255/32 en tant qu'adresse de destination)** : plage d'adresses réservées, anciennement connue sous le nom d'espace d'adressage de classe E.

Vous pouvez également ajouter de nouvelles adresses martiennes pour la protection contre les DoS. Les paquets présentant une adresse martienne sont abandonnés.

Pour définir des adresses martiennes :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Adresses martiennes**.

ÉTAPE 2 Sélectionnez **Adresses martiennes réservées** et cliquez sur **Appliquer** pour inclure les adresses martiennes réservées dans la liste Protection de niveau système.

ÉTAPE 3 Pour ajouter une adresse martienne, cliquez sur **Ajouter**.

ÉTAPE 4 Saisissez les paramètres.

- **Version IP** : indique la version IP prise en charge. À l'heure actuelle, la prise en charge n'est proposée que pour IPv4.

- **Adresse IP** : saisissez une adresse IP à rejeter. Ce champ peut prendre les valeurs suivantes :
  - *De la liste réservée* : sélectionnez une adresse IP bien connue dans la liste réservée.
  - *Nouvelle adresse IP* : saisissez une adresse IP.
- **Masque** : saisissez le masque de l'adresse IP pour définir une plage d'adresses IP à rejeter. Les valeurs disponibles sont les suivantes :
  - *Masque de réseau* : le masque de réseau est présenté dans un format décimal séparé par des points.
  - *Longueur du préfixe* : saisissez le préfixe de l'adresse IP afin de définir la plage des adresses IP pour laquelle la Prévention du déni de service sera activée.

ÉTAPE 5 Cliquez sur **Appliquer**. Les adresses martiennes sont écrites dans le fichier de Configuration d'exécution.

Filtrage SYN

La page SYN Filtering (Filtrage SYN) permet de filtrer les paquets TCP qui comportent un indicateur SYN et qui sont destinés à un ou plusieurs ports.

Pour définir un filtre SYN :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Filtrage SYN**.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez l'interface sur laquelle le filtre est défini.
- **Adresse IPv4** : saisissez l'adresse IP pour laquelle le filtre est défini ou sélectionnez *Toutes les adresses*.
- **Masque de réseau** : saisissez le masque de réseau pour lequel le filtre est activé au format d'adresse IP. Renseignez l'une des informations suivantes :
  - *Masque* : le masque de réseau est présenté dans un format décimal séparé par des points.
  - *Longueur du préfixe* : saisissez le préfixe de l'adresse IP afin de définir la plage des adresses IP pour laquelle la Prévention du déni de service sera activée.

- **Port TCP** : sélectionnez le port TCP de destination filtré :
  - *Ports connus* : sélectionnez un port dans la liste.
  - *Défini par l'utilisateur* : saisissez un numéro de port.
  - *Tous les ports* : sélectionnez cette option pour indiquer que tous les ports seront filtrés.

ÉTAPE 4 Cliquez sur **Appliquer**. Le filtre SYN est défini et le fichier de Configuration d'exécution est mis à jour.

Protection du débit SYN

La page SYN Rate Protection (Protection du débit SYN) permet de limiter le nombre de paquets SYN reçus sur le port d'entrée. Cela permet d'atténuer l'effet d'une saturation SYN sur les serveurs en limitant, au niveau du débit, le nombre de nouvelles connexions ouvertes pour gérer les paquets.

Pour définir la protection du débit SYN :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Protection du débit SYN**.

Cette page affiche la protection du débit SYN actuellement définie par interface.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez l'interface à partir de laquelle la protection du débit sera définie.
- **Adresse IP** : saisissez l'adresse IP pour laquelle la protection du débit SYN est définie ou sélectionnez *Toutes les adresses*. Si vous saisissez l'adresse IP, saisissez également le masque ou la longueur du préfixe.
- **Masque de réseau** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs suivants :
  - *Masque* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Longueur du préfixe* : sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l'adresse IP source.

- **Limite du débit SYN** : saisissez le nombre des paquets SYN pouvant être reçus.

ÉTAPE 4 Cliquez sur **Appliquer**. La protection du débit SYN est définie et le fichier de Configuration d'exécution est mis à jour.

Filtrage ICMP

La page ICMP Filtering (Filtrage ICMP) permet de bloquer les paquets ICMP en provenance de certaines sources. Cela peut permettre de réduire la charge du réseau en cas d'attaque ICMP.

Pour définir le filtrage ICMP :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Filtrage ICMP**.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez l'interface sur laquelle le filtrage ICMP est défini.
- **Adresse IP** : saisissez l'adresse IPv4 pour laquelle le filtrage des paquets ICMP est activé ou sélectionnez *Toutes les adresses* pour bloquer les paquets ICMP en provenance de toutes les adresses source. Si vous saisissez l'adresse IP, saisissez également le masque ou la longueur du préfixe.
- **Masque de réseau** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs suivants :
  - *Masque* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Longueur du préfixe* : sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l’adresse IP source.

ÉTAPE 4 Cliquez sur **Appliquer**. Le filtrage ICMP est défini et le fichier de Configuration d'exécution est mis à jour.

Filtrage de fragments IP

La page IP Fragmented (IP fragmenté) permet de bloquer les paquets IP fragmentés.

Pour configurer le blocage IP fragmenté :

ÉTAPE 1 Cliquez sur **Sécurité** > **Prévention du déni de service** > **Filtrage de fragments IP**.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez l'interface sur laquelle la fragmentation IP est définie.
- **Adresse IP** : saisissez un réseau IP à partir duquel les paquets IP fragmentés sont filtrés ou sélectionnez *Toutes les adresses* pour bloquer les paquets IP fragmentés en provenance de toutes les adresses. Si vous saisissez l'adresse IP, saisissez également le masque ou la longueur du préfixe.
- **Masque de réseau** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs suivants :
  - *Masque* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Longueur du préfixe* : sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l’adresse IP source.

ÉTAPE 4 Cliquez sur **Appliquer**. La fragmentation IP est définie et le fichier de Configuration d'exécution est mis à jour.

21

Sécurité : Authentification 802.1X

Cette section décrit l'authentification 802.1X.

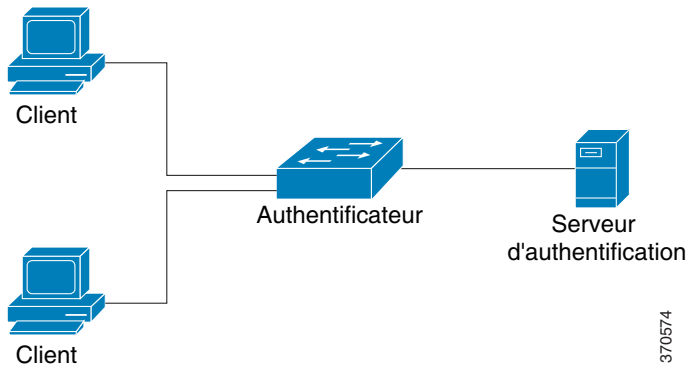
Elle couvre les rubriques suivantes :

Présentation

L'authentification 802.1x empêche les clients non autorisés de se connecter à un réseau LAN par le biais de ports accessibles à la publicité. L'authentification 802.1x est un modèle client-serveur. Dans ce modèle, les périphériques réseau ont les rôles spécifiques suivants.

- Client ou demandeur
- Authentificateur
- Serveur d'authentification

Il est décrit dans la figure ci-dessous :



Sur chaque port, un périphérique réseau peut être un client/demandeur, un authentificateur ou les deux.

Client ou demandeur

Un client ou un demandeur est un périphérique réseau qui demande accès au LAN. Le client est connecté à un authentificateur.

Si le client utilise le protocole 802.1x pour l'authentification, il exécute la partie demandeur du protocole 802.1x et la partie client du protocole EAP.

Aucun logiciel spécial n'est nécessaire sur le client pour utiliser l'authentification MAC ou Web.

Authentificateur

Un authentificateur est un périphérique réseau qui fournit des services réseau et auquel les ports du demandeur sont connectés.

Les méthodes d'authentification suivantes sont prises en charge :

- **802.1x** : prise en charge dans tous les modes d'authentification.
- **MAC** : prise en charge dans tous les modes d'authentification.
- **WEB** : prise en charge uniquement dans les modes à sessions multiples.

Pour l'authentification 802.1x, l'authentificateur extrait les messages EAP des messages 802.1x (paquets EAPOL) et les transmet au serveur d'authentification via le protocole RADIUS.

Avec l'authentification MAC ou Web, l'authentificateur exécute lui-même la partie client EAP du logiciel pour les clients qui souhaitent accéder au réseau.

Les ports sont configurés sur les modes d'authentification. Pour plus d'informations, reportez-vous à la section Modes hôte de port.

Serveur d'authentification

Le serveur d'authentification effectue l'authentification du client. Le serveur d'authentification pour le périphérique est un serveur d'authentification RADIUS avec extensions EAP.

Accès ouvert

La fonction Open (Monitoring) Access (Accès (en surveillance) ouvert) facilite la distinction entre les échecs d'authentification véritables et les échecs causés par une configuration incorrecte et/ou un manque de ressources dans un environnement 802.1x.

La fonction Open Access (Accès ouvert) permet aux administrateurs système de mieux comprendre les problèmes de configuration des hôtes qui se connectent au réseau, de surveiller les situations critiques et de résoudre ces problèmes.

Lorsque la fonction Open Access (Accès ouvert) est activée sur une interface, le commutateur considère tous les échecs reçus d'un serveur RADIUS comme des réussites et autorise les stations connectées à l'interface à accéder au réseau quels que soient les résultats de l'authentification.

La fonction Open Access (Accès ouvert) modifie le paramétrage standard qui consiste à bloquer le trafic sur un port à authentification jusqu'à la réussite des procédures d'authentification et d'autorisation. Le comportement d'authentification par défaut est toujours de bloquer l'ensemble du trafic à l'exception du protocole EAPoL (Extensible Authentication Protocol over LAN). Toutefois, la fonction Open Access (Accès ouvert) offre à l'administrateur la possibilité de donner un libre accès à l'ensemble du trafic, même si l'authentification (802.1X, MAC et/ou Web) est activée.

Lorsque la gestion de comptes RADIUS est activée, vous pouvez consigner les tentatives d'authentification et obtenir une meilleure visibilité sur les utilisateurs et les appareils qui se connectent au réseau grâce à une piste d'audit.

Tout se déroule sans impact sur les utilisateurs finaux ni sur les hôtes connectés au réseau. Vous pouvez activer la fonction Open Access (Accès ouvert) sur la page Authentification des ports.

États d'authentification du port

L'état d'authentification du port détermine si le client a accès au réseau.

L'état administratif du port peut être configuré sur la page Authentification des ports.

Les valeurs suivantes sont disponibles :

- **Autorisation forcée**

  L'authentification du port est désactivée et le port transmet tout le trafic conformément à sa configuration statique sans demander d'authentification. Le commutateur envoie le paquet EAP 802.1x qui intègre le message de réussite EAP lorsqu'il reçoit le message de démarrage EAPOL 802.1x.

  Il s'agit de l'état par défaut.

- **Non-autorisation forcée**

  L'authentification du port est désactivée et le port transmet tout le trafic via le VLAN invité et les VLAN non authentifiés. Pour plus d'informations, reportez-vous à la section Authentification hôtes et sessions. Le commutateur envoie les paquets EAP 802.1x qui intègrent les messages d'erreur EAP lorsqu'il reçoit les messages de démarrage EAPOL 802.1x.

- **Auto**

  Active les authentifications du port conformément au mode hôte configuré et aux méthodes d'authentification définies sur le port.

Modes hôte de port

Les ports peuvent être configurés sur les modes hôte de port suivants (configurés sur la page Authentification hôtes et sessions) :

- **Mode Hôte unique**

  Un port est autorisé s'il y a un client autorisé. Un seul hôte peut être autorisé sur un port.

  Lorsqu'un port n'est pas autorisé et que le VLAN invité est activé, le trafic non balisé est remappé sur le VLAN invité. Le trafic balisé est abandonné sauf s'il appartient au VLAN invité ou à un VLAN non authentifié. Si un VLAN invité n'est pas activé sur le port, seul le trafic balisé appartenant aux VLAN non authentifiés est ponté.

Lorsqu'un port est autorisé, le trafic balisé et non balisé provenant de l'hôte autorisé est ponté en fonction de la configuration du port d'appartenance au VLAN statique. Le trafic provenant des autres hôtes est abandonné.

Un utilisateur peut spécifier que le trafic non balisé provenant de l'hôte autorisé doit être remappé sur un VLAN qui est attribué par un serveur RADIUS au cours du processus d'authentification. Le trafic balisé est abandonné sauf s'il appartient au VLAN affecté par RADIUS ou aux VLAN non authentifiés. Vous pouvez définir l'affectation VLAN RADIUS sur un port via la page Authentification des ports.

- **Mode Hôtes multiples**

  Un port est autorisé s'il y a au moins un client autorisé.

  Lorsqu'un port n'est pas autorisé et qu'un VLAN invité est activé, le trafic non balisé est remappé sur le VLAN invité. Le trafic balisé est abandonné sauf s'il appartient au VLAN invité ou à un VLAN non authentifié. Si le VLAN invité n'est pas activé sur un port, seul le trafic balisé appartenant aux VLAN non authentifiés est ponté.

  Lorsqu'un port est autorisé, le trafic balisé et non balisé provenant de tous les hôtes connectés au port est ponté en fonction de la configuration du port d'appartenance au VLAN statique.

  Vous pouvez spécifier que le trafic non balisé provenant du port autorisé doit être remappé sur un VLAN qui est attribué par un serveur RADIUS au cours du processus d'authentification. Le trafic balisé est abandonné sauf s'il appartient au VLAN affecté par RADIUS ou aux VLAN non authentifiés. Vous pouvez définir l'affectation VLAN RADIUS sur un port via la page Authentification des ports.

- **Mode Sessions multiples**

  À la différence des modes Hôte unique et Hôtes multiples, un port en mode Sessions multiples n'a pas d'état d'authentification. Cet état est attribué à chaque client connecté au port.

  Le trafic balisé appartenant à un VLAN non authentifié est toujours ponté, que l'hôte soit autorisé ou pas.

  Le trafic balisé et non balisé qui provient d'hôtes non autorisés n'appartenant pas à un VLAN non authentifié est remappé sur le VLAN invité s'il est défini et activé sur le VLAN, ou est abandonné si le VLAN invité n'est pas activé sur le port.

  Vous pouvez spécifier que le trafic non balisé provenant du port autorisé doit être remappé sur un VLAN qui est attribué par un serveur RADIUS au cours du processus d'authentification. Le trafic balisé est abandonné sauf s'il appartient au VLAN affecté par RADIUS ou aux VLAN non authentifiés. Vous pouvez définir l'affectation VLAN RADIUS sur un port via la page Authentification des ports.

Méthodes d'authentification multiples

Si plus d'une méthode d'authentification est activée sur le commutateur, la hiérarchie suivante des méthodes d'authentification est appliquée :

- Authentification 802.1x : la plus haute
- Authentification Web
- Authentification MAC : la plus basse

Plusieurs méthodes peuvent être exécutées simultanément. Lorsqu'une méthode est exécutée avec succès, le client est alors autorisé. Les méthodes ayant une priorité plus basse sont arrêtées et celles ayant une priorité plus haute continuent.

Lorsque l'une des méthodes d'authentification exécutées simultanément échoue, les autres méthodes continuent.

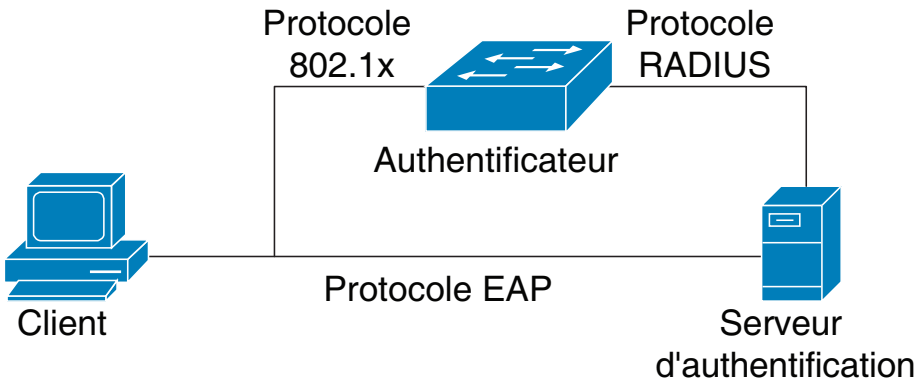
Lorsqu'une méthode d'authentification s'exécute avec succès pour un client authentifié par une méthode d'authentification ayant une priorité plus basse, les attributs de la nouvelle méthode d'authentification sont appliqués. Lorsque la nouvelle méthode échoue, le client continue à être autorisé pour l'ancienne méthode.

Authentification 802.1x

L'authentificateur 802.1x relaie les messages EAP transparents entre les demandeurs 802.1x et les serveurs d'authentification. Les messages EAP entre les demandeurs et l'authentificateur sont encapsulés dans les messages 802.1x, et les messages EAP entre l'authentificateur et les serveurs d'authentification sont encapsulés dans les messages RADIUS.

Ce processus est décrit dans la figure ci-dessous :

Figure 1 Authentification 802.1x

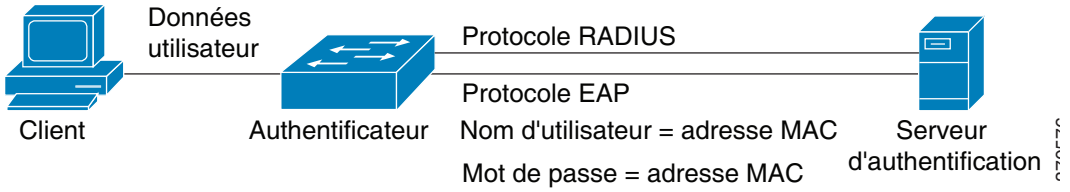


Authentification MAC

L'authentification MAC est une alternative à l'authentification 802.1X qui offre un accès réseau aux périphériques (comme les imprimantes et les téléphones IP) ne disposant pas de la fonctionnalité de demandeur 802.1X. L'authentification MAC utilise l'adresse MAC du périphérique qui se connecte pour accorder ou refuser l'accès au réseau.

Dans ce cas, le commutateur prend en charge la fonctionnalité EAP MD5 avec un nom d'utilisateur et un mot de passe identiques à l'adresse MAC du client, comme indiqué ci-dessous.

Figure 2 Authentification MAC



Cette méthode n'a pas de configuration spécifique.

Authentification Web

L'authentification Web permet d'authentifier les utilisateurs qui demandent accès à un réseau via un commutateur. Elle permet aux clients directement connectés au commutateur d'être authentifiés par l'intermédiaire d'un mécanisme de portail captif avant que le client ne se voit accorder l'accès au réseau. L'authentification Web est une authentification client et est prise en charge en mode Sessions multiples en Couche 2 et Couche 3.

Cette méthode d'authentification est activée par port et lorsqu'un port est activé, chaque hôte doit s'authentifier afin d'accéder au réseau. Ainsi, sur un port activé, vous pouvez avoir des hôtes authentifiés et non authentifiés.

Lorsque l'authentification Web est activée sur un port, le commutateur abandonne tout le trafic envoyé par les clients non autorisés vers le port, à l'exception des paquets ARP, DHCP et DNS. Ces paquets sont autorisés à être transférés par le commutateur, afin que même les clients non autorisés puissent obtenir une adresse IP et soient en mesure de résoudre les noms d'hôte ou de domaine.

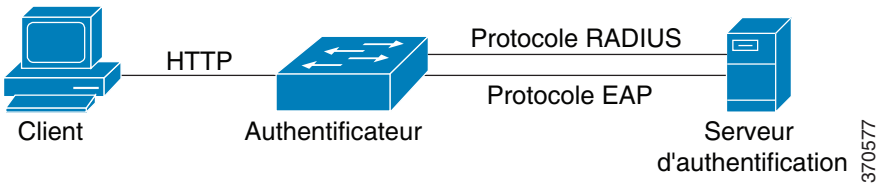
Tous les paquets HTTP/HTTPS sur IPv4 issus des clients non autorisés sont interceptés par le processeur sur le commutateur. Si l'authentification Web est activée sur le port, une page de connexion apparaît avant que la page demandée ne s'affiche. L'utilisateur doit saisir son nom d'utilisateur et son mot de passe qui sont authentifiés par un serveur RADIUS utilisant le protocole EAP. Si l'authentification réussit, l'utilisateur en est informé.

L'utilisateur a maintenant une session authentifiée. La session reste ouverte tant qu'elle est utilisée. Si elle n'est pas utilisée pendant un certain laps de temps, elle est fermée. Cette durée, appelée Période silencieuse, peut être définie par l'administrateur système. Une fois que la session a expiré, le nom d'utilisateur et le mot de passe sont supprimés et l'invité doit de nouveau les saisir pour ouvrir une nouvelle session.

Reportez-vous à la section Méthodes d'authentification et modes de port.

Lorsque l'authentification est terminée, le commutateur transfère tout le trafic provenant du client sur le port, comme illustré dans la figure ci-dessous.

Figure 3 Authentification Web



L'authentification Web ne peut pas être configurée sur un port pour lequel la fonction VLAN invité ou VLAN affecté par RADIUS est activée.

L'authentification Web prend en charge les pages suivantes :

- Page de connexion
- Page de réussite de connexion

Il existe un groupe prédéfini et intégré de ces pages.

Ces pages peuvent être modifiées sur la page Authentification Web.

Vous pouvez prévisualiser chacune des pages personnalisées. La configuration est enregistrée dans le fichier de Configuration d'exécution.

VLAN non authentifiés et VLAN invité

Les VLAN non authentifiés et le VLAN invité permettent d'accéder aux services qui ne nécessitent pas que les ports ou appareils demandeurs disposent d'une authentification et d'une autorisation.

Le VLAN invité est le VLAN attribué à un client non autorisé. Vous pouvez configurer le VLAN invité et un ou plusieurs VLAN non authentifiés sur la page Propriétés.

Un VLAN non authentifié est un VLAN qui autorise l'accès via des appareils ou ports autorisés et non autorisés.

Un VLAN non authentifié est doté des caractéristiques suivantes :

- Il doit s'agir d'un VLAN statique ; il ne peut correspondre au VLAN invité ni au VLAN par défaut.
- Les ports membres doivent être configurés manuellement en tant que membres balisés.
- Les ports membres doivent être des ports réseau et/ou généraux. Un port d'accès ne peut pas être membre d'un VLAN non authentifié.

Le VLAN invité, s'il est configuré, est un VLAN statique doté des caractéristiques suivantes :

- Il doit être défini manuellement à partir d'un VLAN statique existant.
- Le VLAN invité ne peut être utilisé en tant que VLAN voix ni en tant que VLAN non authentifié.

Pour obtenir un récapitulatif des modes dans lesquels le VLAN invité est pris en charge, reportez-vous au Prise en charge de l'affectation VLAN RADIUS.

Modes hôte avec VLAN invité

Les modes hôte fonctionnent avec le VLAN invité de la manière suivante :

- **Mode Hôte unique et Hôtes multiples**

  Le trafic non balisé et le trafic balisé appartenant au VLAN invité arrivant sur un port non autorisé sont pontés via le VLAN invité. Tout autre trafic est ignoré. Le trafic appartenant à un VLAN non authentifié est ponté via le VLAN.

- **Mode Sessions multiples**

  Le trafic non balisé et le trafic balisé, n'appartenant pas aux VLAN non authentifiés et provenant de clients non autorisés, sont attribués au VLAN invité à l'aide de la règle TCAM et sont pontés via le VLAN invité. Le trafic balisé appartenant à un VLAN non authentifié est ponté via le VLAN.

  Ce mode ne peut pas être configuré sur la même interface avec des VLAN basés sur une stratégie.

Affectation VLAN RADIUS ou Affectation VLAN dynamique

Un client autorisé peut se voir attribuer un VLAN par le serveur RADIUS, si l'option est activée sur la page Authentification des ports. Elle porte le nom d'Affectation dynamique de VLAN (AVD) ou d'Affectation VLAN RADIUS. Dans ce guide, le terme VLAN affecté par RADIUS est utilisé.

Le trafic non balisé et le trafic balisé n'appartenant pas aux VLAN non authentifiés et provenant du client sont attribués au VLAN affecté par RADIUS à l'aide de la règle TCAM et sont pontés via le VLAN.

Pour plus d'informations sur le comportement des différents modes lorsque la fonction VLAN affecté par RADIUS est activée sur le périphérique, reportez-vous à Prise en charge de l'affectation VLAN RADIUS.

Pour qu'un périphérique soit authentifié et autorisé sur un port activé pour l'ADV :

- Le serveur RADIUS doit authentifier l'appareil et lui affecter de façon dynamique un VLAN. Vous pouvez définir le champ RADIUS VLAN Assignment (Affectation VLAN RADIUS) sur Static (Statique) sur la page Authentification des ports. L'hôte peut ainsi être ponté conformément à la configuration statique.
- Un serveur RADIUS doit prendre en charge l'ADV avec les attributs RADIUS tunnel-type (64) = VLAN (13), tunnel-media-type (65) = 802 (6) et tunnel-private-group-id = un ID VLAN.

Si l'attribut tunnel-private-group-id est fourni sous forme de nom du VLAN, le VLAN portant ce nom doit être configuré de manière statique sur le périphérique. Si un ID VLAN (2-4094) est utilisé dans cet attribut, après l'authentification d'un demandeur, le VLAN sera créé de façon dynamique.

Lorsque la fonction VLAN affecté par RADIUS est activée, les modes hôte se comportent comme suit :

- **Mode Hôte unique et Hôtes multiples**

  Le trafic non balisé et le trafic balisé appartenant au VLAN affecté par RADIUS sont pontés via ce VLAN. Tout autre trafic n'appartenant pas aux VLAN non authentifiés est ignoré.

- **Mode Sessions multiples**

  Le trafic non balisé et le trafic balisé n'appartenant pas aux VLAN non authentifiés et provenant du client sont attribués au VLAN affecté par RADIUS à l'aide des règles TCAM et sont pontés via le VLAN.

Le tableau suivant décrit la prise en charge de l'affectation VLAN invité et VLAN RADIUS en fonction de la méthode d'authentification et du mode de port.

Prise en charge de l'affectation VLAN RADIUS

Méthode d'authentification	Hôte unique	Hôtes multiples	Sessions multiples
802.1x	†	†	†
MAC	†	†	†
WEB	**N/C**	**N/C**	**N/C**

Légende :

† : le mode de port prend en charge l'attribution VLAN invité et VLAN RADIUS.

N/C : le mode de port ne prend pas en charge la méthode d'authentification.

Mode Violation

En mode Hôte unique, vous pouvez configurer l'action à effectuer lorsqu'un hôte non autorisé sur un port autorisé tente d'accéder à l'interface. Cela s'effectue sur la page Authentification hôtes et sessions.

Les options suivantes sont disponibles :

- **Restreindre** : génère une interception lorsqu'une station, dont l'adresse MAC n'est pas l'adresse MAC du demandeur, tente d'accéder à l'interface. La durée minimale entre les interceptions est de 1 seconde. Ces trames sont transmises, mais leurs adresses sources ne sont pas apprises.
- **Protéger** : ignore les trames dont l'adresse source n'est pas celle du demandeur.
- **Arrêter** : ignore les trames dont l'adresse source n'est pas celle du demandeur et ferme le port.

Vous pouvez aussi configurer le périphérique pour qu'il envoie des interceptions SNMP, avec une durée minimale configurable entre deux interceptions consécutives. Si secondes = 0, les interceptions sont désactivées. Si aucune durée minimale n'est spécifiée, la valeur par défaut utilisée est 1 seconde pour le mode restreindre et 0 pour les autres modes.

Période silencieuse

La période silencieuse est une période au cours de laquelle le port (mode Hôte unique ou Hôtes multiples) ou le client (mode Sessions multiples) ne peut pas effectuer de tentative d'authentification suite à l'échec d'un échange d'authentification. En mode Hôte unique ou Hôtes multiples, la période est définie par port ; en mode Sessions multiples, la période est définie par client. Au cours de la période silencieuse, le commutateur ne peut pas accepter, ni initialiser les requêtes d'authentification.

La période ne s'applique qu'aux authentifications Web et 802.1x.

Vous pouvez aussi spécifier le nombre maximal de tentatives de connexion avant le début de la période silencieuse. La valeur 0 indique un nombre illimité de tentatives de connexion.

La durée de la période silencieuse et le nombre maximal de tentatives de connexion peuvent être définis sur la page Authentification des ports.

Prise en charge des méthodes d'authentification et des modes de port

Le tableau suivant indique les combinaisons de méthode d'authentification et de mode de port qui sont prises en charge.

Méthodes d'authentification et modes de port

Méthode d'authentification	Hôte unique	Hôtes multiples	Sessions multiples	
			Périphérique en L3	Périphérique en L2
802.1x	†	†	†	†
MAC	†	†	†	†
WEB	N/C	N/C	N/C	†

Légende :

† : le mode de port prend aussi en charge l'attribution VLAN invité et VLAN RADIUS.

N/C : la méthode d'authentification ne prend pas en charge le mode de port.

REMARQUE Vous pouvez simuler le mode hôte unique en réglant le paramètre Max Hosts (Nombre d'hôtes max.) sur 1 à la page Authentification des ports.

Comportement des modes

Le tableau suivant décrit la façon dont le trafic authentifié et non authentifié est traité dans diverses situations.

	Trafic non authentifié				Trafic authentifié			
	Avec VLAN invité		Sans VLAN invité		Avec VLAN Radius		Sans VLAN Radius	
	Non balisé	Balisé	Non balisé	Balisé	Non balisé	Balisé	Non balisé	Balisé
Hôte unique	Les trames sont remappées sur le VLAN invité	Les trames sont abandonnées sauf si elles appartiennent au VLAN invité ou aux VLAN non authentifiés	Les trames sont abandonnées	Les trames sont abandonnées sauf si elles appartiennent aux VLAN non authentifiés	Les trames sont remappées sur le VLAN affecté par RADIUS	Les trames sont abandonnées sauf si elles appartiennent au VLAN RADIUS ou aux VLAN non authentifiés	Les trames sont pontées sur la base de la configuration VLAN statique	Les trames sont pontées sur la base de la configuration VLAN statique
Hôtes multiples	Les trames sont remappées sur le VLAN invité	Les trames sont abandonnées sauf si elles appartiennent au VLAN invité ou aux VLAN non authentifiés	Les trames sont abandonnées	Les trames sont abandonnées sauf si elles appartiennent aux VLAN non authentifiés	Les trames sont remappées sur le VLAN affecté par RADIUS	Les trames sont abandonnées sauf si elles appartiennent au VLAN RADIUS ou aux VLAN non authentifiés	Les trames sont pontées sur la base de la configuration VLAN statique	Les trames sont pontées sur la base de la configuration VLAN statique
Sessions multiples allégées	N/C	N/C	Les trames sont abandonnées	Les trames sont abandonnées sauf si elles appartiennent aux VLAN non authentifiés	N/C	N/C	Les trames sont pontées sur la base de la configuration VLAN statique	Les trames sont pontées sur la base de la configuration VLAN statique

	Trafic non authentifié				Trafic authentifié			
	Avec VLAN invité		Sans VLAN invité		Avec VLAN Radius		Sans VLAN Radius	
	Non balisé	Balisé	Non balisé	Balisé	Non balisé	Balisé	Non balisé	Balisé
Sessions multiples complètes	Les trames sont remappées sur le VLAN invité	Les trames sont remappées sur le VLAN invité sauf si elles appartiennent aux VLAN non authentifiés	Les trames sont abandonnées	Les trames sont abandonnées sauf si elles appartiennent aux VLAN non authentifiés	Les trames sont remappées sur le VLAN affecté par RADIUS	Les trames sont remappées sur le VLAN Radius sauf si elles appartiennent aux VLAN non authentifiés	Les trames sont pontées sur la base de la configuration VLAN statique	Les trames sont pontées sur la base de la configuration VLAN statique

Commutateur agissant en tant que demandeur 802.1x

Outre sa capacité d'agir en tant qu'authentificateur 802.1x, le commutateur lui-même peut être configuré pour agir en tant que demandeur 802.1x et solliciter une autorisation d'accès au port à un périphérique voisin. Le demandeur utilise la méthode de vérification EAP-MD5 spécifiée dans le standard RFC3748. Cette méthode authentifie un client à l'aide de son nom et de son mot de passe.

Quand l'option demandeur est activée sur une interface, l'interface devient non autorisée. Quand le processus d'authentification 802.1X réussit, l'interface devient autorisée.

Les événements qui suivent lancent l'authentification 802.1X sur un port :

- L'option demandeur est activée sur un port à l'état Actif.
- Le statut du port passe à Actif et l'option demandeur est activée sur le port.
- Un message de demande d'identifiant EAP est reçu sur le port et le demandeur est activé sur le port.

Les options authentificateur 802.1x et demandeur ne peuvent pas être activées simultanément sur une même interface.

Tâches courantes

Flux de travail 1 : activer l'authentification 802.1x sur un port

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X > Propriétés** pour activer globalement l'authentification 802.1X.

ÉTAPE 2 Activez l'authentification basée sur les ports.

ÉTAPE 3 Sélectionnez la **Méthode d'authentification**.

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

ÉTAPE 5 **Cliquez sur Sécurité > Authentification 802.1X > Hôtes et sessions.**

ÉTAPE 6 Sélectionnez le port souhaité et cliquez sur **Modifier**.

ÉTAPE 7 Définissez le mode Authentification des hôtes.

ÉTAPE 8 Cliquez sur **Appliquer** ; le fichier de Configuration d'exécution est mis à jour.

ÉTAPE 9 Cliquez sur **Sécurité > Authentification 802.1X > Authentification des ports**.

ÉTAPE 10 Sélectionnez un port et cliquez sur **Edit**.

ÉTAPE 11 Définissez le champ Contrôle de port administratif sur **Auto**.

ÉTAPE 12 Définissez les méthodes d'authentification.

ÉTAPE 13 Cliquez sur **Appliquer** ; le fichier de Configuration d'exécution est mis à jour.

Flux de travail 2 : configurer les interceptions

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X** > **Propriétés**.

ÉTAPE 2 Sélectionnez les interceptions requises.

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

Flux de travail 3 : configurer l'authentification 802.1x, ou l'authentification MAC ou Web

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X > Authentification des ports**.

ÉTAPE 2 Sélectionnez le port souhaité et cliquez sur **Modifier**.

ÉTAPE 3 Renseignez les champs requis pour le port.

Les champs de cette page sont décrits à la section Authentification des ports.

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

Utilisez le bouton **Copier les paramètres** pour copier les paramètres d'un port vers un autre.

Flux de travail 4 : configurer la période silencieuse

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X > Authentification des ports**.

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

ÉTAPE 3 Saisissez la période silencieuse dans le champ Période silencieuse.

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

Flux de travail 5 : Pour configurer le VLAN invité :

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X > Propriétés**.

ÉTAPE 2 Sélectionnez **Activer** dans le champ VLAN invité.

ÉTAPE 3 Sélectionnez le VLAN invité dans le champ ID du VLAN invité.

ÉTAPE 4 Définissez le Délai d'expiration VLAN invité sur Immédiat ou entrez une valeur dans le champ Défini par l'utilisateur.

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

Flux de travail 6 : configurer les VLAN non authentifiés

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X** > **Propriétés**.

ÉTAPE 2 Sélectionnez un VLAN, puis cliquez sur **Modifier**.

ÉTAPE 3 Sélectionnez un VLAN.

ÉTAPE 4 Vous pouvez également décocher **Authentification** pour faire du VLAN un VLAN non authentifié.

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

Flux de travail 7 : configurer un demandeur 802.1X sur une interface

ÉTAPE 1 Cliquez sur **Sécurité > 802.1X > Informations d'identification du demandeur** pour configurer les informations d'identification du demandeur.

ÉTAPE 2 Cliquez sur **Sécurité > 802.1X > Authentification des ports**.

ÉTAPE 3 Sélectionnez le port souhaité et cliquez sur **Modifier**.

ÉTAPE 4 Activez l'option demandeur, puis précisez les informations d'identification à utiliser.

Les champs de cette page sont décrits à la section **Authentification des ports**.

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

Propriétés

Utilisez la page Properties (Propriétés) pour activer globalement l'authentification du port/du périphérique. Pour que l'authentification puisse fonctionner, elle doit être activée à la fois globalement et individuellement sur chaque port.

Pour définir l'authentification basée sur les ports :

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X > Propriétés**.

ÉTAPE 2 Saisissez les paramètres.

- **Authentification basée sur les ports** : activez ou désactivez l'authentification basée sur les ports.

  Si cette fonction est désactivée, les authentifications 802.1X, MAC et Web ainsi que la fonctionnalité de demandeur 802.1X sont désactivées.

- **Méthode d'authentification** : sélectionnez les méthodes d'authentification des utilisateurs. Les options sont les suivantes :

  - *RADIUS, aucune* : effectue tout d'abord l'authentification des ports en utilisant le serveur RADIUS. Si aucune réponse n'est reçue du serveur RADIUS (par exemple s'il n'est pas actif), aucune authentification n'est réalisée et la session est autorisée. Si le serveur est disponible, mais que les informations d'identification de l'utilisateur sont incorrectes, l'accès est refusé et la session prend fin.

- *RADIUS* : authentifie l'utilisateur sur le serveur RADIUS. Si aucune authentification n'est effectuée, la session n'est pas autorisée.
- *Aucune* : n'authentifie pas l'utilisateur. Autorise la session.

- **VLAN invité** : sélectionnez cette option pour permettre l'utilisation d'un VLAN invité pour les ports non autorisés. Si un VLAN invité est activé, tous les ports non autorisés se connectent automatiquement au VLAN sélectionné dans le champ *ID du VLAN invité*. Si un port est par la suite autorisé, il est supprimé du VLAN invité.

  Le VLAN invité peut être défini comme une interface de couche 3 (reçoit une adresse IP) comme tout autre VLAN. Cependant, la gestion des appareils n'est pas disponible via l'adresse IP du VLAN invité.
- **ID du VLAN invité** : sélectionnez le VLAN invité dans la liste des VLAN.
- **Délai d'expiration VLAN invité** : choisissez l'option **Immédiat** ou saisissez une valeur dans **Défini par l'utilisateur**. Cette valeur est utilisée comme suit :

  Une fois la connexion établie, si le logiciel ne détecte pas le demandeur 802.1X ou si l'authentification a échoué, le port est ajouté au VLAN invité mais seulement lorsque le *Délai d'expiration VLAN invité* a expiré.

  Si l'état du port passe d'*Autorisé* à *Non autorisé*, le port est ajouté au VLAN invité, mais seulement lorsque le délai d'expiration du *VLAN invité* a expiré.
- **Paramètres d'interception** : pour activer les interceptions, sélectionnez au moins une des options suivantes :
  - *Interceptions d'échec d'authentification 802.1x* : sélectionnez cette option pour générer une interception si l'authentification 802.1x échoue.
  - *Interceptions de réussite d'authentification 802.1x* : sélectionnez cette option pour générer une interception si l'authentification 802.1x réussit.
  - *Interceptions d'échec d'authentification MAC* : sélectionnez cette option pour générer une interception en cas d'échec de l'authentification MAC.
  - *Interceptions de réussite d'authentification MAC* : sélectionnez cette option pour générer une interception si l'authentification MAC réussit.
  - *Interceptions d'échec d'authentification demandeur* : sélectionnez cette option pour générer une interception en cas d'échec de l'authentification demandeur.
  - *Interceptions de réussite d'authentification demandeur* : sélectionnez cette option pour générer une interception si l'authentification demandeur réussit.
  - *Interceptions d'échec d'authentification Web* : sélectionnez cette option pour générer une interception si l'authentification Web échoue.

- *Interceptions de réussite d'authentification Web* : sélectionnez cette option pour générer une interception si l'authentification Web réussit.
- *Interceptions silencieuses d'authentification Web* : sélectionnez cette option pour générer une interception si une période silencieuse commence.

La Table d'authentification des VLAN affiche tous les VLAN et indique si l'authentification a été activée sur chacun d'eux.

ÉTAPE 3 Cliquez sur **Appliquer**. Les propriétés 802.1X sont écrites dans le fichier de Configuration d'exécution.

Pour activer ou désactiver l'authentification sur un VLAN, sélectionnez ce dernier, cliquez sur **Edit** (Modifier) et sélectionnez **Enable** (Activer) ou **Disable** (Désactiver).

Authentification des ports

La page Port Authentication (Authentification des ports) permet de définir les paramètres pour chaque port. Puisque certaines modifications de la configuration ne sont possibles que si le port a l'état Autorisation forcée (par exemple, l'authentification des hôtes), il est recommandé de changer le contrôle du port en Autorisation forcée avant d'effectuer des modifications. Une fois la configuration terminée, rétablissez l'état précédent du contrôle de port.

REMARQUE Un port sur lequel 802.1X est défini ne peut pas devenir membre d'un LAG. L'authentification 802.1X et la sécurité des ports ne peuvent pas être activées sur le même port simultanément. Si vous activez la sécurité des ports sur une interface, le Contrôle de port administratif ne peut pas être défini sur le mode Auto.

Pour définir l'authentification 802.1X :

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X** > **Authentification des ports**.

Cette page affiche les paramètres d'authentification de tous les ports. Outre les champs décrits sur la page **Ajouter**, les champs suivants s'affichent pour chaque port :

- **État du demandeur** : cet état peut être Autorisé ou Non autorisé pour une interface sur laquelle l'option demandeur 802.1x a été activée.
- **Informations d'identification** : nom de la structure des informations d'identification utilisée pour l'interface du demandeur. Cette valeur peut être un nom ou N/A si le demandeur n'est pas activé. Si un port dispose d'un nom d'identification du demandeur configuré, la valeur du paramètre de contrôle de port est Demandeur. Cette valeur remplace toute autre information de contrôle de port reçue depuis le port.

ÉTAPE 2 Sélectionnez un port (autre que le port OOB) et cliquez sur **Modifier**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez un port (autre que le port OOB).
- **Contrôle de port actuel** : affiche l'état actuel de l'autorisation du port. Si l'état est *Autorisé*, le port est authentifié ou le *Contrôle de port administratif* est en *Autorisation forcée*. À l'inverse, si l'état est *Non autorisé*, le port est non authentifié ou le *Contrôle de port administratif* est en *Non-autorisation forcée*. Si l'option demandeur est activée sur une interface, le contrôle de port actuel sera Demandeur.
- **Contrôle de port administratif** : affiche l'état d'autorisation du port administratif. Les options sont les suivantes :
  - *Non-autorisation forcée* : refuse l'accès à l'interface en passant cette dernière en mode non autorisé. Le périphérique ne fournit pas de services d'authentification au client via l'interface.
  - *Automatique* : active l'authentification et l'autorisation basées sur les ports sur le périphérique. L'interface bascule entre un état autorisé ou non autorisé en fonction de l'échange d'authentification entre le périphérique et le client.
  - *Autorisation forcée* : autorise l'interface sans authentification.
- **Affectation VLAN RADIUS** : sélectionnez cette option pour activer l'affectation dynamique de VLAN sur le port sélectionné.
  - **Désactiver** : la fonction n'est pas activée.
  - **Rejeter** : si le serveur RADIUS a autorisé le demandeur, mais n'a pas fourni de VLAN demandeur, le demandeur est rejeté.
  - **Statique** : si le serveur RADIUS a autorisé le demandeur, mais n'a pas fourni de VLAN demandeur, le demandeur est accepté.
- **VLAN invité** : sélectionnez cette option pour permettre l'utilisation d'un VLAN invité pour les ports non autorisés. Si un VLAN invité est activé, le port non autorisé rejoint automatiquement le VLAN sélectionné dans le champ Guest VLAN ID (ID du VLAN invité) de la page Authentification des ports. 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.
- **Accès ouvert** : sélectionnez cette option pour authentifier le port même en cas d'échec de l'authentification. Reportez-vous à la section Accès ouvert.
- **802.1X Based Authentication** (Authentification 802.1X) : sélectionnez cette option pour activer l'authentification 802.1X sur le port.

- **MAC Based Authentication** (Authentification MAC) : sélectionnez cette option pour activer l'authentification du port en fonction de l'adresse MAC du demandeur. Seules huit authentifications basées sur MAC peuvent être utilisées sur le port.

  REMARQUE Pour que l'authentification MAC réussisse, le nom d'utilisateur et le mot de passe de demandeur du serveur RADIUS doivent être l'adresse MAC du demandeur. L'adresse MAC doit être en minuscules et saisie sans les séparateurs « . » ou « - », par exemple : 0020aa00bbcc.

- **Web Based Authentication** (Authentification Web) : sélectionnez cette option pour activer l'authentification Web en fonction de l'adresse MAC du demandeur.
- **Réauthentification périodique** : sélectionnez cette option pour autoriser les tentatives de réauthentification du port une fois la Période de réauthentification spécifiée expirée.
- **Reauthentication Period** : saisissez le délai (en secondes) au bout duquel le port sélectionné est réauthentifié.
- **Réauthentifier maintenant** : sélectionnez cette option pour permettre la réauthentification immédiate du port.
- **Authenticator State** : affiche l'état défini de l'autorisation du port. Les options sont les suivantes :
  - *Initialiser* : processus de démarrage.
  - *Force-Authorized* : l'état du port contrôlé est défini sur Force-Authorized (le trafic est réacheminé).
  - *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.
- **Période** : sélectionnez cette option pour limiter l'authentification à une période spécifique.
- **Nom de période** : si l'option **Période** est sélectionnée, choisissez la période à utiliser. Les périodes sont définies dans la section Configuration de l'heure système.
- **Nombre maximal de tentatives de connexion WBA** : saisissez le nombre maximal de tentatives de connexion autorisé pour l'authentification Web. Sélectionnez **Infini** pour ne spécifier aucune limite ou **Défini par l'utilisateur** pour spécifier une limite.

- **Maximum WBA Silence Period** (Période de silence WBA maximale) : saisissez la durée maximale de la période de silence pour l'authentification Web autorisée sur l'interface. Sélectionnez **Infini** pour ne spécifier aucune limite ou **Défini par l'utilisateur** pour spécifier une limite.
- **Nombre d'hôtes max.** : entrez le nombre maximal d'hôtes autorisés dans l'interface. Sélectionnez **Infini** pour ne spécifier aucune limite ou **Défini par l'utilisateur** pour spécifier une limite.

  REMARQUE Définissez cette valeur à 1 pour simuler le mode Hôte unique pour l'authentification Web en mode Sessions multiples.
- **Période silencieuse** : saisissez la durée de la période silencieuse.
- **Renvoi d'EAP** : saisissez le nombre de secondes pendant lesquelles le périphérique attend une réponse à une demande/trame d'identité EAP (Extensible Authentication Protocol) du demandeur (client) avant de renvoyer la demande.
- **Nombre maximum de demandes EAP** : 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.
- **Nombre maximum de demandes EAP** : saisissez le nombre maximum de demandes EAP pouvant être envoyées.
- **Délai d'expiration de la demande EAP** : saisissez la durée maximale d'attente de la réponse à la demande EAP avant son expiration.
- **Délai d'expiration demandeur** : spécifiez le délai (en secondes) à respecter avant que les demandes EAP soient renvoyées au demandeur.
- **Délai d'expiration serveur** : spécifiez le délai (en secondes) à respecter avant que le périphérique renvoie une demande au serveur d'authentification.
- **Demandeur** : sélectionnez cette option pour activer l'option 802.1X.
- **Informations d'identification** : sélectionnez dans la liste déroulante les informations d'identification à utiliser pour ce demandeur. Ce paramètre n'est disponible que si l'option demandeur est activée sur l'interface. **Modifier** vous permet d'accéder à la page des **Informations d'identification du demandeur** où ces informations peuvent être configurées.
- **Délai d'attente du demandeur** : spécifiez le délai que doit respecter le demandeur avant de relancer l'authentification après avoir reçu une réponse ÉCHEC du serveur RADIUS.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres des ports sont écrits dans le fichier de Configuration d'exécution.

Authentification hôtes et sessions

La page Authentification hôtes et sessions permet de définir le mode de fonctionnement de 802.1X sur le port, ainsi que l'action à réaliser si une violation a été détectée.

Pour obtenir une explication de ces modes, reportez-vous à la section Modes hôte de port.

Pour définir les paramètres 802.1X avancés pour les ports :

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X** > **Authentification hôtes et sessions**.

Les paramètres d'authentification sont décrits pour tous les ports. Tous les champs à l'exception des suivants sont décrits sur la page **Modifier**.

- **Nombre de violations** : affiche le nombre de paquets qui arrivent sur l'interface en mode hôte unique en provenance d'un hôte dont l'adresse MAC ne correspond pas à celle du demandeur.

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

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : entrez un numéro de port pour lequel l'authentification des hôtes est activée. Le port OOB n'est pas inclus.
- **Authentification des hôtes** : sélectionnez l'un des modes. Ces modes sont décrits ci-dessus dans la rubrique Modes hôte de port.

Paramètres de violation d'hôte unique (option seulement affichée si l'authentification des hôtes est définie sur Hôte unique) :

- **Action en cas de violation** : sélectionnez l'action à appliquer aux paquets arrivant en mode session unique/hôte unique en provenance d'un hôte dont l'adresse MAC ne correspond pas à celle du demandeur. Les options sont les suivantes :
  - *Protéger (Abandonner)* : abandonne les paquets.
  - *Restreindre (Transférer)* : transfère les paquets.
  - *Arrêter* : abandonne les paquets et ferme le port. Les ports restent fermés jusqu'à ce qu'ils soient réactivés ou jusqu'à ce que le périphérique soit réinitialisé.
- **Message « trap »** : sélectionnez cette option pour activer les « traps ».
- **Fréquence des interceptions** : définit la fréquence d'envoi des interceptions à l'hôte. Ce champ ne peut être défini que si plusieurs hôtes sont désactivés.

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

Hôtes authentifiés

Pour consulter les informations sur les utilisateurs authentifiés, cliquez sur **Sécurité > Authentification 802.1X** > **Hôtes authentifiés**.

Cette rubrique affiche les champs suivants :

- **Nom d'utilisateur** : nom des demandeurs authentifiés sur chaque port.
- **Port** : numéro du port.
- **Session Time (DD:HH:MM:SS)** (Heure de session [JJ:HH:MM:SS]) : durée pendant laquelle le demandeur a été authentifié et autorisé à accéder au port.
- **Méthode d'authentification** : méthode utilisée pour l'authentification de la dernière session.
- **Serveur d'authentification** : serveur RADIUS.
- **MAC Address** : affiche l'adresse MAC du demandeur.
- **ID du VLAN** : VLAN du port.

Clients verrouillés

Pour afficher les clients qui ont été verrouillés en raison d'échecs de tentative de connexion et pour déverrouiller un client verrouillé :

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X** > **Client verrouillé**.

Les champs suivants s'affichent :

- **Interface** : port verrouillé.
- **Adresse MAC** : affiche l'état actuel de l'autorisation du port. Si l'état est *Autorisé*, le port est authentifié ou le *Contrôle de port administratif* est en *Autorisation forcée*. À l'inverse, si l'état est *Non autorisé*, le port est non authentifié ou le *Contrôle de port administratif* est en *Non-autorisation forcée*.
- **Temps restant (s)** : temps restant avant le verrouillage du port.

ÉTAPE 2 Sélectionnez un port.

ÉTAPE 3 Cliquez sur **Déverrouiller**.

Personnalisation de l'authentification Web

Cette page permet de concevoir des pages d'authentification Web dans différentes langues.

Vous pouvez ajouter 4 langues maximum.

REMARQUE Jusqu'à 5 utilisateurs HTTP et 1 utilisateur HTTPS peuvent demander simultanément l'authentification Web. Lorsque ces utilisateurs sont authentifiés, d'autres utilisateurs peuvent demander l'authentification.

Pour ajouter une langue pour l'authentification Web :

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X** > **Personnalisation de l'authentification Web**.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Sélectionnez une langue dans la liste déroulante **Langue**.

ÉTAPE 4 Si cette langue est la langue par défaut, sélectionnez **Définir comme langue d'affichage par défaut**. Si l'utilisateur ne sélectionne pas de langue, les pages s'affichent dans la langue par défaut.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres sont enregistrés dans le fichier de Configuration d'exécution.

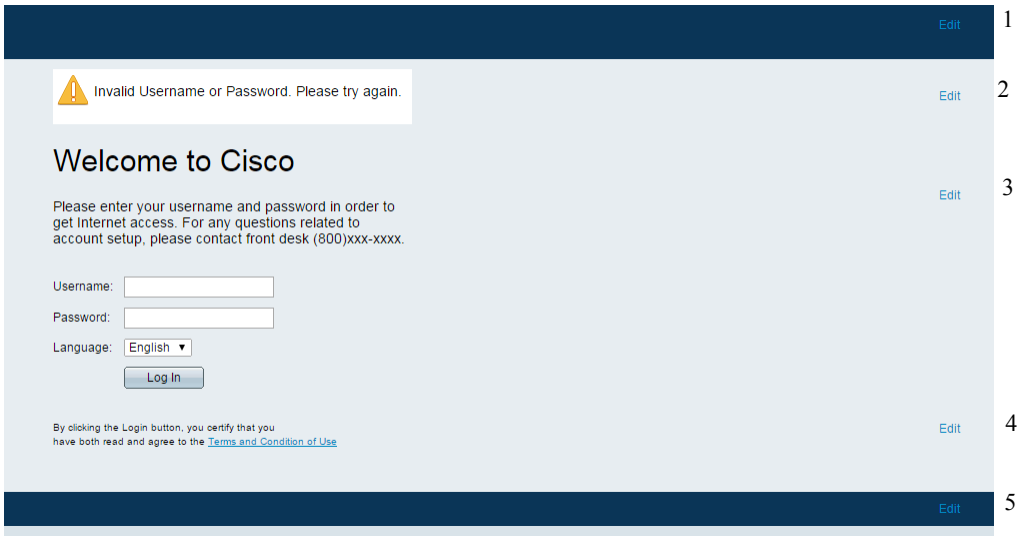
Pour personnaliser les pages d'authentification Web, procédez comme suit :

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X** > **Personnalisation de l'authentification Web**.

Cette page affiche les langues pouvant être personnalisées.

ÉTAPE 2 Cliquez sur **Modifier la page de connexion**.

La page suivante s'affiche :



ÉTAPE 3 Cliquez sur **Modifier l'étiquette 1**. Les champs suivants s'affichent :

- **Langue** : affiche la langue de la page.
- **Modèle de couleurs** : sélectionnez l'une des options de contraste.

  Si le modèle de couleurs **Personnalisé** est sélectionné, les options suivantes sont disponibles :

  - *Couleur d'arrière-plan de la page* : entrez le code ASCII de la couleur d'arrière-plan. La couleur sélectionnée apparaît dans le champ Texte.
  - *Couleur du texte de la page* : entrez le code ASCII de la couleur du texte. La couleur sélectionnée apparaît dans le champ Texte.
  - *Couleur d'arrière-plan des en-têtes et pieds de page* : entrez le code ASCII de la couleur d'arrière-plan des en-têtes et pieds de page. La couleur sélectionnée apparaît dans le champ Texte.

- *Couleur du texte des en-têtes et pieds de page* : entrez le code ASCII de la couleur du texte des en-têtes et pieds de page. La couleur sélectionnée apparaît dans le champ Texte.
- *Couleur du lien hypertexte* : entrez le code ASCII de la couleur du lien hypertexte. La couleur sélectionnée apparaît dans le champ Texte.

- **Image du logo actuel** : affiche le nom du fichier contenant l'image du logo actuel.
- **Logo Image** (Image du logo) : sélectionnez l'une des options suivantes :
  - *Aucun* : aucun logo.
  - *Par défaut* : utilisez le logo par défaut.
  - *Autre* : sélectionnez cette option pour entrer un logo personnalisé.

  Si l'option de logo **Autre** est sélectionnée, les options suivantes sont disponibles :
  - *Nom de fichier de l'image du logo* : entrez le nom de fichier du logo ou cliquez sur **Parcourir** pour accéder à l'image.
  - *Texte d'application* : entrez le texte qui accompagnera le logo.
  - *Texte du titre de la fenêtre* : entrez le titre de la page de connexion.

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

ÉTAPE 5 Cliquez sur **Modifier l'étiquette 2**. Les champs suivants s'affichent :

- **Infos d'ident. utilisateur non valides** : saisissez le texte du message à afficher lorsque l'utilisateur entre un nom d'utilisateur ou un mot de passe incorrect.
- **Service non disponible** : saisissez le texte du message à afficher lorsque le service d'authentification n'est pas disponible.

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

ÉTAPE 7 Cliquez sur **Modifier l'étiquette 3**. Les champs suivants s'affichent :

- **Message de bienvenue** : saisissez le texte du message à afficher lorsque l'utilisateur se connecte.
- **Message d'instruction** : saisissez les instructions qui s'afficheront pour l'utilisateur.
- **Authentification RADIUS** : indique si l'authentification RADIUS est activée. Si c'est le cas, le nom d'utilisateur et le mot de passe doivent être inclus dans la page de connexion.

- **Zone de texte nom d'utilisateur** : sélectionnez cette option pour afficher une zone de texte de nom d'utilisateur.
- **Étiqu. zone de texte nom d'utilisateur** : sélectionnez l'étiquette à afficher avant la zone de texte de nom d'utilisateur.
- **Zone de texte mot de passe** : sélectionnez cette option pour afficher une zone de texte de mot de passe.
- **Étiqu. zone de texte mot de passe** : sélectionnez l'étiquette à afficher avant la zone de texte de mot de passe.
- **Sélection de la langue** : sélectionnez cette option pour permettre à l'utilisateur de sélectionner une langue.
- **Étiquette de liste déroulante de langues** : entrez l'étiquette de liste déroulante de sélection de la langue.
- **Étiquette de bouton de connexion** : entrez l'étiquette du bouton de connexion.
- **Étiquette de progression de connexion** : entrez le texte qui sera affiché lors du processus de connexion.

ÉTAPE 8 Cliquez sur **Appliquer**. Les paramètres sont enregistrés dans le fichier de Configuration d'exécution.

ÉTAPE 9 Cliquez sur **Modifier l'étiquette 4**. Les champs suivants s'affichent :

- **Termes et conditions** : sélectionnez cette option pour activer une zone de texte de conditions d'utilisation.
- **Avertissement des termes et conditions** : saisissez le texte du message à afficher pour indiquer comment les conditions d'utilisation doivent être saisies.
- **Contenu des termes et conditions** : saisissez le texte du message des conditions d'utilisation à afficher.

ÉTAPE 10 Cliquez sur **Appliquer**. Les paramètres sont enregistrés dans le fichier de Configuration d'exécution.

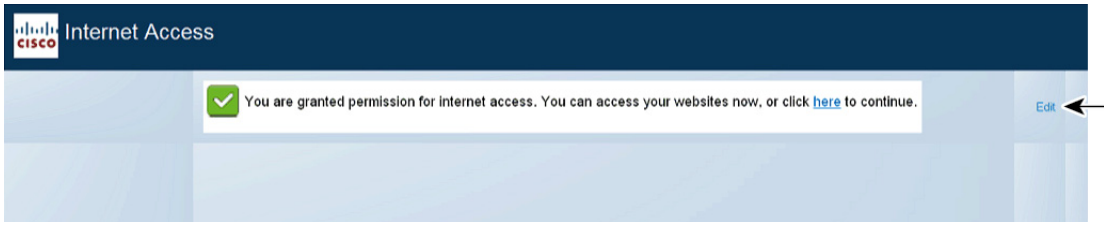
ÉTAPE 11 **Modifiez l'étiquette 5**. Les champs suivants s'affichent :

- **Copyright** : sélectionnez cette option pour activer l'affichage du texte de copyright.
- **Texte de copyright** : entrez le texte de copyright.

ÉTAPE 12 Cliquez sur **Appliquer**. Les paramètres sont enregistrés dans le fichier de Configuration d'exécution.

ÉTAPE 13 Cliquez sur **Modifier la page de réussite**.

Figure 4 La page suivante s'affiche



ÉTAPE 14 Cliquez sur le bouton **Modifier** à droite sur la page.

ÉTAPE 15 Saisissez le **Message de réussite**. Il s'agit du texte qui s'affichera si l'utilisateur réussit à se connecter.

ÉTAPE 16 Cliquez sur **Appliquer**. Les paramètres sont enregistrés dans le fichier de Configuration d'exécution.

Pour prévisualiser le message de connexion ou de réussite, cliquez sur **Aperçu**.

Pour définir la langue par défaut de l'interface utilisateur graphique comme langue par défaut pour l'authentification Web, cliquez sur **Définir la langue d'affichage par défaut**.

Informations d'identification du demandeur

Cette page permet de créer et de configurer les informations d'identification pouvant être utilisées par une interface configurée en tant que demandeur 802.1x.

Pour ajouter les informations d'identification du demandeur, procédez comme suit :

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X** > **Informations d'identification du demandeur**.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Renseignez les champs suivants :

- **Nom des informations d'identification** : nom associé aux informations d'identification.
- **Nom d'utilisateur** : saisissez le nom d'utilisateur correspondant au nom associé aux informations d'identification.

- **Description** : saisissez un texte décrivant l'événement.
- **Mot de passe** : sélectionnez un type de mot de passe parmi **Chiffré** ou **Texte en clair**, puis ajoutez le mot de passe.

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

22

Sécurité : Gestion sécurisée des données sensibles

Secure Sensitive Data (SSD) est une architecture qui simplifie la protection des données confidentielles, comme les mots de passe et les clés, sur un appareil. Cette fonctionnalité utilise les mots de passe, le cryptage, le contrôle d'accès et l'authentification des utilisateurs afin de fournir une solution sécurisée pour la gestion des données confidentielles.

Elle a été étendue afin de protéger l'intégrité des fichiers de configuration, sécuriser le processus de configuration et prendre en charge la configuration automatique sans intervention SSD.

Introduction

SSD protège les données confidentielles présentes sur un appareil, telles que les mots de passe et les clés, autorise et refuse l'accès aux données confidentielles sous forme chiffrée et de texte en clair en fonction des informations d'identification de l'utilisateur et des règles SSD, mais protège également contre toute altération des fichiers de configuration contenant des données confidentielles.

En outre, SSD permet la sauvegarde et le partage sécurisés des fichiers de configuration qui contiennent des données confidentielles.

SSD offre aux utilisateurs la flexibilité de configurer le niveau de protection souhaité pour leurs données confidentielles, à savoir aucune protection des données confidentielles sous forme de texte en clair, une protection minimale avec un cryptage basé sur le mot de passe par défaut ou une protection améliorée avec un cryptage basé sur le mot de passe défini par l'utilisateur.

SSD accorde une autorisation en lecture sur les données confidentielles uniquement aux utilisateurs authentifiés et autorisés, et conformément aux règles SSD. Un appareil authentifie et autorise l'accès de gestion pour les utilisateurs par l'intermédiaire du processus d'authentification des utilisateurs.

Que vous utilisiez ou non SSD, il est recommandé que l'administrateur sécurise le processus d'authentification par l'intermédiaire de la base de données d'authentification locale, et/ou sécurise la communication vers les serveurs d'authentification externes utilisés dans le processus d'authentification des utilisateurs.

En résumé, SSD protège les données sensibles sur un appareil à l'aide des règles SSD, des propriétés SSD et de l'authentification des utilisateurs. Par ailleurs, les règles SSD, les propriétés SSD et les configurations d'authentification des utilisateurs sur le périphérique sont elles-mêmes des données protégées par SSD.

Gestion SSD

La gestion SSD inclut un ensemble de paramètres de configuration qui définissent le traitement et la sécurité des données confidentielles. Les paramètres de configuration SSD eux-mêmes sont des données confidentielles et sont protégés par SSD.

Toute la configuration de SSD s'effectue via les pages SSD qui sont uniquement disponibles pour les utilisateurs disposant des autorisations appropriées (reportez-vous à la section Règles SSD).

Règles SSD

Les règles SSD définissent les autorisations en lecture et le mode de lecture par défaut attribués à une session utilisateur sur un canal de gestion.

Une règle SSD est identifiée de manière unique par son utilisateur et le canal de gestion SSD. Il peut y avoir différentes règles SSD pour le même utilisateur mais pour différents canaux. Inversement, il peut y avoir différentes règles pour le même canal, mais pour différents utilisateurs.

Les autorisations de lecture déterminent sous quelle forme les données confidentielles peuvent être affichées : sous forme chiffrée uniquement, sous forme de texte en clair uniquement, sous forme chiffrée ou de texte en clair, ou aucune autorisation d'afficher les données confidentielles. Les règles SSD elles-mêmes sont protégées en tant que données confidentielles.

Un appareil peut prendre en charge un total de 32 règles SSD.

Un appareil accorde à un utilisateur l'autorisation en lecture SSD de la règle SSD qui correspond le mieux à l'identité/aux informations d'identification de l'utilisateur et au type de canal de gestion à partir duquel l'utilisateur accède ou accédera aux données confidentielles.

À l'origine, un appareil comporte un ensemble de règles SSD par défaut. Un administrateur peut ajouter, supprimer et modifier des règles SSD comme il le souhaite.

REMARQUE Il se peut qu'un appareil ne puisse pas prendre en charge tous les canaux définis par SSD.

Éléments d'une règle SSD

Une règle SSD inclut les éléments suivants :

- **User type** (Type d'utilisateur) : les types d'utilisateurs pris en charge dans l'ordre de préférence (de la plus haute à la plus basse) sont les suivants : (Si un utilisateur correspond à plusieurs règles SSD, la règle avec le Type d'utilisateur ayant la préférence la plus haute sera appliquée).
  - **Spécifique** : la règle s'applique à un utilisateur spécifique.
  - **Utilisateur par défaut (cisco)** : la règle s'applique à l'utilisateur par défaut (cisco).
  - **Niveau 15** : la règle s'applique aux utilisateurs ayant le niveau de privilège 15.
  - **Tous** : la règle s'applique à tous les utilisateurs.
- **Nom d'utilisateur** : si le type d'utilisateur est Spécifique, un nom d'utilisateur est requis.
- **Canal :** type de canal de gestion SSD auquel la règle s'applique. Les types de canaux pris en charge sont :
  - **Sécurisé** : spécifie que la règle s'applique uniquement aux canaux sécurisés. Selon le périphérique, elle peut prendre en charge tous les canaux sécurisés suivants ou seulement certains d'entre eux :
    Interface de port de console, SCP, SSH et HTTPS.

- **Non sécurisé** : spécifie que cette règle s'applique uniquement aux canaux non sécurisés. Selon le périphérique, elle peut prendre en charge tous les canaux non sécurisés suivants ou seulement certains d'entre eux :
  Telnet, TFTP et HTTP.
- **SNMP XML sécurisé** : spécifie que cette règle s'applique uniquement au XML sur HTTPS ou SNMPv3 avec confidentialité. Un appareil est susceptible de ne pas prendre en charge tous les canaux XML et SNMP sécurisés.
- **SNMP XML non sécurisé** : spécifie que cette règle s'applique uniquement au XML sur HTTP ou SNMPv1/v2 et SNMPv3 sans confidentialité. Un appareil est susceptible de ne pas prendre en charge tous les canaux XML et SNMP sécurisés.

• **Autorisation en lecture** : autorisations en lecture associées aux règles. Elles peuvent être les suivantes :

- (Basse) **Exclure** : les utilisateurs ne sont pas autorisés à accéder aux données confidentielles sous quelque forme que ce soit.
- (Moyenne) **Chiffré uniquement** : les utilisateurs sont autorisés à accéder aux données confidentielles sous forme chiffrée uniquement.
- (Haute) **Texte en clair uniquement** : les utilisateurs sont autorisés à accéder aux données confidentielles sous forme de texte en clair uniquement. Les utilisateurs sont également autorisés à accéder aux paramètres SSD en lecture et en écriture.
- (Très haute) **Les deux** : les utilisateurs ont les autorisations Chiffré et Texte en clair, et sont autorisés à accéder aux données confidentielles sous forme chiffrée et de texte en clair. Les utilisateurs sont également autorisés à accéder aux paramètres SSD en lecture et en écriture.

Chaque canal de gestion permet des autorisations en lecture spécifiques. Elles sont récapitulées dans le tableau suivant.

Canal de gestion	Options d'autorisation en lecture permises
Sécurisé	Les deux, Chiffré uniquement
Non sécurisé	Les deux, Chiffré uniquement
SNMP XML sécurisé	Exclure, Texte en clair uniquement
SNMP XML non sécurisé	Exclure, Texte en clair uniquement

- **Mode de lecture par défaut** : tous les modes de lecture par défaut sont sujets à l'autorisation en lecture de la règle. Les options suivantes sont disponibles, mais certaines sont susceptibles d'être refusées en fonction de l'autorisation en lecture. Si l'autorisation en lecture définie par l'utilisateur pour un utilisateur est Exclure (par exemple), et que le mode de lecture par défaut est Chiffré, l'autorisation en lecture définie par l'utilisateur s'applique.
  - **Exclure** : n'autorise pas la lecture des données confidentielles.
  - **Chiffré** : les données confidentielles sont présentées sous forme chiffrée.
  - **Texte en clair** : les données confidentielles sont présentées sous forme de texte en clair.

  Chaque canal de gestion permet des autorisations en lecture spécifiques. Elles sont récapitulées dans le tableau suivant.

Autorisation en lecture	Mode de lecture par défaut autorisé
Exclure	Exclure
Chiffré uniquement	Chiffré*
Texte en clair uniquement	Texte en clair*
Les deux	Texte en clair, Chiffré*

* Le mode de lecture d'une session peut être temporairement modifié sur la page Propriétés SSD si le nouveau mode de lecture n'enfreint pas l'autorisation en lecture.

REMARQUE Notez les éléments suivants :

- Le mode de lecture par défaut pour les canaux de gestion SNMP XML sécurisé et SNMP XML non sécurisé doit être identique à leur autorisation en lecture.
- L'autorisation en lecture Exclure est uniquement permise pour les canaux de gestion SNMP XML sécurisé et SNMP XML non sécurisé ; l'autorisation Exclure n'est pas permise pour les canaux sécurisés et non sécurisés standard.
- L'exclusion des données confidentielles dans les canaux de gestion SNMP XML sécurisé et SNMP XML non sécurisé indique que les données confidentielles sont présentées en tant que 0 (ce qui signifie une chaîne nulle ou numérique 0). Si l'utilisateur souhaite afficher les données confidentielles, la règle doit être changée en texte en clair.
- Par défaut, un utilisateur SNMPv3 ayant des autorisations de canaux confidentiels et XML-over-secure est considéré comme un utilisateur de niveau 15.

- Les utilisateurs SNMP sur un canal SNMP et XML non sécurisé (SNMPv1, v2 et v3 sans confidentialité) sont considérés comme Tous les utilisateurs.
- Les noms de communauté SNMP ne sont pas utilisés comme noms d'utilisateur pour correspondre aux règles SSD.
- L'accès d'un utilisateur SNMPv3 spécifique peut être contrôlé en configurant une règle SSD avec un nom d'utilisateur qui correspond au nom d'utilisateur SNMPv3.
- Il doit toujours y avoir au moins une règle avec une autorisation en lecture : Texte en clair uniquement ou Les deux, car seuls les utilisateurs qui disposent de ces autorisations peuvent accéder aux pages SSD.
- Les changements apportés au mode de lecture par défaut et aux autorisations en lecture d'une règle deviennent effectifs et sont appliqués aux utilisateurs concernés et au canal de toutes les sessions de gestion actives immédiatement, à l'exclusion de la session qui effectue les changements même si la règle est applicable. Lorsqu'une règle est changée (ajout, suppression, modification), un système met à jour toutes les sessions CLI/GUI concernées.

REMARQUE Lorsque la règle SSD appliquée lors de la connexion à une session est modifiée à partir de cette session, l'utilisateur doit se déconnecter puis se reconnecter pour voir la modification.

REMARQUE Lors d'un transfert de fichier initié par une commande XML ou SNMP, le protocole sous-jacent utilisé est TFTP. Par conséquent, la règle SSD du canal non sécurisé s'appliquera.

Règles SSD et authentification des utilisateurs

SSD accorde une autorisation SSD uniquement aux utilisateurs authentifiés et autorisés, et conformément aux règles SSD. Un appareil dépend de son processus d'authentification des utilisateurs pour authentifier et autoriser l'accès de gestion. Pour protéger un appareil et ses données contre tout accès non autorisé, y compris les données confidentielles et les configurations SSD, il est recommandé de sécuriser le processus d'authentification des utilisateurs. Pour sécuriser le processus d'authentification des utilisateurs, vous pouvez utiliser la base de données d'authentification locale, mais aussi sécuriser la communication via les serveurs d'authentification externes, tels qu'un serveur RADIUS. La configuration de la communication sécurisée vers les serveurs d'authentification externes constitue des données confidentielles et est protégée par SSD.

REMARQUE Les informations d'identification des utilisateurs contenues dans la base de données d'authentification locale sont déjà protégées par un mécanisme non lié à SSD.

Si un utilisateur présent sur un canal exécute une action qui utilise un autre canal, l'appareil applique l'autorisation en lecture et le mode de lecture par défaut à partir de la règle SSD qui correspond aux informations d'identification des utilisateurs et à l'autre canal. Par exemple, si un utilisateur se connecte via un canal sécurisé et démarre une session de chargement TFTP, l'autorisation en lecture SSD de l'utilisateur sur le canal non sécurisé (TFTP) est appliquée.

Règles SSD par défaut

Les règles par défaut suivantes sont définies pour le périphérique :

Clé de règle		Action de règle	
Utilisateur	Canal	Autorisation en lecture	Mode de lecture par défaut
Niveau 15	SNMP XML sécurisé	Texte en clair uniquement	Texte en clair
Niveau 15	Sécurisé	Les deux	Chiffré
Niveau 15	Non sécurisé	Les deux	Chiffré
Tout	SNMP XML non sécurisé	Exclure	Exclure
Tout	Sécurisé	Chiffré uniquement	Chiffré
Tout	Non sécurisé	Chiffré uniquement	Chiffré

Il est possible de modifier les règles par défaut, mais pas de les supprimer. Si les règles par défaut SSD ont été modifiées, elles peuvent être restaurées.

Remplacement du mode de lecture par défaut SSD de la session

Le système affiche les données confidentielles dans une session, sous forme chiffrée ou de texte en clair, en fonction de l'autorisation en lecture et du mode de lecture par défaut de l'utilisateur.

Le mode de lecture par défaut peut être temporairement remplacé tant que cela n'occasionne pas de conflit avec l'autorisation en lecture SSD de la session. Cette modification est effective immédiatement dans la session actuelle, jusqu'à ce que l'un des événements suivants se produise :

- L'utilisateur le change à nouveau.
- La session est terminée.
- L'autorisation en lecture de la règle SSD qui est appliquée à l'utilisateur de la session est modifiée et n'est plus compatible avec le mode de lecture actuel de la session. Dans ce cas, le mode de lecture de la session redevient le mode de lecture par défaut de la règle SSD.

Propriétés SSD

Les propriétés SSD sont un ensemble de paramètres qui, conjointement avec les règles SSD, définissent et contrôlent l'environnement SSD d'un appareil. L'environnement SSD comporte les propriétés suivantes :

- Contrôle de la façon dont les données confidentielles sont chiffrées.
- Contrôle du niveau de sécurité sur les fichiers de configuration.
- Contrôle de la façon dont les données confidentielles sont affichées dans la session en actuelle.

Mot de passe

Le mot de passe constitue la base du mécanisme de sécurité dans la fonction SSD. Il permet de générer la clé de cryptage et de décryptage des données confidentielles. Les appareils qui possèdent le même mot de passe peuvent déchiffrer mutuellement leurs données sensibles qui ont été chiffrées avec la clé générée à partir du mot de passe.

Un mot de passe doit respecter les règles suivantes :

- **Longueur** : entre 8 et 16 caractères.
- **Classes de caractères** : le mot de passe doit comporter au moins un caractère en majuscule, un caractère en minuscule, un chiffre et un caractère spécial (# ou $, par exemple).

Mot de passe par défaut et mot de passe défini par l'utilisateur

Tous les appareils disposent d'un mot de passe par défaut qui est transparent pour les utilisateurs. Le mot de passe par défaut ne s'affiche jamais dans le fichier de configuration ou la CLI/GUI.

Pour bénéficier d'une meilleure sécurité et d'une meilleure protection, un administrateur doit configurer SSD sur un appareil, afin qu'il utilise un mot de passe défini par l'utilisateur au lieu du mot de passe par défaut. Un mot de passe défini par l'utilisateur doit être gardé secret pour que la sécurité des données confidentielles sur l'appareil ne soit pas compromise.

Un mot de passe défini par l'utilisateur peut être configuré manuellement sous forme de texte en clair. Il peut aussi être issu d'un fichier de configuration. (Reportez-vous à la section Configuration automatique sans intervention des données confidentielles.) Un appareil affiche toujours sous forme chiffrée les mots de passe définis par l'utilisateur.

Mot de passe local

Un appareil conserve un mot de passe local qui est celui de sa configuration d'exécution. SSD effectue normalement le cryptage et le décryptage des données confidentielles avec la clé générée à partir du mot de passe local.

Le mot de passe local peut être configuré pour être le mot de passe par défaut ou un mot de passe défini par l'utilisateur. Par défaut, le mot de passe local et le mot de passe par défaut sont identiques. Il peut être changé via des actions d'administration à partir de l'interface de ligne de commande (si disponible) ou de l'interface Web. Il est automatiquement remplacé par le mot de passe figurant dans le fichier de Configuration de démarrage lorsque la configuration de démarrage devient la configuration active de l'appareil. Lorsqu'un appareil est réinitialisé à ses valeurs par défaut, le mot de passe local est réinitialisé au mot de passe par défaut.

Contrôle du mot de passe du fichier de configuration

Le contrôle du mot de passe du fichier constitue une protection supplémentaire pour un mot de passe défini par l'utilisateur, et les données confidentielles qui sont chiffrées avec la clé générée à partir du mot de passe défini par l'utilisateur, dans les fichiers de configuration textuels.

Les modes de contrôle du mot de passe existants sont indiqués ci-après :

- **Sans restriction** (par défaut) : l'appareil inclut son mot de passe lors de la création d'un fichier de configuration. Cela permet à tout appareil qui accepte le fichier de configuration d'apprendre le mot de passe à partir du fichier.
- **Restreint** : l'appareil empêche l'exportation de son mot de passe vers un fichier de configuration. Le mode Restreint protège les données confidentielles chiffrées présentes dans un fichier de configuration contre les appareils qui ne disposent pas de mot de passe. Ce mode doit être utilisé lorsqu'un utilisateur ne souhaite pas exposer le mot de passe dans un fichier de configuration.

Une fois qu'un appareil a été réinitialisé à ses valeurs par défaut, son mot de passe local est réinitialisé au mot de passe par défaut. Ainsi, l'appareil ne pourra plus décrypter les données confidentielles chiffrées à partir d'un mot de passe défini par l'utilisateur qui a été entré depuis une session de gestion (GUI/CLI), ou dans tout fichier de configuration avec le mode Restreint, y compris les fichiers créés par l'appareil lui-même avant qu'il ne soit réinitialisé à ses valeurs par défaut. Cette situation reste inchangée tant que l'appareil n'est pas manuellement reconfiguré avec le mot de passe défini par l'utilisateur ou qu'il n'apprend pas le mot de passe défini par l'utilisateur à partir d'un fichier de configuration.

Contrôle de l'intégrité du fichier de configuration

Un utilisateur peut protéger un fichier de configuration contre toute altération ou modification en créant le fichier de configuration avec le Contrôle de l'intégrité du fichier de configuration. Il est recommandé d'activer le Contrôle de l'intégrité du fichier de configuration lorsqu'un appareil utilise un mot de passe défini par l'utilisateur et que le Contrôle du mot de passe du fichier de configuration est défini sur Sans restriction.

PRÉCAUTION Toute modification apportée à un fichier de configuration dont l'intégrité est protégée est considérée comme une altération.

Un appareil détermine si l'intégrité d'un fichier de configuration est protégée en examinant la commande Contrôle de l'intégrité du fichier dans le bloc de contrôle SSD du fichier. Si la protection de l'intégrité est définie pour un fichier, mais qu'un appareil détecte que l'intégrité du fichier n'est pas intacte, l'appareil refuse le fichier. Sinon, le fichier est accepté pour traitement ultérieur.

Un appareil vérifie l'intégrité d'un fichier de configuration textuel lorsque le fichier est téléchargé ou copié vers le fichier de Configuration de démarrage.

Mode Lecture

Chaque session comporte un mode de lecture. Il détermine la façon dont les données confidentielles s'affichent. Le mode de lecture peut être Texte en clair, auquel cas les données confidentielles apparaissent en texte normal ou Chiffré, auquel cas les données confidentielles apparaissent sous forme chiffrée.

Fichiers de configuration

Un fichier de configuration contient la configuration d'un appareil. Un appareil comporte un fichier de Configuration d'exécution, un fichier de Configuration de démarrage, un fichier de Configuration miroir (facultatif) et un fichier de Configuration de secours. Un utilisateur peut charger et télécharger un fichier de configuration depuis et vers un serveur de fichiers distant. Un appareil peut télécharger automatiquement sa configuration de démarrage à partir d'un serveur de fichiers distant pendant l'étape de configuration automatique via DHCP. Les fichiers de configuration stockés sur des serveurs de fichiers distants sont appelés des fichiers de configuration à distance.

Un fichier de Configuration d'exécution contient la configuration actuellement utilisée par un appareil. La configuration dans un fichier de Configuration de démarrage devient la configuration d'exécution une fois le redémarrage effectué. Les fichiers de Configuration d'exécution et de Configuration de démarrage ont un format interne. Les fichiers de Configuration miroir, de secours et à distance sont des fichiers textuels qui sont généralement stockés à des fins d'archivage, d'enregistrement ou de récupération. Lors de la copie, du chargement et du téléchargement d'un fichier de configuration source, un appareil convertit automatiquement le contenu source dans le format du fichier de destination si les deux fichiers ont un format différent.

Indicateur SSD de fichier

Lors de la copie du fichier de Configuration d'exécution ou de démarrage dans un fichier de configuration textuel, l'appareil génère et place l'indicateur SSD de fichier dans le fichier de configuration textuel pour indiquer si le fichier contient des données confidentielles sous forme chiffrée, des données confidentielles sous forme de texte en clair, ou s'il exclut les données confidentielles.

- L'indicateur SSD, s'il existe, doit se trouver dans le fichier d'en-tête de configuration.
- Une configuration textuelle qui n'inclut pas d'indicateur SSD ne contient normalement pas de données confidentielles.
- L'indicateur SSD permet d'appliquer les autorisations en lecture SSD à des fichiers de configuration textuels, mais il est ignoré lors de la copie des fichiers de configuration vers le fichier de Configuration d'exécution ou de démarrage.

L'indicateur SSD dans un fichier est défini conformément à l'instruction de l'utilisateur, au cours de la copie, pour inclure les données confidentielles sous forme chiffrée ou de texte en clair, ou exclure les données confidentielles d'un fichier.

Bloc de contrôle SSD

Lorsqu'un appareil crée un fichier de configuration textuel à partir de son fichier de Configuration de démarrage ou d'exécution, il insère un bloc de contrôle SSD dans le fichier si un utilisateur demande que le fichier doit inclure les données confidentielles. Le bloc de contrôle SSD, qui est protégé contre toute altération, contient les règles SSD et les propriétés SSD de l'appareil qui crée le fichier. Un bloc de contrôle SSD commence et finit respectivement avec « ssd-control-start » et « ssd-control-end ».

Fichier de Configuration de démarrage

L'appareil prend actuellement en charge la copie depuis les fichiers de Configuration d'exécution, de secours, miroir et à distance vers un fichier de Configuration de démarrage. Les configurations définies dans la configuration de démarrage sont effectives et deviennent la configuration d'exécution une fois le redémarrage effectué. Un utilisateur peut récupérer les données confidentielles sous forme chiffrée ou de texte en clair à partir d'un fichier de Configuration de démarrage, sujet à l'autorisation en lecture SSD et au mode de lecture SSD actuel de la session de gestion.

L'accès en lecture aux données confidentielles dans la configuration de démarrage sous toutes ses formes est exclu si le mot de passe défini dans le fichier de Configuration de démarrage diffère du mot de passe local.

SSD ajoute les règles suivantes lors de la copie des fichiers de Configuration de secours, miroir et à distance vers le fichier de Configuration de démarrage :

- Une fois qu'un appareil a été réinitialisé à ses valeurs par défaut, toutes ses configurations y compris les règles et les propriétés SSD sont réinitialisées à leurs valeurs par défaut.
- Si un fichier de configuration source contient des données confidentielles chiffrées, mais pas de bloc de contrôle SSD, l'appareil refuse le fichier source et la copie échoue.
- S'il n'y a pas de bloc de contrôle SSD dans le fichier de configuration source, la configuration SSD définie dans le fichier de Configuration de démarrage est réinitialisée à ses valeurs par défaut.
- Si un mot de passe est présent dans le bloc de contrôle SSD du fichier de configuration source, l'appareil refuse le fichier source, et la copie échoue s'il y a des données confidentielles chiffrées dans le fichier qui ne sont pas chiffrées par la clé générée à partir du mot de passe dans le bloc de contrôle SSD.
- S'il y a un bloc de contrôle SSD dans le fichier de configuration source et que le fichier échoue lors du contrôle d'intégrité SSD et/ou lors du contrôle d'intégrité du fichier, l'appareil refuse le fichier source et la copie échoue.
- S'il n'y a aucun mot de passe dans le bloc de contrôle SSD du fichier de configuration source, toutes les données confidentielles chiffrées dans le fichier doivent être chiffrées soit par la clé générée à partir du mot de passe local, soit par la clé générée à partir du mot de passe par défaut, mais pas par les deux. Sinon, le fichier source est refusé et la copie échoue.

- L'appareil configure le mot de passe, le contrôle du mot de passe et l'intégrité du fichier le cas échéant à partir du bloc de contrôle SSD dans le fichier de configuration source vers le fichier de Configuration de démarrage. Il configure le fichier de Configuration de démarrage avec le mot de passe qui est utilisé pour générer la clé permettant de décrypter les données confidentielles dans le fichier de configuration source. Toutes les configurations SSD introuvables sont réinitialisées à leurs valeurs par défaut.
- S'il y a un bloc de contrôle SSD dans le fichier de configuration source et que le fichier contient des données confidentielles sous forme de texte en clair, à l'exclusion des configurations SSD dans le bloc de contrôle SSD, le fichier est accepté.

Fichier de Configuration d'exécution

Un fichier de Configuration d'exécution contient la configuration actuellement utilisée par l'appareil. Un utilisateur peut récupérer les données confidentielles sous forme chiffrée ou de texte en clair à partir d'un fichier de Configuration d'exécution, sujet à l'autorisation en lecture SSD et au mode de lecture SSD actuel de la session de gestion. L'utilisateur peut changer la configuration d'exécution en copiant les fichiers de Configuration de secours ou miroir, à travers d'autres actions de gestion via CLI, XML, SNMP, etc.

Un appareil applique les règles suivantes lorsqu'un utilisateur change directement la configuration SSD dans la configuration d'exécution :

- Si l'utilisateur qui a ouvert la session de gestion ne dispose pas des autorisations SSD (à savoir les autorisations en lecture Les deux ou Texte en clair uniquement), l'appareil refuse toutes les commandes SSD.
- En cas de copie à partir d'un fichier source, l'indicateur SSD de fichier, l'intégrité du bloc de contrôle SSD et l'intégrité du fichier SSD ne sont ni vérifiés ni appliqués.
- En cas de copie à partir d'un fichier source, la copie échoue si le mot de passe contenu dans le fichier source est sous forme de texte en clair. Si le mot de passe est chiffré, il est ignoré.
- Lors de la configuration directe du mot de passe (pas de copie de fichier), dans la configuration d'exécution, le mot de passe contenu dans la commande doit être saisi sous forme de texte en clair. Sinon, la commande est refusée.
- Les commandes de configuration contenant des données confidentielles chiffrées, qui sont chiffrées avec la clé générée à partir du mot de passe local, sont configurées dans la configuration d'exécution. Sinon, la commande de configuration échoue et n'est pas intégrée au fichier de Configuration d'exécution.

Fichier de configuration de secours et miroir

Un appareil génère fréquemment son fichier de Configuration miroir à partir du fichier de Configuration de démarrage si le service de configuration miroir automatique est activé. Un appareil génère toujours un fichier de Configuration miroir avec des données confidentielles chiffrées. Par conséquent, l'indicateur SSD de fichier dans un fichier de Configuration miroir indique toujours que le fichier contient des données confidentielles chiffrées.

Par défaut, le service de configuration miroir automatique est activé. Pour activer ou désactiver la configuration miroir automatique, cliquez sur **Administration > Gestion des fichiers > Opérations du microprogramme**.

Un utilisateur peut afficher, copier et charger les fichiers complets de Configuration miroir et de secours, sujets à l'autorisation en lecture SSD, au mode de lecture actuel dans la session et à l'indicateur SSD de fichier dans le fichier source comme suit :

- S'il n'y a pas d'indicateur SSD de fichier dans un fichier de configuration miroir ou de sauvegarde, tous les utilisateurs sont autorisés à accéder au fichier.
- Un utilisateur disposant de l'autorisation en lecture Les deux peut accéder à tous les fichiers de Configuration miroir et de secours. Toutefois, si le mode de lecture actuel de la session est différent de l'indicateur SSD de fichier, l'utilisateur reçoit un message indiquant que cette action n'est pas autorisée.
- Un utilisateur disposant de l'autorisation Texte en clair uniquement peut accéder aux fichiers de Configuration miroir et de secours si leur indicateur SSD de fichier affiche les données confidentielles Exclure ou Texte en clair uniquement.
- Un utilisateur disposant de l'autorisation Chiffré uniquement peut accéder aux fichiers de Configuration miroir et de secours si leur indicateur SSD de fichier affiche les données confidentielles Exclure ou Chiffré.
- Un utilisateur disposant de l'autorisation Exclure ne peut pas accéder aux fichiers de Configuration miroir et de secours si leur indicateur SSD de fichier affiche les données confidentielles Chiffré ou Texte en clair.

L'utilisateur ne doit pas changer manuellement l'indicateur SSD de fichier en cas de conflit (le cas échéant) avec les données confidentielles dans le fichier. Sinon, les données confidentielles sous forme de texte en clair peuvent être exposées de manière inattendue.

Configuration automatique sans intervention des données confidentielles

La configuration automatique sans intervention SSD est la configuration automatique des appareils cibles contenant des données confidentielles. Elle ne nécessite pas de préconfigurer manuellement les appareils cibles avec le mot de passe dont la clé permet de crypter les données confidentielles.

L'appareil prend actuellement en charge la Configuration automatique, qui est activée par défaut. Lorsque la Configuration automatique est activée sur un appareil et que l'appareil reçoit les options DHCP qui spécifient un serveur de fichiers et un fichier de démarrage, l'appareil télécharge le fichier de démarrage (fichier de configuration à distance) dans le fichier de Configuration de démarrage à partir d'un serveur de fichiers, puis redémarre.

REMARQUE Le serveur de fichiers peut être spécifié par les champs bootp siaddr et sname, ainsi que l'option DHCP 150 et statiquement configuré sur l'appareil.

L'utilisateur peut en toute sécurité configurer automatiquement les appareils cibles contenant des données confidentielles, en créant d'abord le fichier de configuration qui doit être utilisé dans la configuration automatique à partir d'un appareil qui contient les configurations. L'appareil doit être configuré et défini pour :

- Crypter les données confidentielles dans le fichier
- Assurer l'intégrité du contenu du fichier
- Inclure les règles SSD et les commandes de configuration d'authentification sécurisées qui contrôlent et sécurisent correctement l'accès aux appareils et aux données confidentielles

Si le fichier de configuration a été généré avec un mot de passe utilisateur et que le contrôle du mot de passe du fichier SSD est Restreint, le fichier de configuration qui en résulte peut être configuré automatiquement pour les appareils cibles souhaités. Néanmoins, pour que la configuration automatique réussisse avec un mot de passe défini par l'utilisateur, les appareils cibles doivent être préconfigurés manuellement avec le même mot de passe que celui de l'appareil qui génère les fichiers, ce qui ne correspond donc pas à une configuration sans intervention.

Si l'appareil qui crée le fichier de configuration est défini sur le mode de contrôle du mot de passe Sans restriction, l'appareil inclut le mot de passe dans le fichier. Par conséquent, l'utilisateur peut configurer automatiquement les appareils cibles, y compris les appareils neufs ou définis à leurs paramètres par défaut, avec le fichier de configuration sans devoir manuellement préconfigurer les appareils cibles avec le mot de passe. Il s'agit là d'une configuration sans intervention, car les appareils cibles apprennent le mot de passe directement à partir du fichier de configuration.

REMARQUE Les appareils neufs ou définis à leurs paramètres par défaut recourent à l'utilisateur anonyme par défaut pour accéder au serveur SCP.

Canaux de gestion SSD

Les appareils peuvent être gérés via des canaux de gestion comme telnet, SSH et web. SSD classe les canaux selon les types suivants en fonction de leur sécurité et/ou leurs protocoles : sécurisé, non sécurisé, SNMP XML sécurisé et SNMP XML non sécurisé.

Le tableau suivant indique si chaque canal de gestion est considéré par SSD comme sécurisé ou non sécurisé. S'il est non sécurisé, le tableau indique le canal sécurisé parallèle.

Canal de gestion	Type de canal de gestion SSD	Canal de gestion sécurisé parallèle
Console	Sécurisé	
Telnet	Non sécurisé	SSH
SSH	Sécurisé	
GUI/HTTP	Non sécurisé	GUI/HTTPS
GUI/HTTPS	Sécurisé	
XML/HTTP	SNMP XML non sécurisé	XML/HTTPS
XML/HTTPS	SNMP XML sécurisé	
SNMPv1/v2/v3 sans confidentialité	SNMP XML non sécurisé	SNMP XML sécurisé
SNMPv3 avec confidentialité	SNMP XML sécurisé (utilisateurs de niveau 15)	
TFTP	Non sécurisé	SCP
SCP (Secure Copy Protocol)	Sécurisé	
Transfert de fichier basé sur HTTP	Non sécurisé	Transfert de fichier basé sur HTTPS
Transfert de fichier basé sur HTTPS	Sécurisé	

Interface de ligne de commande (CLI) et récupération du mot de passe

L'interface de ligne de commande (CLI) est uniquement accessible aux utilisateurs dont les autorisations en lecture sont Les deux ou Texte en clair uniquement. Les autres utilisateurs n'y ont pas accès. Les données confidentielles contenues dans l'interface de ligne de commande (CLI) s'affichent toujours sous forme de texte en clair.

La récupération du mot de passe est actuellement activée à partir du menu de démarrage et permet à l'utilisateur de se connecter au terminal sans authentification. Si SSD est pris en charge, cette option est uniquement autorisée lorsque le mot de passe local est identique au mot de passe par défaut. Si un appareil est configuré avec un mot de passe défini par l'utilisateur, l'utilisateur ne peut pas activer la récupération du mot de passe.

Configuration de SSD

La configuration de la fonction SSD est décrite aux pages suivantes :

- Vous pouvez définir les propriétés SSD sur la page Propriétés SSD.
- Les règles SSD sont définies sur la page Règles SSD.

Propriétés SSD

Seuls les utilisateurs qui disposent de l'autorisation en lecture SSD Texte en clair uniquement ou Les deux sont autorisés à définir les propriétés SSD.

Pour définir les propriétés SSD globales :

ÉTAPE 1 Cliquez sur **Sécurité** > **Gestion sécurisée des données confidentielles** > **Propriétés**.

Le champ suivant s'affiche :

- **Type de mot de passe local actuel** : indique si le mot de passe par défaut ou un mot de passe défini par l'utilisateur est actuellement utilisé.

ÉTAPE 2 Renseignez les champs **Paramètres persistants** suivants :

- **Contrôle du mot de passe du fichier de configuration** : sélectionnez une option, comme indiqué à la section Contrôle du mot de passe du fichier de configuration.
- **Contrôle de l'intégrité du fichier de configuration** : sélectionnez cette fonction pour l'activer. Reportez-vous à la section Contrôle de l'intégrité du fichier de configuration.

ÉTAPE 3 Sélectionnez un mode de lecture pour la session actuelle (reportez-vous à Éléments d'une règle SSD).

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres sont enregistrés dans le fichier Configuration d'exécution.

Pour changer le mot de passe local :

ÉTAPE 1 Cliquez sur **Modifier le mot de passe local**, puis entrez un nouveau **Mot de passe local** :

- **Par défaut** : permet d'utiliser le mot de passe par défaut des appareils.
- **Défini par l'utilisateur (texte en clair)** : saisissez un nouveau mot de passe.
- **Confirmer le mot de passe** : confirmez le nouveau mot de passe.

ÉTAPE 2 Cliquez sur **Appliquer**. Les paramètres sont enregistrés dans le fichier Configuration d'exécution.

Configuration des règles SSD

Seuls les utilisateurs qui disposent de l'autorisation en lecture SSD Texte en clair uniquement ou Les deux sont autorisés à définir les règles SSD.

Pour configurer les règles SSD :

ÉTAPE 1 Cliquez sur **Sécurité** > **Gestion sécurisée des données confidentielles** > **Règles SSD**.

Les règles actuellement définies sont affichées. Le champ **Type de la règle** indique s'il s'agit d'une règle par défaut ou définie par l'utilisateur.

ÉTAPE 2 Pour ajouter une nouvelle règle, cliquez sur **Ajouter**. Renseignez les champs suivants :

- **Utilisateur** : définit le ou les utilisateurs auxquels la règle s'applique : Sélectionnez l'une des options suivantes :
  - *Utilisateur spécifique* : sélectionnez et entrez le nom d'utilisateur spécifique auquel cette règle s'applique (cet utilisateur ne doit pas nécessairement être défini).
  - *Utilisateur par défaut (cisco)* : indique que cette règle s'applique à l'utilisateur par défaut.
  - *Niveau 15* : indique que cette règle s'applique à tous les utilisateurs ayant le niveau de privilège 15.
  - *Tous* : indique que cette règle s'applique à tous les utilisateurs.

- **Canal** : définit le niveau de sécurité du canal d'entrée auquel la règle s'applique : Sélectionnez l'une des options suivantes :
  - *Sécurisé* : indique que cette règle s'applique uniquement aux canaux sécurisés (console, SCP, SSH et HTTPS), mais pas les canaux SNMP et XML.
  - *Non sécurisé* : indique que cette règle s'applique uniquement aux canaux non sécurisés (Telnet, TFTP et HTTP), mais pas aux canaux SNMP et XML.
  - *SNMP XML sécurisé* : indique que cette règle s'applique uniquement au XML sur HTTPS et SNMPv3 avec confidentialité.
  - *SNMP XML non sécurisé* : indique que cette règle s'applique uniquement au XML sur HTTP ou/et au SNMPv1/v2 et SNMPv3 sans confidentialité.
- **Autorisation en lecture** : autorisations en lecture associées aux règles. Elles peuvent être les suivantes :
  - *Exclure* : autorisation en lecture la plus basse. Les utilisateurs ne sont pas autorisés à accéder aux données confidentielles sous quelque forme que ce soit.
  - *Texte en clair uniquement* : autorisation en lecture de niveau plus élevé que la précédente. Les utilisateurs sont autorisés à accéder aux données confidentielles sous forme de texte en clair uniquement.
  - *Chiffré uniquement* : autorisation en lecture de niveau moyen. Les utilisateurs sont autorisés à accéder aux données confidentielles sous forme chiffrée uniquement.
  - *Les deux (Texte en clair et Chiffré)* : autorisation en lecture la plus haute. Les utilisateurs ont les autorisations Chiffré et Texte en clair, et sont autorisés à accéder aux données confidentielles sous forme chiffrée et de texte en clair.
- **Mode de lecture par défaut** : tous les modes de lecture par défaut sont sujets à l'autorisation en lecture de la règle. Les options suivantes sont disponibles, mais certaines sont susceptibles d'être refusées en fonction de l'autorisation en lecture de la règle.
  - *Exclure* : n'autorise pas la lecture des données confidentielles.
  - *Chiffré* : les données confidentielles sont présentées sous forme chiffrée.
  - *Texte en clair* : les données confidentielles sont présentées sous forme de texte en clair.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres sont enregistrés dans le fichier Configuration d'exécution.

ÉTAPE 4 Les actions suivantes peuvent être effectuées sur les règles sélectionnées :

- **Ajouter**, **Modifier** ou **Supprimer** des règles ou **Restaurer les valeurs par défaut**.
- **Restore All Rules to Default** (Restaurer toutes les règles par défaut) : rétablit les valeurs d'origine d'une règle par défaut qui a été modifiée par l'utilisateur.

23

Sécurité : Serveur SSH

Cette section décrit la façon d'établir une session SSH sur le périphérique.

Elle couvre les sujets suivants :

Vue d'ensemble

La fonction SSH Server (Serveur SSH) permet aux utilisateurs distants de créer des sessions SSH sur le périphérique. Elle est similaire à la fonction permettant d'établir une session telnet, sauf que cette session est sécurisée.

En tant que serveur SSH, le périphérique prend en charge l'authentification des utilisateurs SSH, qui permet d'authentifier un utilisateur distant soit par mot de passe soit par clé publique. Par ailleurs, en tant que client SSH, l'utilisateur distant peut faire appel à l'authentification du serveur SSH pour authentifier le périphérique à l'aide de la clé publique (empreinte) de ce dernier.

Le serveur SSH peut fonctionner dans les modes suivants :

- **Par des clés RSA/DSA générées en interne (paramètre par défaut)** : une clé RSA et une clé DSA sont générées. Les utilisateurs se connectent à l'application serveur SSH et sont automatiquement authentifiés pour ouvrir une session sur l'appareil lorsqu'ils fournissent l'adresse IP de l'appareil.
- **Mode de clé publique** : les utilisateurs sont définis sur l'appareil. Leurs clés RSA/DSA sont générées dans une application serveur SSH externe, telle que PuTTY. Les clés publiques sont entrées dans l'appareil. Les utilisateurs peuvent alors ouvrir une session SSH sur l'appareil par le biais de l'application serveur SSH externe.

Tâches courantes

Cette section décrit quelques tâches courantes réalisées à l'aide de la fonction Serveur SSH.

Flux de travail 1 : procédure de création d'une session SSH sans authentification des utilisateurs SSH :

ÉTAPE 1 Activez le serveur SSH sur la page Services TCP/UDP.

ÉTAPE 2 Désactivez l'authentification des utilisateurs SSH par mot de passe et par clé publique sur la page Authentification des utilisateurs SSH.

ÉTAPE 3 Créez des sessions SSH sur le périphérique à partir d'une application cliente SSH telle que PUTTY.

Flux de travail 2 : procédure de création d'une session SSH avec authentification des utilisateurs SSH par mot de passe :

ÉTAPE 1 Activez le serveur SSH sur la page Services TCP/UDP.

ÉTAPE 2 Activez l'authentification des utilisateurs SSH par mot de passe sur la page Authentification des utilisateurs SSH.

ÉTAPE 3 Créez des sessions SSH sur le périphérique à partir d'une application cliente SSH telle que PUTTY.

Flux de travail 3 : procédure de création d'une session SSH avec authentification des utilisateurs SSH par clé publique en contournant ou pas l'authentification de gestion :

ÉTAPE 1 Activez le serveur SSH sur la page Services TCP/UDP.

ÉTAPE 2 Activez l'authentification des utilisateurs SSH par clé publique sur la page Authentification des utilisateurs SSH. La clé publique doit avoir été préalablement créée sur le client SSH ; elle sera utilisée par ce dernier pour établir une session SSH sur le serveur SSH du périphérique.

ÉTAPE 3 Le cas échéant, activez la connexion automatique en contournant l'authentification de gestion sur la page Authentification des utilisateurs SSH.

ÉTAPE 4 Ajoutez les utilisateurs et leur clé publique au tableau Authentification des utilisateurs SSH de la page Authentification des utilisateurs SSH.

ÉTAPE 5 Créez des sessions SSH sur le périphérique à partir d'une application cliente SSH telle que PUTTY.

Authentification des utilisateurs SSH

Utilisez la page SSH User Authentication (Authentification des utilisateurs SSH) pour activer l'authentification des utilisateurs SSH par clé publique et/ou par mot de passe. Un utilisateur faisant appel à une clé publique pour créer un serveur SSH doit saisir son nom d'utilisateur et sa clé publique dans le tableau SSH User Authentication (Authentification des utilisateurs SSH). Pour un utilisateur faisant appel à un mot de passe pour créer une session SSH, le nom d'utilisateur et le mot de passe doivent correspondre à ceux d'un utilisateur dotés d'un accès en gestion.

Avant de pouvoir ajouter un utilisateur, vous devez générer une clé RSA ou DSA pour cet utilisateur dans l'application client/de génération de clé SSH externe (telle que PuTTY).

Connexion automatique

Si vous définissez, à l'aide de la page Authentification des utilisateurs SSH, le nom d'utilisateurs déjà configurés dans la base de données locale des utilisateurs, configurer la fonctionnalité **Connexion automatique** permet d'ignorer les autres étapes du processus d'authentification. Cette fonctionnalité opère comme suit :

- **Activer** : les utilisateurs présents dans la base de données locale qui passent l'étape d'authentification SSH par clé publique n'ont pas besoin de s'authentifier à l'aide de leur nom d'utilisateur et mot de passe définis localement.

  REMARQUE La méthode d'authentification configurée pour ce mode de gestion spécifique (console, Telnet, SSH, etc.) doit être une *méthode locale* (c.-à-d., une méthode autre que *RADIUS* ou *TACACS+*). Pour en savoir plus à ce sujet, reportez-vous à la section Méthode d'accès de gestion.

- **Not Enabled** (Désactivé) : après authentification réussie par clé publique SSH, les utilisateurs, même s'ils sont répertoriés dans la base de données locale des utilisateurs, doivent de nouveau s'authentifier, et ce conformément aux méthodes d'authentification configurées à l'aide de la page Authentification de l'accès de gestion.

Cette page est facultative. Il n'est pas nécessaire de recourir à l'authentification des utilisateurs dans SSH.

Pour activer l'authentification et ajouter un utilisateur :

ÉTAPE 1 Cliquez sur **Sécurité > Serveur SSH > Authentification des utilisateurs SSH**.

ÉTAPE 2 Sélectionnez les champs suivants :

- **Authentification des utilisateurs SSH par mot de passe** : permet l'authentification des utilisateurs client SSH à l'aide des noms d'utilisateur et mots de passe définis dans la base de données locale (pour plus d'informations à ce sujet, reportez-vous à la section Comptes d'utilisateur).

- **Authentification des utilisateurs SSH par clé publique** : permet l'authentification des utilisateurs client SSH à l'aide de la clé publique.
- **Connexion automatique** : l'activation de ce champ dépend de la sélection de la fonctionnalité **Authentification des utilisateurs SSH par clé publique**.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres sont enregistrés dans le fichier Configuration d'exécution.

Les champs suivants sont affichés pour les utilisateurs déjà configurés :

- **Nom de l'utilisateur SSH** : nom de l'utilisateur.
- **Type de clé** : indique s'il s'agit d'une clé RSA ou DSA.
- **Empreinte** : empreinte générée à partir des clés publiques.

ÉTAPE 4 Cliquez sur **Ajouter** pour ajouter un nouvel utilisateur, puis renseignez les champs suivants :

- **Nom de l'utilisateur SSH** : saisissez un nom d'utilisateur.
- **Type de clé** : sélectionnez **RSA** ou **DSA**.
- **Clé publique** : copiez la clé publique générée par une application client SSH externe (telle que PuTTY) dans la zone de texte.

ÉTAPE 5 Cliquez sur **Appliquer** pour enregistrer le nouvel utilisateur.

Les champs suivants sont affichés pour tous les utilisateurs actifs :

- **Adresse IP** : adresse IP de l'utilisateur actif.
- **Nom de l'utilisateur SSH** : nom de l'utilisateur actif.
- **Version SSH** : version du serveur SSH utilisé par l'utilisateur actif.
- **Chiffrer** : chiffrement de l'utilisateur actif.
- **Code d'authentification** : code d'authentification de l'utilisateur actif.

Authentification du serveur SSH

Un client SSH distant peut utiliser l'authentification du serveur SSH pour s'assurer qu'il établit une session SSH sur le pilote SSH attendu. Pour procéder à une authentification du serveur SSH, le client SSH distant doit disposer d'une copie de la clé publique (ou de l'empreinte) du serveur SSH cible.

La page d'authentification du serveur SSH génère/importe la clé privée/publique du périphérique en tant que serveur SSH. Un utilisateur doit copier la clé publique (ou l'empreinte) du serveur SSH de ce périphérique dans l'application s'il souhaite utiliser l'authentification du serveur SSH dans ses sessions SSH. Les clés RSA et DSA publique et privée sont générées automatiquement lors du démarrage de l'appareil avec les paramètres d'usine. Chaque clé est aussi automatiquement créée lorsque la clé appropriée configurée par l'utilisateur est supprimée par celui-ci.

Pour regénérer une clé RSA ou DSA, ou copier une clé RSA/DSA générée sur un autre appareil :

ÉTAPE 1 Cliquez sur **Sécurité > Serveur SSH > Authentification du serveur SSH**.

Les champs suivants sont affichés pour chaque clé :

- **Type de clé** : RSA ou DSA.
- **Source de la clé** : Autogénérée ou Définie par l'utilisateur.
- **Empreinte** : empreinte générée à partir de la clé.

ÉTAPE 2 Sélectionnez une clé RSA ou DSA.

ÉTAPE 3 Vous pouvez effectuer l'une des opérations suivantes :

- **Générer** : permet de générer une clé du type sélectionné.
- **Modifier** : permet de copier une clé depuis un autre appareil. Renseignez les champs suivants :
  - *Type de clé* : comme décrit ci-dessus.
  - *Clé publique* : saisissez la clé publique.
  - *Clé privée* : sélectionnez une clé **cryptée** ou en **texte en clair** et saisissez la clé privée.

  Cliquez sur **Afficher les données sensibles sous forme chiffrée** ou **Afficher les données sensibles sous forme de texte clair** pour déterminer comment les données sensibles seront affichées.
- **Supprimer** : permet de supprimer une clé.
- **Détails** : permet d'afficher la clé générée. La fenêtre Détails vous permet aussi de cliquer sur **Afficher les données sensibles en texte clair**. Si vous cliquez sur cette option, les clés apparaissent sous forme de texte en clair et non sous forme chiffrée. Si la clé apparaît déjà sous forme de texte en clair, vous pouvez cliquer sur **Afficher les données sensibles sous forme chiffrée** pour afficher le texte sous forme chiffrée.

24

Sécurité : Client SSH

Cette section décrit l'appareil lorsqu'il fonctionne en tant que client SSH.

Elle couvre les sujets suivants :

- Vue d'ensemble
- Authentification des utilisateurs SSH
- Authentification du serveur SSH
- Modification du mot de passe utilisateur du serveur SSH

Vue d'ensemble

Secure Copy (SCP) et SSH

Secure Shell ou SSH est un protocole réseau qui permet aux données d'être échangées sur un canal sécurisé entre un client SSH (dans ce cas précis, l'appareil) et un serveur SSH.

Le client SSH aide l'utilisateur à gérer un réseau composé d'un ou plusieurs commutateurs dans lesquels différents systèmes de fichiers sont stockés sur un serveur SSH central. Lorsque les fichiers de configuration sont transférés via le réseau, Secure Copy (SCP), qui est une application utilisant le protocole SSH, s'assure que les données sensibles telles que le nom d'utilisateur/mot de passe ne sont pas interceptées.

Secure Copy (SCP) permet de transférer de manière sécurisée le micrologiciel, l'image d'amorçage, les fichiers de configuration, les fichiers de langue et les fichiers journaux d'un serveur SCP central vers un appareil.

En ce qui concerne SSH, la SCP exécutée sur l'appareil est une application client SSH et le serveur SCP est une application serveur SSH.

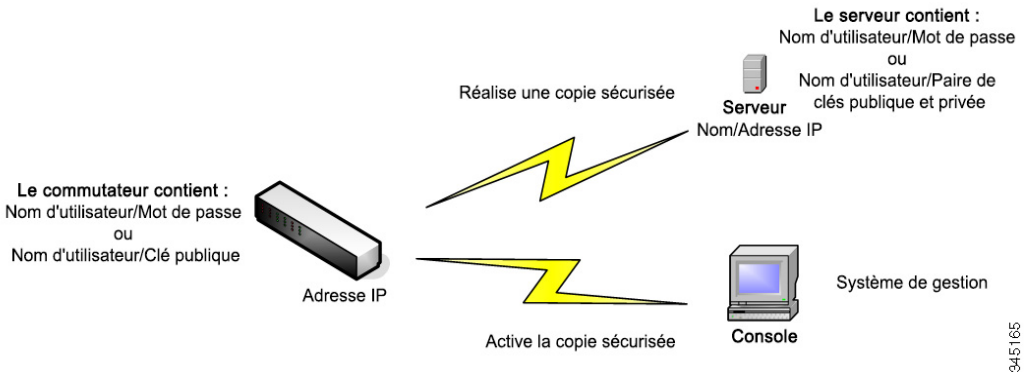
Lorsque des fichiers sont téléchargés via TFTP ou HTTP, le transfert des données n'est pas sécurisé.

Lorsque des fichiers sont téléchargés via SCP, les informations sont téléchargées du serveur SCP vers l'appareil via un canal sécurisé. La création de ce canal sécurisé est précédée d'une authentification, ce qui garantit que l'utilisateur est autorisé à effectuer l'opération.

Les informations d'authentification doivent être entrées par l'utilisateur sur l'appareil et le serveur SSH, même si ce guide ne décrit pas les opérations réalisées sur le serveur.

Vous trouverez ci-après la présentation d'une configuration réseau standard dans laquelle la fonctionnalité SCP peut être utilisée.

Configuration réseau standard



Authentification du serveur SSH

En tant que clients SSH, les appareils communiquent seulement avec le serveur SSH de confiance. Lorsque l'authentification du serveur SSH est désactivée (paramètre par défaut), tout serveur SSH est considéré comme étant de confiance. Lorsque l'authentification du serveur SSH est activée, l'utilisateur doit ajouter une entrée pour les serveurs de confiance dans la Table des serveurs SSH de confiance. Cette table stocke les informations suivantes pour chaque serveur SSH de confiance, pour un maximum de 16 serveurs :

- Adresse IP/nom d'hôte du serveur
- Empreinte de clé publique du serveur

Lorsque l'authentification du serveur SSH est activée, le client SSH exécuté sur l'appareil authentifie le serveur SSH à l'aide du processus d'authentification suivant :

- L'appareil calcule l'empreinte de la clé publique du serveur SSH reçue.

- Le périphérique recherche l'adresse IP/le nom d'hôte du serveur SSH dans la Table des serveurs SSH de confiance. Trois cas peuvent se présenter :
  - Si une correspondance est trouvée pour l'adresse IP/le nom d'hôte du serveur et son empreinte, le serveur est authentifié.
  - Si une adresse IP/un nom d'hôte correspondant(e) est trouvé(e), mais qu'il n'y a aucune empreinte associée, la recherche continue. Si aucune empreinte correspondante n'est trouvée, la recherche prend fin et l'authentification échoue.
  - Si aucune adresse IP/aucun nom d'hôte correspondant(e) n'est trouvé(e), la recherche prend fin et l'authentification échoue.
- Si l'entrée du serveur SSH n'est pas trouvée dans la liste des serveurs de confiance, le processus échoue.

Afin de prendre en charge la configuration automatique d'un appareil directement opérationnel (appareil avec configuration d'usine), l'authentification du serveur SSH est désactivée par défaut.

Authentification des utilisateurs SSH

Lorsqu'un périphérique (client SSH) tente de créer une session SSH sur un serveur SSH, ce dernier fait appel à différentes méthodes pour authentifier le client. Elles sont décrites ci-dessous.

Mots de passe

Pour utiliser la méthode du mot de passe, assurez-vous d'abord qu'un nom d'utilisateur/mot de passe a été défini sur le serveur SSH. Cette opération ne s'effectue pas via le système de gestion de l'appareil même si, lorsqu'un nom d'utilisateur a été défini sur le serveur, le mot de passe du serveur peut être modifié par l'intermédiaire de ce système de gestion.

Le nom d'utilisateur/mot de passe doit alors être créé directement sur l'appareil. Lorsque le périphérique tente de créer une session SSH sur un serveur SSH, le nom d'utilisateur/mot de passe fourni par le périphérique doit correspondre au nom d'utilisateur/mot de passe sur le serveur.

Les données peuvent être chiffrées à l'aide d'une clé symétrique unique négociée pendant la session.

Chaque appareil géré doit avoir son propre nom d'utilisateur/mot de passe, bien que le même nom d'utilisateur/mot de passe puisse être utilisé pour plusieurs commutateurs.

La méthode du mot de passe est la méthode par défaut sur l'appareil.

Clés publiques/privées

Pour utiliser la méthode de clé publique/privée afin d'authentifier le client via un serveur, créez un utilisateur et générez/importez une clé publique/privée sur le périphérique qui est un client SSH. Créez ensuite le même utilisateur sur le serveur SSH et copiez la clé publique (ou l'empreinte) générée/saisie via le client SSH sur le serveur SSH. La création de l'utilisateur et la copie de la clé publique (ou de l'empreinte) sur le serveur SSH n'entrent pas dans le champ d'application de ce guide.

Les paires de clés par défaut RSA et DSA sont générées pour l'appareil au démarrage de celui-ci. L'une de ces clés est utilisée pour crypter les données téléchargées à partir du serveur SSH. La clé RSA est utilisée par défaut.

Si l'utilisateur supprime l'une de ces clés, ou les deux, elles sont régénérées.

Les clés publique/privée sont chiffrées et stockées dans la mémoire de l'appareil. Les clés sont incluses dans le fichier de configuration de l'appareil et la clé privée peut être visualisée par l'utilisateur, sous forme chiffrée ou de texte en clair.

Puisque la clé privée ne peut pas être copiée directement vers la clé privée d'un autre appareil, une méthode d'importation vous permet de copier des clés privées d'un appareil à un autre (reportez-vous à la section *Importation de clés*).

Importation de clés

Dans le cadre de la méthode par clé, des clés publiques/privées individuelles doivent être créées pour chaque appareil. Ces clés privées ne peuvent pas, pour des raisons de sécurité, être copiées directement d'un appareil à un autre.

Si plusieurs commutateurs sont présents sur le réseau, le processus de création des clés publique/privée pour tous les commutateurs peut prendre beaucoup de temps, car chaque clé publique/privée doit être créée puis chargée sur le serveur SSH.

Pour faciliter ce processus, une autre fonction permet le transfert sécurisé de la clé privée chiffrée vers tous les commutateurs du système.

Lorsqu'une clé privée est créée sur un appareil, un *mot de passe* peut être défini et associé à cette clé. Ce mot de passe permet de crypter la clé privée et de l'importer dans les commutateurs restants. De cette manière, tous les commutateurs peuvent utiliser la même clé publique/privée.

Mot de passe par défaut

L'authentification de l'utilisateur SSH par mot de passe est activée par défaut, le nom d'utilisateur/mot de passe étant « anonyme ».

L'utilisateur doit configurer les informations suivantes pour l'authentification :

- La méthode d'authentification à utiliser.
- Le nom d'utilisateur/mot de passe ou la paire de clés publique/privée.

Algorithmes pris en charge

Lorsque la connexion entre un appareil (en tant que client SSH) et un serveur SSH est établie, le client et le serveur SSH échangent des données afin de déterminer les algorithmes à utiliser dans la couche transport SSH.

Les algorithmes suivants sont pris en charge côté client :

- Algorithme d'échange de clés Diffie-Hellman
- Algorithmes de cryptage
  - aes128-ctr
  - aes192-ctr
  - aes256-ctr
  - Chacha
  - Poly1305
- Algorithmes de code d'authentification de message
  - hmac-sha1

REMARQUE Les algorithmes de compression ne sont pas pris en charge.

Avant de commencer

Vous devez effectuer les actions suivantes avant d'utiliser la fonction SCP :

- Lorsque vous utilisez la méthode d'authentification par mot de passe, un nom d'utilisateur/mot de passe doit être configuré sur le serveur SSH.
- Lorsque vous utilisez la méthode d'authentification par clés publique/privée, la clé publique doit être stockée sur le serveur SSH.

Tâches courantes

Cette section décrit certaines tâches courantes réalisées par le périphérique en tant que client SSH. Toutes les pages référencées sont disponibles sous la branche Client SSH de l'arborescence du menu.

Flux de travail 1 : pour configurer le client SSH et transférer des données de/vers un serveur SSH distant, procédez comme suit :

ÉTAPE 1 Déterminez la méthode à utiliser : mot de passe ou clé publique/privée. Utilisez la page Authentification des utilisateurs SSH.

ÉTAPE 2 Si la méthode du mot de passe a été sélectionnée, procédez comme suit :

a. Créez un mot de passe global sur la page Authentification des utilisateurs SSH, ou un mot de passe temporaire sur la page Opérations du microprogramme ou Opérations de fichiers au moment où vous activez le transfert de données sécurisé.

b. Mettez à niveau le microprogramme, l'image d'amorçage ou le fichier de langue via le protocole SCP en sélectionnant l'option **SCP** sur la page Opérations du microprogramme. Vous pouvez saisir le mot de passe directement sur cette page ou utiliser le mot de passe saisi sur la page Authentification des utilisateurs SSH.

c. Téléchargez/sauvegardez le fichier de configuration, via SCP, en sélectionnant l'option **via SCP (over SSH)** (via SCP [sur SSH]) sur la page Opérations de fichiers. Vous pouvez saisir le mot de passe directement sur cette page ou utiliser le mot de passe saisi sur la page Authentification des utilisateurs SSH.

ÉTAPE 3 Définissez un nom d'utilisateur/mot de passe ou modifiez le mot de passe sur le serveur SSH distant. Cette activité dépend du serveur et n'est pas décrite ici.

ÉTAPE 4 Si la méthode de la clé publique/privée est utilisée, procédez comme suit :

a. Indiquez si vous souhaitez utiliser une clé RSA ou DSA, créez un nom d'utilisateur, puis générez les clés publique/privée.

b. Affichez la clé générée en cliquant sur le bouton **Détails**, puis transférez le nom d'utilisateur et la clé publique vers le serveur SSH. Cette action dépend du serveur et n'est pas décrite dans ce guide.

c. Mettez à niveau/sauvegardez le microprogramme via SCP en sélectionnant l'option **SCP** sur la page Opérations du microprogramme.

d. Téléchargez/sauvegardez le fichier de configuration via SCP en sélectionnant l'option**SCP** sur la page Opérations de fichiers.

Flux de travail 2 : pour importer des clés publiques/privées d'un appareil vers un autre :

ÉTAPE 1 Générez une clé publique/privée sur la page Authentification des utilisateurs SSH.

ÉTAPE 2 Définissez les propriétés SSD et créez un nouveau mot de passe local sur la page Propriétés SSD.

ÉTAPE 3 Cliquez sur **Détails** pour afficher les clés chiffrées générées, puis copiez-les (y compris les pieds de page Début et Fin) de la page Détails vers un appareil externe. Copiez séparément les clés publique et privée.

ÉTAPE 4 Connectez-vous à un autre périphérique et ouvrez la page Authentification des utilisateurs SSH. Sélectionnez le type de clé requis, puis cliquez sur **Modifier**. Collez-le dans les clés publiques/privées.

ÉTAPE 5 Cliquez sur **Appliquer** pour copier les clés publiques/privées vers le deuxième appareil.

Flux de travail 3 : pour modifier votre mot de passe sur un serveur SSH :

ÉTAPE 1 Identifiez le serveur sur la page Modification du mot de passe utilisateur du serveur SSH.

ÉTAPE 2 Saisissez le nouveau mot de passe.

ÉTAPE 3 Cliquez sur **Appliquer**.

Flux de travail 4 : pour définir un serveur de confiance :

ÉTAPE 1 Activez l'authentification du serveur SSH sur la page Authentification du serveur SSH.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un nouveau serveur, puis entrez ses informations d'identification.

ÉTAPE 3 Cliquez sur **Appliquer** pour ajouter le serveur à la Table des serveurs SSH de confiance.

Authentification des utilisateurs SSH

Utilisez cette page pour sélectionner une méthode d'authentification des utilisateurs SSH, définir un nom d'utilisateur et un mot de passe sur l'appareil, si la méthode du mot de passe est sélectionnée ou générer une clé RSA ou DSA, si la méthode de la clé publique/privée est sélectionnée.

Pour sélectionner une méthode d'authentification et définir le nom d'utilisateur/le mot de passe/les clés :

ÉTAPE 1 Cliquez sur **Sécurité > Client SSH > Authentification des utilisateurs SSH**.

ÉTAPE 2 Sélectionnez une **Méthode d'authentification des utilisateurs SSH**. Il s'agit de la méthode globale définie pour la copie sécurisée (SCP). Sélectionnez l'une des options disponibles :

- **Par mot de passe** : il s'agit du paramètre par défaut. Si vous sélectionnez cette option, conservez le mot de passe par défaut ou saisissez-en un nouveau.
- **Par clé publique RSA** : si vous sélectionnez cette option, créez une clé privée et publique RSA dans le bloc **Table des clés des utilisateurs SSH**.
- **Par clé publique DSA** : si vous sélectionnez cette option, créez une clé privée et publique DSA dans le bloc **Table des clés des utilisateurs SSH**.

ÉTAPE 3 Saisissez le **Nom d'utilisateur** (peu importe la méthode sélectionnée) ou conservez le nom d'utilisateur par défaut. Il doit correspondre au nom d'utilisateur défini sur le serveur SSH.

ÉTAPE 4 Si la méthode *Par mot de passe* a été sélectionnée, entrez un mot de passe (**Chiffré** ou **Texte en clair**) ou conservez le mot de passe chiffré par défaut.

ÉTAPE 5 Effectuez l'une des actions suivantes :

- **Appliquer** : les méthodes d'authentification sélectionnées sont associées à la méthode d'accès.
- **Restaurer les infos d'identification par défaut** : le nom d'utilisateur et le mot de passe (anonymes) par défaut sont restaurés.
- **Afficher les données sensibles en texte clair** : les données sensibles de la page actuelle sont affichées sous forme de texte en clair.

La **Table des clés des utilisateurs SSH** affiche les champs suivants pour chaque clé :

- **Type de clé** : RSA ou DSA.
- **Source de la clé** : Autogénérée ou Définie par l'utilisateur.
- **Empreinte** : empreinte générée à partir de la clé.

ÉTAPE 6 Pour gérer une clé RSA ou DSA, sélectionnez RSA ou DSA et effectuez l'une des actions suivantes :

- **Générer** : générez une nouvelle clé.
- **Modifier** : affichez les clés pour effectuer un copier/coller vers un autre appareil.
- **Supprimer** : supprimez la clé.
- **Détails** : affichez les clés.

Authentification du serveur SSH

Pour activer l'authentification du serveur SSH et définir les serveurs de confiance :

ÉTAPE 1 Cliquez sur **Sécurité > Client SSH > Authentification du serveur SSH**.

ÉTAPE 2 Sélectionnez **Activer** pour activer l'authentification du serveur SSH.

- **Interface source IPv4** : sélectionnez l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source pour les messages utilisés dans les communications avec les serveurs SSH IPv4.
- **Interface source IPv6** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source pour les messages utilisés dans les communications avec les serveurs SSH IPv6.

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

ÉTAPE 3 Cliquez sur **Appliquer**.

ÉTAPE 4 Cliquez sur **Ajouter** et renseignez les champs suivants pour le serveur de confiance SSH :

- **Définition du serveur** : sélectionnez l'une des méthodes d'identification du serveur SSH ci-après :
  - *Par adresse IP* : si vous avez sélectionné cette option, entrez l'adresse IP du serveur dans les champs situés au-dessous.
  - *Par nom* : si vous avez sélectionné cette option, entrez le nom du serveur dans le champ **Nom/Adresse IP du serveur**.

- **Version IP** : si vous avez choisi de définir le serveur SSH par son adresse IP, indiquez s'il s'agit d'une adresse IPv6 IPv4.
- **IPv6 Address Type** (Type d'adresse IPv6) : si l'adresse IP du serveur SSH est une adresse IPv6, sélectionnez le type d'adresse correspondant, à savoir IPv6. Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe FE80, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez, dans la liste des interfaces, l'interface de liaison locale.
- **Adresse IP/Nom serveur** : saisissez l'adresse IP ou le nom du serveur SSH, selon l'information sélectionnée dans le champ **Définition de serveur**.
- **Empreinte** : entrez l'empreinte du serveur SSH (copiée à partir de ce serveur).

ÉTAPE 5 Cliquez sur **Appliquer**. La définition du serveur de confiance est stockée dans le fichier de Configuration d'exécution.

Modification du mot de passe utilisateur du serveur SSH

Pour modifier un mot de passe sur un serveur SSH :

ÉTAPE 1 Cliquez sur **Sécurité > Client SSH > Modifier le mot de passe utilisateur du serveur SSH**.

ÉTAPE 2 Renseignez les champs suivants :

- **Définition de serveur** : définissez le serveur SSH en sélectionnant **Par adresse IP** ou **Par nom**. Saisissez le nom ou l'adresse IP du serveur dans le champ **Adresse IP/Nom serveur**.
- **Version IP** : si vous avez choisi de définir le serveur SSH par son adresse IP, indiquez s'il s'agit d'une adresse IPv6 IPv4.

- **IPv6 Address Type** (Type d'adresse IPv6) : si l'adresse IP du serveur SSH est une adresse IPv6, sélectionnez le type d'adresse correspondant, à savoir IPv6. Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe FE80, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez, dans la liste des interfaces, l'interface de liaison locale.
- **Adresse IP/Nom serveur** : saisissez l'adresse IP ou le nom du serveur SSH, selon l'information sélectionnée dans le champ **Définition de serveur**.
- **Nom d'utilisateur** : doit correspondre au nom d'utilisateur défini sur le serveur.
- **Ancien mot de passe** : doit correspondre au mot de passe défini sur le serveur.
- **Nouveau mot de passe** : saisissez le nouveau mot de passe, puis confirmez-le dans le champ **Confirmer le mot de passe**.

ÉTAPE 3 Cliquez sur **Appliquer**. Le mot de passe du serveur SSH a été modifié.

25

Sécurité : Sécurité du premier saut IPv6

Cette section décrit le fonctionnement de la Sécurité du premier saut IPv6 (First Hop Security, FHS) et la procédure de configuration correspondante dans l'interface utilisateur graphique.

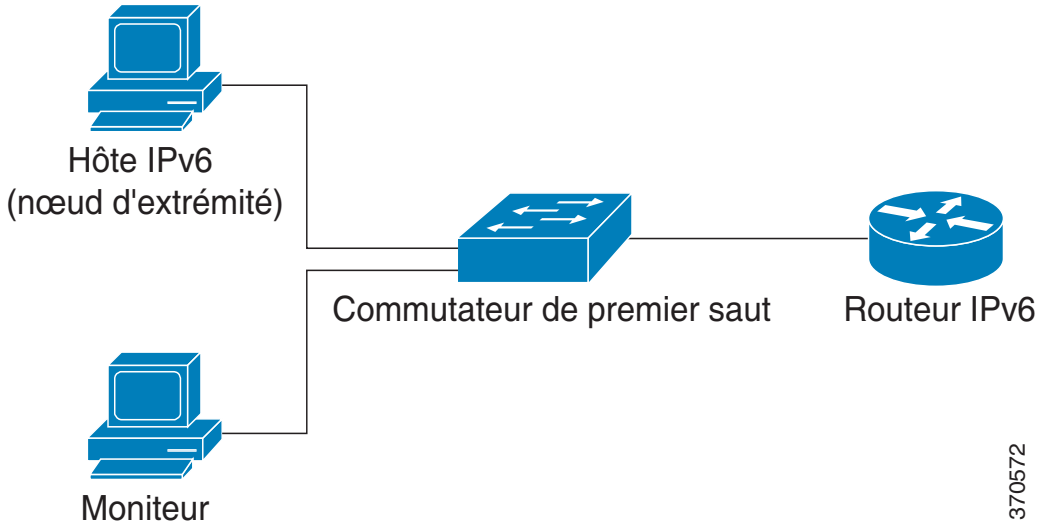
Elle couvre les rubriques suivantes :

Présentation de la Sécurité du premier saut IPv6

La Sécurité du premier saut IPv6 (IPv6 FHS) est une suite de fonctionnalités conçues pour sécuriser les opérations de liaison dans un réseau IPv6. Elle est basée sur le protocole Neighbor Discovery Protocol (NDP) et les messages DHCPv6.

Dans cette fonction, un commutateur de couche 2 (comme indiqué à la Figure 1) filtre les messages Neighbor Discovery Protocol (NDP), les messages DHCPv6 et les messages de données utilisateur sur la base de différentes règles.

Figure 1 Configuration de la Sécurité du premier saut IPv6



Une instance séparée et indépendante de la sécurité du premier saut IPv6 s'exécute sur chaque VLAN où la fonction est activée.

Abréviations

Nom	Description
Message CPA	Message Certification Path Advertisement
Message CPS	Message Certification Path Solicitation
Message DAD-NS	Message Duplicate Address Detection Neighbor Solicitation

Nom	Description
FCFS-SAVI	First Come First Served - Source Address Validation Improvement
Message NA	Message Neighbor Advertisement
NDP	Neighbor Discovery Protocol
Message NS	Message Neighbor Solicitation
Message RA	Message Router Advertisement
Message RS	Message Router Solicitation
SAVI	Source Address Validation Improvement

Composants de la Sécurité du premier saut IPv6

La Sécurité du premier saut IPv6 inclut les fonctions suivantes :

- Sécurité du premier saut IPv6 commune
- Protection RA
- Inspection ND
- Intégrité de la liaison de voisin
- Protection DHCPv6
- Protection de la source IPv6

Ces composants peuvent être activés ou désactivés sur les VLAN.

Pour chaque fonction, vous disposez de deux stratégies vides et prédéfinies portant les noms suivants : vlan_default et port_default. La première est associée à chaque VLAN non rattaché à une stratégie définie par l'utilisateur. La seconde est connectée à chaque interface et chaque VLAN qui n'est pas associé à une stratégie définie par l'utilisateur. Ces stratégies ne peuvent pas être explicitement associées par l'utilisateur. Reportez-vous à la section Stratégies, paramètres globaux et valeurs par défaut du système.

Canal de Sécurité du premier saut IPv6

Si la Sécurité du premier saut IPv6 est activée sur un VLAN, le commutateur intercepte les messages suivants :

- Messages Router Advertisement (RA)
- Messages Router Solicitation (RS)
- Messages Neighbor Advertisement (NA)
- Messages Neighbor Solicitation (NS)
- Messages ICMPv6 Redirect
- Messages Certification Path Advertisement (CPA)
- Messages Certification Path Solicitation (CPS)
- Messages DHCPv6

Les messages RA, CPA et ICMPv6 Redirect interceptés sont transmis à la fonction Protection RA. La fonction Protection RA valide ces messages, élimine les messages incorrects et envoie les messages corrects à la fonction Inspection ND.

La fonction Inspection ND valide ces messages, élimine les messages incorrects et envoie les messages corrects à la fonction Protection de la source IPv6.

Les messages DHCPv6 interceptés sont transmis à la fonction Protection DHCPv6. La fonction Protection DHCPv6 valide ces messages, élimine les messages incorrects et envoie les messages corrects à la fonction Protection de la source IPv6.

Les messages de données interceptés sont transmis à la fonction Protection de la source IPv6. La Protection de la source IPv6 valide les messages reçus (messages de données interceptés, messages NDP provenant de l'Inspection ND et messages DHCPv6 provenant de la protection DHCPv6) par l'intermédiaire de la Table de liaisons de voisins, élimine les messages incorrects et transmet les messages corrects en vue du transfert.

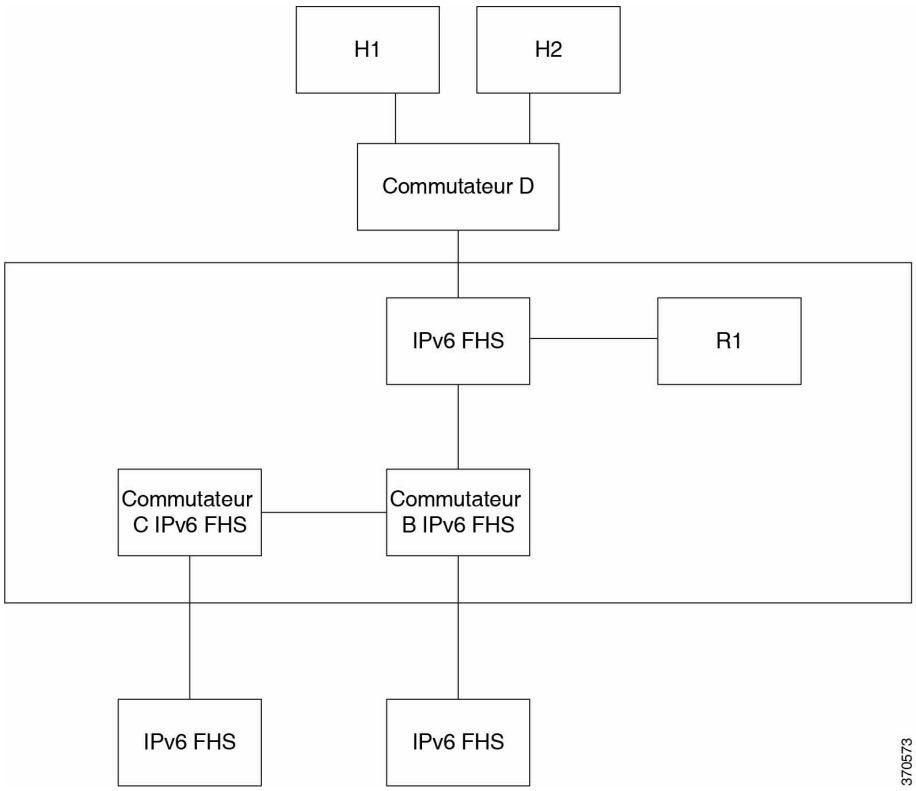
L'Intégrité de la liaison de voisin acquiert (apprend) les voisins à partir des messages reçus (messages NDP et DHCPv6) et les stocke dans la Table de liaisons de voisins. En outre, les entrées statiques peuvent être ajoutées manuellement. Une fois les adresses apprises, la fonction NBI transmet les trames en vue du transfert.

Les messages RS,CPS NS et NA interceptés sont également transmis à la fonction Inspection ND. La fonction Inspection ND valide ces messages, élimine les messages incorrects et envoie les messages corrects à la fonction Protection de la source IPv6.

Périmètre de la Sécurité du premier saut IPv6

Les commutateurs de la Sécurité du premier saut IPv6 peuvent former un périmètre séparant une zone non sécurisée d'une zone sécurisée. Tous les commutateurs situés à l'intérieur du périmètre prennent en charge la Sécurité du premier saut IPv6. Les hôtes et routeurs situés à l'intérieur de ce périmètre sont des périphériques de confiance. Par exemple, dans la Figure 2, les commutateurs B et C sont des liaisons internes dans la zone protégée.

Figure 2 Périmètre de la Sécurité du premier saut IPv6



La commande **device-role** dans l'écran de configuration de la stratégie Neighbor Binding (Liaison de voisin) spécifie le périmètre.

Chaque commutateur Sécurité du premier saut IPv6 établit une liaison pour les voisins partitionnés par le point d'accès. De cette manière, les entrées de liaison sont distribuées sur les périphériques Sécurité du premier saut IPv6 formant le périmètre. Les périphériques Sécurité du premier saut IPv6 peuvent alors assurer l'intégrité de la liaison à l'intérieur du périmètre, sans configurer de liaisons pour toutes les adresses sur chaque périphérique.

Protection Router Advertisement

La protection Router Advertisement (RA) est la première fonction FHS qui traite les messages RA interceptés. La protection RA prend en charge les fonctions suivantes :

- Filtrage des messages de redirection RA, CPA et ICMPv6 reçus.
- Validation des messages RA reçus.

Filtrage des messages de redirection RA, CPA et ICMPv6 reçus

La protection RA élimine les messages RA et CPA reçus sur les interfaces n'ayant pas le rôle de routeur. Vous pouvez configurer le rôle d'interface voix sur la page Paramètres de protection RA.

Validation des messages RA

La protection RA valide les messages RA par l'intermédiaire du filtrage basé sur la stratégie Protection RA associée à l'interface. Ces stratégies peuvent être configurées sur la page Paramètres de protection RA.

Si un message échoue lors de la vérification, celui-ci est éliminé. Si la configuration de la journalisation des abandons de paquets est activée sur le composant Sécurité du premier saut IPv6 commune, un message SYSLOG limité en débit est envoyé.

Inspection Neighbor Discovery

L'inspection Neighbor Discovery (ND) prend en charge les fonctions suivantes :

- Validation des messages de protocole Neighbor Discovery reçus.
- Filtrage en sortie

Validation des messages

L'inspection ND valide les messages de protocole Neighbor Discovery en fonction de la stratégie Inspection ND associée à l'interface. Cette stratégie peut être définie sur la page Paramètres d'inspection ND.

Si un message échoue lors de la vérification définie dans la stratégie, il est éliminé et un message SYSLOG à débit limité est envoyé.

Filtrage en sortie

L'inspection ND bloque le transfert des messages RS et CPS sur les interfaces configurées comme interfaces hôtes.

Protection DHCPv6

La protection DHCPv6 traite les messages DHCPv6 interceptés. La protection DHCPv6 prend en charge les fonctions suivantes :

- Filtrage des messages DHCPv6 reçus.

  La protection DHCP élimine les messages de réponse DHCPv6 reçus sur les interfaces ayant le rôle client. Vous pouvez configurer le rôle d'interface voix sur la page Paramètres de protection DHCPv6.

- Validation des messages DHCPv6 reçus.

  La protection DHCPv6 valide les messages DHCPv6 qui correspondent au filtrage basé sur la stratégie Protection DHCPv6 associée à l'interface.

Si un message échoue lors de la vérification, celui-ci est éliminé. Si la configuration de la journalisation des abandons de paquets est activée sur le composant Sécurité du premier saut IPv6 commune, un message SYSLOG limité en débit est envoyé.

Intégrité de la liaison de voisin

L'intégrité de la liaison de voisin (Neighbor Binding (NB) Integrity) établit la liaison des voisins.

Une instance séparée et indépendante de l'intégrité de la liaison de voisin s'exécute sur chaque VLAN où la fonction est activée.

Apprentissage des préfixes IPv6 annoncés

L'intégrité de la liaison de voisin apprend les préfixes IPv6 annoncés dans les messages RA et les enregistre dans la table des préfixes de voisins. Les préfixes sont utilisés pour la vérification des adresses IPv6 globales attribuées.

Par défaut, cette validation est désactivée. Si elle est activée, les adresses sont validées en fonction des préfixes sur la page Paramètres de liaison de voisin.

Les préfixes statiques utilisés pour la validation des adresses peuvent être ajoutés sur la page Table des préfixes de voisins.

Validation des adresses IPv6 globales

L'intégrité de la liaison de voisin procède aux validations suivantes :

- Si l'adresse cible dans un message NS ou NA est une adresse IPv6 globale, elle doit appartenir à l'un des préfixes définis dans la table des préfixes RA.
- Une adresse IPv6 globale fournie par un serveur DHCPv6 doit appartenir à l'un des préfixes définis dans la liste de préfixes IPv6 (sur la page Préfixes IPv6).

Si un message échoue lors de cette vérification, il est éliminé et un message SYSLOG à débit limité est envoyé.

Présentation de la table de liaisons de voisins

En l'absence d'espace disponible pour créer une entrée, aucune entrée n'est créée et un message SYSLOG est envoyé.

Établissement d'une liaison de voisin

Un commutateur Sécurité du premier saut IPv6 peut détecter et enregistrer les informations de liaison grâce aux méthodes suivantes :

- **Méthode NBI-NDP** : apprentissage des adresses IPv6 à partir des messages Neighbor Discovery Protocol tracés
- **Méthode NBI-DHCP** : apprentissage des adresses IPv6 à partir des messages DHCPv6 tracés
- **Méthode NBI manuelle :** par configuration manuelle

Une adresse IPv6 est liée à une propriété de couche de liaison de l'association réseau de l'hôte. Cette propriété, appelée « ancre de liaison » se compose de l'identifiant d'interface (ifIndex) via lequel l'hôte est connecté et de l'adresse MAC de l'hôte.

Le commutateur Sécurité du premier saut IPv6 établit la liaison uniquement sur les interfaces périmétriques (voir Périmètre de la Sécurité du premier saut IPv6).

Les informations de liaison sont enregistrées dans la table de liaisons de voisins.

Méthode NBI-NDP

La méthode NBI-NDP utilisée est basée sur la méthode FCFS- SAVI spécifiée dans RFC6620, avec les différences suivantes :

- À la différence de FCFS-SAVI, qui prend uniquement en charge la liaison pour les adresses IPv6 de liaison locale, NBI-NDP prend également en charge les adresses IPv6 de liaison globale.
- NBI-NDP prend en charge la liaison d'adresse IPv6 pour les adresses IPv6 apprises à partir des messages NDP. La validation d'adresse source pour le message de données est fournie par la protection d'adresse source IPv6.
- Avec NBI-NDP, la vérification de la propriété d'adresse est basée sur le principe Premier arrivé premier servi (First-Come, First-Served). Le premier hôte qui demande une adresse source donnée est jusqu'à nouvel ordre le propriétaire de cette adresse. Aucune modification de l'hôte n'étant possible, il faut trouver une solution pour confirmer la propriété de l'adresse sans avoir recours à un nouveau protocole. Pour cette raison, lorsqu'une adresse IPv6 est d'abord apprise à partir d'un message NDP, le commutateur lie l'adresse à l'interface. Les messages NDP suivants qui contiennent cette adresse IPV6 peuvent être contrôlés par rapport à la même ancre de liaison, afin de s'assurer que l'initiateur possède l'adresse IP source.

  L'exception à cette règle survient lorsqu'un hôte IPv6 se déplace dans le domaine L2 ou change son adresse MAC. Dans ce cas, l'hôte est toujours le propriétaire de l'adresse IP, mais l'ancre de liaison associée peut avoir changé. Pour faire face à cette situation, le comportement NBI-NDP défini implique de vérifier si l'hôte est toujours accessible en envoyant des messages DAD-NS à l'interface de liaison précédente. Si l'hôte n'est plus accessible via l'ancre de liaison précédemment enregistrée, NBI-NDP part du principe que la nouvelle ancre est valide et change l'ancre de liaison. Si l'hôte est encore accessible via l'ancre de liaison précédemment enregistrée, l'interface de liaison n'est pas changée.

Pour réduire la taille de la table de liaisons de voisins, NBI-NDP établit la liaison uniquement sur les interfaces périmétriques (voir Périmètre de la Sécurité du premier saut IPv6) et distribue les informations de liaison dans les interfaces internes via les messages NS et NA. Avant de créer une liaison locale NBI-NDP, le périphérique envoie un message DAD-NS pour obtenir l'adresse impliquée. Si un hôte répond à ce message par un message NA, le périphérique qui a envoyé le message DAD-NS en conclut qu'il existe une liaison pour cette adresse sur un autre périphérique et ne crée pas de liaison locale pour celui-ci. Si aucun message NA n'est reçu en tant que réponse au message DAD-NS, le périphérique local en conclut qu'il n'existe aucune liaison pour cette adresse sur les autres périphériques et crée la liaison locale pour cette adresse.

NBI-NDP prend en charge un minuteur de durée de vie. Une valeur du minuteur est configurable sur la page Paramètres de liaison de voisin. Le minuteur est redémarré à chaque fois que l'adresse IPv6 liée est confirmée. Si le minuteur arrive à expiration, le périphérique envoie un maximum de 2 messages DAD-NS à de courts intervalles afin de valider le voisin.

Méthode NBI-DHCP

La méthode NBI-NDP est basée sur la méthode SAVI-DHCP spécifiée dans la solution SAVI pour DHCP, draft-ietf-savi-dhcp-15, 11 septembre 2012.

Comme NBI-NDP, NBI-DHCP fournit une liaison périmétrique à des fins d'évolutivité. La méthode NBI-DHCP et la méthode NBI-FCFS présentent la différence suivante : NBI-DHCP suit l'état annoncé dans les messages DHCPv6 ; il n'est donc pas nécessaire de distribuer l'état par les messages NS/NA.

Stratégie d'intégrité de la liaison de voisin

À l'instar des autres fonctions Sécurité du premier saut IPv6, le comportement Intégrité de la liaison de voisin sur une interface est spécifié par une stratégie Intégrité de la liaison de voisin associée à une interface. Ces stratégies sont configurées sur la page Paramètres de liaison de voisin.

Protection de la source IPv6

Si la fonction Intégrité de la liaison de voisin est activée, la fonction Protection de la source IPv6 valide les adresses IPv6 sources des messages NDP et DHCPv6, qu'elle soit activée ou non. Si la fonction Protection de la source IPv6 est activée en même temps que la fonction Intégrité de la liaison de voisin, elle configure la mémoire TCAM afin de spécifier les trames de données IPv6 à transférer, à abandonner ou à intercepter par le processeur et valide les adresses IPv6 sources des messages de données IPv6 interceptés. Si la fonction Intégrité de la liaison de voisin n'est pas activée, la fonction Protection de la source IPv6 ne devient pas active, qu'elle soit activée ou non.

En l'absence d'espace disponible dans la mémoire TCAM pour l'ajout d'une nouvelle règle, le compteur de débordement TCAM est incrémenté et un message SYSLOG à débit limité contenant l'identifiant d'interface, l'adresse MAC hôte et l'adresse IPv6 hôte est envoyé.

La fonction Protection de la source IPv6 valide les adresses sources de tous les messages IPv6 reçus au moyen de la table Liaison de voisin, à l'exception des messages ci-dessous qui sont transmis sans validation :

- Messages RS, si l'adresse IPv6 source équivaut à l'adresse IPv6 non spécifiée.
- Messages NS, si l'adresse IPv6 source équivaut à l'adresse IPv6 non spécifiée.
- Messages NA, si l'adresse IPv6 source équivaut à l'adresse cible.

La fonction Protection de la source IPv6 abandonne tous les autres messages IPv6 dont l'adresse IPv6 source équivaut à l'adresse IPv6 non spécifiée.

La fonction Protection de la source IPv6 s'exécute uniquement sur les interfaces non sécurisées appartenant au périmètre.

La fonction Protection de la source IPv6 abandonne un message IPv6 d'entrée dans les cas suivants :

- La table Liaison de voisin ne contient pas l'adresse IPv6.
- La table Liaison de voisin contient l'adresse IPv6, mais elle est liée à une autre interface.

La fonction Protection de la source IPv6 initie le processus de récupération de voisin en envoyant des messages DAD_NS pour les adresses IPv6 sources inconnues.

Protection contre les attaques

Cette section décrit la protection contre les attaques qu'offre la Sécurité du premier saut IPv6.

Protection contre l'usurpation de routeur IPv6

Un hôte IPv6 peut utiliser les messages RA reçus pour :

- Détection de routeur IPv6
- Configuration d'adresse sans état

Un hôte malveillant peut envoyer des messages RA qui l'annoncent lui-même comme routeur IPv6 et fournissant des préfixes contrefaits pour la configuration d'adresse statique.

La protection RA offre une protection contre ces attaques en configurant le rôle d'interface comme interface hôte pour toutes les interfaces où les routeurs IPv6 ne peuvent pas être connectés.

Protection contre l'usurpation de résolution d'adresse IPv6

Un hôte malveillant peut envoyer des messages NA qui l'annoncent lui-même comme hôte IPv6 disposant de l'adresse IPv6 donnée.

L'intégrité de la liaison de voisin offre une protection contre ces attaques comme suit :

- Si l'adresse IPv6 donnée est inconnue, le message Neighbor Solicitation (NS) est uniquement transféré sur les interfaces internes.
- Si l'adresse IPv6 donnée est connue, le message NS est uniquement transféré sur l'interface à laquelle l'adresse IPv6 est liée.
- Un message Neighbor Advertisement (NA) est éliminé si l'adresse IPv6 cible est liée à une autre interface.

Protection contre l'usurpation de détection des adresses en double IPv6

Un hôte IPv6 doit réaliser la détection des adresses en double (Duplication Address Detection) pour chaque adresse IPv6 attribuée en envoyant un message NS spécial (message Duplicate Address Detection Neighbor Solicitation (DAD_NS)).

Un hôte malveillant peut envoyer une réponse à un message DAD_NS en s'annonçant comme hôte IPv6 disposant de l'adresse IPv6 donnée.

L'intégrité de la liaison de voisin offre une protection contre ces attaques comme suit :

- Si l'adresse IPv6 donnée est inconnue, le message DAD_NS est uniquement transféré sur les interfaces internes.
- Si l'adresse IPv6 donnée est connue, le message DAD_NS est uniquement transféré sur l'interface à laquelle l'adresse IPv6 est liée.
- Un message NA est éliminé si l'adresse IPv6 cible est liée à une autre interface.

Protection contre l'usurpation de serveur DHCPv6

Un hôte IPv6 peut utiliser le protocole DHCPv6 pour :

- Configuration d'informations sans état
- Configuration d'adresse avec état

Un hôte malveillant peut envoyer des messages de réponse DHCPv6 qui l'annoncent lui-même comme serveur DHCPv6 et fournissant des adresses IPv6 et des informations sans état contrefaites. La protection DHCPv6 offre une protection contre ces attaques en configurant le rôle d'interface comme port client pour tous les ports auxquels les serveurs DHCPv6 ne peuvent pas être connectés.

Protection contre l'usurpation de cache NBD

Un routeur IPv6 prend en charge le cache NDP (Neighbor Discovery Protocol) qui mappe l'adresse IPv6 sur l'adresse MAC pour le routage du dernier saut.

Un hôte malveillant peut envoyer des messages IPv6 avec une autre adresse IPv6 de destination pour le transfert du dernier saut, générant ainsi un débordement du cache NBD.

Un mécanisme intégré dans l'implémentation NDP limite le nombre d'entrées autorisées dans l'état INCOMPLET dans le cache Détection de voisin. Cela assure une protection contre toute saturation (inondation) de la table par des pirates informatiques.

Stratégies, paramètres globaux et valeurs par défaut du système

Chaque fonction de la Sécurité du premier saut (First Hop Security, FHS) peut être activée ou désactivée individuellement. Aucune fonction n'est activée par défaut.

Initialement, les fonctions doivent être activées sur des VLAN spécifiques. Lorsque vous activez la fonction, vous pouvez aussi définir les valeurs de configuration globale pour les règles de vérification de cette fonction. Si vous ne définissez pas de stratégie contenant différentes valeurs pour ces règles de vérification, les valeurs globales sont utilisées pour appliquer la fonction aux paquets.

Stratégies

Les stratégies contiennent les règles de vérification exécutées sur les paquets entrants. Elles peuvent être associées aux VLAN, mais également aux ports et aux LAG. Si la fonction n'est pas activée sur un VLAN, les stratégies n'ont aucun effet.

Il peut s'agir de stratégies définies par l'utilisateur ou de stratégies par défaut (voir ci-dessous).

Stratégies par défaut

Il existe des stratégies par défaut vides pour chaque fonction FHS. Par défaut, elles sont associées aux VLAN et aux interfaces. Les stratégies par défaut sont nommées : « vlan_default » et « port_default » (pour chaque fonction) :

- Vous pouvez ajouter des règles à ces stratégies par défaut. Vous ne pouvez pas associer manuellement des stratégies par défaut à des interfaces. Elles sont associées par défaut.
- Vous ne pouvez pas supprimer les stratégies par défaut. Vous pouvez uniquement supprimer la configuration ajoutée par l'utilisateur.

Stratégies définies par l'utilisateur

Vous pouvez définir d'autres stratégies que les stratégies par défaut.

Lorsqu'une stratégie définie par l'utilisateur est associée à une interface, la stratégie par défaut de cette interface est dissociée. Si la stratégie définie par l'utilisateur est dissociée de l'interface, la stratégie par défaut est de nouveau associée.

Les stratégies ne prennent pas effet tant que :

- la fonction dans la stratégie n'est pas activée sur le VLAN qui contient l'interface ;
- la stratégie n'est pas associée à l'interface (VLAN, port ou LAG).

Lorsque vous associez une stratégie, la stratégie par défaut de cette interface est dissociée. Lorsque vous supprimez la stratégie de l'interface, la stratégie par défaut est de nouveau associée.

Vous pouvez seulement associer 1 stratégie (pour une fonction spécifique) à un VLAN.

Vous pouvez associer plusieurs stratégies (pour une fonction spécifique) à une interface si elles spécifient différents VLAN.

Niveaux des règles de vérification

Le groupe de règles final appliqué à un paquet entrant sur une interface est construit de la manière suivante :

- Les règles configurées dans les stratégies associées à l'interface (port ou LAG) sur laquelle le paquet est arrivé sont ajoutées au groupe.
- Les règles configurées dans la stratégie associée au VLAN sont ajoutées au groupe si elles n'ont pas été ajoutées au niveau du port.

- Les règles globales sont ajoutées au groupe si elles n'ont pas été ajoutées au niveau du VLAN ou du port.

Les règles définies au niveau du port remplacent les règles définies au niveau du VLAN. Les règles définies au niveau du VLAN remplacent les règles configurées de manière globale. Les règles configurées de manière globale remplacent les valeurs par défaut du système.

Tâches courantes

Flux de travail de la sécurité du premier saut IPv6 commune

ÉTAPE 1 Sur la page Paramètres FHS, entrez la liste des VLAN sur lesquels cette fonction est activée.

ÉTAPE 2 Sur cette même page, définissez la fonction Journalisation des abandons de paquets.

ÉTAPE 3 Si nécessaire, configurez une stratégie définie par l'utilisateur ou ajoutez des règles aux stratégies par défaut pour la fonction.

ÉTAPE 4 Associez la stratégie à un VLAN, un port ou un LAG à l'aide de la page Association de stratégie (VLAN) ou Association de stratégie (Port).

Flux de travail de protection Annonce de routeur (Router Advertisement, RA)

ÉTAPE 1 Sur la page Paramètres de protection RA, entrez la liste des VLAN sur lesquels cette fonction est activée.

ÉTAPE 2 Sur cette même page, définissez les valeurs de configuration globale utilisées si aucune valeur n'est définie dans une stratégie.

ÉTAPE 3 Si nécessaire, configurez une stratégie définie par l'utilisateur ou ajoutez des règles aux stratégies par défaut pour la fonction.

ÉTAPE 4 Associez la stratégie à un VLAN, un port ou un LAG à l'aide de la page Association de stratégie (VLAN) ou Association de stratégie (Port).

Flux de travail de protection DHCPv6

ÉTAPE 1 Sur la page Paramètres de protection DHCPv6, entrez la liste des VLAN sur lesquels cette fonction est activée.

ÉTAPE 2 Sur cette même page, définissez les valeurs de configuration globale utilisées si aucune valeur n'est définie dans une stratégie.

ÉTAPE 3 Si nécessaire, configurez une stratégie définie par l'utilisateur ou ajoutez des règles aux stratégies par défaut pour la fonction.

ÉTAPE 4 Associez la stratégie à un VLAN, un port ou un LAG à l'aide de la page Association de stratégie (VLAN) ou Association de stratégie (Port).

Flux de travail d'inspection Neighbor Discovery

ÉTAPE 1 Sur la page Paramètres d'inspection ND, entrez la liste des VLAN sur lesquels cette fonction est activée.

ÉTAPE 2 Sur cette même page, définissez les valeurs de configuration globale utilisées si aucune valeur n'est définie dans une stratégie.

ÉTAPE 3 Si nécessaire, configurez une stratégie définie par l'utilisateur ou ajoutez des règles aux stratégies par défaut pour la fonction.

ÉTAPE 4 Associez la stratégie à un VLAN, un port ou un LAG à l'aide de la page Association de stratégie (VLAN) ou Association de stratégie (Port).

Flux de travail de liaison de voisin

ÉTAPE 1 Sur la page Paramètres de liaison de voisin, entrez la liste des VLAN sur lesquels cette fonction est activée.

ÉTAPE 2 Sur cette même page, définissez les valeurs de configuration globale utilisées si aucune valeur n'est définie dans une stratégie.

ÉTAPE 3 Si nécessaire, configurez une stratégie définie par l'utilisateur ou ajoutez des règles aux stratégies par défaut pour la fonction.

ÉTAPE 4 Ajoutez toutes les entrées manuelles requises sur la page Table de liaisons de voisins.

ÉTAPE 5 Associez la stratégie à un VLAN, un port ou un LAG à l'aide de la page Association de stratégie (VLAN) ou Association de stratégie (Port).

Flux de travail de la Protection de la source IPv6

ÉTAPE 1 Sur la page Paramètres de la Protection de la source IPv6, entrez la liste des VLAN sur lesquels cette fonction est activée.

ÉTAPE 2 Si nécessaire, configurez une stratégie définie par l'utilisateur ou ajoutez des règles aux stratégies par défaut pour la fonction.

ÉTAPE 3 Associez la stratégie à un VLAN, un port ou un LAG à l'aide de la page Association de stratégie (VLAN) ou Association de stratégie (Port).

Configuration et paramètres par défaut

Si la Sécurité du premier saut IPv6 est activée sur un VLAN, le commutateur intercepte les messages suivants par défaut :

- Messages Router Advertisement (RA)
- Messages Router Solicitation (RS)
- Messages Neighbor Advertisement (NA)
- Messages Neighbor Solicitation (NS)
- Messages ICMPv6 Redirect
- Messages Certification Path Advertisement (CPA)
- Messages Certification Path Solicitation (CPS)
- Messages DHCPv6

Les fonctions FHS sont désactivées par défaut.

Configuration de la Sécurité du premier saut IPv6 via l'interface utilisateur graphique Web

Paramètres FHS

Utilisez la page Paramètres FHS pour activer la fonction Sécurité du premier saut IPv6 commune sur un groupe de VLAN spécifique, ainsi que pour définir la valeur de configuration globale pour la journalisation des paquets abandonnés. Si nécessaire, vous pouvez ajouter une stratégie ou ajouter la journalisation des abandons de paquets à la stratégie par défaut définie par le système.

Pour définir les paramètres de la fonction Sécurité du premier saut IPv6 commune :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut IPv6** > **Paramètres FHS**.

Les stratégies actuellement définies s'affichent. Pour chacune d'elles, le **Type de stratégie** est précisé pour indiquer s'il s'agit d'une stratégie par défaut ou définie par l'utilisateur.

ÉTAPE 2 Renseignez les champs de configuration globale suivants :

- **FHS VLAN List** (Liste des VLAN FHS) : saisissez un ou plusieurs VLAN sur lesquels la fonction IPv6 First Hop Security (Sécurité du premier saut IPv6) est activée.
- **Packet Drop Logging** (Journalisation des abandons de paquets) : sélectionnez cette option pour créer un SYSLOG lorsqu'un paquet est abandonné par une stratégie de sécurité du premier saut. Il s'agit de la valeur globale par défaut si aucune stratégie n'est définie.

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

ÉTAPE 4 Si nécessaire, créez une stratégie FHS en cliquant sur **Ajouter**.

Renseignez les champs suivants :

- **Policy Name** (Nom de la stratégie) : saisissez un nom de stratégie défini par l'utilisateur.
- **Packet Drop Logging** (Journalisation des abandons de paquets) : sélectionnez cette option pour créer un SYSLOG lorsqu'un paquet est abandonné suite à l'application d'une fonction Sécurité du premier saut dans cette stratégie.
  - *Inherited* (Hériter) : utilisez la valeur issue de la configuration globale ou du VLAN.
  - *Activer* : créez un SYSLOG lorsqu'un paquet est abandonné suite à la Sécurité du premier saut.
  - *Désactiver* : ne créez pas de SYSLOG lorsqu'un paquet est abandonné suite à la Sécurité du premier saut.

ÉTAPE 5 Cliquez sur **Appliquer** pour ajouter les paramètres au fichier de Configuration d'exécution.

ÉTAPE 6 Pour associer cette stratégie à une interface :

- **Associer la stratégie au VLAN** : cliquez sur cette option pour accéder à la page Association de stratégie (VLAN), qui permet d'associer cette stratégie à un VLAN.
- **Associer la stratégie à l'interface** : cliquez sur cette option pour accéder à la page Association de stratégie (Port), qui permet d'associer cette stratégie à un port.

Paramètres de protection RA

Utilisez la page Paramètres de protection RA pour activer la fonction Protection RA sur un groupe de VLAN spécifique, mais aussi pour définir les valeurs de configuration globale de cette fonction. Si nécessaire, vous pouvez ajouter une stratégie ou configurer les stratégies Protection RA par défaut, définies par le système, sur cette page.

Pour configurer la fonction Protection RA :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut IPv6** > **Paramètres de protection RA**.

Les stratégies actuellement définies s'affichent. Pour chacune d'elles, le **Type de stratégie** est précisé pour indiquer s'il s'agit d'une stratégie par défaut ou définie par l'utilisateur.

ÉTAPE 2 Renseignez le champ de configuration globale suivant :

- **RA Guard VLAN List** (Liste VLAN de protection RA) : entrez un ou plusieurs VLAN sur lesquels la protection RA est activée.

Renseignez les autres champs de configuration qui sont décrits ci-dessous.

ÉTAPE 3 Pour ajouter une stratégie, cliquez sur **Ajouter**, puis renseignez les champs suivants :

- **Policy Name** (Nom de la stratégie) : saisissez un nom de stratégie défini par l'utilisateur.
- **Rôle du périphérique** : affiche l'une des options ci-dessous permettant d'indiquer le rôle du périphérique connecté au port dans le cadre de la stratégie Protection RA.
  - *Inherited* (Hérité) : le rôle du périphérique est hérité du VLAN ou du paramètre système par défaut (client).
  - *Hôte* (Hôte) : le périphérique a un rôle d'hôte.
  - *Router* (Routeur) : le périphérique a un rôle de routeur.

- **Managed Configuration Flag** (Drapeau de configuration gérée) : ce champ spécifie la vérification du drapeau Configuration d'adresse gérée annoncé au sein d'une stratégie de protection RA IPv6.
  - *Inherited* (Hérité) : la fonction est héritée du VLAN ou du paramètre système par défaut (client).
  - *Aucune vérification* : désactive la vérification du drapeau Configuration d'adresse gérée annoncé.
  - *Activé* : active la vérification du drapeau Configuration d'adresse gérée annoncé.
  - *Désactivé* : la valeur du drapeau doit être 0.
- **Other Configuration Flag** (Autre drapeau de configuration) : ce champ spécifie la vérification du drapeau Autre configuration annoncé au sein d'une stratégie Protection RA IPv6.
  - *Inherited* (Hérité) : la fonction est héritée du VLAN ou du paramètre système par défaut (client).
  - *Aucune vérification* : désactive la vérification du drapeau Autre configuration annoncé.
  - *Activé* : active la vérification du drapeau Autre configuration annoncé.
  - *Désactivé* : la valeur du drapeau doit être 0.
- **RA Address List** (Liste d'adresses RA) : spécifiez la liste d'adresses à filtrer :
  - *Hérité* : la valeur est héritée du VLAN ou du paramètre système par défaut (aucune vérification).
  - *No Verification* (Aucune vérification) : les adresses annoncées ne sont pas vérifiées.
  - *Liste des correspondances* : liste des adresses IPv6 à utiliser pour la mise en correspondance.
- **Liste de préfixes RA** : spécifiez la liste d'adresses à filtrer :
  - *Hérité* : la valeur est héritée du VLAN ou du paramètre système par défaut (aucune vérification).
  - *Aucune vérification* : les préfixes annoncés ne sont pas vérifiés.
  - *Liste des correspondances* : liste des préfixes à utiliser pour la mise en correspondance.

- **Minimal Hop Limit** (Limite de saut minimale) : indique si la stratégie Protection RA contrôle la limite de saut minimale du paquet reçu.
  - *Inherited* (Hérité) : la fonction est héritée du VLAN ou du paramètre système par défaut (client).
  - *No Limit* (Aucune limite) : désactive la vérification de la limite inférieure pour la limite de nombre de sauts.
  - *Défini par l'utilisateur* : vérifie que la limite de nombre de sauts est supérieure ou égale à cette valeur.
- **Maximal Hop Limit** (Limite de saut maximale) : indique si la stratégie Protection RA contrôle la limite de saut maximale du paquet reçu.
  - *Inherited* (Hérité) : la fonction est héritée du VLAN ou du paramètre système par défaut (client).
  - *No Limit* (Aucune limite) : désactive la vérification de la limite supérieure pour la limite de nombre de sauts.
  - *Défini par l'utilisateur* : vérifie que la limite de nombre de sauts est inférieure ou égale à cette valeur. La valeur de la limite haute doit être égale ou supérieure à la valeur de la limite basse.
- **Minimal Router Preference** (Préférence de routeur minimale) : ce champ indique si la stratégie Protection RA vérifie la valeur minimale Préférence de routeur par défaut annoncée dans les messages RA dans le cadre d'une stratégie Protection RA.
  - *Inherited* (Hérité) : la fonction est héritée du VLAN ou du paramètre système par défaut (client).
  - *Aucune vérification* : désactive la vérification de la limite inférieure de la Préférence de routeur par défaut annoncée.
  - *Faible* : spécifie la valeur minimale Préférence de routeur par défaut annoncée autorisée. Les valeurs acceptées sont les suivantes : faible, moyenne et élevée (voir RFC4191).
  - *Moyenne* : spécifie la valeur minimale Préférence de routeur par défaut annoncée autorisée. Les valeurs acceptées sont les suivantes : faible, moyenne et élevée (voir RFC4191).
  - *Élevée* : spécifie la valeur minimale Préférence de routeur par défaut annoncée autorisée. Les valeurs acceptées sont les suivantes : faible, moyenne et élevée (voir RFC4191).

- **Maximal Router Preference** (Préférence de routeur maximale) : ce champ indique si la stratégie Protection RA vérifie la valeur maximale Préférence de routeur par défaut annoncée dans les messages RA dans le cadre d'une stratégie Protection RA.
  - *Hérité* : la fonction est héritée du VLAN ou du paramètre système par défaut (client).
  - *Aucune vérification* : désactive la vérification de la limite supérieure de la Préférence de routeur par défaut annoncée.
  - *Faible* : spécifie la valeur maximale Préférence de routeur par défaut annoncée autorisée. Les valeurs acceptées sont les suivantes : faible, moyenne et élevée (voir RFC4191).
  - *Moyenne* : spécifie la valeur maximale Préférence de routeur par défaut annoncée autorisée. Les valeurs acceptées sont les suivantes : faible, moyenne et élevée (voir RFC4191).
  - *Élevée* : spécifie la valeur maximale Préférence de routeur par défaut annoncée autorisée. Les valeurs acceptées sont les suivantes : faible, moyenne et élevée (voir RFC4191).

ÉTAPE 4 Cliquez sur **Appliquer** pour ajouter les paramètres au fichier de Configuration d'exécution.

ÉTAPE 5 Pour configurer des stratégies par défaut définies par le système ou une stratégie existante définie par l'utilisateur, sélectionnez la stratégie dans la table des stratégies et cliquez sur **Modifier**.

ÉTAPE 6 Pour associer cette stratégie à une interface :

- **Associer la stratégie au VLAN** : cliquez sur cette option pour accéder à la page Association de stratégie (VLAN), qui permet d'associer cette stratégie à un VLAN.
- **Associer la stratégie à l'interface** : cliquez sur cette option pour accéder à la page Association de stratégie (Port), qui permet d'associer cette stratégie à un port.

Paramètres de protection DHCPv6

Utilisez la page Paramètres de protection DHCPv6 pour activer la fonction Protection DHCPv6 sur un groupe de VLAN spécifique, mais aussi pour définir les valeurs de configuration globale de cette fonction. Si nécessaire, vous pouvez ajouter une stratégie ou configurer les stratégies Protection DHCPv6 par défaut, définies par le système, sur cette page.

Pour configurer la fonction Protection DHCPv6 :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut IPv6** > **Paramètres de protection DHCPv6**.

Les stratégies actuellement définies s'affichent. Pour chacune d'elles, le **Type de stratégie** est précisé pour indiquer s'il s'agit d'une stratégie par défaut ou définie par l'utilisateur.

ÉTAPE 2 Renseignez les champs de configuration globale suivants :

- **DHCPv6 Guard VLAN List** (Liste de VLAN de protection DHCPv6) : entrez un ou plusieurs VLAN sur lesquels la protection DHCPv6 est activée.
- **Rôle du périphérique** : affiche le rôle du périphérique. Reportez-vous à la définition figurant sur la page **Ajouter**.
- **Préférence minimale** : ce champ indique si la stratégie Protection DHCPv6 contrôle la valeur minimale de préférence annoncée du paquet reçu.
  - *Aucune vérification* : désactive la vérification de la valeur minimale de préférence annoncée du paquet reçu.
  - *Défini par l'utilisateur* : vérifie que la valeur de préférence annoncée est supérieure ou égale à cette valeur. Cette valeur doit être inférieure à la valeur de Préférence maximale.
- **Maximal Preference** (Préférence maximale) : ce champ indique si la stratégie Protection DHCPv6 contrôle la valeur maximale de préférence annoncée du paquet reçu. Cette valeur doit être supérieure à la valeur de Préférence minimale.
  - *Aucune vérification* : désactive la vérification de la limite inférieure pour la limite de nombre de sauts.
  - *Défini par l'utilisateur* : vérifie que la valeur de préférence annoncée est inférieure ou égale à cette valeur.

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

Les stratégies existantes sont affichées. Les champs sont affichés ci-dessous, sauf le champ **Type de stratégie**. Ce dernier indique s'il s'agit d'une stratégie par défaut ou définie par l'utilisateur.

ÉTAPE 4 Si nécessaire, cliquez sur **Ajouter** pour créer une stratégie DHCPv6.

ÉTAPE 5 Renseignez les champs suivants :

- **Policy Name** (Nom de la stratégie) : saisissez un nom de stratégie défini par l'utilisateur.

- **Rôle du périphérique** : sélectionnez **Serveur** ou **Client** afin de spécifier le rôle du périphérique associé au port pour la protection DHCPv6.
  - *Hérité* : le rôle du périphérique est hérité du VLAN ou du paramètre système par défaut (client).
  - *Client* : le rôle du périphérique est client.
  - *Hôte* : le périphérique a un rôle de serveur.
- **Trouver préfixes de rép. correspondants** : sélectionnez cette option pour activer la vérification des préfixes annoncés dans les messages de réponse DHCP reçus au sein d'une stratégie Protection DHCPv6.
  - *Hérité* : la valeur est héritée du VLAN ou du paramètre système par défaut (aucune vérification).
  - *Aucune vérification* : les préfixes annoncés ne sont pas vérifiés.
  - *Liste des correspondances* : liste des préfixes IPv6 à utiliser pour la mise en correspondance.
- **Adresse du serveur** : sélectionnez cette option pour activer la vérification de l'adresse IPv6 du relais et du serveur DHCP dans les messages de réponse DHCP reçus au sein d'une stratégie Protection DHCPv6.
  - *Hérité* : la valeur est héritée du VLAN ou du paramètre système par défaut (aucune vérification).
  - *Aucune vérification* : désactive la vérification de l'adresse IPv6 du relais et du serveur DHCP.
  - *Liste des correspondances* : liste des préfixes IPv6 à utiliser pour la mise en correspondance.
- **Minimal Preference** (Préférence minimale) : ce champ indique si la stratégie Protection DHCPv6 contrôle la valeur minimale de préférence annoncée du paquet reçu.
  - *Hérité* : la préférence minimale est héritée du VLAN ou du paramètre système par défaut (client).
  - *Aucune vérification* : désactive la vérification de la valeur minimale de préférence annoncée du paquet reçu.
  - *Défini par l'utilisateur* : vérifie que la valeur de préférence annoncée est supérieure ou égale à cette valeur. Cette valeur doit être inférieure à la valeur de Préférence maximale.

- **Maximal Preference** (Préférence maximale) : ce champ indique si la stratégie Protection DHCPv6 contrôle la valeur maximale de préférence annoncée du paquet reçu. Cette valeur doit être supérieure à la valeur de Préférence minimale.
  - *Hérité* : la préférence minimale est héritée du VLAN ou du paramètre système par défaut (client).
  - *Aucune vérification* : désactive la vérification de la limite inférieure pour la limite de nombre de sauts.
  - *Défini par l'utilisateur* : vérifie que la valeur de préférence annoncée est inférieure ou égale à cette valeur.

ÉTAPE 6 Cliquez sur **Appliquer** pour ajouter les paramètres au fichier de Configuration d'exécution.

ÉTAPE 7 Pour associer cette stratégie à une interface :

- **Associer la stratégie au VLAN** : cliquez sur cette option pour accéder à la page Association de stratégie (VLAN), qui permet d'associer cette stratégie à un VLAN.
- **Associer la stratégie à l'interface** : cliquez sur cette option pour accéder à la page Association de stratégie (Port), qui permet d'associer cette stratégie à un port.

Paramètres d'inspection ND

Utilisez la page Paramètres d'inspection ND (Détection de voisin) pour activer la fonction Inspection ND sur un groupe de VLAN spécifique, ainsi que pour définir les valeurs de configuration globale de cette fonction. Si nécessaire, vous pouvez ajouter une stratégie ou configurer les stratégies Inspection ND par défaut, définies par le système, sur cette page.

Pour configurer la fonction Inspection ND :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut IPv6** > **Paramètres d'inspection ND**.

Les stratégies existantes sont affichées. Les champs sont affichés ci-dessous, sauf le champ **Type de stratégie**. Ce dernier indique s'il s'agit d'une stratégie par défaut ou définie par l'utilisateur.

ÉTAPE 2 Renseignez les champs de configuration globale suivants :

- **Liste de VLAN d'inspection ND** : entrez un ou plusieurs VLAN sur lesquels l'inspection ND est activée.
- **Rôle du périphérique** : affiche le rôle du périphérique qui est expliqué ci-dessous.

- **Drop Unsecure** (Supprimer non sûr) : sélectionnez cette option pour activer l'élimination des messages sans option Signature RSA ou CGA au sein d'une stratégie Inspection ND IPv6.
- **Minimal Security Level** (Niveau de sécurité minimal) : si les messages non sûrs ne sont pas éliminés, sélectionnez le niveau de sécurité en dessous duquel les messages ne sont pas transmis.
  - *Aucune vérification* : désactive la vérification du niveau de sécurité.
  - *Défini par l'utilisateur* : spécifiez le niveau de sécurité du message à transférer.
- **Valider MAC source** : spécifiez si vous souhaitez activer globalement la vérification de l'adresse MAC source par rapport à l'adresse de la couche de liaison.

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

ÉTAPE 4 Si nécessaire, cliquez sur **Ajouter** pour créer une stratégie Inspection ND.

ÉTAPE 5 Renseignez les champs suivants :

- **Policy Name** (Nom de la stratégie) : saisissez un nom de stratégie défini par l'utilisateur.
- **Rôle du périphérique** : sélectionnez l'une des options ci-dessous pour indiquer le rôle de l'appareil connecté au port dans le cadre de la fonction Inspection ND.
  - *Hérité* : le rôle du périphérique est hérité du VLAN ou du paramètre système par défaut (client).
  - *Hôte* : le rôle du périphérique est hôte.
  - *Routeur* : le périphérique a un rôle de routeur.
- **Drop Unsecure** (Supprimer non sûr) : sélectionnez l'une des options suivantes :
  - *Hérité* : la valeur est héritée du VLAN ou du paramètre système par défaut (désactivé).
  - *Enable* (Activer) : activez l'élimination des messages sans option Signature RSA ou CGA au sein d'une stratégie Inspection ND IPv6.
  - *Disable* (Désactiver) : désactivez l'élimination des messages sans option Signature RSA ou CGA au sein d'une stratégie Inspection ND IPv6.
- **Minimal Security Level** (Niveau de sécurité minimal) : si les messages non sûrs ne sont pas éliminés, sélectionnez le niveau de sécurité en dessous duquel les messages ne sont pas transmis.
  - *Hérité* : la valeur est héritée du VLAN ou du paramètre système par défaut (désactivé).

- *Aucune vérification* : désactive la vérification du niveau de sécurité.
- *Défini par l'utilisateur* : spécifiez le niveau de sécurité du message à transférer.

- **Valider MAC source** : spécifiez si vous souhaitez activer globalement la vérification de l'adresse MAC source par rapport à l'adresse de couche de liaison :
  - *Hérité* : la valeur est héritée du VLAN ou du paramètre système par défaut (désactivé).
  - *Activer* : activez la vérification de l'adresse MAC source par rapport à l'adresse de couche de liaison.
  - *Désactiver* : désactivez la vérification de l'adresse MAC source par rapport à l'adresse de couche de liaison.

ÉTAPE 6 Cliquez sur **Appliquer** pour ajouter les paramètres au fichier de Configuration d'exécution.

ÉTAPE 7 Pour associer cette stratégie à une interface :

- **Associer la stratégie au VLAN** : cliquez sur cette option pour accéder à la page Association de stratégie (VLAN), qui permet d'associer cette stratégie à un VLAN.
- **Associer la stratégie à l'interface** : cliquez sur cette option pour accéder à la page Association de stratégie (Port), qui permet d'associer cette stratégie à un port.

Paramètres de liaison de voisin

La Table de liaisons de voisins est une table de base de données de voisins IPv6 connectés à un périphérique, qui est créée à partir de sources d'informations telles que l'usurpation Neighbor Discovery Protocol (NDP). Cette table de base de données, ou liaison, est utilisée par diverses fonctions de protection IPv6 pour empêcher l'usurpation et les attaques de redirection.

Utilisez la page Paramètres de liaison de voisin pour activer la fonction Liaison de voisin sur un groupe de VLAN spécifique, mais aussi pour définir les valeurs de configuration globale de cette fonction. Si nécessaire, vous pouvez ajouter une stratégie ou configurer les stratégies Liaison de voisin par défaut, définies par le système, sur cette page.

Pour configurer la fonction Liaison de voisin :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut IPv6** > **Paramètres de liaison de voisin**.

ÉTAPE 2 Renseignez les champs de configuration globale suivants :

- **Neighbor Binding VLAN List** (Liste de VLAN de liaison de voisins) : entrez un ou plusieurs VLAN sur lesquels la liaison de voisin est activée.

- **Device Role** (Rôle du périphérique) : affiche le rôle par défaut global du périphérique (périmètre).
- **Neighbor Binding Lifetime** (Durée de vie de la liaison de voisins) : entrez la durée pendant laquelle les adresses sont conservées dans la table de liaisons de voisins.
- **Journalisation des liaisons de voisins** : sélectionnez cette option pour activer la journalisation des événements principaux de la table Liaison de voisin.
- **Address Prefix Validation** (Validation de préfixe d'adresse) : sélectionnez cette option pour activer la validation des adresses par la fonction Protection de la source IPv6.

Configuration globale de la liaison d'adresse :

- **Binding from NDP Messages (Liaison à partir des messages NDP)** : pour modifier la configuration globale des méthodes de configuration autorisées pour les adresses IPv6 globales dans le cadre d'une stratégie Liaison de voisin IPv6, sélectionnez l'une des options ci-dessous :
  - *Tous* : toutes les méthodes de configuration (statiques et manuelles) sont autorisées pour les adresses IPv6 globales liées à partir des messages NDP.
  - *Statique* : seule la configuration automatique statique est autorisée pour les adresses IPv6 globales liées à partir des messages NDP.
  - *Désactiver* : la liaison à partir des messages NDP est désactivée.
- **Liaison à partir des messages DHCPv6** : la liaison à partir des messages DHCPv6 est autorisée.

Limites d'entrées de liaisons de voisins : permet d'indiquer le nombre maximal d'entrées de liaisons de voisins par type d'interface ou d'adresse :

- **Entrées par VLAN** : spécifie la limite de liaisons de voisins par VLAN. Sélectionnez **Aucune limite** ou saisissez une valeur dans le champ **Défini par l'utilisateur**.
- **Entrées par interface** : spécifie la limite de liaisons de voisins par interface. Sélectionnez **Aucune limite** ou entrez une valeur dans le champ **Défini par l'utilisateur**.
- **Entrées par adresse MAC** : spécifie la limite de liaisons de voisins par adresse MAC. Sélectionnez **Aucune limite** ou entrez une valeur dans le champ **Défini par l'utilisateur**.

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

ÉTAPE 4 Si nécessaire, cliquez sur **Ajouter** pour créer une stratégie de liaison de voisin.

ÉTAPE 5 Renseignez les champs suivants :

- **Policy Name** (Nom de la stratégie) : saisissez un nom de stratégie défini par l'utilisateur.
- **Rôle du périphérique** : sélectionnez l'**une des** options ci-dessous afin de spécifier le rôle du périphérique connecté au port dans le cadre de la stratégie Liaison de voisin.
  - *Hérité* : le rôle du périphérique est hérité du VLAN ou du paramètre système par défaut (client).
  - *Périmètre* : le port est connecté à des périphériques qui ne prennent pas en charge la fonction Sécurité du premier saut IPv6.
  - *Interne* : le port est connecté à des périphériques qui prennent en charge la fonction Sécurité du premier saut IPv6.
- **Journalisation des liaisons de voisins** : sélectionnez l'une des options suivantes pour la journalisation :
  - *Hérité* : l'option de journalisation est la même que la valeur globale.
  - *Activer* : permet d'activer la journalisation des événements principaux de la table de liaisons.
  - *Désactiver* : permet de désactiver la journalisation des événements principaux de la table de liaisons.
- **Address Prefix Validation (Validation de préfixe d'adresse)** : sélectionnez l'une des options suivantes pour définir la validation des adresses :
  - *Hérité* : l'option de validation est la même que la valeur globale.
  - *Activer* : permet d'activer la validation des adresses.
  - *Désactiver* : permet de désactiver la validation des adresses.

Configuration globale de la liaison d'adresse :

- **Hériter des paramètres de liaisons d'adresse** : permet d'utiliser les paramètres globaux de liaisons d'adresse.
- **Binding from NDP Messages (Liaison à partir des messages NDP)** : pour modifier la configuration globale des méthodes de configuration autorisées pour les adresses IPv6 globales dans le cadre d'une stratégie Liaison de voisin IPv6, sélectionnez l'une des options ci-dessous :
  - *Tous* : toutes les méthodes de configuration (statiques et manuelles) sont autorisées pour les adresses IPv6 globales liées à partir des messages NDP.

- *Statique* : seule la configuration automatique statique est autorisée pour les adresses IPv6 globales liées à partir des messages NDP.
- *Désactiver* : la liaison à partir des messages NDP est désactivée.

- **Liaison à partir des messages DHCPv6** : sélectionnez cette option pour activer la liaison à partir des messages DHCPv6.

Limites d'entrées de liaisons de voisins : voir ci-dessus.

- **Entries per VLAN** (Entrées par VLAN) : sélectionnez **Inherited** (Hérité) pour utiliser la valeur globale, **No Limit** (Aucune limite) pour qu'il n'y ait aucune limite quant au nombre d'entrées ou **User Defined** (Défini par l'utilisateur) pour définir une valeur spéciale pour cette stratégie.
- **Entries per Interface** (Entrées par interface) : sélectionnez **Inherited** (Hérité) pour utiliser la valeur globale, **No Limit** (Aucune limite) pour qu'il n'y ait aucune limite quant au nombre d'entrées ou **User Defined** (Défini par l'utilisateur) pour définir une valeur spéciale pour cette stratégie.
- **Entries per MAC Adress** (Entrées par adresse MAC) : sélectionnez **Inherited** (Hérité) pour utiliser la valeur globale, **No Limit** (Aucune limite) pour qu'il n'y ait aucune limite quant au nombre d'entrées ou **User Defined** (Défini par l'utilisateur) pour définir une valeur spéciale pour cette stratégie.

ÉTAPE 6 Cliquez sur **Appliquer** pour ajouter les paramètres au fichier de Configuration d'exécution.

ÉTAPE 7 Pour associer cette stratégie à une interface :

- **Associer la stratégie au VLAN** : cliquez sur cette option pour accéder à la page Association de stratégie (VLAN), qui permet d'associer cette stratégie à un VLAN.
- **Associer la stratégie à l'interface** : cliquez sur cette option pour accéder à la page Association de stratégie (Port), qui permet d'associer cette stratégie à un port.

Paramètres de la Protection de la source IPv6

Utilisez la page des paramètres de la Protection de la source IPv6 pour activer la fonction Protection de la source IPv6 sur un groupe de VLAN spécifique. Si nécessaire, vous pouvez ajouter une stratégie ou configurer les stratégies Protection de la source IPv6 par défaut, définies par le système, sur cette page.

Pour configurer la fonction Protection de la source IPv6 :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut IPv6** > **Paramètres de la Protection de la source IPv6**.

Les stratégies existantes sont affichées. Les champs sont affichés ci-dessous, sauf le champ **Type de stratégie**. Ce dernier indique s'il s'agit d'une stratégie par défaut ou définie par l'utilisateur.

ÉTAPE 2 Renseignez les champs de configuration globale suivants :

- **Liste de VLAN de protection de la source IPv6** : saisissez un ou plusieurs VLAN sur lesquels la fonction Protection de la source IPv6 est activée.
- **Confiance de port** : indique que les stratégies concernent par défaut les ports non sécurisés. Vous pouvez modifier la valeur pour chaque stratégie.

ÉTAPE 3 Si nécessaire, cliquez sur **Ajouter** pour créer une stratégie Sécurité du premier saut.

ÉTAPE 4 Renseignez les champs suivants :

- **Policy Name** (Nom de la stratégie) : saisissez un nom de stratégie défini par l'utilisateur.
- **Confiance de port** : sélectionnez l'état de confiance de port de la stratégie :
  - *Hérité* : lorsque la stratégie est associée à un port, l'état n'est pas sécurisé.
  - *Validé* : lorsque la stratégie est associée à un port, l'état est sécurisé.

ÉTAPE 5 Cliquez sur **Appliquer** pour associer la stratégie.

ÉTAPE 6 Pour associer cette stratégie à une interface, cliquez sur **Associer la stratégie à l'interface**. Vous accédez à la page Association de stratégie (Port), qui vous permet d'associer cette stratégie à un port.

Association de stratégie (VLAN)

Pour associer une stratégie à un ou plusieurs VLAN :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut IPv6** > **Association de stratégie (VLAN)**.

Les stratégies qui sont déjà associées sont affichées sous forme de liste, avec le **Type de stratégie**, le **Nom de la stratégie** et la **Liste de VLAN**.

ÉTAPE 2 Pour associer une stratégie à un VLAN, cliquez sur **Ajouter** et renseignez les champs suivants :

- **Type de stratégie** : sélectionnez le type de stratégie à associer à l'interface.
- **Nom de la stratégie** : sélectionnez le nom de la stratégie à associer à l'interface.
- **Liste de VLAN** : sélectionnez les VLAN auxquels la stratégie est associée.

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

Association de stratégie (Port)

Pour associer une stratégie à un ou plusieurs ports ou LAG :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut IPv6** > **Association de stratégie (Port)**.

Les stratégies qui sont déjà associées sont affichées sous forme de liste, avec leur **Interface**, le **Type de stratégie**, le **Nom de la stratégie** et la **Liste de VLAN**.

ÉTAPE 2 Pour associer une stratégie à un port ou LAG, cliquez sur **Ajouter** et renseignez les champs suivants :

- **Interface** : sélectionnez l'interface à laquelle la stratégie sera associée.
- **Type de stratégie** : sélectionnez le type de stratégie à associer à l'interface. Présentation de la Sécurité du premier saut IPv6.
- **Nom de la stratégie** : sélectionnez le nom de la stratégie à associer à l'interface.
- **Liste de VLAN** : sélectionnez les VLAN auxquels la stratégie est associée.

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

Table de liaisons de voisins

Pour afficher les entrées de la table de liaisons de voisins :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut IPv6** > **Table de liaisons de voisins**.

ÉTAPE 2 Sélectionnez une des options d'effacement de table suivantes :

- **Statique uniquement** : efface toutes les entrées statiques de la table.

- **Dynamique uniquement** : efface toutes les entrées dynamiques de la table.
- **Dynamique et statique** : efface toutes les entrées statiques et dynamiques de la table.

Les champs suivants s'affichent pour chaque stratégie (seuls les champs de la page Add [Ajouter] sont affichés) :

- **Origine** : protocole ayant ajouté l'adresse IPv6 (uniquement disponible pour les entrées dynamiques) :
  - *Statique* : ajoutée manuellement.
  - *NDP* : apprise à partir des messages Neighbor Discovery Protocol.
  - *DHCP* : apprise à partir des messages du protocole DHCPv6.
- **État** : état de l'entrée :
  - *Tentative* : la nouvelle adresse IPv6 hôte est en cours de validation. Sa durée de vie étant inférieure à 1 seconde, son délai d'expiration n'est pas affiché.
  - *Valide* : l'adresse IPv6 hôte était liée.
- **Délai d'expiration (sec)** : temps restant en secondes avant la suppression de l'entrée si elle n'est pas confirmée.
- **Débordement TCAM** : les entrées marquées **No** (Non) n'ont pas été ajoutées à la mémoire TCAM en raison d'un débordement de TCAM.

ÉTAPE 3 Pour ajouter une stratégie, cliquez sur **Ajouter**, puis renseignez les champs suivants :

- **ID VLAN** : ID du VLAN de l'entrée.
- **Adresse IPv6** : adresse IPv6 source de l'entrée.
- **Interface** : port sur lequel le paquet est reçu.
- **Adresse MAC** : adresse MAC du voisin du paquet.

ÉTAPE 4 Cliquez sur **Appliquer** pour ajouter les paramètres au fichier de Configuration d'exécution.

Table des préfixes de voisins

Vous pouvez ajouter des préfixes statiques aux adresses IPv6 globales liées à partir de messages NDP dans la table des préfixes de voisins. Les entrées dynamiques font l'objet d'un apprentissage, comme décrit dans Apprentissage des préfixes IPv6 annoncés.

Pour ajouter des entrées à la table des préfixes de voisins :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut IPv6** > **Table des préfixes de voisins**.

ÉTAPE 2 Sélectionnez l'une des options ci-dessous dans le champ **Effacer la table** afin d'effacer la table des préfixes de voisins :

- **Static Only** (Statique uniquement) : efface uniquement les entrées statiques.
- **Dynamic Only** (Dynamique uniquement) : efface uniquement les entrées dynamiques.
- **All Dynamic & Static** (Dynamique et statique) : efface les entrées statiques et dynamiques.

ÉTAPE 3 Les champs suivants s'affichent pour les entrées existantes :

- **VLAN ID** (ID de VLAN) : VLAN sur lequel les préfixes sont pertinents.
- **IPv6 Prefix** (Préfixe IPv6) : préfixe IPv6.
- **Longueur du préfixe** : longueur du préfixe IPv6.
- **Origin** (Origine) : l'entrée est dynamique (apprise) ou statique (configurée manuellement).
- **Autoconfig** (Configuration automatique) : le préfixe peut être utilisé pour la configuration statique.
- **Expiry Time (Sec)** (Délai d'expiration [en s]) : laps de temps pendant lequel l'entrée est conservée avant sa suppression.

ÉTAPE 4 Cliquez sur **Ajouter** pour ajouter une nouvelle entrée à la table et renseignez les champs ci-dessus pour la nouvelle entrée.

État FHS

Pour afficher la configuration globale des fonctions Sécurité du premier saut (First Hop Security, FHS) :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut IPv6** > **État FHS**.

ÉTAPE 2 Sélectionnez un port, LAG ou VLAN pour lequel l'état FHS est indiqué.

ÉTAPE 3 Les champs suivants s'affichent pour l'interface sélectionnée :

- **État FHS**
  - *État FHS sur le VLAN actuel* : indique si la fonction FHS est activée sur le VLAN actuel.
  - *Journalisation des abandons de paquets* : indique si cette fonction est activée pour l'interface actuelle (au niveau de la configuration globale ou dans une stratégie associée à l'interface).
- **État de protection RA**
  - *RA Guard State on Current VLAN* (État de protection RA sur le VLAN actuel) : indique si la fonction Protection RA est activée sur le VLAN actuel.
  - *Rôle du périphérique* : rôle du périphérique RA.
  - *Managed Configuration Flag* (Drapeau de configuration gérée) : indique si la vérification du drapeau de configuration gérée est activée.
  - *Other Configuration Flag* (Autre drapeau de configuration) : indique si la vérification de l'autre drapeau de configuration est activée.
  - *Liste d'adresses RA* : liste d'adresses RA à mettre en correspondance.
  - *Liste de préfixes RA* : liste de préfixes RA à mettre en correspondance.
  - *Minimal Hop Limit* (Limite de saut minimale) : indique si la vérification de la limite de saut RA minimale est activée.
  - *Maximal Hop Limit* (Limite de saut maximale) : indique si la vérification de la limite de saut RA maximale est activée.
  - *Minimal Router Preference* (Préférence de routeur minimale) : indique si la vérification de la préférence de routeur minimale est activée.
  - *Maximal Router Preference* (Préférence de routeur maximale) : indique si la vérification de la préférence de routeur maximale est activée.

- **État de protection DHCPv6**
  - *DHCPv6 Guard State on Current VLAN* (État de protection DHCPv6 sur le VLAN actuel) : indique si la fonction Protection DHCPv6 est activée sur le VLAN actuel.
  - *Rôle du périphérique* : rôle du périphérique DHCP.
  - *Match Reply Prefixes* (Trouver préfixes de rép. correspondants) : indique si la vérification des préfixes de réponse DHCP est activée.
  - *Match Server Address* (Adresse du serveur) : indique si la vérification des adresses de serveur DHCP est activée.
  - *Préférence minimale* : indique si la vérification de la préférence minimale est activée.
  - *Maximal Preference* (Préférence maximale) : indique si la vérification de la préférence maximale est activée.
- **État de l'inspection ND**
  - *État d'inspection ND sur le VLAN actuel* : indique si la fonction Inspection ND est activée sur le VLAN actuel.
  - *Rôle du périphérique* : rôle du périphérique d'inspection ND.
  - *Abandonner non sûr* : indique si les messages non sûrs sont abandonnés.
  - *Niveau de sécurité minimal* : si les messages non sûrs ne sont pas éliminés, indique le niveau de sécurité minimal des paquets à transférer.
  - *Valider MAC source :* indique si la vérification d'adresse MAC source est activée.
- **État de la liaison de voisin**
  - *Neighbor Binding State on Current VLAN* (État de liaison de voisin sur le VLAN actuel) : indique si la fonction Liaison de voisin est activée sur le VLAN actuel.
  - *Device Role* (Rôle du périphérique) : rôle du périphérique Liaison de voisin.
  - *Logging Binding* (Liaison de journalisation) : indique si la journalisation des événements de la table de liaisons de voisins est activée.
  - *Address Prefix Validation (Validation de préfixe d'adresse)* : indique si la validation de préfixe d'adresse est activée.
  - *Global Address Configuration* (Configuration d'adresse globale) : indique les messages validés.

- *Max Entries per VLAN* (Entrées max par VLAN) : nombre maximal autorisé d'entrées de Table de liaisons de voisins dynamiques par VLAN.
- *Max Entries per Interface* (Entrées max par interface) : nombre maximal autorisé d'entrées de Table de liaisons de voisins par interface.
- *Max Entries per MAC Address* (Nombre d'entrées max. par adresse MAC) : nombre maximal autorisé d'entrées de Table de liaisons de voisins par adresse MAC.

• **État de la protection de la source IPv6 :**

- *IPv6 Source Guard State on Current VLAN* (État de la protection de la source IPv6 sur le VLAN actuel) : indique si la fonction Protection de la source IPv6 est activée sur le VLAN actuel.
- *Port Trust* (Confiance de port) : indique si le port est sécurisé et la manière dont il a reçu son état sécurisé.

Statistiques FHS

Pour afficher les statistiques FHS :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut IPv6** > **Statistiques FHS**.

ÉTAPE 2 Sélectionnez la fréquence d'actualisation dans **Fréq. d'actualisation**, c'est-à-dire le délai qui s'écoule avant l'actualisation des statistiques.

ÉTAPE 3 Les compteurs de débordement globaux suivants s'affichent :

- **Table de liaisons de voisins** : nombre d'entrées qui n'ont pas pu être ajoutées à cette table, car celle-ci a atteint sa taille maximale.
- **Neighbor Prefix Table (Table des préfixes de voisins)** : nombre d'entrées qui n'ont pas pu être ajoutées à cette table, car celle-ci a atteint sa taille maximale.
- **TCAM** : nombre d'entrées qui n'ont pas pu être ajoutées en raison d'un débordement de la mémoire TCAM.

ÉTAPE 4 Sélectionnez une interface ; les champs suivants s'affichent :

• **NDP (Neighbor Discovery Protocol) Messages** (Messages NDP [Neighbor Discovery Protocol]) : le nombre de messages **reçus** et **abandonnés** est affiché pour les types de messages suivants :

- *RA* : messages Router Advertisement

- *REDIR* : messages de redirection
- *NS* : messages Neighbor Solicitation
- *NA* : messages d'annonce de voisin
- *RS* : messages Router Solicitation

- **DHCPv6 Messages** (Messages DHCPv6) : le nombre de messages **reçus** et **abandonnés** est affiché pour les types de messages DHCPv6 suivants :
  - *ADV* : messages d'annonce
  - *REP* : messages de réponse
  - *REC* : messages de reconfiguration
  - *REL-REP* : messages de réponse de relais
  - *LEAS-REP* : messages de réponse de demande de location
  - *RLS* : messages validés
  - *DEC* : messages déclinés

Les champs suivants sont affichés dans la Table de messages abandonnés FHS.

- **Fonctionnalité** : type de message abandonné (Protection DHCPv6, Protection RA, etc.).
- **Nombre** : nombre de messages abandonnés.
- **Motif** : motif d'abandon des messages.

ÉTAPE 5 Cliquez sur **Effacer les compteurs globaux** pour effacer les compteurs de débordement globaux.

26

Contrôle d'accès

La fonction de liste de contrôle d'accès (ACL, Access Control List) fait partie intégrante du mécanisme de sécurité. Les définitions ACL permettent, entre autres, de définir les flux de trafic auxquels est attribuée une qualité de service (QoS) spécifique. Pour plus d'informations, reportez-vous à la section 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 l'appareil au niveau d'un port ou LAG disposant d'une ACL active sont soit acceptés, soit refusés.

Cette section contient les rubriques suivantes :

Présentation

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.

Les différents périphériques ne prennent pas tous en charge le même nombre d'ACL et d'ACE :

Appareil	Nombre max. d'ACL	Nombre max. d'ACE
SG550XG	2 000	2 000
Sx550X	3 000	3 000
SG350XG	2 000	2 000
SG350 et Sx350	1 000	1 000
Sx250	512	512

Jusqu'à 256 ACE peuvent être configurés sur un seul port ou dans une seule 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 explicitement ajouter les ACE dans l'ACL pour autoriser le trafic souhaité, y compris le trafic de gestion tel que Telnet, HTTP ou SNMP qui est dirigé vers l'appareil 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 la surveillance IGMP/MLD est activée sur un port associé à une ACL, ajoutez les filtres ACE dans l'ACL pour transférer les paquets IGMP/MLD vers l'appareil. Dans le cas contraire, la surveillance IGMP/MLD 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 seul ACL par port, à une exception près : il est possible d'associer à la fois une ACL basée sur IP et une ACL basée sur IPv6 à un port unique.

Pour associer plusieurs ACL à un port, vous devez utiliser une stratégie comportant un ou plusieurs mappages de classe.

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 à la section *Définition des ACL basées sur MAC*.
- ACL IP : examine la Couche 3 des trames IP, comme décrit à la section *ACL basées sur IPv4*.
- ACL IPv6 : examine la Couche 3 des trames IPv4, comme décrit à la section *Définition de l'ACL basée 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.

Journalisation ACL

Cette fonction permet l'ajout d'une option de journalisation aux modules ACE. Lorsque la fonction est activée, tout paquet autorisé ou refusé par l'ACE entraîne la génération d'un message d'information SYSLOG correspondant.

Si la journalisation ACL est activée, vous pouvez la spécifier pour chaque interface par liaison de l'ACL à l'interface concernée. Dans ce cas, des messages SYSLOG sont générés pour les paquets correspondant aux ACE d'autorisation ou de refus associés à l'interface.

Un flux est un flot de paquets possédant des caractéristiques identiques, par exemple :

- **Paquets de couche 2** : adresses MAC de source et de destination identiques
- **Paquets de couche 3** : adresses IP de source et de destination identiques
- **Paquets de couche 4** : port L4 et adresses IP de source et de destination identiques

Pour tout nouveau flux, le premier paquet intercepté à partir d'une interface spécifique entraîne la génération d'un message d'information SYSLOG. Les paquets supplémentaires issus du même flux sont interceptés par le processeur, mais les messages SYSLOG de ce flux se limitent à un message toutes les 5 minutes. Ce message SYSLOG indique qu'un paquet au moins a été intercepté au cours des 5 dernières minutes.

Une fois le paquet intercepté traité, les paquets sont acheminés en cas d'autorisation ou abandonnés en cas de refus.

Le nombre de flux pris en charge est défini ainsi :

- Gamme SG350xx : 150 par unité
- Gamme SG550XG : 150 par unité dans la pile

Messages SYSLOG

Les messages SYSLOG présentent le niveau de gravité Information. Ils indiquent si le paquet correspond à une règle de refus ou d'autorisation.

- Pour les paquets de couche 2, le SYSLOG inclut les informations suivantes (le cas échéant) : MAC source, MAC de destination, Ethertype, ID de VLAN et file d'attente CoS.
- Pour les paquets de couche 3, le SYSLOG inclut les informations suivantes (le cas échéant) : adresse IP source, adresse IP de destination, protocole, valeur DSCP, type ICMP, code ICMP, type IGMP.
- Pour les paquets de couche 4, le SYSLOG inclut les informations suivantes (le cas échéant) : port source, port de destination et indicateur TCP.

Voici des exemples de messages SYSLOG possibles :

- Pour un paquet non-IP :
  - 06-Jun-2013 09:49:56 %3SWCOS-I-LOGDENYMAC: gi0/1: deny ACE 00:00:00:00:00:01 -> ff:ff:ff:ff:ff:ff, Ethertype-2054, VLAN-20, CoS-4, trapped
- Pour un paquet IP (v4 et v6) :
  - 06-Jun-2013 12:38:53 %3SWCOS-I-LOGDENYINET: gi0/1: deny ACE IPv4(255) 1.1.1.1 -> 1.1.1.10, protocol-1, DSCP-54, ICMP Type-Echo Reply, ICMP code-5 , trapped
- Pour un paquet L4 :
  - 06-Jun-2013 09:53:46 %3SWCOS-I-LOGDENYINETPORTS: gi0/1: deny ACE IPv4(TCP) 1.1.1.1(55) -> 1.1.1.10(66), trapped

Configuration des ACL

Cette section décrit la façon de créer des ACL et d'y ajouter des règles (ACE).

Création d'un flux de travail d'ACL

Pour créer des ACL et les associer à une interface, procédez comme suit :

1. Créez un ou plusieurs des types d'ACL suivants :
    a. ACL basée sur MAC en utilisant la page ACL basée sur MAC et la page ACE basé sur MAC
    b. ACL basée sur IP en utilisant la page ACL basée sur IPv4 et la page ACE basé sur IPv4
    c. ACL basée sur IPv6 en utilisant la page ACL basée sur IPv6 et la page ACE basé sur IPv6
2. Associez l'ACL aux interfaces via la page Liaison ACL (VLAN) ou Liaison ACL (port).

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 :

1. Si l'ACL n'appartient pas à une « class-map » du mode avancé de QoS, mais qu'elle a été associée à une interface, supprimez sa liaison avec l'interface en utilisant la page Liaison ACL (VLAN) *ou* Liaison ACL (port).
2. Si l'ACL fait partie de la « class-map » et qu'elle n'est pas liée à une interface, vous pouvez la modifier.
3. 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 à l'aide de *Liaison de stratégies*.
    - Supprimez de la stratégie le plan de classe contenant l'ACL à l'aide de *Configuration d'une stratégie* (**Modifier**).
    - Supprimez le plan de classe contenant l'ACL à l'aide de *Définition d'un mappage de classes*.

À ce stade seulement vous pouvez modifier l'ACL, comme indiqué dans cette section.

Création 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.

Les ACL basées sur MAC sont définies sur la page ACL basée sur MAC. Leurs règles sont définies sur la page ACE basé sur MAC.

ACL basée sur MAC

Pour définir une ACL basée sur MAC :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACL basée sur MAC**.

Cette page affiche une liste de toutes les ACL basées sur MAC qui sont actuellement définies.

ÉTAPE 2 Cliquez sur **Ajouter**.

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 **Appliquer**. L'ACL basée sur MAC est consigné dans le fichier de Configuration d'exécution.

ACE basé sur MAC

REMARQUE Chaque règle basée sur MAC consomme une règle TCAM. Veuillez noter que l'allocation TCAM s'effectue par couples. De cette façon, pour le premier ACE, 2 règles TCAM sont allouées et la deuxième règle TCAM est allouée au ACE suivant, et ainsi de suite.

Pour ajouter des règles (ACE) à une ACL :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACE basé sur MAC**.

ÉTAPE 2 Sélectionnez une ACL et cliquez sur **Go**. Les ACE de l'ACL sont répertoriés.

ÉTAPE 3 Cliquez sur **Add**.

ÉTAPE 4 Saisissez les paramètres.

- **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 :
  - *Autoriser* : transfère les paquets qui répondent aux critères de l'ACE.
  - *Refuser* : abandonne les paquets qui répondent aux critères de l'ACE.
  - *Arrêter* : abandonne les paquets qui répondent aux critères de l'ACE et désactive le port à partir duquel les paquets ont été reçus. Ces ports peuvent être réactivés sur la page Paramètres de reprise après erreur.
- **Journalisation** : sélectionnez cette option pour activer les flux ACL correspondant à la règle ACL.
- **Période** : limite l'utilisation de l'ACL à une période spécifique.
- **Nom de période** : si l'option **Période** est sélectionnée, choisissez la période à utiliser. Les périodes sont définies dans la section Configuration de l'heure système.
- **Adresse MAC de destination** : sélectionnez *Indiffér.* si toutes les adresses de destination sont possibles ou *Défini par l'utilisateur* pour entrer une adresse de destination ou une plage d'adresses de destination.
- **Valeur de l'adresse MAC de destination** : saisissez l'adresse MAC avec laquelle l'adresse MAC de destination sera mise en correspondance et saisissez également, le cas échéant, son masque.
- **Destination MAC Wildcard Mask** : saisissez le masque pour définir une plage d'adresses MAC. Veuillez noter que ce masque est différent de ceux employés à d'autres fins comme un masque de sous-réseau. Dans le cas présent, définir un bit sur **1** signifie « ignorer cette valeur » ; définir un bit sur **0** signifie « masquer cette valeur ».

  REMARQUE Prenons l'exemple d'un masque de 0000 0000 0000 0000 0000 0000 1111 1111 (ce qui signifie que vous établissez une correspondance avec les bits égaux à 0, mais pas avec ceux égaux à 1). Vous devez convertir les 1 en un entier décimal et vous remplacez chaque ensemble de quatre zéros par 0. Dans cet exemple, étant donné que 1111 1111 = 255, le masque serait : 0.0.0.255.
- **Adresse MAC source** : sélectionnez *Indiffér.* si toutes les adresses source sont possibles ou *Défini par l'utilisateur* pour entrer une adresse source ou une plage d'adresses source.
- **Valeur de l'adresse MAC source** : saisissez l'adresse MAC avec laquelle l'adresse MAC source sera mise en correspondance et saisissez également, le cas échéant, son masque.
- **Source MAC Wildcard Mask** : saisissez le masque afin de définir une plage d'adresses MAC.

- **ID VLAN** : saisissez la partie ID VLAN de la balise VLAN à mettre en correspondance.
- **802.1p** : sélectionnez **Inclure** pour utiliser 802.1p.
- **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 **Appliquer**. L'ACE basé sur MAC est consigné dans le fichier de Configuration d'exécution.

Création 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)
- Ports source/de destination pour le trafic TCP/UDP
- Valeurs des balises pour les trames TCP
- Type et code ICMP et IGMP
- Adresses IP source/de destination (y compris les caractères génériques)
- Valeur de priorité DSCP/IP

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.

La page ACL basée sur IPv4 permet d'ajouter des ACL au système. Leurs règles sont définies sur la page ACE basé sur IPv4.

Vous pouvez définir les ACL basées sur IPv6 sur la page ACL basée sur IPv6.

ACL basée sur IPv4

Pour définir une ACL basée sur IPv4 :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACL basée sur IPv4**.

Cette page affiche toutes les ACL basées sur IPv4 actuellement définies.

ÉTAPE 2 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 **Appliquer**. L'ACL basée sur IPv4 est consigné dans le fichier de Configuration d'exécution.

ACE basé sur IPv4

REMARQUE Chaque règle basée sur IPv4 consomme une règle TCAM. Veuillez noter que l'allocation TCAM s'effectue par couples. De cette façon, pour le premier ACE, 2 règles TCAM sont allouées et la deuxième règle TCAM est allouée au ACE suivant, et ainsi de suite.

Pour ajouter des règles (ACE) à une ACL basée sur IPv4 :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACE basé sur IPv4**.

ÉTAPE 2 Sélectionnez une ACL et cliquez sur **Go**. Toutes les ACE IP actuellement définies pour l'ACL sélectionnée s'affichent.

ÉTAPE 3 Cliquez sur **Add**.

ÉTAPE 4 Saisissez les paramètres.

- **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 disponibles sont les suivantes :
  - *Autoriser* : transfère les paquets qui répondent aux critères de l'ACE.
  - *Refuser* : abandonne les paquets qui répondent aux critères de l'ACE.
  - *Arrêter* : abandonne le paquet qui répond aux critères de l'ACE et désactive le port auquel le paquet était adressé. Les ports sont réactivés à partir de la page Paramètres de reprise après erreur.

- **Journalisation** : sélectionnez cette option pour activer les flux ACL correspondant à la règle ACL.
- **Période** : limite l'utilisation de l'ACL à une période spécifique.
- **Nom de période** : si l'option **Période** est sélectionnée, choisissez la période à utiliser. Les périodes sont définies dans la section Configuration de l'heure système.
- **Protocole** : sélectionnez cette option pour créer un ACE basé sur un protocole ou un ID de protocole spécifique. Sélectionnez *Tout (IPv4)* pour accepter tous les protocoles IP. Sinon, sélectionnez l'un des protocoles suivants dans la liste déroulante **Selected from list** (Sélection sur liste) :
  - *ICMP* : Internet Control Message Protocol
  - *IGMP* : Internet Group Management Protocol
  - *IP in IP* : encapsulation IP in IP
  - *TCP* : Transmission Control Protocol
  - *EGP* : Exterior Gateway Protocol
  - *IGP* : Interior Gateway Protocol
  - *UDP* : User Datagram Protocol
  - *HMP* : Host Mapping Protocol
  - *RDP* : Reliable Datagram Protocol
  - *IDPR* : Inter-Domain Policy Routing Protocol
  - *IPV6* : tunnellisation IPv6 sur IPv4
  - *IPV6:ROUT* : fait correspondre les paquets appartenant à la route IPv6 sur IPv4 par le biais d'une passerelle
  - *IPV6:FRAG* : fait correspondre les paquets appartenant à l'en-tête de fragment IPv6 sur IPv4
  - *IDRP* : Inter-Domain Routing Protocol
  - *RSVP* : ReSerVation Protocol
  - *AH* : Authentication Header
  - *IPV6:ICMP* : Internet Control Message Protocol
  - *EIGRP* : Enhanced Interior Gateway Routing Protocol

- *OSPF* : Open Shortest Path First
- *IPIP* : IP in IP
- *PIM* : Protocol Independent Multicast
- *L2TP* : Layer 2 Tunneling Protocol
- *ISIS* : protocole spécifique à IGP
- *ID protocole de mise en correspondance* : au lieu de sélectionner le nom, saisissez l'ID du protocole.

- **Adresse IP source** : sélectionnez *Indiffér.* si toutes les adresses source sont acceptables ou *Défini par l'utilisateur* pour entrer une adresse source ou une plage d'adresses source.
- **Valeur de l'adresse IP source** : saisissez l'adresse IP avec laquelle l'adresse IP source sera mise en correspondance.
- **Source IP Wildcard Mask** : saisissez le masque pour définir une plage d'adresses IP. Veuillez noter que ce masque est différent de ceux employés à d'autres fins comme un masque de sous-réseau. Pour un bit, 1 indique d'ignorer cette valeur, 0 indique de masquer cette valeur.

  REMARQUE Prenons l'exemple d'un masque de 0000 0000 0000 0000 0000 0000 1111 1111 (ce qui signifie que vous établissez une correspondance avec les bits égaux à 0, mais pas avec ceux égaux à 1). Vous devez convertir les 1 en un entier décimal et vous remplacez chaque ensemble de quatre zéros par 0. Dans cet exemple, étant donné que 1111 1111 = 255, le masque serait : 0.0.0.255.
- **Adresse IP de destination** : sélectionnez *Indiffér.* si toutes les adresses de destination sont acceptables ou *Défini par l'utilisateur* pour entrer une adresse de destination ou une plage d'adresses de destination.
- **Valeur de l'adresse IP de destination** : saisissez l'adresse IP avec laquelle l'adresse IP de destination sera mise en correspondance.
- **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 from list (Unique dans la liste)* : sélectionnez un seul port TCP/UDP source avec lequel les paquets sont mis en correspondance. Ce champ n'est actif que si 800/6-TCP ou 800/17-UDP est sélectionné dans le menu déroulant Sélectionner dans la liste.

- *Unique par le numéro* : saisissez un seul port TCP/UDP source avec lequel les paquets sont mis en correspondance. Ce champ n'est actif que si 800/6-TCP ou 800/17-UDP est sélectionné dans le menu déroulant Sélectionner dans la liste.
- *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.

- **Port de destination** : sélectionnez l'une des valeurs disponibles. Elles sont identiques à celles du champ Source Port (Port source) décrit ci-dessus.

  REMARQUE vous devez spécifier le protocole IP de l'ACE avant de pouvoir entrer le port source et/ou de destination.

- **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.
- **Type de service** : type de service du paquet IP.
  - *Indiffér.* : tout type de service.
  - *DSCP en correspondance* : DSCP (Differentiated Serves Code Point) à mettre en correspondance.
  - *IP Precedence 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. Sélectionnez le type de message en fonction de son nom ou saisissez le numéro du type de message :
  - *Indiffér.* : tous les types de message sont acceptés.
  - *Select from list* : permet de sélectionner le type de message en fonction de son nom.
  - *Type ICMP de mise en correspondance* : numéro du type de message à utiliser afin de filtrer.
- **ICMP Code** : les messages ICMP peuvent disposer d'un champ de code indiquant comment gérer le message. Sélectionnez l'une des options suivantes pour indiquer si le filtrage s'effectuera en fonction de ce code :
  - *Indiffér.* : tous les codes sont acceptés.
  - *Défini par l'utilisateur* : saisissez un code ICMP à des fins de filtrage.

- **IGMP** : si l'ACL est basée sur IGMP, sélectionnez le type de message IGMP à utiliser afin de filtrer. Sélectionnez le type de message en fonction de son nom ou saisissez le numéro du type de message :
  - *Indifférent* : tous les types de message sont acceptés.
  - *Select from list* : permet de sélectionner le type de message en fonction de son nom.
  - *Type IGMP de mise en correspondance* : numéro du type de message qui sera utilisé pour filtrer.

ÉTAPE 5 Cliquez sur **Appliquer**. L'ACE basé sur IPv4 est consigné dans le fichier de Configuration d'exécution.

Création d'ACL basées sur IPv6

La page ACL basée sur IPv6 affiche les ACL IPv6 existantes, qui vérifient le trafic purement IPv6, et permet également d'en créer. Les ACL IPv6 ne vérifient pas les paquets IPv6 sur IPv4 ou ARP.

REMARQUE Les ACL sont également utilisées en tant qu'éléments de base pour les définitions de flux relatifs à la gestion de la QoS par flux.

ACL basée sur IPv6

Pour définir une ACL basée sur IPv6 :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACL basée sur IPv6**.

Cette fenêtre affiche la liste des ACL définies et leur contenu.

ÉTAPE 2 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 **Appliquer**. L'ACL basée sur IPv6 est consigné dans le fichier de Configuration d'exécution.

ACE basé sur IPv6

REMARQUE Chaque règle basée sur IPv6 consomme deux règles TCAM.

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACE basé sur IPv6**.

Cette fenêtre affiche les ACE (règles) d'une ACL spécifiée (groupe de règles).

ÉTAPE 2 Sélectionnez une ACL et cliquez sur **Go**. Toutes les ACE IP actuellement définies pour l'ACL sélectionnée s'affichent.

ÉTAPE 3 Cliquez sur **Add**.

ÉTAPE 4 Saisissez les paramètres.

- **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 disponibles sont les suivantes :
  - *Autoriser* : transfère les paquets qui répondent aux critères de l'ACE.
  - *Refuser* : abandonne les paquets qui répondent aux critères de l'ACE.
  - *Arrêter* : abandonne les paquets qui répondent aux critères de l'ACE et désactive le port auquel les paquets étaient adressés. Les ports sont réactivés à partir de la page Paramètres de reprise après erreur.
- **Journalisation** : sélectionnez cette option pour activer les flux ACL correspondant à la règle ACL.
- **Période** : limite l'utilisation de l'ACL à une période spécifique.
- **Nom de période** : si l'option **Période** est sélectionnée, choisissez la période à utiliser. Les périodes sont décrites dans la section Heure système.
- **Protocole** : sélectionnez cette option pour créer une ACE basée sur un protocole spécifique. Sélectionnez *Tout (IPv6)* pour accepter tous les protocoles IP.

  Sinon, sélectionnez l'un des protocoles suivants :
  - *TCP* : Transmission Control Protocol. Permet à deux hôtes de communiquer et d'échanger des flux de données. TCP garantit la livraison des paquets et également que les paquets sont 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).

Ou

- *ID protocole de mise en correspondance* : saisissez l'ID du protocole avec lequel établir la correspondance.

- **Adresse IP source** : sélectionnez *Indiffér.* si toutes les adresses source sont acceptables ou *Défini par l'utilisateur* pour entrer une adresse source ou une plage d'adresses source.
- **Valeur de l'adresse IP source** : saisissez l'adresse IP avec laquelle l'adresse IP source sera mise en correspondance et saisissez également, le cas échéant, son masque.
- **Source IP Prefix Length** : saisissez la longueur du préfixe de l'adresse IP source.
- **Adresse IP de destination** : sélectionnez *Indiffér.* si toutes les adresses de destination sont acceptables ou *Défini par l'utilisateur* pour entrer une adresse de destination ou une plage d'adresses de destination.
- **Valeur de l'adresse IP de destination** : saisissez l'adresse IP avec laquelle l'adresse MAC 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 from list (Unique dans la liste)* : sélectionnez un seul port TCP/UDP source avec lequel les paquets sont mis en correspondance. Ce champ n'est actif que si 800/6-TCP ou 800/17-UDP est sélectionné dans le menu déroulant Protocole IP.
  - *Single by number* (Unique par le numéro) : saisissez un seul port TCP/UDP source avec lequel les paquets sont mis en correspondance. Ce champ n'est actif que si 800/6-TCP ou 800/17-UDP est sélectionné dans le menu déroulant Protocole IP.
  - *Range* : sélectionnez une plage de ports source TCP/UDP avec lesquels le paquet est mis en correspondance.
- **Port de destination** : sélectionnez l'une des valeurs disponibles. Elles sont identiques à celles du champ **Port source** décrit ci-dessus.

  REMARQUE Vous devez spécifier le protocole IPv6 de l'ACL avant de pouvoir configurer le port source et/ou de destination.

- **Étiquette de flux** : Classe le trafic IPv6 en fonction d'un champ d'étiquette de flux IPv6. Il s'agit d'un champ de 20 bits qui fait partie de l'en-tête de paquet IPv6. Une étiquette de flux IPv6 peut être utilisée par une station source pour étiqueter un jeu de paquets appartenant au même flux. Sélectionnez *Indifférente* si toutes les étiquettes de flux sont acceptées ou *Définie par l'utilisateur* pour saisir une étiquette de flux spécifique qui sera acceptée par l'ACL.
- **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. Pour chaque type d'indicateur, sélectionnez l'une des options suivantes :
  - *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 de service** : type de service du paquet IP.
  - *Indiffér.* : tout type de service.
  - *DSCP en correspondance* : DSCP (Differentiated Serves Code Point) à mettre en correspondance.
  - *IP Precedence 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. Sélectionnez le type de message en fonction de son nom ou saisissez le numéro du type de message. Si tous les types de message sont acceptés, sélectionnez « *Indiffér.* ».
  - *Indiffér.* : tous les types de message sont acceptés.
  - *Sélectionner dans la liste* : permet de sélectionner le type de message en fonction de son nom dans la liste déroulante.
  - *Type ICMP de mise en correspondance* : numéro du type de message qui sera utilisé pour filtrer.

- **Code ICMP** : les messages ICMP peuvent disposer d'un champ de code indiquant comment gérer le message. Sélectionnez l'une des options suivantes pour indiquer si le filtrage s'effectuera en fonction de ce code :
  - *Indifférent* : tous les codes sont acceptés.
  - *Défini par l'utilisateur* : saisissez un code ICMP à des fins de filtrage.

ÉTAPE 5 Cliquez sur **Appliquer**.

Liaison ACL

Lorsqu'une ACL est liée à une interface (port, LAG ou VLAN), ses règles ACE sont appliquées aux paquets qui arrivent sur cette interface. Les paquets qui ne correspondent à aucune des règles ACE de l'ACL sont mis en correspondance avec une règle par défaut, dont l'action consiste à abandonner les paquets sans correspondance.

Bien que chaque interface ne puisse être liée qu'à une seule ACL, plusieurs interfaces peuvent être liées à la même ACL en les regroupant dans une « policy-map » (principes directeurs), puis en liant cette dernière à l'interface.

Une fois qu'une ACL est liée à une interface, elle ne peut être éditée, modifiée ou supprimée qu'une fois enlevée de tous les ports auxquels elle est liée ou sur lesquels elle est utilisée.

REMARQUE Il est possible de lier une interface (port, LAG ou VLAN) à une stratégie ou à une ACL, mais il est impossible de la lier à la fois à une stratégie et à une ACL.

REMARQUE Dans le même mappage de classe, une ACL MAC ne peut pas être utilisée avec une ACE IPv6 dont l'adresse IPv6 de destination est définie comme condition de filtrage.

Liaison ACL (VLAN)

Pour lier une ACL à un VLAN :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **Liaison ACL (VLAN)**.

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

Si le VLAN souhaité ne s'affiche pas, ajoutez-en un nouveau.

ÉTAPE 3 Sélectionnez l'une des options suivantes :

- **ACL basée sur MAC** : sélectionnez une ACL basée sur MAC à lier à l'interface.
- **ACL basée sur IPv4** : sélectionnez une ACL basée sur IPv4 à lier à l'interface.
- **ACL basée sur IPv6** : sélectionnez une ACL basée sur IPv6 à lier à l'interface.
- **Action par défaut** : sélectionnez l'une des options suivantes :
  - *Tout refuser* : si un paquet ne correspond pas à une ACL, il est refusé (rejeté).
  - *Tout autoriser* : si un paquet ne correspond pas à une ACL, il est autorisé (transmis).

  REMARQUE L'option Action par défaut ne peut être définie que si l'option Protection de la source IP n'est pas activée sur l'interface.

ÉTAPE 4 Cliquez sur **Appliquer**. La liaison ACL est modifiée et le fichier de Configuration d'exécution est mis à jour.

REMARQUE Si aucune ACL n'est sélectionnée, la ou les ACL précédemment liées au VLAN sont supprimées.

Liaison ACL (port)

Pour lier une ACL à un port ou un LAG :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **Liaison ACL (port)**.

ÉTAPE 2 Sélectionnez le type d'interface **Ports/LAG** (Port ou LAG).

ÉTAPE 3 Cliquez sur **Go**. Pour chaque type d'interface sélectionné, toutes les interfaces de ce type sont affichées avec la liste de leurs ACL actuelles (pour les **ACL d'entrée** et les **ACL de sortie**) :

- **Interface** : identifiant de l'interface sur laquelle l'ACL est définie.
- **ACL MAC** : les ACL de type MAC qui sont liées à l'interface (le cas échéant).
- **ACL IPv4** : les ACL de type IPv4 qui sont liées à l'interface (le cas échéant).
- **ACL IPv6** : les ACL de type IPv6 qui sont liées à l'interface (le cas échéant).
- **Action par défaut** : action des règles d'ACL (tout abandonner ou tout autoriser).

  REMARQUE Pour supprimer la liaison de toutes les ACL au niveau d'une interface, sélectionnez cette dernière puis cliquez sur **Clear**.

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

ÉTAPE 5 Saisissez les informations suivantes pour les ACL d'entrée et de sortie :

ACL d'entrée

- **ACL basée sur MAC** : sélectionnez une ACL basée sur MAC à lier à l'interface.
- **ACL basée sur IPv4** : sélectionnez une ACL basée sur IPv4 à lier à l'interface.
- **ACL basée sur IPv6** : sélectionnez une ACL basée sur IPv6 à lier à l'interface.
- **Action par défaut** : sélectionnez l'une des options suivantes :
  - *Tout refuser* : si un paquet ne correspond pas à une ACL, il est refusé (rejeté).
  - *Tout autoriser* : si un paquet ne correspond pas à une ACL, il est autorisé (transmis).

  REMARQUE L'option Action par défaut ne peut être définie que si l'option Protection de la source IP n'est pas activée sur l'interface.

ACL de sortie

- **ACL basée sur MAC** : sélectionnez une ACL basée sur MAC à lier à l'interface.
- **ACL basée sur IPv4** : sélectionnez une ACL basée sur IPv4 à lier à l'interface.
- **ACL basée sur IPv6** : sélectionnez une ACL basée sur IPv6 à lier à l'interface.
- **Action par défaut** : sélectionnez l'une des options suivantes :
  - *Tout refuser* : si un paquet ne correspond pas à une ACL, il est refusé (rejeté).
  - *Tout autoriser* : si un paquet ne correspond pas à une ACL, il est autorisé (transmis).

  REMARQUE L'option Action par défaut ne peut être définie que si l'option Protection de la source IP n'est pas activée sur l'interface.

ÉTAPE 6 Cliquez sur **Appliquer**. La liaison ACL est modifiée et le fichier de Configuration d'exécution est mis à jour.

REMARQUE Si aucune ACL n'est sélectionnée, la ou les ACL précédemment liées à l'interface sont supprimées.

27

Qualité de service

La fonction QoS (Quality of Service, qualité de service) est appliquée à l'ensemble du réseau pour garantir que le trafic réseau est géré en fonction des critères fixés et que les données voulues reçoivent un traitement préférentiel.

Cette section couvre les sujets suivants :

Fonctions et composants QoS

La fonction QoS permet d'optimiser les performances du réseau.

La QoS fournit les éléments suivants :

- Classification du trafic entrant en différentes classes sur la base d'attributs, notamment :
  - Configuration du périphérique
  - Interface d'entrée
  - Contenu des paquets
  - Combinaison de ces attributs

La QoS inclut :

- **Traffic Classification** : permet de marquer chaque paquet entrant comme appartenant à un flux de trafic spécifique, sur la base du contenu de ce paquet et/ou du port. Cette classification est réalisée à l'aide d'une liste de contrôle d'accès (ACL). Seul le trafic répondant aux critères de l'ACL est soumis à la classification CoS ou QoS.
- **Assignment to Software Queues** (Affectation à des files d'attente logicielles) : affecte les paquets entrants à des files d'attente de transfert. Les paquets sont envoyés à une file d'attente particulière pour gestion en tant que fonction de la classe de trafic à laquelle ils appartiennent. Reportez-vous à la section File d'attente.
- **Autre attribut de gestion de classe de trafic** : applique des mécanismes QoS à diverses classes, y compris la gestion de bande passante.

Fonctionnement de QoS

Vous pouvez entrer le type de champ d'en-tête auquel faire confiance sur la page Paramètres globaux. Pour chaque valeur de ce champ, une file d'attente de sortie est désignée, indiquant la file d'attente choisie pour l'envoi de la trame sur la page CoS/802.1p vers une file d'attente ou sur la page DSCP vers file d'attente (selon que le mode de confiance choisi est respectivement CoS/802.1p ou DSCP).

Modes QoS

Le mode de QoS sélectionné s'applique à toutes les interfaces du système.

- **Mode de base** : CoS (Class of Service, classe de service).

  Tout le trafic d'une même classe reçoit un traitement identique, à savoir l'action unique de QoS consistant à déterminer la file d'attente de sortie sur le port de sortie, ceci sur la base de la valeur QoS indiquée dans la trame entrante. Il peut s'agir de la valeur VPT (VLAN Priority Tag, balise de priorité VLAN) 802.1p en mode Couche 2 et de la valeur DSCP (Differentiated Service Code Point, point de code de service différencié) pour IPv4 ou de la valeur TC (Traffic Class, classe de trafic) pour IPv6 en mode Couche 3. Lorsqu'il fonctionne en mode de base, le périphérique considère cette valeur de QoS affectée en externe comme fiable. La valeur de QoS affectée en externe à un paquet détermine sa classe de trafic et la QoS.

  Vous pouvez entrer le champ d'en-tête auquel faire confiance sur la page Paramètres globaux. Pour chaque valeur de ce champ, une file d'attente de sortie est désignée dans laquelle la trame est envoyée sur la page CoS/802.1p vers une file d'attente ou sur la page DSCP vers file d'attente (selon que le mode de confiance choisi est respectivement CoS/802.1p ou DSCP).

- **Mode Avancé** : QoS (Quality of Service, qualité de service) pour chaque flux.

  En mode Avancé, la QoS de chaque flux est 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).

- **Mode Désactivé** : dans ce mode, tout le trafic est mappé sur une seule file d'attente de type « meilleur effort » (best effort) et aucun type de trafic n'est prioritaire sur les autres.

Vous ne pouvez activer qu'un seul mode à la fois. Lorsque le système est configuré pour fonctionner en mode de QoS avancé, les paramètres du mode de base de QoS sont inactifs, et inversement.

Lorsque vous changez de mode, les événements suivants se produisent :

- Lorsque vous passez du mode de QoS avancé à un autre mode, les définitions de profil de stratégie et les mappages de classe sont supprimés. Les ACL directement liées aux interfaces restent liées.
- Lorsque vous passez du mode de base de QoS au mode avancé, la configuration du mode de confiance QoS sur le mode De base n'est pas conservée.
- Lorsque vous désactivez la QoS, les paramètres de 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 QoS

Pour définir les paramètres de QoS généraux, procédez comme suit :

ÉTAPE 1 Choisissez le mode de QoS du système (Basic [De base], Advanced [Avancé] ou Disabled [Désactivé], comme décrit à la section « QoS Modes » [Modes de QoS]) via la page Propriétés de QoS. Les étapes de flux de travail suivantes décrites ici considèrent que vous avez choisi d'activer la QoS.

ÉTAPE 2 Attribuez à chaque interface une priorité CoS par défaut, via la page Propriétés de QoS.

ÉTAPE 3 Attribuez une méthode de planification (Strict Priority [Priorité stricte] ou WRR) et une valeur d'allocation de bande passante WRR aux files d'attente de sortie, via la page File d'attente.

ÉTAPE 4 Désignez une file d'attente de sortie pour chaque valeur IP DSCP/TC sur la page DSCP vers file d'attente. Si le périphérique fonctionne en mode de confiance DSCP, les paquets entrants sont placés dans les files d'attente de sortie en fonction de leur valeur DSCP/TC.

ÉTAPE 5 Associez une file d'attente de sortie à chaque priorité CoS/802.1p. Si le périphérique fonctionne en mode de confiance CoS/802.1, tous les paquets entrants sont placés dans les files d'attente de sortie prévues en fonction de la priorité CoS/802.1 des paquets. Utilisez pour cela la page CoS/802.1p vers une file d'attente.

ÉTAPE 6 Si nécessaire (uniquement pour le trafic de la Couche 3), affectez une file d'attente à chaque valeur DSCP/TC sur la page DSCP vers file d'attente.

ÉTAPE 7 Saisissez les limites de bande passante et de débit dans les pages suivantes :

a. Définissez le lissage en sortie par file d'attente sur la page Modelage de sortie par file d'attente.

b. Définissez la limite de vitesse d'entrée et le taux de lissage en sortie pour chaque port sur la page Bande passante.

ÉTAPE 8 Configurez le mode sélectionné en réalisant l'une des opérations suivantes :

a. Configurez le mode De base comme le décrit la section *Flux de travail de configuration du mode de base de QoS*

b. Configurez le mode avancé comme le décrit la section *Flux de travail de configuration du mode de QoS avancé*.

Flux de travail de QoS

Pour définir les paramètres de QoS généraux, procédez comme suit :

ÉTAPE 1 Activez QoS dans la page Propriétés QoS pour sélectionner le mode de confiance. Activez ensuite QoS sur les ports dans la page Paramètres d'interface.

ÉTAPE 2 Attribuez à chaque interface une priorité CoS ou DSCP par défaut, via la page Propriétés de QoS.

ÉTAPE 3 Attribuez une méthode de planification (Priorité stricte ou WRR) et une valeur d'allocation de bande passante WRR aux files d'attente de sortie, via la page File d'attente.

ÉTAPE 4 Désignez une file d'attente de sortie pour chaque valeur IP DSCP/TC sur la page DSCP vers la file d'attente. Si le périphérique fonctionne en mode de confiance DSCP, les paquets entrants sont placés dans les files d'attente de sortie en fonction de leur valeur DSCP/TC.

ÉTAPE 5 Associez une file d'attente de sortie à chaque priorité CoS/802.1p. Si le périphérique fonctionne en mode de confiance CoS/802.1, tous les paquets entrants sont placés dans les files d'attente de sortie prévues en fonction de la priorité CoS/802.1 des paquets. Pour ce faire, utilisez la page CoS/802.1p vers file d'attente.

ÉTAPE 6 Saisissez les limites de bande passante et de débit dans les pages suivantes :

a. Définissez le lissage en sortie pour chaque file d'attente sur la page Modelage de sortie par file d'attente.

b. Définissez la limite de vitesse d'entrée et le taux de lissage en sortie pour chaque port sur la page Bande passante.

Général

Cette section couvre les sujets suivants :

- Propriétés de QoS
- File d'attente
- CoS/802.1p vers une file d'attente
- DSCP vers file d'attente
- Bande passante
- Modelage de sortie par file d'attente
- Limite de débit d'entrée VLAN
- iSCSI
- Évitement des congestions TCP

Propriétés de QoS

La rubrique Propriétés de QoS contient des champs permettant de définir le mode de QoS du système (De base, Avancé ou Désactivé, comme le décrit la section “Modes QoS”).

Pour activer la QoS et sélectionner le mode de QoS, procédez comme suit :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Propriétés de QoS**.

ÉTAPE 2 Définissez le mode QoS. Les options suivantes sont disponibles :

- **Désactiver** : QoS est désactivé sur le périphérique.
- **De base** : QoS est activé sur le périphérique en mode De base.
- **Avancé** : QoS est activé sur le périphérique en mode Avancé.

ÉTAPE 3 Sélectionnez **Port/LAG** et cliquez ensuite sur **Ok** pour afficher/modifier tous les ports/LAG sur le périphérique, ainsi que leurs informations de CoS.

Les champs suivants sont affichés pour tous les ports/LAG :

- **Interface** : type de l'interface.

- **CoS par défaut** : Valeur VPT par défaut pour les paquets entrants qui ne possèdent pas de balise VLAN. La valeur CoS par défaut est 0. La valeur par défaut s'applique seulement aux trames non balisées et uniquement lorsque le système fonctionne en mode De base et que l'option CoS de confiance est sélectionnée sur la page Paramètres globaux.

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

Pour définir une QoS sur une interface, sélectionnez-la et cliquez sur **Modifier**.

ÉTAPE 1 Saisissez les paramètres.

- **Interface** : sélectionnez le port ou LAG.
- **CoS par défaut** : sélectionnez la valeur de CoS (Class-of-Service, classe de service) à affecter aux paquets entrants qui ne possèdent pas de balise VLAN.

ÉTAPE 2 Cliquez sur **Appliquer**. La valeur CoS par défaut de l'interface est enregistrée dans le fichier de Configuration d'exécution.

Pour restaurer les valeurs CoS par défaut, cliquez sur **Restaurer les valeurs CoS par défaut**.

File d'attente

L'appareil prend en charge 8 files d'attente par interface. La file d'attente 8 est celle qui dispose de la priorité la plus élevée. La file d'attente 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 et WRR (Weighted Round Robin, technique du tourniquet pondéré).

- **Priorité stricte** : le trafic sortant émanant de la file d'attente de priorité la plus élevée est transmis en premier. Le trafic des files d'attente de priorité(s) plus faible(s) n'est traité qu'après transmission des files d'attente de priorité(s) supérieure(s), ce qui donne le niveau de priorité le plus élevé au trafic de la file d'attente portant le numéro le plus élevé.
- **Weighted Round Robin (WRR)** : en mode WRR, le nombre de paquets envoyés depuis la file d'attente est proportionnel à la pondération de cette file d'attente (plus la pondération est élevée, plus le nombre de trames transmises est important). Par exemple, s'il y a un maximum de quatre files d'attente possible et qu'elles sont toutes de type WRR et que les pondérations par défaut sont appliquées, la file d'attente 1 reçoit 1/15 de la bande passante (en supposant que toutes les files d'attente sont saturées et qu'il y a encombrement), la file d'attente 2 en reçoit 2/15, la file d'attente 3 en reçoit 4/15 et la file d'attente 4 reçoit 8/15 de la bande passante. Le type d'algorithme WRR utilisé sur le périphérique n'est pas l'algorithme standard DWRR (Deficit WRR, WRR avec déficit) mais l'algorithme SDWRR (Shaped Deficit WRR, WRR avec déficit lissé).

Vous sélectionnez les modes de mise en file d'attente dans la page File d'attente. Lorsque 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 parcelle dont la priorité est la plus élevée, puis en passant à la file d'attente de niveau immédiatement inférieur à la fin du traitement de chaque file.

Lorsque la mise en file d'attente est de type WRR (Weighted Round Robin), chaque file d'attente est traitée jusqu'à ce que son quota soit atteint. Le système passe ensuite à une autre file d'attente.

Il est également possible d'affecter une WRR à certaines des files d'attente de priorité plus faible tout en maintenant le traitement Priorité stricte pour des files d'attente de niveau(x) plus élevé(s). Dans ce cas, le trafic des files d'attente à priorité stricte est toujours envoyé avant celui des files d'attente WRR. Le trafic des files d'attente WRR n'est transféré que lorsque les files d'attente à priorité stricte sont vides. (La portion relative en provenance de chaque file d'attente WRR dépend de sa pondération.)

Pour sélectionner la méthode de priorité et entrer les données WRR :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **File d'attente**.

ÉTAPE 2 Saisissez les paramètres.

- **Queue** : affiche le numéro de la file d'attente.
- **Méthode de planification** : 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). Cette division ne s'applique que si les files d'attente à priorité stricte sont vides.
  - *Pondération WRR* : si vous choisissez WRR, saisissez la pondération WRR attribuée à la file d'attente.
  - *% de bande passante WRR* : affiche la quantité de bande passante affectée à la file d'attente. Ces valeurs représentent un pourcentage de la pondération WRR.

ÉTAPE 3 Cliquez sur **Appliquer**. Les files d'attente sont configurées et le fichier de Configuration d'exécution est mis à jour.

CoS/802.1p vers une file d'attente

La page CoS/802.1p vers file d'attente mappe des priorités 802.1p sur des files d'attente de sortie. La table CoS/802.1p vers file d'attente détermine les files d'attente de sortie des paquets entrants sur la base de la priorité 802.1p figurant dans leurs balises VLAN. Pour les paquets entrants non balisés, la priorité 802.1p utilisée est la priorité CoS/802.1p par défaut affectée aux ports d'entrée.

Le tableau suivant décrit le mappage par défaut lorsque 8 files d'attente sont utilisées :

Valeurs 802.1p (0 à 7, 7 étant la valeur la plus élevée)	File d'attente (8 files numérotées de 1 à 8, 8 est la priorité la plus élevée)	7 files d'attente : (8 est la priorité la plus élevée utilisée pour contrôler le trafic de pile) Pile	Notes
0	1	1	Arrière-plan
1	2	1	Meilleur effort
2	3	2	Excellent effort
3	6	5	Application critique - SIP pour téléphone LVS
4	5	4	Vidéo
5	8	7	Voix - Valeur par défaut de téléphone IP Cisco
6	8	7	Contrôle de l’interfonctionnement RTP pour téléphone LVS
7	7	6	Contrôle du réseau

En modifiant le mappage CoS/802.1p vers file d'attente (CoS/802.1p vers file d'attente), et la méthode de planification des files d'attente ainsi que l'allocation de la bande passante (page File d'attente), il est possible d'obtenir la qualité de service voulue sur un réseau.

Le mappage CoS/802.1p à file d'attente s'applique uniquement si l'une des conditions suivantes est remplie :

- Le périphérique est en mode de base de QoS et en mode de confiance CoS/802.1p
- Le périphérique est en mode de QoS avancé et les paquets appartiennent à des flux en mode de confiance CoS/802.1p

La file d'attente 1 est celle qui dispose de la priorité la plus basse, tandis que la priorité la plus élevée est affectée à la file d'attente 8 des gammes 350 et 550.

Pour mapper des valeurs de CoS sur des files d'attente de sortie :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **CoS/802.1p vers file d'attente**.

ÉTAPE 2 Saisissez les paramètres.

- **802.1p** : affiche les valeurs de balise de priorité 802.1p à affecter à une file d'attente de sortie, où 0 est la priorité la plus faible et 7 la plus élevée.
- **Output Queue** : sélectionnez la file d'attente de sortie sur laquelle la priorité 802.1p est mappée. Le système prend en charge quatre ou huit files d'attente de sortie, parmi lesquelles la File d'attente 4 ou 8 dispose de la priorité la plus élevée et la File d'attente 1 de la priorité la plus faible.

ÉTAPE 3 Pour chaque priorité 802.1p, sélectionnez la file d'attente de sortie sur laquelle elle est mappée.

ÉTAPE 4 Cliquez sur **Appliquer, Annuler** ou **Restaurer déf.** Les valeurs de priorité 801.1p vers les files d'attente sont mappées et le fichier de configuration d'exécution est mis à jour. Les modifications saisies sont annulées ou les valeurs préalablement définies sont restaurées.

DSCP vers file d'attente

La page DSCP (IP Differentiated Services Code Point, point de code de service différencié IP) vers file d'attente mappe des valeurs DSCP vers des files d'attente de sortie. La table DSCP vers file d'attente détermine la file d'attente de sortie des paquets IP entrants sur la base de leur valeur DSCP. La valeur VPT (VLAN Priority Tag, marquage de priorité VLAN) du paquet reste inchangée.

En modifiant simplement le mappage DSCP vers file d'attente, la méthode de planification des files d'attente ainsi que l'allocation de bande passante, il est possible d'obtenir la qualité de service voulue sur un réseau.

Le mappage DSCP à file d'attente s'applique aux paquets IP si :

- Le périphérique est en mode QoS de base et DSCP est en mode de confiance ;
- le périphérique est en mode de QoS avancé et les paquets appartiennent à des flux en mode de confiance DSCP.

Les paquets non IP sont toujours classifiés comme appartenant à la file d'attente Meilleur effort (Best effort).

Le tableau suivant décrit le mappage DSCP vers file d'attente par défaut pour un système à 8files d'attente, dans lequel la file d'attente 7 a la priorité la plus élevée et la file d'attente 8 est utilisée à des fins de contrôle de pile.

DSCP	63	55	47	39	31	23	15	7
File d'attente	6	6	7	5	4	3	2	1
DSCP	62	54	46	38	30	22	14	6
File d'attente	6	6	7	5	4	3	2	1
DSCP	61	53	45	37	29	21	13	5
File d'attente	6	6	7	5	4	3	2	1
DSCP	60	52	44	36	28	20	12	4
File d'attente	6	6	7	5	4	3	2	1
DSCP	59	51	43	35	27	19	11	3
File d'attente	6	6	7	5	4	3	2	1
DSCP	58	50	42	34	26	18	10	2
File d'attente	6	6	7	5	4	3	2	1
DSCP	57	49	41	33	25	17	9	1
File d'attente	6	6	7	5	4	3	2	1
DSCP	56	48	40	32	24	16	8	0
File d'attente	6	6	6	7	6	6	1	1

Les tableaux suivants décrivent le mappage DSCP vers file d'attente par défaut pour un

système à 8 files d'attente où 8 est la valeur la plus élevée :

DSCP	63	55	47	39	31	23	15	7
File d'attente	7	7	8	6	5	4	3	1
DSCP	62	54	46	38	30	22	14	6
File d'attente	7	7	8	6	5	4	3	1
DSCP	61	53	45	37	29	21	13	5
File d'attente	7	7	8	6	5	4	3	1
DSCP	60	52	44	36	28	20	12	4
File d'attente	7	7	8	6	5	4	3	1
DSCP	59	51	43	35	27	19	11	3
File d'attente	7	7	8	6	5	4	3	1
DSCP	58	50	42	34	26	18	10	2
File d'attente	7	7	8	6	5	4	3	1
DSCP	57	49	41	33	25	17	9	1
File d'attente	7	7	8	6	5	4	3	1
DSCP	56	48	40	32	24	16	8	0
File d'attente	7	7	7	8	7	7	1	2

Pour mapper DSCP à des files d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **DSCP vers file d'attente**.

La page DSCP vers file d'attente contient **DSCP d'entrée**. Il affiche la valeur DSCP du paquet entrant et la classe associée.

ÉTAPE 2 Sélectionnez la **file d'attente de sortie** (file d'attente de transfert du trafic) sur laquelle la valeur DSCP est mappée.

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

Bande passante

La page Bande passante affiche les informations de bande passante de chaque interface.

Pour afficher les informations relatives à la bande passante, procédez comme suit :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Bande passante**.

Les champs de cette page sont décrits sur la page Modifier ci-dessous, sauf les champs suivants :

- **Limite de débit d'entrée :**
  - *État* : indique si la limite de débit d'entrée est activée.
  - *Limite de débit (Kbit/s)* : affiche la limite de débit d'entrée du port.
  - *%* : indique la limite de débit d'entrée pour le port divisée par la bande passante totale du port.
  - *CBS (octets)* : taille de rafale maximale de données de l'interface d'entrée, en octets.
- **Taux de modelage en sortie :**
  - *État* : indique si le taux de modelage en sortie est activé.
  - *CIR (Kbit/s)* : affiche la bande passante maximale de l'interface de sortie.
  - *CBS (octets)* : taille de rafale maximale de données de l'interface de sortie, en octets.

ÉTAPE 2 Sélectionnez une interface et cliquez sur **Edit**.

ÉTAPE 3 Sélectionnez le **port ou l'interface LAG**.

ÉTAPE 4 Remplissez les champs pour l'interface sélectionnée :

- **Limite de débit d'entrée** : sélectionnez cette option pour activer la limite de débit d'entrée, que vous définissez ensuite dans le champ situé au-dessous. (Cela ne concerne pas les LAG.)
- **Limite de débit d'entrée (Kbit/s)** : saisissez la bande passante maximale autorisée sur l'interface. (Cela ne concerne pas les LAG.)
- **Taille de rafale garantie (CBS)** : saisissez la taille maximale de rafale de données de l'interface d'entrée, en octets de données. Cette quantité de données peut être envoyée même si cela provoque un dépassement temporaire de la limite de la bande passante autorisée. Ce champ est disponible uniquement si l'interface est un port. (Cela ne concerne pas les LAG.)
- **Taux de lissage en sortie (egress shaping)** : sélectionnez cette option pour activer le lissage en sortie (egress shaping) sur le port.
- **Débit minimal garanti (CIR)** : saisissez la quantité maximale de bande passante de l'interface de sortie.
- **Taille de rafale garantie en sortie (CBS)** : saisissez la taille maximale de rafale de données de l'interface de sortie, en octets de données. Cette quantité de données peut être envoyée même si cela provoque un dépassement temporaire de la limite de la bande passante autorisée.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres de bande passante sont écrits dans le fichier de Configuration d'exécution.

Modelage de sortie par file d'attente

Outre la limitation du débit de transmission de chaque port, que vous configurez dans la page Bande passante, le périphérique peut limiter le débit de transmission des trames en sortie sélectionnées pour chaque file d'attente et pour chaque port. La limitation du débit en sortie est réalisée par mise en forme de la charge de sortie.

Le périphérique limite toutes les trames, à l'exception des trames de gestion. Toutes les trames non limitées sont ignorées dans le calcul du débit, ce qui signifie que leur taille n'est pas incluse dans la limite totale.

Vous pouvez désactiver le lissage (shaping) du débit en sortie pour chaque file d'attente.

Pour définir la mise en forme en sortie pour chaque file d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Modelage de sortie par file d'attente**.

La page Modelage de sortie par file d'attente affiche la limite de débit et la taille de rafale applicables à chaque file d'attente.

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

ÉTAPE 3 Sélectionnez un port/LAG et cliquez sur **Modifier**.

Cette page vous permet de lisser la sortie pour un maximum de huit files d'attente sur chaque interface.

ÉTAPE 4 Sélectionnez l'**interface** voulue.

ÉTAPE 5 Pour chacune des files d'attente nécessaires, remplissez les champs suivants :

- **Activer le lissage** : sélectionnez cette option pour activer le modelage en sortie sur cette file d'attente.
- **Débit minimal garanti (CIR)** : saisissez le débit maximal (CIR) en kilobits par seconde (kbit/s). Le CIR est la quantité maximale moyenne de données pouvant être envoyée.
- **Taille de rafale garantie (CBS)** : saisissez la taille maximale de rafale (CBS), en octets. Le CBS indique la taille maximale de rafale de données dont l'envoi est autorisé même si cela dépasse le CIR.

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

Limite de débit d'entrée VLAN

La limitation du débit pour chaque VLAN, que vous réalisez sur la page Limite de débit d'entrée VLAN, permet de limiter le trafic sur les VLAN. Lorsque vous configurez des limites de débit d'entrée VLAN, cela limite le trafic agrégé de tous les ports du périphérique.

Les contraintes suivantes s'appliquent à la limitation du débit pour chaque VLAN :

- La priorité est inférieure à celle de toute autre stratégie de trafic définie dans le système. 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.

- Cela s'applique au niveau du périphérique et dans le périphérique au niveau du processeur de paquets. S'il y a plusieurs processeurs de paquets sur le périphérique, la valeur limite de débit configurée sur le VLAN est appliquée à chacun des processeurs de paquets, de manière indépendante. Les périphériques présentant jusqu'à 24 ports possèdent un seul processeur de paquets, tandis que les périphériques de 48 ports ou plus possèdent deux processeurs de paquets.

La limitation de débit est calculée séparément pour chaque processeur de paquets dans une unité et pour chaque unité dans une pile.

Pour définir la limite de débit d'entrée VLAN :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Limite de débit d'entrée VLAN**.

Cette page affiche la table des limites de débit d'entrée VLAN.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez les paramètres.

- **VLAN ID** : sélectionnez un VLAN.
- **Committed Information Rate (CIR)** (Débit minimal garanti [CIR]) : saisissez la quantité moyenne maximale de données qui peut être acceptée sur le VLAN, en kilobits par seconde.
- **Taille de rafale garantie (CBS)** : saisissez la taille maximale de rafale de données de l'interface de sortie, en octets. Cette quantité de données peut être envoyée même si cela provoque un dépassement temporaire de la limite de la bande passante autorisée. Cette valeur ne peut pas être saisie pour un LAG.

ÉTAPE 4 Cliquez sur **Appliquer**. La limite de débit VLAN est ajoutée et le fichier de Configuration d'exécution est mis à jour.

iSCSI

Cette page active l'optimisation iSCSI, laquelle consiste à configurer un mécanisme afin de donner la priorité au trafic iSCSI par rapport à d'autres types de trafic. Si cette fonctionnalité est activée sur un périphérique, le trafic iSCSI transitant sur une interface se voit attribuer la priorité définie. De plus, ce trafic n'est pas soumis aux règles de politique ou ACL définies sur l'interface.

Le trafic iSCSI est identifié par le port TCP sur lequel les cibles iSCSI écoutent les demandes et éventuellement par l'adresse IPv4 sur laquelle ces mêmes cibles écoutent les demandes. Deux flux iSCSI IPv4 avec des ports TCP 3260 et 860 bien connus sont définis par défaut sur le périphérique. L'optimisation du flux iSCSI est bidirectionnelle, ce qui signifie qu'elle est appliquée aux flux dans les deux sens : en provenance et en direction des cibles.

Pour activer et configurer le mécanisme de hiérarchisation et, éventuellement, de marquage du trafic iSCSI :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **iSCSI**.

ÉTAPE 2 Renseignez les champs suivants :

- **État iSCSI** : sélectionnez cette option pour activer le traitement du trafic iSCSI sur le périphérique.
- **Affectation VPT** : sélectionnez **Non modifié** pour laisser la valeur VPT (VLAN Priority Tag) dans le paquet ou saisissez une nouvelle valeur dans le champ **Réaffecté**.
- **DSCP Assignment (Affectation DSCP)** : sélectionnez **Unchanged (Non modifié)** pour laisser la valeur DSCP dans le paquet ou saisissez une valeur dans le champ **Reassigned (Réaffecté)**.
- **Queue Assignment (Affectation de file d'attente)** : saisissez l'affectation de file d'attente pour le trafic iSCSI. Par défaut, ce trafic est affecté à la file d'attente 7.

ÉTAPE 3 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Le tableau des flux iSCSI affiche les différents flux iSCSI qui ont été définis. Deux flux iSCSI, avec les ports TCP 3260 et 860, sont affichés. Le **Type de flux** de ces flux est défini sur **Par défaut**. Si vous ajoutez un nouveau flux, son **Type de flux** est **Statique**.

Pour ajouter un nouveaux flux :

ÉTAPE 4 Cliquez sur **Ajouter**, puis renseignez les champs suivants :

- **Port TCP** : il s'agit du numéro de port TCP sur lequel la cible iSCSI écoute les demandes. Vous pouvez configurer jusqu'à 8 ports TCP cibles sur le commutateur.
- **Adresse IP cible** : indique l'adresse IP de la cible iSCSI (où les données sont stockées). Il s'agit également de la source du trafic iSCSI. Vous pouvez sélectionner **Tout** pour définir un flux en fonction du paramètre de port TCP ou saisir une adresse IP dans le champ **Défini par l'utilisateur** pour définir une adresse cible spécifique.

ÉTAPE 5 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Cliquez sur **Restaurer les flux par défaut** pour restaurer les flux par défaut.

Évitement des congestions TCP

La page Évitement de l'encombrement TCP vous permet d'activer un algorithme d'évitement de l'encombrement TCP. Cet algorithme casse ou évite la synchronisation TCP globale sur un nœud encombré lorsque 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 **Qualité de service** > **Général** > **Évitement des congestions TCP**.

ÉTAPE 2 Cliquez sur **Activer** pour activer l'évitement des congestions TCP, puis cliquez sur **Appliquer**.

Mode de base de QoS

Cette section couvre les sujets suivants :

- Vue d'ensemble
- Paramètres globaux
- Paramètres d'interface

Vue d'ensemble

En mode de base de QoS, vous pouvez définir un domaine spécifique du réseau en tant que domaine de confiance. Dans ce domaine, les paquets sont marqués avec la priorité 802.1p et/ou DSCP afin de signaler le type de service qu'ils nécessitent. Les nœuds du domaine utilisent ces champs pour affecter les paquets à une file d'attente de sortie spécifique. La classification initiale des paquets et le marquage de ces champs s'effectuent dans les données d'entrée du domaine validé.

Flux de travail de configuration du mode de base de QoS

Pour configurer le mode de base de QoS, procédez comme suit :

1. Sélectionnez le mode De base pour le système sur la page Propriétés de QoS.
2. Sélectionnez le comportement de confiance par l'intermédiaire de la page Paramètres globaux. Le périphérique prend en charge le mode de confiance CoS/802.1p et le mode de confiance 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.

S'il existe un port qui fait exception et ne doit pas faire confiance au marquage CoS entrant, désactivez l'état de QoS sur ce port à l'aide de la page Paramètres d'interface.

Activez ou désactivez le mode de confiance sélectionné au niveau global sur les divers ports via la page Paramètres d'interface. 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 de confiance sur les ports où les valeurs CoS/802.1p et/ou DSCP des paquets entrants ne sont pas dignes de confiance. Dans le cas contraire, cela peut avoir un impact négatif sur les performances de votre réseau.

Paramètres globaux

La page Paramètres globaux contient des informations concernant l'activation du mode de confiance sur l'appareil (reportez-vous au champ Mode de confiance ci-dessous). Cette configuration est active lorsque le mode de QoS est De base. Les paquets entrant dans un domaine QoS sont classifiés à la bordure du domaine QoS.

Pour définir la configuration de mode de confiance :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de base de QoS** > **Paramètres globaux**.

ÉTAPE 2 Sélectionnez le **Mode de confiance** à appliquer lorsque le périphérique est en mode De base. Si le niveau de CoS et la balise DSCP d'un paquet sont mappés sur des files d'attente distinctes, le mode de confiance détermine la file d'attente à laquelle ce paquet doit être affecté :

- **CoS/802.1p** : le trafic est mappé sur des files d'attente en fonction du champ VPT 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). Configurez le mappage VPT vers la file d'attente réelle sur la page CoS/802.1p vers la file d'attente.
- **DSCP** : tout le trafic IP est mappé sur des files d'attente en fonction du champ DSCP de l'en-tête IP. Vous pouvez configurer le mappage DSCP vers file d'attente sur la page DSCP vers file d'attente. Si le trafic n'est pas de type IP, il est mappé sur la file d'attente de meilleur effort.
- **CoS/802.1p-DSCP** : CoS/802.1p ou DSCP, selon l'option que vous avez sélectionnée.

ÉTAPE 3 Sélectionnez **Remplacer DSCP d'entrée** pour remplacer les valeurs DSCP d'origine des paquets entrants par celles saisies dans la table de substitution DSCP. Lorsque la fonction Remplacer DSCP d'entrée est activée, l'appareil utilise les nouvelles valeurs DSCP pour la mise en file d'attente des données en sortie. Il remplace également les valeurs DSCP d'origine figurant dans les paquets par les nouvelles valeurs DSCP.

REMARQUE La trame est mappée sur une file d'attente en sortie à l'aide de la nouvelle valeur réécrite et non de la valeur DSCP d'origine.

ÉTAPE 4 Si vous avez activé l'option **Remplacer DSCP d'entrée**, cliquez sur **Table de substitution DSCP** pour reconfigurer le DSCP. (Voir **Table de substitution DSCP**).

ÉTAPE 5 **DSCP en entrée** affiche la valeur DSCP du paquet entrant qui doit à nouveau être marqué d'une autre valeur. Sélectionnez la valeur **DSCP en sortie** pour indiquer que la valeur sortante est mappée.

ÉTAPE 6 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour avec les nouvelles valeurs DSCP.

Paramètres d'interface

La page Paramètres d'interface vous permet de configurer la QoS sur chaque port du périphérique, comme suit :

- **QoS désactivée sur l'interface** : tout le trafic entrant sur le port est mappé sur la file d'attente Meilleur effort (Best effort) et aucune classification/attribution de priorité n'est effectuée.
- **QoS activée sur le port** : le trafic d'entrée sur le port reçoit un ordre de priorité qui dépend du mode de confiance configuré à l'échelle du système, à savoir CoS/802.1p ou DSCP.

Pour entrer les paramètres de QoS de chaque interface :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de base de QoS** > **Paramètres d'interface**.

ÉTAPE 2 Sélectionnez **Port** ou **LAG** pour afficher la liste des ports ou LAG.

État de QoS indique si la QoS est activée sur l'interface.

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

ÉTAPE 4 Sélectionnez le **port** ou l'interface **LAG**.

ÉTAPE 5 Cliquez pour activer ou désactiver l'**état de QoS** pour cette interface.

ÉTAPE 6 Cliquez sur **Appliquer**. Le fichier de configuration d'exécution est mis à jour.

Mode de QoS avancé

Cette section couvre les sujets suivants :

Vue d'ensemble

Les trames qui correspondent à une ACL et sont autorisées à entrer sur le système sont implicitement marquées du nom de l'ACL qui a donné cette autorisation. Vous pouvez alors appliquer des actions de QoS en mode avancé à ces flux.

En mode de QoS avancé, le périphérique 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 : le gestionnaire de stratégie individuelle et le gestionnaire de stratégie d'agrégats. Chaque gestionnaire de stratégie est configuré avec une spécification de QoS. Le gestionnaire de stratégie individuelle applique la QoS à un seul mappage de classe, c'est-à-dire à un seul flux, en se fondant sur la spécification de QoS qu'il contient. Le gestionnaire de stratégie d'agrégats applique la QoS à un ou plusieurs mappages de classe (flux). Un gestionnaire de stratégie d'agrégats peut prendre en charge des mappages de classe issus de plusieurs stratégies.

La fonctionnalité 2R3C (2 Rate 3 Color) est prise en charge sur l'appareil. Ainsi, chaque gestionnaire de stratégie dispose de deux seuils. Si le premier seuil est atteint, une Action si dépassement configurée par l'utilisateur est effectuée. Si le second seuil est atteint, une Action si violation configurée par l'utilisateur est appliquée (reportez-vous à la section Gestion de stratégie d'agrégats).

- La QoS est appliquée à chaque flux par liaison des stratégies aux ports voulus. Vous pouvez lier une stratégie et ses mappages de classe à un ou plusieurs ports mais chaque port ne peut être lié qu'à une seule stratégie.

Remarques :

- Les gestionnaires de stratégie individuelle et d'agrégats sont disponibles lorsque le périphérique fonctionne en mode Couche 2.
- Une ACL peut être configurée sur un ou plusieurs mappages de classe, quelles que soient les stratégies.
- Un mappage de classe ne peut appartenir qu'à une seule stratégie.
- Lorsqu'un mappage de classe utilisant un gestionnaire de stratégie individuelle est lié à plusieurs ports, chaque port possède sa propre instance de gestionnaire de stratégie individuelle ; chacune applique la QoS du mappage de classe (flux) sur un port, indépendamment des autres ports.
- Un gestionnaire de stratégie d'agrégats applique la QoS à tous les flux, de façon agrégée, sans tenir compte des stratégies ni des ports.

Les paramètres de QoS avancé se composent de trois parties :

- Définition des règles à mettre en correspondance. Toutes les trames qui correspondent à un groupe unique de règles sont considérées comme constituant un *flux*.
- Définition des actions à appliquer aux trames de chaque flux qui correspondent aux règles.
- Liaison de combinaisons règles-action à une ou plusieurs interfaces.

Flux de travail de configuration du mode de QoS avancé

Pour configurer le mode de QoS avancé, procédez comme suit :

1. Sélectionnez le mode Avancé pour le système sur la page Propriétés de QoS. Sélectionnez le Mode de confiance par l'intermédiaire de la page Paramètres globaux. Si le niveau de CoS et la balise DSCP d'un paquet sont mappés sur des files d'attente distinctes, le mode de confiance détermine la file d'attente à laquelle ce paquet doit être affecté :

- Si les valeurs DSCP internes sont différentes de celles utilisées dans les paquets entrants, mappez les valeurs externes sur des valeurs internes via la page Nouveau marquage DSCP hors profil. Cette opération ouvre alors la page Nouveau marquage DSCP.

2. Créez des ACL, comme le décrit la section Flux de travail de création d'une ACL.
3. Si des ACL ont été définies, créez des mappages de classes et associez-leur ces ACL via la page Mappage de classes.
4. Créez une stratégie dans la page Table des stratégies puis associez cette stratégie à un ou plusieurs mappages de classe dans la page Mappages de classe de stratégies. Vous pouvez également spécifier la QoS, si nécessaire, en affectant un gestionnaire de stratégie à un mappage de classe lors de l'opération d'affectation de ce mappage à la stratégie.
   - **Gestionnaire de stratégie individuelle** : créez une stratégie pour associer un mappage de classe à un gestionnaire de stratégie individuelle, sur la page Table des stratégies et la page Mappage de classes. Dans la stratégie, définissez le gestionnaire de stratégie individuelle.
   - **Gestionnaire de stratégie d'agrégats** : créez une action de QoS pour chaque flux afin d'envoyer toutes les trames concordantes au même gestionnaire de stratégie (d'agrégats), via la page Gestionnaire de stratégie d'agrégats. Créez une stratégie pour associer un mappage de classe à ce gestionnaire de stratégie d'agrégats, via la page Table des stratégies.
5. Liez la stratégie à une interface via la page Liaison de stratégies.

Paramètres globaux

La page Paramètres globaux contient des informations concernant l'activation du mode de confiance sur le périphérique. Les paquets entrant dans un domaine QoS sont classifiés à la bordure du domaine QoS.

Pour définir la configuration de mode de confiance :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Paramètres globaux**.

ÉTAPE 2 Sélectionnez le **Mode de confiance** à appliquer lorsque le périphérique est en mode Avancé. Si le niveau de CoS et la balise DSCP d'un paquet sont mappés sur des files d'attente distinctes, le mode de confiance détermine la file d'attente à laquelle ce paquet doit être affecté :

- **CoS/802.1p** : le trafic est mappé sur des files d'attente en fonction du champ VPT 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). Configurez le mappage VPT vers la file d'attente réelle sur la page CoS/802.1p vers la file d'attente.

- **DSCP** : tout le trafic IP est mappé sur des files d'attente en fonction du champ DSCP de l'en-tête IP. Vous pouvez configurer le mappage DSCP vers file d'attente sur la page DSCP vers file d'attente. Si le trafic n'est pas de type IP, il est mappé sur la file d'attente de meilleur effort.
- **CoS/802.1p-DSCP** : sélectionnez cette option pour utiliser le mode CoS de confiance pour le trafic non IP et DSCP de confiance pour le trafic IP.

ÉTAPE 3 Sélectionnez le mode de confiance Mode avancé de QoS par défaut (validé ou non validé) pour les interfaces dans le champ **État du mode par défaut**. Vous bénéficiez ainsi de la fonction QoS de base pour le QoS avancé, afin d'approuver CoS/DSCP sur le QoS avancé par défaut (sans devoir créer de stratégie).

En **Mode de QoS avancé**, si l'état du mode par défaut est défini sur Non validé, les valeurs CoS par défaut configurées sur l'interface sont ignorées et l'ensemble du trafic est dirigé vers la file d'attente 1. Pour plus d'informations, reportez-vous à la page Qualité de service > Mode de QoS avancé > Paramètres globaux.

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 4 Sélectionnez **Remplacer DSCP d'entrée** pour remplacer les valeurs DSCP d'origine des paquets entrants par d'autres, d'après la table de substitution DSCP. Lorsque la fonction Remplacer DSCP d'entrée est activée, l'appareil utilise les nouvelles valeurs DSCP pour la mise en file d'attente des données en sortie. Il remplace également les valeurs DSCP d'origine figurant dans les paquets par les nouvelles valeurs DSCP.

REMARQUE La trame est mappée sur une file d'attente en sortie à l'aide de la nouvelle valeur réécrite et non de la valeur DSCP d'origine.

ÉTAPE 5 Si vous avez activé l'option **Remplacer DSCP d'entrée**, cliquez sur **Table de substitution DSCP** pour reconfigurer le DSCP.

Table de substitution DSCP

ÉTAPE 1 Renseignez les champs suivants :

- **DSCP en entrée** : affiche la valeur DSCP du paquet entrant qui doit être marquée à nouveau à l'aide d'une autre valeur.
- **DSCP en sortie** : sélectionnez la valeur DSCP en sortie pour indiquer que la valeur sortante est mappée.

ÉTAPE 2 Cliquez sur **Appliquer**.

Nouveau marquage du DSCP hors profil

Lorsque vous associez un gestionnaire de stratégie à un mappage de classe (flux), vous pouvez définir l'action à exécuter lorsque la quantité de trafic de ce flux dépasse les limites définies par la QoS. On appelle *paquets hors profil* la portion du trafic qui provoque ce dépassement de la limite de QoS du flux.

Si l'action appliquée en cas de dépassement/violation est DSCP hors profil, l'appareil mappe à nouveau la valeur DSCP d'origine des paquets IP hors profil à une nouvelle valeur, sur la base de la table Nouveau marquage du DSCP hors profil. Le périphérique emploie les nouvelles valeurs pour affecter des ressources et des files d'attente de sortie à ces paquets. Il remplace aussi physiquement la valeur DSCP d'origine figurant dans les paquets hors profil par la nouvelle valeur DSCP.

Pour utiliser l'action de dépassement DSCP hors profil, remappez la valeur DSCP dans la table Nouveau marquage du DSCP hors profil. Sinon, l'action est Null, car la valeur DSCP de la table remappe le paquet sur lui-même, selon les valeurs par défaut définies en usine.

Cette fonction modifie les balises DSCP du trafic entrant commuté entre des domaines de QoS de confiance. En modifiant les valeurs DSCP utilisées dans un domaine, vous définissez la priorité de ce type de trafic sur la valeur DSCP utilisée dans l'autre domaine pour identifier le même type de trafic.

Ces paramètres sont actifs lorsque le système fonctionne en mode avancé de QoS. Une fois activés, ils s'appliquent à l'échelle globale.

Par exemple, supposez qu'il existe trois niveaux de service : Argent, Or et Platine et que les valeurs DSCP entrantes utilisées pour marquer ces niveaux soient respectivement 10, 20 et 30. Si ce trafic est transféré vers un autre fournisseur de services offrant les mêmes niveaux de service, mais que ce fournisseur emploie les valeurs DSCP 16, 24 et 48, le **nouveau marquage du DSCP hors profil** remplace les valeurs entrantes au fur et à mesure qu'elles sont mappées sur les valeurs sortantes.

Pour mapper des valeurs DSCP :

ÉTAPE 1 Cliquez sur **Qualité de service > Mode de QoS avancé > Nouveau marquage du DSCP hors profil**. Cette page permet de définir la valeur DSCP du trafic qui entre sur l'appareil ou le quitte.

DSCP en entrée affiche la valeur DSCP du paquet entrant qui doit à nouveau être marqué d'une autre valeur.

Vous pouvez filtrer en fonction du **Type d'action** pour afficher l'ensemble des **dépassements** ou des **violations**. Vous pouvez ainsi configurer le re-marquage quand le trafic excède le seuil Dépassement ou Violation d'un gestionnaire de stratégie.

ÉTAPE 2 Sélectionnez la valeur **DSCP en sortie** correspondant à l'endroit sur lequel la valeur entrante est mappée.

ÉTAPE 3 Cliquez sur **Appliquer**. Le fichier de configuration d'exécution est mis à jour avec la nouvelle table Nouveau marquage DSCP.

ÉTAPE 4 Cliquez sur **Restaurer déf.** pour rétablir le paramètre de CoS par défaut défini en usine pour cette interface.

Mappage de classes

Un mappage de classes définit un flux de trafic doté d'ACL (listes de contrôle d'accès). Vous pouvez combiner une ACL MAC, une ACL IP et une ACL IPv6 en un même mappage de classe. Les mappages de classe sont configurés 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 système. Les paquets correspondant au même mappage de classe sont considérés comme appartenant au même flux.

REMARQUE La définition de mappages de classe n'a aucun effet sur la QoS ; il s'agit d'une étape intermédiaire nécessaire pour que les mappages de classe puissent être utilisés ultérieurement.

Si vous avez besoin d'ensembles de règles plus complexes, vous pouvez regrouper plusieurs mappages de classe en un grand groupe, appelé stratégie (reportez-vous à la section Table des stratégies).

REMARQUE Dans le même mappage de classe, une ACL MAC ne peut pas être utilisée avec une ACE IPv6 dont l'adresse IPv6 de destination est définie comme condition de filtrage.

La page Mappage de classes affiche la liste des mappages de classe définis et des ACL qui les constituent ; elle vous permet aussi d'ajouter/de supprimer des mappages de classe.

Pour définir un mappage de classes :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Mappage de classes**.

Pour chaque mappage de classe, les ACL définies sont affichées, de même que les relations qu'elles entretiennent les unes avec les autres. Vous pouvez afficher jusqu'à 3 ACL et leur **correspondance**, qui peut être **Et** ou **Ou**. Ces valeurs indiquent la relation entre les ACL. Le mappage de classe correspond au résultat des trois ACL combinées avec Et ou Ou.

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 paramètres.

- **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 l'une des ACL IP du mappage de classe.
  - *MAC* : un paquet doit correspondre à l'ACL MAC du mappage de classe.
  - *IP et MAC* : un paquet doit correspondre à la fois à l'ACL IP et à l'ACL MAC du mappage de classe.
  - *IP or MAC* : un paquet doit correspondre soit à l'ACL IP, soit à l'ACL MAC du mappage de classe.
- **IP** : sélectionnez l'ACL IPv4 ou IPv6 pour ce mappage de classe.
- **MAC** : sélectionnez l'ACL MAC pour ce mappage de classe.
- **ACL préférée** : indiquez si les paquets sont d'abord comparés à une ACL IP ou à une ACL MAC.

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

Gestion de stratégie d'agrégats

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 un gestionnaire de stratégie individuelle sur la page Table des stratégies.
- **Gestionnaire de stratégie d'agrégats** : le gestionnaire de stratégie d'agrégats applique la QoS à un ou plusieurs mappages de classe ainsi qu'à un ou plusieurs flux. Un gestionnaire de stratégie d'agrégats peut prendre en charge des mappages de classe issus de plusieurs stratégies. Un gestionnaire de stratégie d'agrégats applique la QoS à tous les flux, de façon agrégée, sans tenir compte des stratégies ni des ports. Vous pouvez créer un gestionnaire de stratégie d'agrégats sur la page Gestionnaire de stratégie d'agrégats.

  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 :

- Contrôle de la crête : sélectionnez cette option pour appliquer une action en cas de dépassement de la taille de la rafale maximale.
- **Débit minimal crête (PIR)** : saisissez le débit crête du trafic (PIR) en Kbit par seconde (Kbit/s).
- **Taille de la rafale maximale (PBS)** : saisissez la taille de la rafale maximale en Kbit par seconde (Kbit/s).
- **Action si violation** : sélectionnez l'une des actions suivantes en cas de dépassement de la crête :
  - *Abandonner* : abandonne les trames ne respectant pas la crête.
  - *DSCP hors profil* : marque les trames qui ne respectent pas la crête avec la valeur DSCP définie précédemment.

- Débit maximal autorisé, appelé CIR (Committed Information Rate, débit minimal garanti), mesuré en kbit/s.
- Quantité de trafic, mesurée en octets, appelée CBS (Committed Burst Size, taille de rafale garantie). Il s'agit du trafic autorisé à transiter sous forme de rafale temporaire, même s'il dépasse le débit maximal défini.
- Action à appliquer aux trames qui dépassent les limites (appelées trafic hors profil), à savoir s'il faut transmettre ces trames telles quelles, les éliminer ou les transmettre, mais en les remappant sur une valeur DSCP qui les marque comme trames de priorité faible pour tous les traitements suivants sur le périphérique.
- Configure le maintien de l'ordre du trafic en fonction des débits spécifiés et des actions facultatives. Saisissez le CIR ainsi que les valeurs et les actions facultatives.

Vous affectez un gestionnaire de stratégie à un mappage de classe lorsque vous ajoutez ce mappage à une stratégie. Si vous choisissez un gestionnaire de stratégie d'agrégats, vous devez le créer sur la page Gestionnaire de stratégie d'agrégats.

Pour définir un gestionnaire de stratégie d'agrégats :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Gestionnaire de stratégie d'agrégats**.

Cette page affiche les gestionnaires de stratégie d'agrégats existants.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Saisissez les paramètres.

- **Nom du gestionnaire de stratégie d'agrégats** : saisissez le nom du gestionnaire de stratégie d'agrégats.
- **Ingress Committed Information Rate (CIR)** : saisissez la bande passante maximale autorisée, en bits par seconde. Reportez-vous à la description disponible sur la page Bande passante.
- **Taille de rafale garantie en entrée (CBS)** : saisissez la taille maximale de rafale (même si elle dépasse la valeur CIR), en octets. Reportez-vous à la description disponible sur la page Bande passante.
- **Action si dépassement** : sélectionnez l'action à appliquer aux paquets entrants qui dépassent le seuil CIR. Les valeurs possibles sont les suivantes :
  - *Drop* : les paquets qui dépassent la limite CIR définie sont éliminés.
  - *DSCP hors profil* : les valeurs DSCP des paquets qui dépassent la limite CIR définie sont remappées sur d'autres, d'après la table Nouveau marquage du DSCP hors profil.

- Contrôle de la crête : sélectionnez cette option pour appliquer une action en cas de dépassement de la taille de rafale maximale.
- **Débit minimal crête (PIR)** : saisissez le débit crête du trafic (PIR) en Kbit par seconde (Kbit/s).
- **Taille de la rafale maximale (PBS)** : saisissez la taille de la rafale maximale en Kbit par seconde (Kbit/s).
- **Action si violation** : sélectionnez l'une des actions suivantes en cas de dépassement de la crête :
  - *Abandonner* : abandonne les trames ne respectant pas la crête.
  - *DSCP hors profil* : marque les trames qui ne respectent pas la crête avec la valeur DSCP définie précédemment.

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

Table des stratégies

La page Table des stratégies affiche la liste des stratégies de QoS avancées définies sur le système. Cette page vous permet également de créer et de supprimer des stratégies. Seules les stratégies liées à une interface sont actives (reportez-vous à la page Liaison de stratégies).

Chaque stratégie est constituée des éléments suivants :

- Un ou plusieurs mappages de classe d'ACL, qui définissent les flux de trafic dans la stratégie.
- Un ou plusieurs agrégats qui appliquent la QoS aux flux de trafic dans la stratégie.

Une fois qu'une stratégie a été ajoutée, vous pouvez ajouter des mappages de classe via la page Table des stratégies.

Pour ajouter une stratégie de QoS :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Table des stratégies**.

Cette page affiche la liste des stratégies définies.

ÉTAPE 2 Cliquez sur **Policy Class Map Table** pour afficher la page Policy Class Maps.
- ou
Cliquez sur **Ajouter** pour ouvrir la page Ajouter une table de stratégies.

ÉTAPE 3 Saisissez le nom de la nouvelle stratégie dans le champ **Nom de la nouvelle stratégie**.

ÉTAPE 4 Cliquez sur **Appliquer**. Le profil de stratégie QoS est ajouté et le fichier de Configuration d'exécution est mis à jour.

Mappages de classe de stratégies

Vous pouvez ajouter un ou plusieurs mappages de classe à une stratégie. Un mappage de classe 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 **Qualité de service** > **Mode de QoS avancé** > **Mappages de classe de stratégies**.

ÉTAPE 2 Sélectionnez une stratégie dans le filtre et cliquez sur **OK**. Tous les mappages de classe de cette stratégie sont affichés.

ÉTAPE 3 Pour ajouter un nouveau mappage de classe, cliquez sur **Ajouter**.

ÉTAPE 4 Saisissez les paramètres.

- **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. Vous pouvez créer les mappages de classes sur la page Mappage de classes.
- **Type d'action** : sélectionnez l'action à appliquer concernant la valeur CoS/802.1p et/ou DSCP d'entrée de tous les paquets concordants.
  - *Utiliser le mode de confiance par défaut* : si cette option est sélectionnée, l'état du mode par défaut est utilisé en mode Confiance globale. Si l'état du mode par défaut est défini sur « Non validé », ignorez la valeur DSCP et/ou CoS/802.1p en entrée ; les paquets correspondants sont alors envoyés en mode Meilleur effort (Best effort).
  - *Toujours faire confiance* : si cette option est sélectionnée, le périphérique valide le paquet correspondant en fonction du mode Confiance globale (sélectionné sur la page **Paramètres globaux**). Il ignore l'état Mode par défaut (sélectionné sur la page **Paramètres globaux**).

- *Définir* : si vous sélectionnez cette option, le système utilise le contenu saisi dans le champ **Nouvelle valeur** afin de déterminer la file d'attente de sortie des paquets concordants comme suit :

  Si la nouvelle valeur (0..7) est une priorité CoS/802.1p, utilisez la valeur de priorité ainsi que le contenu de la table CoS/802.1p vers file d'attente afin de déterminer la file d'attente de sortie de tous les paquets concordants.

  Si la nouvelle valeur (0..63) est une valeur DSCP, utilisez la nouvelle valeur DSCP ainsi que le contenu de la table DSCP vers file d'attente afin de déterminer la file d'attente de sortie des paquets IP concordants.

  Sinon, le système utilise la nouvelle valeur (1..8) comme numéro de file d'attente de sortie pour tous les paquets concordants.

- Redirection du trafic : indiquez si vous souhaitez rediriger le trafic concordant. Si vous activez cette option, sélectionnez l'unité/le port vers lequel le trafic sera redirigé.
- **Redirect Target** (Rediriger la cible) : sélectionnez l'unité/le port vers lequel le trafic sera redirigé.
- **Miroir du trafic** : cette option permet de mettre en miroir un flux de trafic sur le port Ethernet de l'analyseur. Si cette option est sélectionnée, le trafic est mis en miroir sur le port de destination spécifié dans l'ID de session SPAN 1. Si aucun port cible n'est spécifié dans l'ID de session SPAN 1, l'action de mise en miroir est sans effet. Si un mappage de classe de stratégie avec une action Miroir du trafic est appliqué à une interface et que cette même interface est définie comme port source pour la session SPAN 1, tout le trafic, pas seulement un flux spécifique, sera mis en miroir.

  Les autres règles et actions de la stratégie (et les ACL) appliquées à l'interface resteront en vigueur, même si l'action Miroir du trafic est configurée. Par exemple :

  - Si l'action ACL du flux en miroir est autorisée, le flux de trafic sera mis en miroir et réacheminé. Si l'action ACL du flux est refusée, le trafic sera mis en miroir, mais pas réacheminé vers l'interface réseau de sortie (abandon).
  - Les flux de trafic sur les interfaces, sur lesquelles une stratégie qui ne correspond pas à la classification du mappage de classe en miroir est appliquée, suivront l'action par défaut de la stratégie par défaut.

- **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.

ÉTAPE 5 Si vous définissez **Police Type** (Type de gest. de stratégie) sur *Aggregate* (Agrégat), définissez le paramètre **Aggregate Policer** (Gestionnaire de stratégies d'agrégats).

ÉTAPE 6 Si **Type de gest. de stratégie** indique *individuelle*, saisissez les paramètres de QoS suivants :

- **Débit minimal garanti en entrée (CIR)** : saisissez la valeur CIR, en kilobits par seconde. Reportez-vous à la description disponible sur la page Bande passante.
- **Taille de rafale garantie en entrée (CBS)** : saisissez la valeur CBS, en octets. Reportez-vous à la description disponible sur la page Bande passante.
- **Action si dépassement** : sélectionnez l'action affectée aux paquets entrants qui dépassent le seuil CIR. Les options sont les suivantes :
  - *Drop* : les paquets qui dépassent la limite CIR définie sont éliminés.
  - *DSCP hors profil* : les paquets IP qui dépassent la limite CIR définie sont transférés avec une nouvelle valeur DSCP, extraite de la table Nouveau marquage du DSCP hors profil.
- Contrôle de la crête : sélectionnez cette option pour appliquer une action en cas de dépassement de la taille de rafale maximale.
- **Débit minimal crête (PIR)** : saisissez le débit crête du trafic (PIR) en Kbit par seconde (Kbit/s).
- **Taille de la rafale maximale (PBS)** : saisissez la taille de la rafale maximale en Kbit par seconde (Kbit/s).
- **Action si violation** : sélectionnez l'une des actions suivantes en cas de dépassement de la crête :
  - *Abandonner* : abandonne les trames ne respectant pas la crête.
  - *DSCP hors profil* : marque les trames qui ne respectent pas la crête avec la valeur DSCP définie précédemment.

ÉTAPE 7 Cliquez sur **Appliquer**.

Liaison de stratégies

La page Liaison de stratégies indique le profil de stratégie lié à chaque port. Une stratégie peut être liée à une interface en tant que stratégie en entrée ou que stratégie en sortie. Lorsqu'un profil de stratégie est lié à un port spécifique, il est actif sur ce port. Vous ne pouvez configurer qu'un seul profil de stratégie par port et par direction, mais il est possible de lier un même profil à plusieurs ports.

Lorsque vous liez une stratégie à un port, ce dernier filtre et applique la QoS au trafic qui correspond aux flux définis au sein de cette stratégie.

Pour modifier une stratégie, vous devez d'abord la supprimer (annuler la liaison) de tous les ports auxquels elle est liée.

REMARQUE Il est possible de lier un port à une stratégie ou à une ACL, mais il est impossible de lier les deux.

Pour définir une association de stratégie :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Liaison de stratégies**.

ÉTAPE 2 Sélectionnez un **Type d'interface** si nécessaire.

ÉTAPE 3 Cliquez sur **Go**. Les stratégies de cette interface s'affichent.

ÉTAPE 4 Cliquez sur **Modifier**.

ÉTAPE 5 Sélectionnez les options suivantes pour la stratégie/l'interface d'entrée :

- **Liaison de stratégies d'entrée** : sélectionnez cette option pour lier la stratégie d'entrée à l'interface.
- **Nom de la stratégie** : sélectionnez le nom de la stratégie d'entrée à lier.
- **Action par défaut** : sélectionnez une action à effectuer si un paquet correspond à une stratégie :
  - *Tout refuser* : sélectionnez cette option pour réacheminer des paquets sur l'interface s'ils correspondent à une stratégie.
  - *Tout autoriser* : sélectionnez cette option pour transférer des paquets sur l'interface s'ils ne correspondent à aucune stratégie.

  REMARQUE L'option Tout autoriser ne peut être définie que si la protection de la source IP n'est pas activée sur l'interface.

ÉTAPE 6 Sélectionnez les options suivantes pour la stratégie/l'interface de sortie :

- **Liaison de stratégies de sortie** : sélectionnez cette option pour lier la stratégie de sortie à l'interface.
- **Nom de la stratégie** : sélectionnez le nom de la stratégie de sortie à lier.
- **Action par défaut** : sélectionnez une action à effectuer si un paquet correspond à une stratégie :
  - *Tout refuser* : sélectionnez cette option pour réacheminer des paquets sur l'interface s'ils correspondent à une stratégie.

- *Tout autoriser* : sélectionnez cette option pour transférer des paquets sur l'interface s'ils ne correspondent à aucune stratégie.

REMARQUE L'option Tout autoriser ne peut être définie que si la protection de la source IP n'est pas activée sur l'interface.

ÉTAPE 7 Cliquez sur **Appliquer**. La liaison de stratégie QoS est définie et le fichier de Configuration d'exécution est mis à jour.

Statistiques de QoS

Sur ces pages, vous pouvez gérer le gestionnaire de stratégie individuelle, le gestionnaire de stratégie d'agrégats et afficher les statistiques des files d'attente.

Statistiques du gestionnaire de stratégie

Un gestionnaire de stratégie individuelle est lié à un mappage de classe issu d'une seule stratégie. Un gestionnaire de stratégie d'agrégats est lié à un ou plusieurs mappages de classe, issus d'une ou plusieurs stratégies.

Affichage des statistiques d'un gestionnaire de stratégie individuelle

La page Statistiques de politique individuelle indique le nombre de paquets hors profil ou conformes au profil reçus depuis une interface, qui répondent aux conditions définies dans le mappage de classe d'une stratégie.

REMARQUE Cette page n'est pas disponible lorsque le périphérique fonctionne en mode Couche 3.

Pour afficher les statistiques du gestionnaire de stratégie :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Statistiques de QoS** > **Statistiques de gestionnaire de stratégie individuelle**.

Cette page affiche les champs suivants :

- **Interface** : interface à laquelle correspondent les statistiques affichées.
- **Stratégie** : stratégie à laquelle correspondent les statistiques affichées.
- **Mappage de classe** : mappage de classe auquel correspondent les statistiques affichées.

- **Octets dans le profil** : nombre d'octets conformes au profil reçus.
- **Octets hors profil** : nombre d'octets hors profil reçus.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez l'interface pour laquelle cumuler les statistiques.
- **Nom de la stratégie** : sélectionnez le nom de la stratégie.
- **Nom du mappage de classe** : sélectionnez le nom du mappage de classe.

ÉTAPE 4 Cliquez sur **Appliquer**. Une demande de statistiques supplémentaire est créée et le fichier de configuration d'exécution est mis à jour.

Affichage des statistiques d'un gestionnaire de stratégie d'agrégats

Pour afficher les statistiques d'un gestionnaire de stratégie d'agrégats :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Statistiques de QoS** > **Statistiques de gestionnaire de stratégie d'agrégats**.

Cette page affiche les champs suivants :

- **Nom du gestionnaire de strat. d'agrégats** : gestionnaire de stratégie sur lequel les statistiques sont fondées.
- **Octets dans le profil** : nombre de paquets conformes au profil reçus.
- **Octets hors profil** : nombre de paquets hors profil reçus.

ÉTAPE 2 Cliquez sur **Add**.

ÉTAPE 3 Sélectionnez un **nom de gestionnaire de stratégie d'agrégats**, parmi les gestionnaires de stratégie précédemment créés, afin d'afficher les statistiques correspondantes.

ÉTAPE 4 Cliquez sur **Appliquer**. Une demande de statistiques supplémentaire est créée et le fichier de Configuration d'exécution est mis à jour.

Statistiques des files d'attente

La page Statistiques des files d'attente affiche les statistiques concernant les files d'attente, dont le nombre de paquets transférés et éliminés, ceci sur la base de l'interface, de la file d'attente et de la priorité d'élimination.

Pour consulter les statistiques des files d'attente et définir celles à afficher (ensemble de compteurs), procédez comme suit :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Statistiques de QoS** > **Statistiques des files d'attente**.

Cette page affiche les champs suivants :

- **Taux d'actualisation** : sélectionnez la durée qui s'écoule avant l'actualisation des statistiques Ethernet de l'interface. Les options disponibles sont les suivantes :
  - *No Refresh* : les statistiques ne sont pas actualisées.
  - *15 s* : les statistiques sont actualisées toutes les 15 secondes.
  - *30 s* : les statistiques sont actualisées toutes les 30 secondes.
  - *60 s* : les statistiques sont actualisées toutes les 60 secondes.

Pour afficher une unité et une interface spécifiques, sélectionnez l'unité/interface dans le filtre et cliquez ensuite sur **Ok**.

Pour afficher une interface spécifique, sélectionnez-la dans le filtre et cliquez ensuite sur **Ok**.

La table Statistiques des files d'attente contient les champs suivants pour chaque file d'attente :

- **File d'attente** : file d'attente d'où proviennent les paquets transférés ou éliminés, la file étant pleine (tail drop).
- **Paquets transmis** : nombre de paquets ayant été transmis.
- **Paquets éliminés** : pourcentage de paquets éliminés, la file étant pleine (tail drop).
- **Octets transmis** : nombre d'octets ayant été transmis.
- **Octets éliminés** : pourcentage d'octets éliminés, la file étant pleine (tail drop).

28

SNMP

Cette section décrit la fonctionnalité SNMP (Simple Network Management Protocol), qui fournit une méthode de gestion des unités de réseau.

Elle couvre les sujets suivants :

- Vue d'ensemble
- ID de moteur
- Vues
- Groupes
- Utilisateurs
- Communautés
- Paramètres de filtre
- Destinataires de notifications
- Filtre de notification

Vue d'ensemble

Versions et flux de travail SNMP

Le périphérique fonctionne comme un agent SNMP et prend en charge SNMPv1, v2 et v3. Il crée également des rapports sur les événements système pour les destinataires des interceptions, à l'aide des interceptions définies dans la base MIB prise en charge.

SNMPv1 et v2

Pour contrôler l'accès au système, une liste d'entrées de communauté est définie. Chaque entrée de communauté est constituée d'une *chaîne de communauté* et de son privilège d'accès. Le système répond uniquement aux messages SNMP spécifiant la communauté qui dispose des autorisations correctes et de l'opération correcte.

Les agents SNMP conservent une liste de variables utilisées pour gérer le périphérique. Ces variables sont définies dans une *base d'informations de gestion* (MIB, Management Information Base).

REMARQUE En raison des vulnérabilités en matière de sécurité détectées dans les autres versions, il est recommandé d'utiliser SNMPv3.

SNMPv3

En plus de la fonctionnalité fournie par SNMPv1 et v2, SNMPv3 applique un contrôle d'accès et de nouveaux mécanismes d'interceptions aux PDU SNMPv1 et SNMPv2. SNMPv3 définit également un modèle de sécurité utilisateur (USM, User Security Model) qui inclut :

- **Authentification** : fournit une intégrité des données et une authentification de leur origine.
- **Confidentialité** : fournit une protection contre la divulgation du contenu des messages. *Cipher Block-Chaining* (CBC-DES) est utilisé pour le cryptage. Sur un message SNMP, vous pouvez activer soit l'authentification seule, soit l'authentification et la confidentialité. Cependant, la confidentialité ne peut pas être activée sans authentification.
- **Actualité** : fournit une protection contre les retards de messages ou les attaques de lecture. L'agent SNMP compare l'horodatage du message entrant par rapport à l'heure d'arrivée du message.
- **Gestion de la clé** : définit la génération, les mises à jour et l'utilisation de la clé. Le périphérique prend en charge les filtres de notification SNMP basés sur les *ID d'objet* (OID). Les ID d'objet sont utilisés par le système pour gérer des fonctionnalités d'unité.

Flux de travail SNMP

REMARQUE Pour des raisons de sécurité, SNMP est désactivé par défaut. Avant de pouvoir gérer le périphérique via SNMP, vous devez activer SNMP sur la page Services TCP/UDP.

Ci-dessous figure une série d'actions recommandées pour la configuration de SNMP :

Si vous décidez d'utiliser SNMPv1 ou v2 :

ÉTAPE 1 Accédez à la page Communautés, puis cliquez sur **Add** (Ajouter). La communauté peut être associée à des droits d'accès et à un affichage en mode De base ou à un groupe en mode Avancé. Il existe deux méthodes pour définir les droits d'accès d'une communauté :

- **Mode De base** : les droits d'accès d'une communauté peuvent être définis en Lecture seule, Lecture/écriture ou Admin SNMP. Vous pouvez en outre restreindre l'accès à la communauté à certains objets MIB uniquement, en sélectionnant une vue (définie sur la page Vues).
- **Advanced Mode** (Mode Avancé) : les droits d'accès à une communauté sont définis par un groupe (défini sur la page Groupes). Vous pouvez configurer le groupe avec un modèle de sécurité spécifique. Les groupes disposent des droits d'accès de lecture, d'écriture et de notification.

ÉTAPE 2 Indiquez si vous souhaitez restreindre la station de gestion SNMP à une seule adresse ou autoriser la gestion SNMP à partir de toutes les adresses. Si vous choisissez de restreindre la gestion SNMP à une seule adresse, saisissez l'adresse de votre ordinateur de gestion SNMP dans le champ Adresse IP.

ÉTAPE 3 Saisissez la chaîne de communauté unique dans le champ Chaîne de communauté.

ÉTAPE 4 (Facultatif) Activez les filtres via la page Paramètres de filtre.

ÉTAPE 5 Vous pouvez éventuellement définir un ou plusieurs filtres de notification sur la page Filtre de notification.

ÉTAPE 6 Configurez les destinataires des notifications sur les pages Destinataires de notifications SNMPv1.2.

Si vous décidez d'utiliser SNMPv3 :

ÉTAPE 1 Définissez le moteur SNMP sur la page ID de moteur. Vous pouvez soit créer un ID de moteur unique, soit utiliser l'ID de moteur par défaut. L'application d'une configuration d'ID de moteur efface la base de données SNMP.

ÉTAPE 2 Vous pouvez éventuellement définir une ou plusieurs vues SNMP à l'aide de la page Vues. Vous limitez ainsi la plage des ID d'objet (OID) disponibles pour une communauté ou un groupe.

ÉTAPE 3 Définissez des groupes sur la page Groupes.

ÉTAPE 4 Définissez des utilisateurs sur la page Utilisateurs, à partir de laquelle ils peuvent être associés à un groupe. Si l'ID de moteur SNMP n'est pas défini, il se peut que vous ne puissiez pas créer d'utilisateurs.

ÉTAPE 5 (Facultatif) Activez ou désactivez les filtres via la page Paramètres de filtre.

ÉTAPE 6 Vous pouvez éventuellement définir un ou plusieurs filtres de notification sur la page Filtre de notification.

ÉTAPE 7 Définissez un ou plusieurs destinataires de notification sur la page Destinataires de notifications SNMPv3.

Bases MIB prises en charge

Pour obtenir la liste des bases MIB prises en charge, visitez l'URL suivante et accédez à la zone de téléchargement nommée **Cisco MIBS** :

www.cisco.com/cisco/software/navigator.html

ID d'objet du modèle

Vous trouverez, ci-dessous, les ID d'objet pour la gamme 550 / 350 .

Nom de la référence	Nom de la gamme	ID d'objet
SG350-8PD	Commutateur administrable PoE à 8 ports, avec 2 ports 2,5 G et 6 ports Gig	9.6.1.95.8.11
SG350X-8PMD	Commutateur administrable empilable PoE 2,5 G à 8 ports	9.6.1.95.8.11
SG350X-24PD	Commutateur administrable empilable PoE à 24 ports, avec 4 ports 2,5 G et 20 ports Gig	9.6.1.94.23.11
SF350-48	SF350-48 - Commutateur administrable 48 ports 10/100	9.6.1.96.48.1
SF350-48P	SF350-48P - Commutateur administrable PoE 48 ports 10/100	9.6.1.96.48.5
SF350-48MP	SF350-48MP - Commutateur administrable PoE 48 ports 10/100	9.6.1.96.48.6
SG350XG-24F	SG350XG-24F - Commutateur administrable empilable SFP+ 10 G 24 ports	9.6.1.91.24.8
SG350XG-24T	SG350XG-24T - Commutateur administrable empilable Base-T 10 G 24 ports	9.6.1.91.24.9

Nom de la référence	Nom de la gamme	ID d'objet
SG350XG-48T	SG350XG-48T - Commutateur administrable empilable Base-T 10G 48 ports	9.6.1.91.48.9
SG350XG-2F10	SG350XG-2F10 - Commutateur administrable empilable 10 G à 12 ports	9.6.1.91.12.9
SG350-8PD		9.6.1.95.8.11
SG350X-8PMD		9.6.1.94.8.12
SG350X-24PD		9.6.1.94.24.11
SG350-10	SG350-10 - Commutateur administrable 10 ports Gigabit	9.6.1.95.10.3
SG350-10P	SG350-10P - Commutateur administrable PoE Gigabit à 10 ports	9.6.1.95.10.5
SG355-10P	SG355-10P - Commutateur administrable PoE Gigabit à 10 ports	9.6.1.95.10.10
SG350-10MP	SG350-10MP - Commutateur administrable PoE Gigabit à 10 ports	9.6.1.95.10.6
SG350-28	SG350-28 - Commutateur administrable 28 ports Gigabit	9.6.1.95.28.1
SG350-28P	SG350-28P - Commutateur administrable PoE 28 ports	9.6.1.95.28.5
SG350-28MP	SG350-28MP - Commutateur administrable PoE 28 ports	9.6.1.95.28.6
SG350X-24	Commutateur administrable empilable 24 ports Gigabit	9.6.1.94.24.1
SG350X-24P	Commutateur administrable empilable PoE 24 ports Gigabit	9.6.1.94.24.5
SG350X-24MP	Commutateur administrable empilable PoE 24 ports Gigabit	9.6.1.94.24.6
SG350X-48	Commutateur administrable empilable 48 ports Gigabit	9.6.1.94.48.1

Nom de la référence	Nom de la gamme	ID d'objet
SG350X-48P	Commutateur administrable empilable PoE 48 ports Gigabit	9.6.1.94.48.5
SG350X-48MP	Commutateur administrable empilable PoE 48 ports Gigabit	9.6.1.94.48.6
SF550X-24	Commutateur administrable empilable 24 ports 10/100	9.6.1.92.24.1
SF550X-24P	Commutateur administrable empilable PoE 10/100 à 24 ports	9.6.1.92.24.5
SF550X-24MP	Commutateur administrable empilable PoE 10/100 à 24 ports	9.6.1.92.24.6
SF550X-48	Commutateur administrable empilable 10/100 à 48 ports	9.6.1.92.48.1
SF550X-48P	Commutateur administrable empilable PoE 10/100 à 48 ports	9.6.1.92.48.5
SF550X-48MP	Commutateur administrable empilable PoE 10/100 à 48 ports	9.6.1.92.48.6
SG550XG-8F8T	SG550XG-8F8T - Commutateur administrable empilable 10 G à 16 ports	9.6.1.90.16.9
SG550XG-24T	SG550XG-24T - Commutateur administrable empilable Base-T 10 G 24 ports	9.6.1.90.24.9
SG550XG-24F	Commutateur empilable 10 Gbit SFP+ à 24 ports (2 ports combo) avec prise en charge d'une alimentation redondante	9.6.1.90.24.8
SG550XG-48T	SG550XG-48T - Commutateur administrable empilable Base-T 10G 48 ports	9.6.1.90.48.9

Les ID d'objet privés sont placés sous : enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1).switch001(101).

ID de moteur

L'ID de moteur est utilisé par des entités SNMPv3 afin de les identifier de façon unique. Un agent SNMP est considéré comme un moteur SNMP faisant autorité. Cela signifie que l'agent répond aux messages entrants (Get, GetNext, GetBulk, Set) et qu'il envoie des interceptions à un gestionnaire. Les informations locales de l'agent sont encapsulées dans des champs au sein du message.

Chaque agent SNMP conserve des informations locales utilisées dans des échanges de messages SNMPv3. L'ID de moteur SNMP par défaut est constitué du numéro d'entreprise et de l'adresse MAC par défaut. Cet ID de moteur doit être unique pour le domaine d'administration afin que deux unités dans un réseau ne possèdent pas le même ID de moteur.

Les informations locales sont stockées dans quatre variables MIB en lecture seule (snmpEngineId, snmpEngineBoots, snmpEngineTime et snmpEngineMaxMessageSize).

PRÉCAUTION Lorsque l'ID de moteur est modifié, tous les utilisateurs et groupes configurés sont effacés.

Pour définir l'ID de moteur SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **ID de moteur**.

ÉTAPE 2 Choisissez l'option souhaitée pour **ID du moteur local**.

- **Valeurs par défaut** : sélectionnez cette option pour utiliser l'ID de moteur généré par le périphérique. L'ID de moteur par défaut utilise l'adresse MAC du périphérique et est défini de façon standard comme suit :
  - *4 premiers octets* : premier bit = 1, le reste correspond au numéro d'entreprise IANA.
  - *Cinquième octet* : défini à l'aide de la valeur 3 pour indiquer l'adresse MAC qui suit.
  - *6 derniers octets* : adresse MAC du périphérique.
- **Aucun** : aucun ID de moteur n'est utilisé.
- **Défini par l'utilisateur** : saisissez l'ID de moteur de périphérique local. 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.

Tous les ID de moteur distant et leurs adresses IP sont affichés dans la table ID de moteur distant.

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

La table ID de moteur distant affiche le mappage entre les adresses IP du moteur et l'ID de moteur.

Pour ajouter l'adresse IP d'un ID de moteur :

ÉTAPE 4 Cliquez sur **Ajouter**. Renseignez les champs suivants :

- **Server Definition** : indiquez si vous souhaitez spécifier le serveur d'ID de moteur par son adresse IP ou son nom.
- **Version IP** : sélectionnez le format IP pris en charge.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée).
- **Adresse IP du serveur/Nom** : saisissez l'adresse IP ou le nom de domaine du serveur de journalisation.
- **ID de moteur** : saisissez l'ID de moteur.

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

Vues

Une vue est une étiquette définie par l'utilisateur pour une collecte de sous-arborescences MIB. Chaque ID de sous-arborescence est défini par l'*ID d'objet* (OID) de la racine des sous-arborescences concernées. Des noms célèbres peuvent être utilisés pour spécifier la racine de la sous-arborescence souhaitée ou un ID d'objet peut être saisi (voir ID d'objet du modèle).

Chaque sous-arborescence est soit incluse, soit exclue dans la vue en cours de définition.

La page Vues permet de créer et de modifier des vues SNMP. Les vues par défaut (Default, DefaultSuper) ne peuvent pas être modifiées.

Vous pouvez joindre des vues à des groupes via la page Groupes ou à une communauté qui utilise le mode d'accès de base via la page Communautés.

Pour définir des vues SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Vues**.

Les champs suivants sont affichés pour chaque vue :

- **Sous-arborescence d'ID d'objet** : sélectionnez le nœud dans l'arborescence MIB, qui est inclus ou exclu dans la vue.
- **Vue de sous-arborescence d'ID d'objet** : indique si le nœud est inclus ou exclu.

ÉTAPE 2 Cliquez sur **Ajouter** pour définir de nouvelles vues.

ÉTAPE 3 Saisissez les paramètres.

- **Nom de la vue** : saisissez un nom de vue qui ne comporte pas plus de 30 caractères.
- **Sous-arborescence d'ID d'objet** : sélectionnez le nœud dans l'arborescence MIB, qui est inclus ou exclu dans la vue SNMP. Les options de sélection de l'objet sont les suivantes :
  - *Sélectionner dans la liste* : vous permet de parcourir l'arborescence MIB. Appuyez sur la touche *Haut* pour accéder au niveau du parent et des frères du nœud sélectionné ; appuyez sur la touche *Bas* pour descendre au niveau des enfants du nœud sélectionné. Cliquez sur les nœuds dans la vue pour passer d'un nœud à son frère. Utilisez la barre de défilement pour faire apparaître les frères dans la vue.
  - *Défini par l'utilisateur* : saisissez un ID d'objet qui n'est pas proposé dans l'option *Sélectionner dans la liste*.

ÉTAPE 4 Sélectionnez ou désélectionnez **Inclure dans la vue**. Si cette option est sélectionnée, les bases MIB sélectionnées sont incluses dans la vue ; sinon, elles sont exclues.

ÉTAPE 5 Cliquez sur **Appliquer**.

ÉTAPE 6 Afin de vérifier votre configuration des vues, sélectionnez les vues définies par l'utilisateur dans la liste **Filtre : Nom de la vue**. Les vues suivantes existent par défaut :

- **Par défaut** : vue SNMP par défaut pour les vues en lecture et en lecture/écriture.
- **DefaultSuper** : vue SNMP par défaut pour les vues d'administrateur.

Groupes

Dans SNMPv1 et SNMPv2, une chaîne de communauté est envoyée accompagnée des trames SNMP. La chaîne de communauté agit en tant que mot de passe pour accéder à un agent SNMP. Cependant, ni les trames, ni la chaîne de communauté ne sont cryptées. Par conséquent, SNMPv1 et SNMPv2 ne sont pas sécurisés.

Dans SNMPv3, les mécanismes de sécurité suivants peuvent être configurés.

- **Authentification** : le périphérique vérifie que l'utilisateur SNMP est un administrateur système autorisé. Cette opération est effectuée pour chaque trame.
- **Confidentialité** : les trames SNMP peuvent accueillir des données cryptées.

Ainsi, dans SNMPv3, il existe trois niveaux de sécurité :

- Pas de sécurité (Aucune authentification et aucune confidentialité)
- Authentification (Authentification et aucune confidentialité)
- Authentification et confidentialité

SNMPv3 permet de contrôler le contenu que chaque utilisateur peut lire ou écrire, ainsi que les notifications qu'il reçoit. Un groupe définit des privilèges de lecture/écriture et un niveau de sécurité. Il devient opérationnel lorsqu'il est associé à un utilisateur ou une communauté SNMP.

REMARQUE Pour associer à un groupe une vue autre que celle par défaut, créez d'abord la vue sur la page Vues.

Pour créer un groupe SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Groupes**.

Cette page contient les groupes SNMP existants ainsi que leurs niveaux de sécurité.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Nom de groupe** : saisissez le nom du nouveau groupe.
- **Modèle de sécurité** : sélectionnez la version SNMP qui est jointe au groupe, à savoir SNMPv1, v2 ou v3.

Il est possible de définir trois types de vues avec différents niveaux de sécurité. Pour chaque niveau de sécurité, sélectionnez les vues correspondant aux privilèges Lecture, Écriture et Notifier en saisissant les champs suivants :

- **Activer** : sélectionnez ce champ pour activer le niveau de sécurité.
- **Niveau de sécurité** : définissez le niveau de sécurité joint au groupe. SNMPv1 et SNMPv2 ne prennent pas en charge l'authentification, ni la confidentialité. Si SNMPv3 est sélectionné, choisissez l'une des options suivantes :
  - *Aucune authentification et aucune confidentialité* : les niveaux de sécurité Authentification ou Confidentialité ne sont pas affectés au groupe.
  - *Authentification et aucune confidentialité* : authentifie les messages SNMP et s'assure que l'origine du message SNMP est authentifiée, mais ne les crypte pas.
  - *Authentification et confidentialité* : authentifie les messages SNMP et les crypte.
- **Afficher** : sélectionnez cette option pour associer une vue avec les privilèges d'accès Lire, Écrire et/ou Notifier du groupe afin de limiter l'étendue de l'arborescence MIB à laquelle le groupe a un accès Lire, Écrire et Notifier.
  - *Read* : l'accès est en lecture seule pour la vue sélectionnée. Sinon, un utilisateur ou une communauté associés à ce groupe peuvent lire toutes les bases MIB, à l'exception de celles qui contrôlent le SNMP lui-même.
  - *Write* : l'accès à la gestion est en écriture pour la vue sélectionnée. Sinon, un utilisateur ou une communauté associés à ce groupe peuvent écrire dans toutes les bases MIB, à l'exception de celles qui contrôlent le SNMP lui-même.
  - *Notifier* : limite le contenu disponible des interceptions à ceux inclus dans la vue sélectionnée. Sinon, il n'existe aucune restriction sur le contenu des filtres. Cette option peut être sélectionnée pour SNMPv3.

ÉTAPE 4 Cliquez sur **Appliquer**. Le groupe SNMP est enregistré dans le fichier Configuration d'exécution.

Utilisateurs

Un utilisateur SNMP est défini par les informations de connexion (nom d'utilisateur, mots de passe et méthode d'authentification), ainsi que par le contexte et l'étendue de son fonctionnement en association avec un groupe et un ID de moteur.

L'utilisateur configuré a les attributs de son groupe et dispose des privilèges d'accès définis dans la vue associée.

Les groupes permettent aux gestionnaires de réseaux d'affecter des droits d'accès à un groupe d'utilisateurs plutôt qu'à un utilisateur unique.

Un utilisateur peut être membre d'un seul groupe.

Pour créer un utilisateur SNMPv3, les éléments ci-dessous doivent exister au préalable :

- Un ID de moteur doit d'abord être configuré sur le périphérique. Cela s'effectue sur la page ID de moteur.
- Un groupe SNMPv3 doit être disponible. Vous pouvez définir un groupe SNMPv3 sur la page Groupes.

Pour afficher des utilisateurs SNMP et en définir de nouveaux :

ÉTAPE 1 Cliquez sur **SNMP** > **Utilisateurs**.

Cette page affiche les utilisateurs existants. Les champs de cette page sont décrits sur la page Ajouter, sauf le champ suivant :

- **Adresse IP** : affiche l'adresse IP du moteur.

ÉTAPE 2 Cliquez sur **Ajouter**.

Cette page fournit des informations quant à l'affectation de privilèges de contrôle d'accès SNMP à des utilisateurs SNMP.

ÉTAPE 3 Saisissez les paramètres.

- **User Name** : saisissez un nom d'utilisateur.
- **ID du moteur** : sélectionnez l'entité SNMP locale ou distante à laquelle l'utilisateur est connecté. La modification ou la suppression de l'ID de moteur SNMP local supprime la base de données d'utilisateurs SNMPv3. Pour recevoir des messages d'information et demander des informations, vous devez définir un utilisateur local et un utilisateur distant.
  - *Local* : l'utilisateur est connecté au périphérique local.
  - *Adresse IP distante* : l'utilisateur est connecté à une autre entité SNMP, en plus du périphérique local. Si un ID de moteur distant est défini, les unités distantes reçoivent des messages d'information, mais ne peuvent effectuer de demandes d'information.

    Saisissez l'ID de moteur distant.

- **Nom du groupe** : sélectionnez le groupe SNMP auquel appartient l'utilisateur SNMP. Vous pouvez définir les groupes SNMP sur la page Ajouter un groupe.

  REMARQUE Les utilisateurs appartenant à des groupes qui ont été supprimés sont conservés, mais sont inactifs.

- **Méthode d'authentification** : sélectionnez la méthode d'authentification qui varie en fonction du Nom de groupe qui a été attribué. Si le groupe ne requiert pas d'authentification, alors l'utilisateur ne peut configurer aucune authentification. Les options sont les suivantes :

  - *None* : aucune authentification d'utilisateur n'est utilisée.
  - *MD5* : mot de passe utilisé pour la génération d'une clé par la méthode d'authentification MD5.
  - *SHA* : mot de passe utilisé pour la génération d'une clé par la méthode d'authentification SHA (Secure Hash Algorithm).

- **Mot de passe d'authentification** : si l'authentification est effectuée via un mot de passe MD5 ou SHA, saisissez le mot de passe de l'utilisateur local en mode **Chiffré** ou **Texte en clair**. Les mots de passe d'utilisateur local sont comparés à la base de données locale et peuvent contenir jusqu'à 32 caractères ASCII.

- **Méthode de confidentialité** : sélectionnez l'une des options suivantes :

  - *Aucune* : le mot de passe de confidentialité n'est pas crypté.
  - *DES* : le mot de passe de confidentialité est crypté conformément à la norme de cryptage de données (DES, Data Encryption Standard).

- **Mot de passe de confidentialité** : 16 octets sont requis (clé de cryptage DES) si la méthode de confidentialité DES a été sélectionnée. Ce champ doit contenir exactement 32 caractères hexadécimaux. Vous pouvez sélectionner le mode **Chiffré** ou **Texte en clair**.

ÉTAPE 4 Cliquez sur **Appliquer** pour enregistrer les paramètres.

Communautés

Vous pouvez gérer les droits d'accès dans SNMPv1 et SNMPv2 en définissant des communautés sur la page Communautés. Le nom de la communauté correspond à un type de mot de passe partagé entre la station de gestion SNMP et l'unité. Il sert à authentifier la station de gestion SNMP.

Les communautés sont uniquement définies dans SNMPv1 et v2, car SNMPv3 fonctionne avec des utilisateurs et non avec des communautés. Les utilisateurs appartiennent à des groupes qui disposent de droits d'accès qui leur sont affectés.

La page Communauté associe des communautés à des droits d'accès, soit directement (mode de base), soit via des groupes (mode avancé) :

- **Mode De base** : les droits d'accès d'une communauté peuvent être définis en Lecture seule, Lecture/écriture ou Admin SNMP. Vous pouvez en outre restreindre l'accès à la communauté à certains objets MIB uniquement, en sélectionnant une vue (définie sur la page Vues).
- **Advanced Mode** (Mode Avancé) : les droits d'accès à une communauté sont définis par un groupe (défini sur la page Groupes). Vous pouvez configurer le groupe avec un modèle de sécurité spécifique. Les groupes disposent des droits d'accès de lecture, d'écriture et de notification.

Pour définir des communautés SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Communautés**.

Cette page contient une table des communautés SNMP configurées et de leurs propriétés. Les champs de cette page sont décrits sur la page Ajouter, sauf le champ suivant :

- **Type de communauté** : affiche le mode de la communauté (**De base** ou **Avancé**).

ÉTAPE 2 Cliquez sur **Ajouter**.

Cette page permet aux gestionnaires de réseaux de définir et de configurer de nouvelles communautés SNMP.

ÉTAPE 3 **Station de gestion SNMP** : cliquez sur **Défini par l'utilisateur** pour saisir l'adresse IP de la station de gestion pouvant accéder à la communauté SNMP. Cliquez sur **Toutes** pour indiquer que n'importe quel périphérique IP peut accéder à la communauté SNMP.

- **Version IP** : sélectionnez IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 pris en charge, en cas d'utilisation d'IPv6. Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.

- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, spécifiez si la réception s'effectue via VLAN ou ISATAP.
- **Adresse IP** : saisissez l'adresse IP de la station de gestion SNMP.
- **Chaîne de communauté** : saisissez le nom de la communauté permettant d'authentifier la station de gestion sur le périphérique.
- **(Type de communauté) De base** : avec ce type, aucune connexion n'est établie avec quelque groupe que ce soit. Vous pouvez uniquement choisir le niveau d'accès de la communauté (Lecture seule, Lecture/écriture ou Admin SNMP) et, facultativement, le faire davantage correspondre à une vue. Par défaut, cela s'applique à la totalité d'une base MIB. Si cette option est sélectionnée, saisissez les champs suivants :
  - *Mode d'accès* : sélectionnez les droits d'accès de la communauté. Les options sont les suivantes :

    Lecture seule : l'accès à la gestion se fait en lecture seule uniquement. Aucune modification ne peut être apportée à la communauté.

    Lecture/écriture : l'accès à la gestion se fait en lecture et écriture. Des modifications ne peuvent être apportées qu'à la configuration d'unité, pas à la communauté.

    Admin SNMP : l'utilisateur dispose d'un accès à toutes les options de configuration d'unité ainsi qu'aux autorisations de modification de la communauté. Admin SNMP équivaut à Lecture/écriture pour toutes les bases MIB, à l'exception des bases MIB SNMP. Admin SNMP est requis pour l'accès aux bases MIB SNMP.
  - *Nom de la vue* : sélectionnez une vue SNMP (collection de sous-arborescences de bases MIB auxquelles un accès est accordé).
- **(Type de communauté) Avancé** : sélectionnez ce type pour une communauté spécifique.
  - *Nom du groupe* : sélectionnez un groupe SNMP qui détermine les droits d'accès.

ÉTAPE 4 Cliquez sur **Appliquer**. La communauté SNMP est définie et le fichier de Configuration d'exécution est mis à jour.

Paramètres de filtre

La page Paramètres de filtre permet de spécifier si les notifications SNMP doivent être envoyées à partir du périphérique, et à quelles conditions. Les destinataires des notifications SNMP peuvent être configurés via la page Destinataires de notifications SNMPv1.2 ou la page Destinataires de notifications SNMPv3.

Pour définir des paramètres d'interception :

ÉTAPE 1 Cliquez sur **SNMP** > **Paramètres de filtre**.

ÉTAPE 2 Sélectionnez **Activer** pour **Notifications SNMP** et indiquez que le périphérique peut envoyer des notifications SNMP.

ÉTAPE 3 Sélectionnez **Activer** pour **Notifications d'authentification** pour activer la notification d'échec d'authentification SNMP.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres de filtre SNMP sont écrits dans le fichier de Configuration d'exécution.

Destinataires de notifications

Des messages de filtre sont générés pour faire état des événements système, comme défini dans la spécification RFC 1215. Le système peut générer des filtres définis dans la base MIB qu'il prend en charge.

Les récepteurs de filtre (connus sous le nom de destinataires de notifications) sont des nœuds réseau auxquels des messages de filtre sont envoyés par le périphérique. Une liste de destinataires de notifications peut être définie.

Une entrée de destination de l'interception contient l'adresse IP du nœud et les informations SNMP qui correspondent à la version qui doit être incluse dans l'interception. Lorsqu'un événement nécessite l'envoi d'un message d'interception, ce dernier est envoyé vers chaque nœud répertorié dans la Table des destinataires de notifications.

La page Destinataires de notifications SNMPv1.2 et la page Destinataires de notifications SNMPv3 permettent la configuration de la destination d'envoi de notifications SNMP, ainsi que les types des notifications SNMP qui sont envoyés vers chaque destination (filtres ou informations). Les messages contextuels Ajouter/Modifier permettent la configuration des attributs des notifications.

Une notification SNMP est un message envoyé depuis le périphérique vers la station de gestion SNMP, qui indique qu'un événement spécifique s'est produit, tel que l'activation ou la désactivation d'une liaison.

Vous pouvez également filtrer certaines notifications. Pour ce faire, vous devez créer un filtre sur la page Filtre de notification et le joindre à un destinataire de notification SNMP. Le filtre de notification permet le filtrage du type des notifications SNMP envoyées à la station de gestion, en fonction de l'ID d'objet de la notification sur le point d'être envoyée.

Destinataires de notifications SNMPv1.2

Pour définir un destinataire dans SNMPv1.2 :

ÉTAPE 1 Cliquez sur **SNMP** > **Destinataires de notifications SNMPv1.2**.

Cette page affiche les destinataires pour SNMPv1.2.

ÉTAPE 2 Renseignez les champs suivants :

- **Informe l'interface IPv4 source** : sélectionnez l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source dans les messages d'information utilisés dans les communications avec les serveurs SNMP IPv4.
- **Déroute l'interface IPv4 source** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source dans les interceptions utilisés dans les communications avec les serveurs SNMP IPv6.
- **Informe l'interface IPv6 source** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source dans les messages d'information utilisés dans les communications avec les serveurs SNMP IPv6.
- **Déroute l'interface IPv6 source** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source dans les interceptions utilisés dans les communications avec les serveurs SNMP IPv6.

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

ÉTAPE 3 Cliquez sur **Ajouter**.

ÉTAPE 4 Saisissez les paramètres.

- **Définition de serveur** : indiquez si vous souhaitez spécifier le serveur de journalisation distant par son adresse IP ou son nom.
- **Version IP** : sélectionnez IPv4 ou IPv6.

- **Type d'adresse IPv6** : sélectionnez soit *Liaison locale*, soit *Global*.
  - *Link Local* (Liaison locale) : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, spécifiez si la réception s'effectue via VLAN ou ISATAP.
- **Adresse IP/Nom du destinataire** : saisissez l'adresse IP ou le nom du serveur où les interceptions sont envoyées.
- **UDP Port** : saisissez le port UDP utilisé pour les notifications sur l'unité du destinataire.
- **Type de notification** : indiquez le type de données à envoyer (interceptions ou informations). Si les deux sont nécessaires, deux destinataires doivent être créés.
- **Délai** : saisissez la durée en secondes pendant laquelle le périphérique doit attendre avant de renvoyer des informations.
- **Tentatives** : saisissez le nombre de fois que le périphérique peut renvoyer une demande d'information.
- **Chaîne de communauté** : dans le menu déroulant, saisissez la chaîne de communauté du gestionnaire de filtres. Les noms de chaîne de communauté sont générés à partir de ceux répertoriés sur la page Communautés.
- **Version de notification** : sélectionnez la version SNMP du filtre.
  Vous pouvez utiliser SNMPv1 ou SNMPv2 comme version des filtres, mais une seule version peut être activée à la fois.
- **Filtre de notification** : sélectionnez cette option pour activer le filtrage du type des notifications SNMP transmises à la station de gestion. Les filtres sont créés via la page Filtre de notification.
- **Nom du filtre** : sélectionnez le filtre SNMP qui définit les informations contenues lors du filtrage (définies sur la page Filtre de notification).

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres de destinataire de notification SNMP sont écrits dans le fichier de Configuration d'exécution.

Destinataires de notifications SNMPv3

Pour définir un destinataire dans SNMPv3 :

ÉTAPE 1 Cliquez sur **SNMP** > **Destinataires de notifications SNMPv3**.

Cette page affiche les destinataires pour SNMPv3.

- **Informe l'interface IPv4 source** : sélectionnez l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source dans les messages d'information utilisés dans les communications avec les serveurs SNMP IPv4.
- **Déroute l'interface IPv4 source** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source dans les interceptions utilisés dans les communications avec les serveurs SNMP IPv6.
- **Informe l'interface IPv6 source** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source dans les messages d'information utilisés dans les communications avec les serveurs SNMP IPv6.
- **Déroute l'interface IPv6 source** : sélectionnez l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source dans les interceptions utilisés dans les communications avec les serveurs SNMP IPv6.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Définition de serveur** : indiquez si vous souhaitez spécifier le serveur de journalisation distant par son adresse IP ou son nom.
- **Version IP** : sélectionnez IPv4 ou IPv6.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie de manière exclusive les hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe **FE80**, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez l'interface de liaison locale dans la liste déroulante (si la liaison locale du type d'adresse IPv6 est sélectionnée).

- **Adresse IP/Nom du destinataire** : saisissez l'adresse IP ou le nom du serveur où les interceptions sont envoyées.
- **Port UDP** : saisissez le port UDP utilisé pour les notifications sur l'unité du destinataire.
- **Type de notification** : indiquez le type de données à envoyer (interceptions ou informations). Si les deux sont nécessaires, deux destinataires doivent être créés.
- **Délai** : saisissez la durée (en secondes) pendant laquelle le périphérique attend avant de renvoyer des informations/filtres. Expiration : plage de 1 à 300, 15 par défaut.
- **Tentatives** : saisissez le nombre de fois que le périphérique peut renvoyer une demande d'information. Tentatives : plage de 1 à 255, 3 par défaut.
- **Nom d'utilisateur** : dans la liste déroulante, sélectionnez l'utilisateur auquel les notifications SNMP sont envoyées. Pour recevoir les notifications, cet utilisateur doit être défini sur la page Utilisateurs, et son ID de moteur doit être distant.
- **Niveau de sécurité** : sélectionnez le niveau d'authentification appliqué au paquet.

  REMARQUE Le niveau de sécurité dépend du nom d'utilisateur qui a été sélectionné. Si le paramètre Aucune authentification a été défini pour ce nom d'utilisateur, le niveau de sécurité est uniquement Aucune authentification. Cependant, si le paramètre Authentication and Privacy (Authentification et confidentialité) a été défini pour ce nom d'utilisateur sur la page Utilisateurs, le niveau de sécurité sur cet écran peut être No Authentication (Aucune authentification), Authentication Only (Authentification) ou Authentication and Privacy (Authentification et confidentialité).

  Les options sont les suivantes :

  - *Aucune authentification* : indique que le paquet n'est pas authentifié ni crypté.
  - *Authentification* : indique que le paquet est authentifié, mais pas crypté.
  - *Confidentialité* : indique que le paquet est à la fois authentifié et crypté.
- **Filtre de notification** : sélectionnez cette option pour activer le filtrage du type des notifications SNMP transmises à la station de gestion. Les filtres sont créés via la page Filtre de notification.
- **Nom du filtre** : sélectionnez le filtre SNMP qui définit les informations contenues lors du filtrage (définies sur la page Filtre de notification).

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres de destinataire de notification SNMP sont écrits dans le fichier de Configuration d'exécution.

Filtre de notification

La page Filtre de notification permet de configurer des filtres de notification SNMP et des ID d'objet (OID) soumis à vérification. Après la création d'un filtre de notification, il est possible de le joindre à un destinataire de notification via la page Destinataires de notifications SNMPv1.2 et via la page Destinataires de notifications SNMPv3.

Le filtre de notification permet le filtrage du type des notifications SNMP envoyées à la station de gestion, en fonction de l'ID d'objet de la notification à envoyer.

Pour définir un filtre de notification :

ÉTAPE 1 Cliquez sur **SNMP** > **Filtre de notification**.

La page Filtre de notification contient les informations de notification relatives à chaque filtre. Ce tableau peut filtrer des entrées de notification par nom de filtre.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Nom du filtre** : saisissez un nom qui ne comporte pas plus de 30 caractères.
- **Sous-arborescence d'ID d'objet** : sélectionnez le nœud dans l'arborescence MIB, qui est inclus dans le filtre SNMP sélectionné ou exclu de celui-ci. Les options de sélection de l'objet sont les suivantes :
  - *Sélectionner dans la liste* : vous permet de parcourir l'arborescence MIB. Appuyez sur la touche *Haut* pour accéder au niveau du parent et des frères du nœud sélectionné ; appuyez sur la touche *Bas* pour descendre au niveau des enfants du nœud sélectionné. Cliquez sur les nœuds dans la vue pour passer d'un nœud à son frère. Utilisez la barre de défilement pour faire apparaître les frères dans la vue.
  - Si vous utilisez l'*ID d'objet*, l'**identificateur d'objet saisi** est inclus dans la vue si l'option **Inclure dans le filtre** est sélectionnée.

ÉTAPE 4 Sélectionnez ou désélectionnez **Inclure dans le filtre**. Si cette option est sélectionnée, les bases MIB sélectionnées sont incluses dans le filtre ; sinon, elles sont exclues.

ÉTAPE 5 Cliquez sur **Appliquer**. Les vues SNMP sont définies et le fichier de Configuration d'exécution est mis à jour.

29

Smart Network Application (SNA)

Cette section décrit le système Smart Network Application (SNA), qui présente une vue d'ensemble de la topologie de réseau comportant des informations détaillées sur les périphériques et le trafic. Il permet d'afficher et de modifier les configurations au niveau global sur tous les périphériques pris en charge du réseau.

Les sujets suivants sont abordés dans ce chapitre :

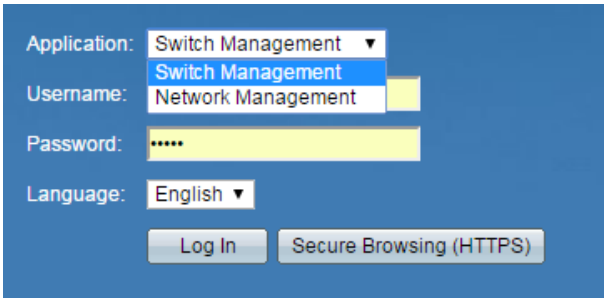
Sessions SNA

Pour lancer le système SNA :

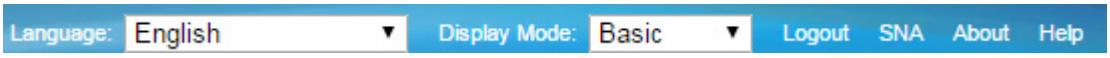
ÉTAPE 1 Ouvrez un navigateur Web.

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

ÉTAPE 3 Lorsque la fenêtre de connexion s'affiche, saisissez votre nom d'utilisateur et votre mot de passe, puis sélectionnez **Gestion du réseau**.



Si l'option Gestion des commutateurs est activée, vous pouvez sélectionner SNA sur la bannière supérieure, comme illustré ci-dessous.



Lors de votre première utilisation de SNA, la carte de topologie est vierge et bloquée par une fenêtre contextuelle. Vous devez saisir vos informations d'identification (nom d'utilisateur et mot de passe aux longueurs maximales respectives de 20 et de 64 caractères). Si les informations d'identification sont rejetées, vous êtes informé de ce rejet et de ses motifs.

Une fois que le système SNA a fini de charger, le système crée une session de gestion avec tous les périphériques prenant ce système en charge dans le réseau sur un protocole WebSocket avec les informations d'identification utilisées pour vous connecter au système SNA. Ainsi, seuls les périphériques prenant en charge le système SNA et utilisant les mêmes informations d'identification peuvent assurer des fonctionnalités relatives aux données et à la gestion. Les autres périphériques n'apparaissent pas en tant que périphériques SNA, même s'ils sont compatibles avec ce système.

Une session SNA peut offrir les niveaux d'autorisation d'accès suivants :

- **Complet** : une session commence en mode d'accès complet. Toutes les opérations SNA sont possibles.
- **Lecture seule** : après une période d'inactivité de 15 minutes, la session devient une session en lecture seule. Dans ce mode, toutes les actions entraînant une écriture ou une modification des paramètres sur des périphériques sont bloquées. Elles ne peuvent être effectuées qu'en réactivant le mode d'accès complet. Pour ce faire, vous devez saisir à nouveau les informations d'identification. Ceci peut être fait à tout moment.

Les opérations n'affectant pas les paramètres des périphériques restent disponibles, quel que soit le mode d'accès à la session.

Le système SNA utilise les mêmes informations d'identification que l'application de gestion du commutateur Web et crée une session de gestion HTTP dans laquelle il fonctionne. La session SNA est prise en compte dans le nombre total de sessions de gestion du Web concurrentes possibles pour le gestionnaire SNA, au même titre que les sessions de gestion du Web régulières actives.

Les paramètres de session peuvent être sauvegardés. Reportez-vous à la section Enregistrement des paramètres SNA.

Graphismes SNA

Cette fonctionnalité SNA est une représentation graphique du réseau utilisateur. Quand la page principale du SNA est ouverte, l'écran se divise pour afficher les parties suivantes :

- Vue de la topologie
- Panneau d'informations s'affichant à droite
- Superpositions topologiques
- Superpositions

Le système SNA utilise les icônes suivantes :

Tableau 1 Description d'icônes

Icône	Description
	Cloud
	Périphérique backbone Le numéro orange correspond au nombre de notifications existant pour le périphérique.
	Périphérique hors connexion (grisé)
	Point d'accès
	PC client
	Téléphone client
	Périphérique inconnu client

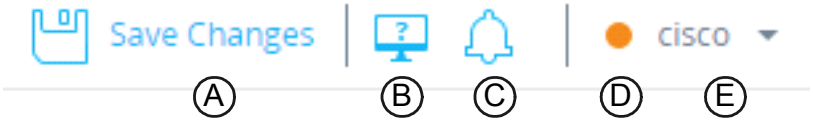
Tableau 1 Description d'icônes

Icône	Description
	Connexion via panneau latéral
	Multisélection via panneau latéral
	Port du panneau latéral

Menu en haut à droite

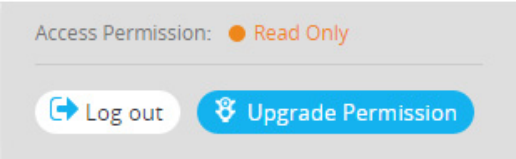
Diverses opérations peuvent être effectuées depuis le menu en haut à droite. Ce menu s'affiche ainsi :

Cliquez sur chaque icône pour effectuer les actions suivantes :



- **A** : enregistrer les modifications apportées à la configuration dans le fichier de Configuration de démarrage.
- **B** : ouvrir le système de gestion des listes DAC. Reportez-vous à la section Fonctionnalité DAC (contrôle des autorisations des périphériques).
- **C** : ouvrir la page des notifications globales. Reportez-vous à la section Notifications.

- **D** : ouvrir cette fenêtre :



  Cette fenêtre affiche ou active les options suivantes :

  - Affiche vos autorisations d'accès.
  - Déconnectez-vous du système en cliquant sur **Déconnexion**.
  - Modifiez vos autorisations en cliquant sur **Modifier le niveau d'autorisation**.

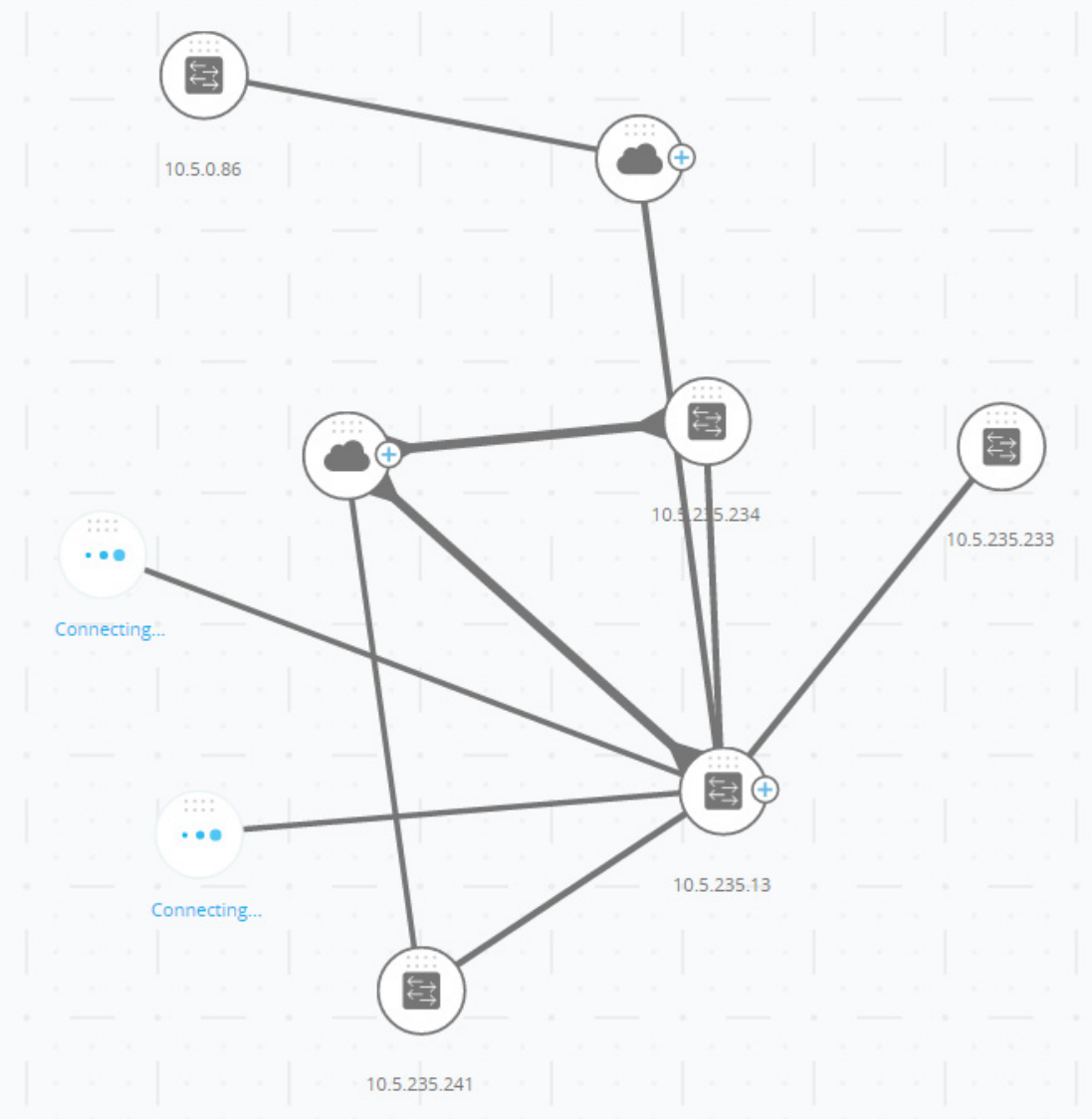
- E : cliquer pour supprimer un périphérique sélectionné.

Vue de la topologie

La vue de la topologie est la vue principale du système SNA.

Figure 1 est une représentation graphique illustrant un exemple de réseau incluant des informations sur des périphériques et des connexions entre les deux.

Figure 1 Vue de la topologie :



Reportez-vous aux Description d'icônes pour obtenir une description des nœuds réseau présentés sur la Figure 1.

Diverses superpositions peuvent être sélectionnées pour modifier la représentation des éléments dans les vues de la topologie. Reportez-vous à la section Superpositions topologiques.

Le mécanisme de détection de la topologie utilise des informations récupérées depuis les TLV LLDP et CDP afin d'identifier les périphériques du réseau.

Pour obtenir le plus d'informations possible sur la topologie, l'ensemble des périphériques du réseau prenant en charge ces protocoles doivent les activer.

Comme la topologie est créée en lançant des sessions de gestion avec les périphériques SNA participants, lors de l'utilisation du protocole HTTPS pour lancer le système SNA, l'ensemble des commutateurs SNA du réseau doivent être autorisés ou ajoutés à la liste des exceptions de certificats sur le client Web (l'explorateur) utilisé pour le système SNA.

Superpositions topologiques

Diverses superpositions pour la vue de la topologie sont prises en charge afin de déterminer les contenus de la représentation graphique d'éléments de cette vue. Les superpositions prises en charge comprennent : Appartenance VLAN, Spanning tree, PoE et Utilisation des liaisons. Si vous sélectionnez la superposition Appartenance VLAN, par exemple, les informations VLAN sont ajoutées à la vue de la topologie. Consultez Superpositions pour une description complète.

Éléments de la topologie

La vue de la topologie affiche les types d'éléments suivants :

- Périphériques
- Ports
- Connexions entre les périphériques
- Nuages

Périphériques

Les périphériques détectés sont représentés sous forme de nœuds dans la vue de la topologie, comme l'illustre la Figure 1.

Cliquez sur un périphérique pour afficher les informations suivantes dans le panneau situé à droite (si ces informations sont disponibles) :

- **Type de périphérique** : la forme de l'icône indique le type de périphérique. Les types de périphériques incluent : commutateur, point d'accès, PC ou téléphone IP. Si le type de périphérique n'est pas prédéfini ou s'il n'est pas détecté correctement, le périphérique s'affiche avec la mention **Inconnu**.

  Les commutateurs détectés sur le réseau sont identifiés selon les types suivants :

  - **Commutateur SNA** : commutateur (exécutant la version 2.2.5 ou supérieure) disposant de toutes les fonctionnalités SNA.
  - **Commutateur SNA partiel** : commutateur auquel vous pouvez accéder à distance en démarrant une session de gestion via un commutateur SNA. Ceci n'inclut pas la détection, les explorateurs de services ni l'intégralité des fonctionnalités SNA.
  - **Commutateur non géré** : commutateur auquel vous ne pouvez pas accéder via le système SNA.
- **Nom de l'appareil**
- **Adresse IP** (une liste si plusieurs adresses sont détectées)
- **Adresse MAC** (une liste si plusieurs adresses sont détectées)
- **Nombre de notifications** : le nombre de notifications est indiqué en orange sur l'icône du périphérique. Les notifications s'affichent dans le panneau d'informations situé à droite.
- **Prise en charge SNA**
- **Fabricant**

Certains périphériques (en particulier ceux qui prennent en charge le système SNA) disposent d'informations supplémentaires, telles que des informations relatives à chaque port. Ces informations peuvent être consultées en cliquant sur leur icône et en affichant un écran correspondant à l'explorateur du périphérique concerné.

Les périphériques se répartissent selon les catégories suivantes :

- **Périphériques backbone** : éléments formant le squelette de base du réseau. Par défaut, tous les commutateurs, routeurs et points d'accès détectés sur le réseau sont automatiquement désignés comme des périphériques backbone.

  Lorsqu'un périphérique backbone est détecté, il demeure sur la carte de topologie jusqu'à sa suppression manuelle. Si le périphérique est déconnecté du réseau, il apparaît encore sur la carte de topologie sous forme de périphérique hors ligne.

Un périphérique prenant en charge le système SNA ou un périphérique géré sera détecté tant qu'il restera connecté au réseau via l'adresse IP qu'il utilisait au préalable.

- **Périphériques hors ligne** : périphériques backbone préalablement ajoutés à la topologie (soit manuellement, soit par détection automatique). Ces périphériques ne sont plus détectés par le système SNA.

  Les périphériques hors ligne présentent les caractéristiques suivantes :

  - Représentation visuelle différente de celle des périphériques en ligne de la carte de topologie (voir «Vue de la topologie :»).
  - Peuvent être déplacés sur la topologie et leur emplacement peut être enregistré. Vous pouvez également ajouter des balises à ces périphériques (voir Balises).
  - Ils peuvent être sélectionnés et détectés par la fonctionnalité de recherche. Quand un périphérique hors ligne est sélectionné, le panneau d'informations affiche ses principales informations d'identification et ses balises, sans préciser les services, les notifications ou d'autres informations d'identification plus précises.
  - Ne peut pas lancer l'explorateur du périphérique ou l'interface utilisateur de gestion des périphériques hors ligne.
  - Peut être supprimé manuellement. Après la suppression d'un périphérique, celui-ci ne figure plus sur la carte de topologie tant qu'il n'est pas détecté ou ajouté manuellement. Toutes les balises associées à ce périphérique sont perdues et ne seront pas restaurées, même en cas de détection ultérieure de ce même périphérique.

  Le système SNA tente régulièrement de se connecter aux périphériques hors ligne afin de vérifier si un commutateur SNA ou un commutateur géré est de nouveau en ligne. Pendant ces tentatives, une indication s'affiche sur le périphérique.

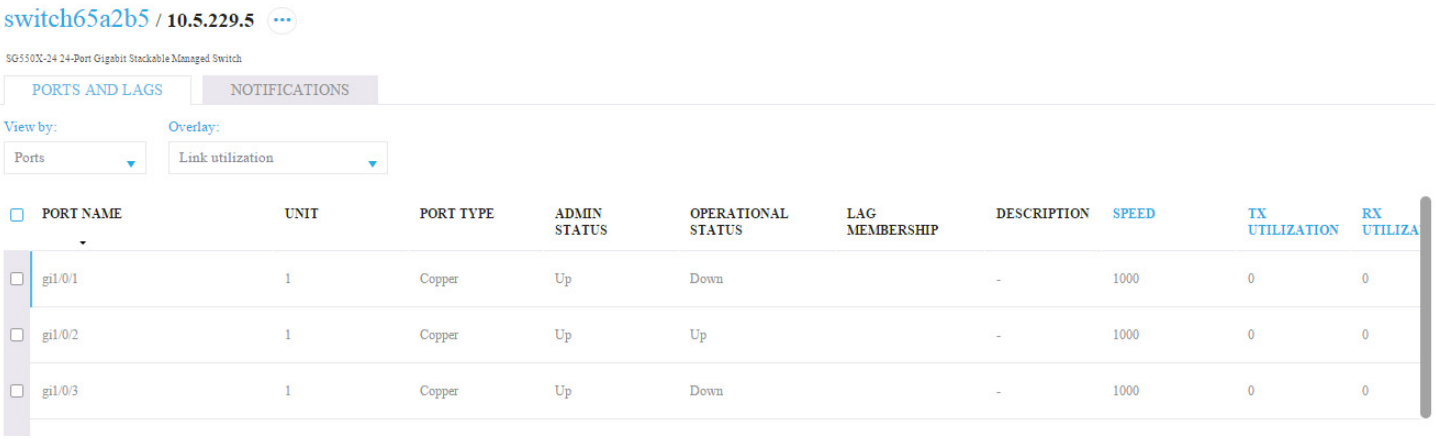
- **Périphériques client** : cette expression désigne les clients d'extrémité du réseau (par exemple les PC ou les téléphones IP), généralement connectés à un périphérique backbone. Dans la carte de topologie, ces périphériques sont regroupés avec les autres périphériques du même type connectés au même périphérique backbone. Ces regroupements de périphériques sont appelés *groupes client* et les clients composant un groupe client peuvent être consultés individuellement en cliquant sur leur explorateur pour y accéder (voir Explorateurs).

Si un périphérique est connecté à au moins un périphérique client, un + s'affiche :

Cliquez sur le + pour afficher les clients. L'exemple suivant présente le cas de deux clients connectés à un périphérique cloud : un PC client et un périphérique de type inconnu.

Ports

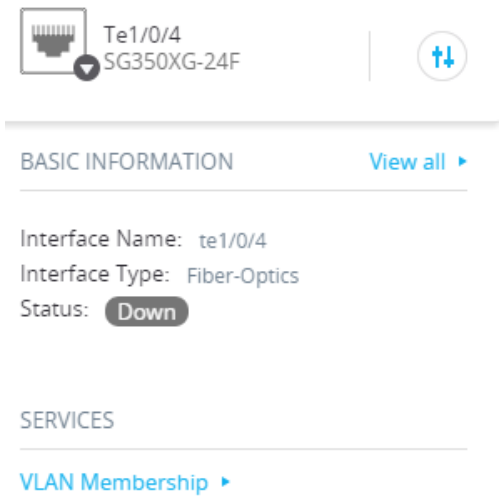
Pour afficher les ports d'un périphérique, sélectionnez ce périphérique, puis faites un double-clic dessus. Cela permet d'ouvrir un panneau présentant tous les ports du périphérique, y compris toutes les unités si ce périphérique est en mode de pile.



Les caractéristiques suivantes s'affichent :

- Nom du port
- Unité
- État administrateur
- État opérationnel (y compris le motif de désactivation si le port a été désactivé par le logiciel).
- Appartenance LAG
- Description (si une description a été saisie).
- Débit
- Mode Switchport
- Utilisation du port (Réception et Transmission)

Lorsque vous sélectionnez un port dans ce panneau, des informations supplémentaires s'affichent sur le panneau latéral, comme illustré ci-dessous :



Définition du nom de l'interface

Les noms des interfaces correspondant aux périphériques SNA ou SNA partiels sont constitués des éléments suivants :

- Un préfixe basé sur le type de port : FE pour les ports rapides, GE pour les ports Giga ou XG pour les ports 10 Gbit.
- Un ID d'interface correspondant au numéro de l'interface sur un périphérique non empilé ou l'ID d'unité suivi d'une barre oblique, puis de l'ID d'interface pour un périphérique appartenant à un empilage.

Le numéro de logement du port n'est pas précisé sur le système SNA. Par exemple, le port Giga-octet **gi1/0/12** s'affiche comme **GE1/12** dans le système SNA.

Les noms des ports détectés sur les périphériques ne prenant pas en charge le système SNA conservent leur nom annoncé, sans modification.

Connexions entre les périphériques

Les connexions entre les périphériques s'affichent selon un code couleur qui varie selon la superposition utilisée (voir Superpositions).

Une connexion peut représenter un lien simple entre des périphériques ou une agrégation de liaisons entre deux périphériques.

L'épaisseur des connexions entre les commutateurs sur la carte de topologie fournit une indication de la bande passante totale disponible sur cette connexion, celle-ci étant déterminée par le débit opérationnel des liaisons utilisées dans cette connexion.

Les épaisseurs de connexion suivantes sont disponibles (de la plus fine à la plus large) :

- Niveau 1 : moins de 1 Go
- Niveau 2 : entre 1 Go et 10 Go
- Niveau 3 : à partir de 10 Go

Les liaisons dont la capacité ne peut pas être calculée ou les liens entre un périphérique backbone et ses clients s'affichent sous forme de liaisons de niveau 1.

La connexion entre des périphériques prenant en charge le système SNA est détectée de part et d'autre. S'il existe une différence entre les capacités calculées de la connexion entre les deux périphériques, l'épaisseur retenue correspond à la plus basse des deux valeurs.

Vous pouvez accéder à un explorateur de connexion pour des liaisons spécifiques en cliquant sur ces liaisons. Les informations suivantes sont indiquées :

- Nom du port ou des ports de part et d'autre de la liaison (si ce nom est connu).
- ID de LAG, le cas échéant.
- Informations de base sur les périphériques connectés : type de périphérique, nom du périphérique, IP.
- Bande passante de chaque liaison assurant la connexion.

Nuages

Les nuages représentent des sections du réseau dont le système SNA ne peut pas afficher une carte détaillée. Ils sont indiqués par l'icône suivante :

Le système SNA identifie la connexion de plusieurs périphériques au réseau via un port spécifique, mais ne peut déterminer les relations existant entre ces périphériques. Ceci se produit lorsqu'aucun périphérique d'un groupe ne prend en charge le système SNA. Le système SNA affiche un nuage sur la carte de topologie et affiche les périphériques détectés dans ce groupe en tant que clients connectés.

La majorité des opérations SNA ne s'appliquent pas à de tels groupes.

Panneau d'informations s'affichant à droite

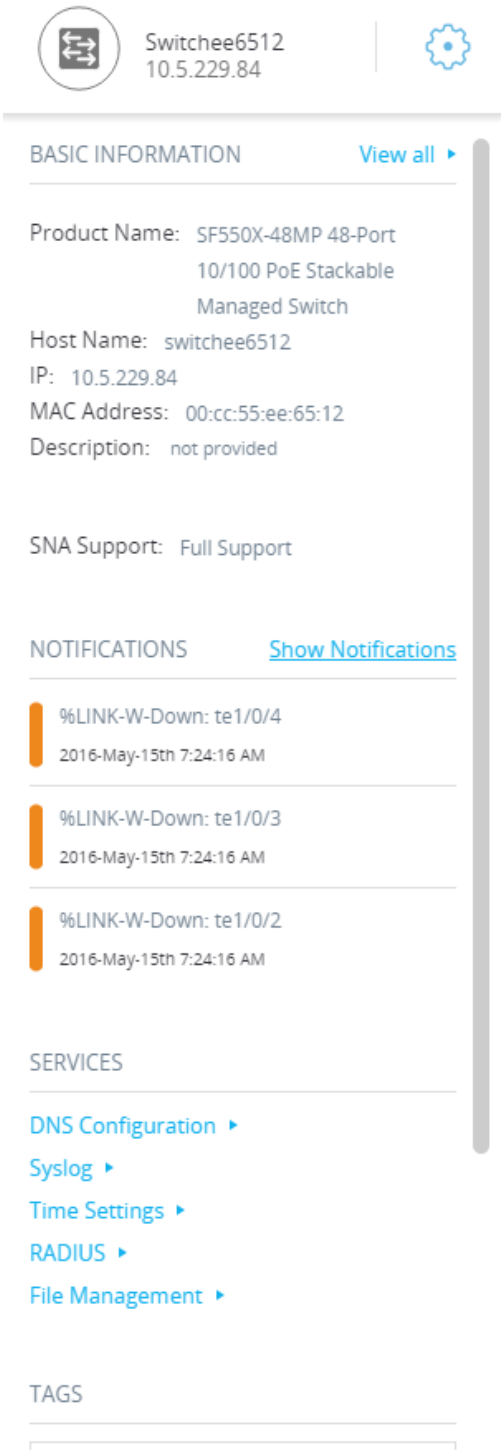
La zone située à droite de la vue de la topologie présente un panneau d'informations regroupant les caractéristiques des éléments sélectionnés et permet d'agir sur ces éléments.

Ce panneau d'informations contient les sections suivantes :

- Section d'en-tête
- Icône représentant un engrenage sur le panneau d'informations s'affichant à droite
- Section Informations de base
- Section Notifications
- Section Services
- Balises
- Statistiques

Figure 2 illustre un exemple de panneau d'informations s'affichant à droite :

Figure 2 Panneau d'informations s'affichant à droite

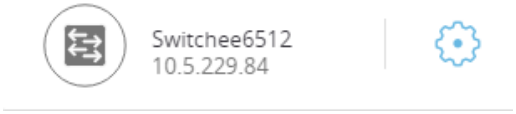


Section d'en-tête

Cette section présente les icônes correspondant aux éléments sélectionnés. S'il s'agit d'un élément seul, cette section d'en-tête affiche ses informations d'identification, comme illustré ci-dessous.

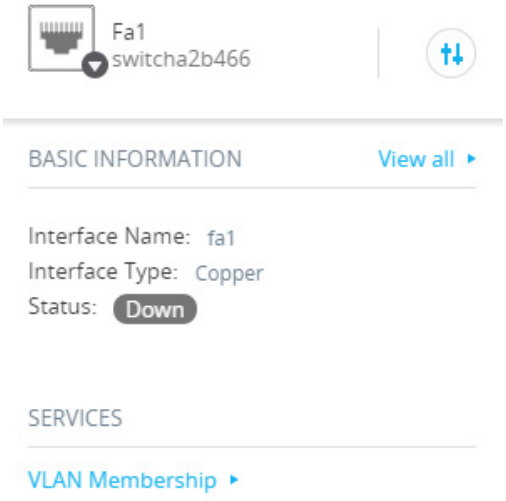
Les informations suivantes s'affichent dans la section d'en-tête, selon le type d'élément sélectionné :

- **Périphériques** : informations d'identification comprenant le type de périphérique et les deux critères d'identification les plus importants détectés pour le périphérique. Voici une liste des méthodes d'identification par ordre d'importance : Nom d'hôte → Adresse IP → Adresse MAC Par exemple :

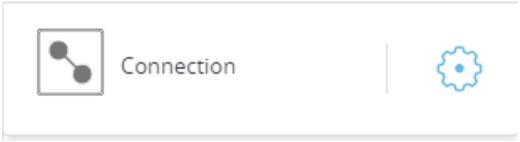


  Si le nom d'hôte, l'adresse IP et l'adresse MAC d'un périphérique sont connus, seuls le nom d'hôte et l'adresse IP s'affichent. Si le nom d'hôte ou l'adresse IP sont inconnus, l'adresse MAC remplace l'attribut manquant.

- **Interfaces** : les informations d'identification correspondent au nom de l'interface et à l'attribut identifiant le plus important du périphérique auquel elle appartient : nom d'hôte, adresse IP si le nom d'hôte est inconnu, adresse MAC si le nom d'hôte et l'adresse IP sont inconnus.



- **Connexions** : les informations d'identification correspondent aux deux attributs d'identification les plus importants des périphériques des deux côtés de la connexion (nom d'hôte → adresse IP → adresse MAC). Une connexion peut contenir une ou plusieurs liaisons.



Si plusieurs éléments sont sélectionnés, la section d'en-tête affiche le nombre d'éléments sélectionnés et si tous les éléments sélectionnés sont du même type, cette section précise également le type en question, comme illustré ci-dessous (ici, le type n'est pas affiché, car les éléments sont hétérogènes).

La sélection d'un groupe client permet de sélectionner instantanément tous les membres du groupe. La section d'en-tête affiche le nombre de périphériques du groupe et leur type.

Lorsque vous sélectionnez un groupe client avec d'autres périphériques, le nombre de périphériques compris dans le groupe est pris en compte. Par exemple, si vous sélectionnez un périphérique backbone et un groupe client contenant 5 clients, cette section indique que 6 périphériques sont sélectionnés.

Si des notifications existent pour le périphérique, leur nombre est affiché :

Icône représentant un engrenage sur le panneau d'informations s'affichant à droite

Les actions suivantes peuvent être effectuées sur les périphériques ou les connexions sélectionnés : Pour effectuer ces actions, cliquez sur l'icône représentant un engrenage située dans le panneau d'informations s'affichant à droite ( ).

- **Gérer le périphérique** : cette option n'est disponible que pour les commutateurs SNA et SNA partiels et à condition qu'un seul périphérique soit sélectionné. Lorsque vous sélectionnez cette action, vous démarrez une session de gestion pour le commutateur sélectionné à l'aide de l'application de gestion du commutateur. Il n'est pas nécessaire de saisir vos informations d'identification pour lancer cette session.

- **Explorer le périphérique** : cette option n'est disponible que pour les commutateurs SNA et à condition qu'un seul périphérique soit sélectionné. Lorsque vous sélectionnez cette action, vous ouvrez l'explorateur du périphérique correspondant au commutateur sélectionné.
- **Localiser le périphérique** : cette option n'est disponible que pour les commutateurs SNA. Cette action permet de faire clignoter les voyants du périphérique pendant 5 minutes. Pendant cet intervalle, une boîte de dialogue s'affiche pour signaler que la fonctionnalité de localisation est activée. Elle permet également d'interrompre cette localisation.
- **Explorer la connexion** : cette option s'affiche lorsqu'une seule connexion est sélectionnée. Lorsque vous sélectionnez cette action, vous ouvrez l'explorateur de connexion correspondant à la connexion sélectionnée.
- **Explorer le groupe client** : cette option s'affiche lorsqu'un groupe client est sélectionné. Lorsque vous sélectionnez cette action, vous ouvrez l'explorateur client, filtré par le type de périphérique dans le groupe client.
- **Supprimer** : cette option s'affiche uniquement lorsque tous les périphériques sélectionnés sont des périphériques hors ligne. Lorsque vous sélectionnez cette action, vous supprimez tous les périphériques sélectionnés de la carte de topologie.

Section Informations de base

La section **Informations de base** affiche les attributs du seul élément sélectionné (voir les tableaux ci-dessous pour une description complète). Cette section ne s'affiche pas quand plusieurs éléments sont sélectionnés.

Certaines informations s'affichent systématiquement, tandis que d'autres ne s'affichent que si vous cliquez sur le bouton **Tout afficher**.

Lorsqu'aucune information n'est reçue pour un paramètre donné, ce paramètre ne s'affiche pas dans la section Informations de base.

Les informations suivantes sont affichées pour chaque **périphérique backbone** :

Nom du paramètre	Notes	Exemple
Nom de produit	D'après la description de la MIB (base d'information de gestion) de l'appareil. Ce champ ne s'affiche que si le périphérique est un commutateur prenant en charge totalement ou partiellement le système SNA.	SG500-52P – Commutateur administrable empilable PoE 52 ports Gigabit
Nom d'hôte	Chaîne d'une longueur maximale de 58 caractères.	RND_1
Adresse IP	Affiche l'adresse IP utilisée par le système SNA pour se connecter au périphérique. Les adresses existantes supplémentaires annoncées (IPv4 et IPv6) peuvent être affichées en cliquant sur l'icône à côté de l'étiquette.	192.168.1.55 923:a8bc::234
Adresse MAC	Adresse MAC de base du périphérique.	00:00:b0:83:1f:ac
Description	Plage modifiable de 80 caractères maximum. Enregistré sur le stockage SNA.	
Prise en charge SNA	Valeurs possibles : • Prise en charge complète des périphériques SNA • Prise en charge partielle des périphériques gérés • Aucune prise en charge SNA pour les périphériques non gérés Ce paramètre ne s'affiche que pour les commutateurs.	
Les paramètres ci-dessous ne s'affichent que lorsque l'option **Tout afficher** est activée. Cette option n'est disponible que si le périphérique est un commutateur prenant en charge totalement ou partiellement le système SNA.		

Nom du paramètre	Notes	Exemple
VLAN existants	Une liste des VLAN créés sur le périphérique Des lignes en pointillé sont utilisées pour relier des VLAN consécutifs.	1, 6, 13-19, 1054, 2012-2100, 4094
Version active du microprogramme	Le numéro de version du microprogramme actif.	2.2.0.53
Temps de disponibilité du système	Le temps écoulé depuis l'activation du périphérique, exprimé en jours, heures, minutes et secondes.	
Heure locale du système	Heure locale sur le périphérique, exprimée au format du fichier de langue actif.	Exemple pour un fichier en anglais : 2015-Nov-04 17:17:53
Nombre d'unités	Ne s'affiche que sur les périphériques empilables.	2
Numéro d'unité d'alimentation PoE/Puissance PoE disponible	Affiché uniquement sur les périphériques prenant en charge l'alimentation PoE. Affiche la puissance disponible utilisée relativement à l'alimentation maximale. S'il s'agit d'un appareil empilé, un champ s'affiche pour chaque unité prenant en charge l'alimentation PoE dans la pile avec son ID d'unité. Si le périphérique est autonome ou isolé, l'étiquette du champ ne mentionne pas son ID d'unité. Ainsi, huit champs maximum peuvent apparaître ici.	15,22 W/18 W

Les informations suivantes sont affichées pour les périphériques backbone hors ligne sous la mention **Dernières informations connues**.

Nom du paramètre	Notes	Exemple
Nom de produit	Issu de la description de la MIB (base d'information de gestion) de l'appareil. Ce champ ne s'affiche que si le périphérique est un commutateur prenant en charge totalement ou partiellement le système SNA.	SG500-52P – Commutateur administrable empilable PoE 52 ports Gigabit
Nom d'hôte	Chaîne d'une longueur maximale de 58 caractères.	RND_1
Adresse IP	Affiche la dernière adresse IP utilisée pour se connecter au périphérique la dernière fois qu'il a été détecté.	192.168.1.55
Adresse MAC	Adresse MAC de base du périphérique.	00:00:b0:83:1f:ac
Description	Plage modifiable de 80 caractères maximum.	
Dernière consultation	Jour et heure de la dernière détection du périphérique par le système SNA, exprimés selon le format correspondant au fichier de langue actif.	Exemple pour un fichier en anglais : 2015-Nov-04 17:17:53

Les informations suivantes s'affichent pour un client (périphérique d'extrémité, tel qu'un PC).

Nom du paramètre	Notes	Exemple
Nom d'hôte	Chaîne d'une longueur maximale de 58 caractères.	RND_1
Adresse IP	Affiche l'adresse IP utilisée par le système SNA pour se connecter au périphérique. Les adresses annoncées supplémentaires (IPv4 et IPv6) peuvent être affichées en cliquant sur une icône à côté de l'étiquette.	192.168.1.55 923:a8bc::234

Nom du paramètre	Notes	Exemple
Adresse MAC	Adresse MAC de base du périphérique.	00:00:b0:83:1f:ac
Type d'appareil	Le type d'appareil client.	Téléphone Hôte Inconnu
Interface connectée	L'interface via laquelle le périphérique se connecte au commutateur le plus proche.	GE1/14
Les paramètres ci-dessous ne s'affichent que lorsque l'option **Tout afficher** est activée.		
Débit de connexion		100M 10G
Appartenance VLAN	Affiche les VLAN actifs auxquels appartient l'interface connectée. Des tirets sont utilisés pour relier des VLAN consécutifs.	1, 6, 13-19, 1054, 2012-2100, 4094
Pourcentage d'utilisation du port (transmission et réception)	En fonction des informations du port connecté.	80/42
Consommation énergétique de l'appareil PoE	Ne s'affiche que si le client est connecté à un port PoE.	8 900 mW

Les informations suivantes sont affichées pour chaque groupe client :

Nom du paramètre	Notes	Exemple
Nom d'hôte	C'est le nom d'hôte du périphérique parent du groupe client. Ce paramètre et toutes les autres informations relatives au périphérique parent s'affichent sous un titre **Connecté à**. Chaîne d'une longueur maximale de 58 caractères.	RND_1
Adresse IP du périphérique parent	Affiche l'adresse IP utilisée par le système SNA pour se connecter au périphérique parent. Les adresses annoncées supplémentaires (IPv4 et IPv6) peuvent être affichées en cliquant sur une icône à côté de l'étiquette.	192.168.1.55 923:a8bc::234
Adresse MAC du périphérique parent	L'adresse MAC de base du périphérique parent.	00:00:b0:83:1f:ac
Connecté via le cloud	Cette étiquette apparaît si le groupe client est connecté au réseau via un cloud. L'étiquette remplace le nom d'hôte, l'adresse IP et l'adresse MAC.	

Les informations suivantes sont affichées pour les **interfaces** :

Nom du paramètre	Notes	Exemple
Nom de l'interface		GE1/14 LAG12
Type d'interface	Affiché uniquement pour les ports.	Copper-1G
État	État opérationnel de l'interface.	Actif Inactif Inactif (ACL)
Les paramètres ci-dessous ne s'affichent que lorsque l'option **Tout afficher** est activée.		

Nom du paramètre	Notes	Exemple
Description de l'interface	Utilise la description MIB ifAlias de l'interface. Chaîne d'une longueur maximale de 64 caractères	« WS 28 »
Débit opérationnel		100M 10G
Appartenance LAG	Affiché uniquement pour les ports. Peut être **Aucune** ou le nom du LAG.	LAG15
Ports membres	S'affichent uniquement pour les LAG et présentent une liste des interfaces qui sont des membres actifs du LAG. Les plages consécutives d'interfaces sont reliées par des tirets.	GE1/4, GE1/6, XG2/4-8
Appartenance VLAN	Indique les VLAN actifs auxquels appartient l'interface. Des lignes en pointillé sont utilisées pour relier des VLAN consécutifs.	1, 6, 13-19, 1054, 2012-2100, 4094
Pourcentage d'utilisation du port (transmission et réception)	S'affiche uniquement pour les ports.	80/42
Type du LAG	S'affiche uniquement pour les LAG. Les valeurs possibles sont **Standard** ou **LACP**.	
Mode Switchboard	Valeurs possibles : • Accès • Liaison • Général • Client • Privé - Hôte • Privé - De proximité	

Nom du paramètre	Notes	Exemple
Consommation énergétique de l'appareil PoE	S'affiche uniquement pour les ports prenant en charge l'alimentation PoE.	8900 MW
État spanning tree	Affiche l'état STP de l'interface.	Blocage Transfert Désactivé

REMARQUE La section Informations de base ne s'affiche pas lorsque vous sélectionnez des clients ou des clouds de couche 2.

Section Notifications

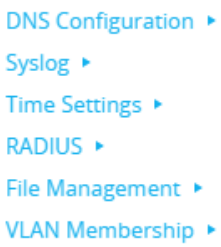
La section Notifications affiche les dernières notifications (SYSLOG) enregistrées sur le périphérique sélectionné.

La section Notification ne s'affiche que lorsque vous sélectionnez un appareil SNA unique.

Pour plus d'informations, consultez Notifications.

Section Services

Cette section de panneau d'informations affiche les services disponibles pour la sélection actuelle d'éléments. Seuls s'affichent les services correspondant aux éléments sélectionnés. Cette section ne s'affiche pas si des éléments ne prenant pas en charge les services sont inclus dans la sélection ou lorsque des périphériques et des interfaces sont sélectionnés ensemble.



Pour plus d'informations, reportez-vous à la section Services.

Balises

Les balises permettent d'identifier les éléments de la topologie via leurs attributs (voir Balises). La section **Balises** du panneau d'informations situé à droite affiche toutes les balises assignées à l'élément par l'utilisateur ou de manière automatique. Vous pouvez également gérer les balises pour les éléments sélectionnés dans cette partie du panneau. Pour plus d'informations, reportez-vous à la section Balises.

Statistiques

Lorsque vous examinez un périphérique prenant en charge le système SNA, ou les interfaces d'un tel périphérique, vous pouvez consulter les informations statistiques historiques relatives à cette interface ou à ce périphérique.

Vous pouvez accéder à la vue Statistiques à partir du panneau d'informations situé à droite.

Pour consulter des statistiques historiques relatives à une interface ou à périphérique, sélectionnez un paramètre spécifique dans une liste de paramètres disponibles en tenant compte des paramètres pris en charge par la fonctionnalité d'historique des compteurs intégrés. Vous pouvez consulter l'état de ce paramètre sur l'interface sélectionnée pour l'année précédente.

Les graphiques suivants peuvent être consultés :

- Graphique représentant l'utilisation du port
- Graphique représentant la consommation PoE (port)
- Graphique représentant la consommation PoE (périphérique)
- Graphique représentant le trafic (octets)
- Graphique représentant le trafic (paquets)

Graphique représentant l'utilisation du port

Ce graphique représente, au niveau du port, le pourcentage d'utilisation du port pendant une période donnée. Il est disponible pour tous les ports des périphériques prenant en charge le système SNA.

Vous pouvez sélectionner plusieurs ports pour effectuer une comparaison sur plusieurs colonnes.

Les données s'affichent sous forme de pourcentage (de 0 à 100) en précisant le nombre et la fréquence des échantillonnages en fonction de la durée affichée :

- Dernières cinq minutes : 20 échantillons (un toutes les 15 secondes)
- Dernière heure : 60 échantillons (un par minute)
- Dernière journée : 24 échantillons (un par heure)
- Dernière semaine : 7 échantillons (un par jour)
- Derniers 3 mois : 12 échantillons (un par semaine)

Graphique représentant la consommation PoE (port)

Ce graphique représente la consommation PoE du port pendant une période donnée. Il est disponible pour tous les ports PoE des périphériques prenant en charge le système SNA.

Vous pouvez sélectionner plusieurs ports pour effectuer une comparaison sur plusieurs colonnes.

Les données sont exprimées en watts (de 0 à 30/60, selon la prise en charge de l'alimentation PoE+) en précisant le nombre et la fréquence des échantillonnages en fonction de la durée affichée :

- Dernière heure : 60 échantillons (un par minute)
- Dernière journée : 24 échantillons (un par heure)
- Dernière semaine : 7 échantillons (un par jour)
- Dernière année : 52 échantillons (un par semaine)

Graphique représentant la consommation PoE (périphérique)

Ce graphique représente la consommation PoE du port au niveau du périphérique pendant une période donnée. Il est disponible pour tous les périphériques PoE prenant en charge le système SNA.

Le graphique représente chaque unité individuellement. Vous pouvez sélectionner plusieurs unités (dans une ou plusieurs piles) pour les afficher simultanément.

Les données sont exprimées en watts (de 0 à la plus grande capacité PoE parmi les unités sélectionnées) et précisent le nombre et la fréquence des échantillonnages en fonction de la durée affichée :

- Dernière heure : 60 échantillons (un par minute)
- Dernière journée : 24 échantillons (un par heure)

- Dernière semaine : 7 échantillons (un par jour)
- Dernière année : 52 échantillons (un par semaine)

Graphique représentant le trafic (octets)

Ce graphique représente le trafic total sur une interface, exprimé en octets, pour une durée donnée, au niveau de l'interface. Il est disponible pour toutes les interfaces des périphériques prenant totalement en charge le système SNA et présente des lignes distinctes pour le trafic transmis et reçu.

Vous pouvez sélectionner plusieurs ports et types de trafic différents pour effectuer une comparaison sur plusieurs colonnes.

Les données sont exprimées en octets (de 0 à l'échantillonnage le plus élevé pour les interfaces ou la période sélectionnées) en précisant le nombre et la fréquence des échantillonnages en fonction de la durée affichée :

- Dernières cinq minutes : 20 échantillons (un toutes les 15 secondes)
- Dernière heure : 60 échantillons (un par minute)
- Dernière journée : 24 échantillons (un par heure)
- Dernière semaine : 7 échantillons (un par jour)
- Derniers 3 mois : 12 échantillons (un par semaine)

Graphique représentant le trafic (paquets)

Ce graphique représente le trafic total sur une interface, exprimé en paquets, pour une durée donnée. Il est disponible pour toutes les interfaces (ports ou LAG) des périphériques prenant totalement en charge le système SNA.

Les données des deux versions sont exprimées en nombre de paquets (0 étant la valeur la plus élevée dans la plage échantillonnée) en précisant le nombre et la fréquence des échantillonnages en fonction de la durée affichée :

- Dernières cinq minutes : 20 échantillons (un toutes les 15 secondes)
- Dernière heure : 60 échantillons (un par minute)
- Dernière journée : 24 échantillons (un par heure)
- Dernière semaine : 7 échantillons (un par jour)
- Derniers 3 mois : 12 échantillons (un par semaine)

Opérations

La vue de la topologie affiche les éléments et leurs connexions dans le réseau. Des opérations peuvent être effectuées sur les éléments affichés dans la vue de la topologie.

Quand vous sélectionnez un élément dans la topologie, il est possible d'effectuer l'une des actions suivantes :

- Consulter les informations relatives à cet élément, voir Explorateurs
- Configurer un élément, voir Services
- Ajouter un périphérique ou un commutateur à la vue de la topologie, voir Ajouter manuellement un périphérique ou un commutateur à la vue de la topologie

REMARQUE Lorsque vous sélectionnez plusieurs éléments, seules les actions disponibles pour l'ensemble des éléments sélectionnés sont proposées.

Vous pouvez effectuer davantage d'opérations sur les périphériques prenant en charge le système SNA que sur les autres périphériques de la topologie.

Les actions suivantes peuvent être effectuées sur les périphériques prenant en charge le système SNA :

- Zoomer pour obtenir une vue plus détaillée de ses interfaces.
- Lancer des sessions de gestion Web sur d'autres périphériques prenant en charge le système SNA et sur des périphériques gérés via le système SNA (sans passer par l'écran de connexion) si le périphérique géré ou le périphérique SNA autorise les sessions de gestion avec les mêmes informations d'identification que celles que vous avez utilisées pour vous connecter au système SNA.

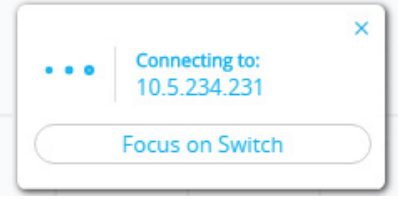
Ajouter manuellement un périphérique ou un commutateur à la vue de la topologie

Des éléments peuvent être ajoutés manuellement à la vue de la topologie. Si un périphérique prenant en charge le système SNA ou un commutateur géré présent sur le réseau n'est pas détecté automatiquement et affiché dans la topologie, vous pouvez l'ajouter manuellement en procédant comme suit :

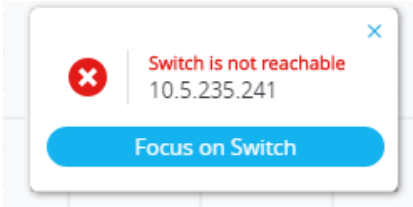
ÉTAPE 1 Cliquez sur 

en haut à droite de la vue de la topologie. Un champ de texte **Saisir une adresse IP** s'affiche.

ÉTAPE 2 Saisissez l'adresse IP du commutateur que vous souhaitez ajouter. Le message suivant s'affiche :



Si le périphérique n'est pas détecté, un message s'affiche, puis le périphérique est ajouté à la vue de la topologie en tant que commutateur hors ligne non géré.



Les périphériques ajoutés selon cette méthode restent sur la carte de topologie jusqu'à ce qu'ils soient supprimés manuellement. Si de tels périphériques ne sont pas connectés ou détectés par le système SNA, ils s'affichent comme des périphériques hors ligne.

Explorateurs

Les explorateurs vous permettent d'afficher des informations supplémentaires pour les commutateurs prenant en charge le système SNA, les connexions et les groupes client.

REMARQUE Pour accéder à un explorateur, cliquez sur la note représentant le périphérique ou une connexion. Les informations affichées par l'explorateur peuvent varier en fonction de la superposition sélectionnée (voir Superpositions).

Les explorateurs suivants sont disponibles :

- Explorateur de périphérique
- Explorateur de connexion
- Explorateur client

Explorateur de périphérique

Cet explorateur fournit des informations supplémentaires sur les périphériques prenant totalement en charge le système SNA et leurs interfaces.

Il affiche un tableau des ports et des LAG existant dans le commutateur. Chaque entrée du tableau a plusieurs colonnes principales ainsi que des colonnes supplémentaires qui n'apparaissent que si la superposition correspondante est activée.

Vous pouvez également modifier et enregistrer le nom d'hôte du périphérique depuis cet écran.

Les colonnes suivantes sont affichées dans le tableau de l'explorateur de périphérique :

- **Nom du port/LAG** : nom complet de l'interface.
- **ID de l'unité** : ne s'affiche que dans le tableau des ports et pour les commutateurs empilés.
- **Type de port** : affiche le type du port. Type physique du port.
- **État administrateur** : état d'administration de l'interface.
- **État opérationnel** : état opérationnel de l'interface. Si l'interface est suspendue, le motif de cette suspension est précisé entre parenthèses.
- **Appartenance LAG** : ne s'affiche que dans le tableau des ports. Si le port appartient à un LAG, cette colonne indique l'ID du LAG.
- **Ports membres** : ne s'affiche que dans le tableau du LAG. Présente une liste des ports membres du LAG. Ce champ peut contenir une longue liste de ports. Si la liste ne tient pas dans le tableau, elle peut être consultée dans le panneau d'information situé à droite.
- **Description** : description de l'interface. Cette description s'appuie sur la description MIB ifAlias.
- Quand la superposition **Utilisation des liaisons** est sélectionnée, les colonnes suivantes s'affichent :
  - **Débit actuel** : débit actuel de l'interface (10 Mo, 100 Mo, 1 Go…).
  - **Utilisation de la transmission** : utilisation de la transmission par l'interface, exprimée en pourcentage du débit actuel. Cette colonne ne s'affiche pas pour les LAG.
  - **Utilisation de la réception** : utilisation de la réception par l'interface, exprimée en pourcentage du débit actuel. Cette colonne ne s'affiche pas pour les LAG.
- Quand la **superposition PoE** est sélectionnée, les colonnes suivantes s'affichent :
  - **Affectation de puissance maximale** : ne s'affiche que dans le tableau des ports. Affiche l'allocation de puissance maximale en mW. Si un port ne prend pas en charge l'alimentation PoE, la mention **N/A** s'affiche.

- **Consommation électrique** : ne s'affiche que dans le tableau des ports. Affiche la consommation électrique constatée en mW. Si un port ne prend pas en charge l'alimentation PoE, la mention **N/A** s'affiche.

- Quand la **superposition VLAN** est sélectionnée, les colonnes suivantes s'affichent :
  - **Mode Switchport** : mode VLAN actif de l'interface.
  - **Appartenance VLAN** : liste des VLAN auxquels appartient l'interface. En mode liaison, cette colonne affiche un **U** à côté du VLAN sans balise. Ce champ peut contenir une longue liste de VLAN. Si la liste ne tient pas dans le tableau, elle peut être consultée dans le panneau d'information situé à droite.
- Quand la superposition **Spanning tree** est sélectionnée, les colonnes suivantes s'affichent :
  - **Mode STP** : mode STP actif de l'interface.
  - **Rôle du port** : rôle STP de l'interface.
  - **État Spanning tree** : état STP de l'interface.

Explorateur de connexion

Cet explorateur affiche des détails supplémentaires sur les liaisons individuelles rassemblées au sein d'une même connexion entre des périphériques backbone ou entre des périphériques prenant en charge le système SNA et un cloud.

Quand vous accédez à l'explorateur correspondant à une connexion spécifique, une présentation individuelle de chaque liaison présente dans la connexion examinée s'affiche.

L'explorateur affiche des informations de base sur les périphériques de part et d'autre de la connexion. Ces informations correspondent à celles qui s'affichent dans le panneau d'informations situé à droite. L'explorateur affiche les interfaces jouant le rôle d'ancre de part et d'autre de la connexion. Certaines informations relatives aux interfaces seront uniquement disponibles si l'interface appartient à un périphérique prenant en charge le système SNA.

Pour afficher ces informations, faites un double-clic sur une connexion jusqu'à ce qu'elle s'affiche en gras, puis cliquez une nouvelle fois afin de faire apparaître les éléments suivants :

Pour chaque liaison dans la connexion, les informations de base suivantes s'affichent :

- Les noms des interfaces de part et d'autre de la liaison.
- Le nom du LAG (le cas échéant) de part et d'autre de la liaison.
- Le débit de la liaison.

Ces informations relatives aux noms des interfaces et à l'appartenance LAG sont uniquement disponibles aux extrémités de connexion appartenant à des périphériques prenant en charge le système SNA. Si l'une des extrémités de la connexion n'est pas un commutateur, ses ports ne s'affichent pas.

Les liaisons spécifiques dans l'explorateur sont également affectées par la superposition active, qui modifie leur apparence en fonction de leur état. Reportez-vous à la section Superpositions.

Lorsque vous sélectionnez une liaison dans l'explorateur de connexion, les interfaces jouant le rôle d'ancre de part et d'autre de la liaison sont sélectionnées.

Explorateur client

Cet explorateur permet de visualiser des informations sur certains clients d'un groupe client, tels qu'un groupe de téléphones IP.

Il comprend un tableau comportant une ligne par périphérique du groupe client. Certaines colonnes de ce tableau ne s'affichent que si des superpositions spécifiques sont activées.

L'explorateur client n'est pas pris en charge pour les groupes client connectés au réseau via un cloud.

Les informations suivantes sont affichées dans le tableau de l'explorateur client :

- **ID de périphérique** : informations connues sur le périphérique, comme son nom d'hôte, l'adresse IP utilisée pour se connecter à son commutateur parent et l'adresse MAC du périphérique. Seules les informations disponibles s'affichent ici. Le tableau ne présente pas de texte provisoire pour les informations non disponibles.
- **Type de périphérique** : type de périphérique client.
- **Port connecté** : port du commutateur parent auquel ce client est connecté.
- **Colonnes de la superposition Utilisation des liaisons**
  - **Débit de connexion** : affiche le débit de la connexion au commutateur parent (10 Mo, 100 Mo, 1 Go).
  - **Utilisation de la transmission** : utilisation de la transmission par le périphérique (réception du port connecté), exprimée en pourcentage du débit actuel.

  - **Utilisation de la réception** : utilisation de la réception par le périphérique (transmission du port connecté), exprimée en pourcentage du débit actuel.

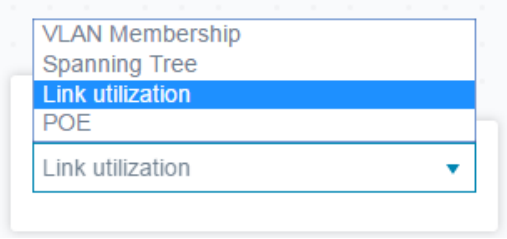
- **Colonne de la superposition PoE**
  - **Consommation électrique** : puissance électrique consommée par le périphérique en mW. Si le port connecté ne prend pas en charge l'alimentation PoE, la mention N/A s'affiche.
- **Colonne de la superposition VLAN** : VLAN connectés. Affiche les VLAN auxquels appartient le port connecté. Ce champ peut contenir une longue liste de VLAN. Si la liste ne tient pas dans le tableau, elle peut être consultée dans le panneau d'information situé à droite lorsque vous sélectionnez le client.

L'explorateur client n'est pas pris en charge pour les groupes client connectés au réseau via un cloud.

Superpositions

Les superpositions sont des couches d'informations qui peuvent être activées sur la vue de la topologie pour ajouter des précisions ou modifier l'affichage de cette topologie. Cela peut se traduire, par exemple, par l'attribution de couleurs différentes aux éléments de la topologie en fonction de différents critères ou par la modification des icônes associées aux éléments de la topologie afin d'afficher des données détaillées correspondant à la superposition sélectionnée.

Sélectionnez la superposition que vous souhaitez utiliser dans une liste de superpositions disponibles.



Certaines superpositions comportent des paramètres qui leur sont propres. C'est le cas pour la superposition VLAN. Quand vous sélectionnez cette superposition VLAN, par exemple, vous devez également sélectionner un VLAN spécifique.

Vous ne pouvez pas activer plus d'une superposition à la fois. La sélection d'une superposition désactive donc automatiquement toute autre superposition active.

Les superpositions suivantes sont prises en charge :

- Utilisation des liaisons
- Informations PoE
- Appartenance VLAN
- Informations sur le fournisseur de téléphonie Internet (ITSP)

Utilisation des liaisons

Cette superposition ajoute des informations à la carte de topologie et aux écrans des explorateurs concernant le niveau d'utilisation actuel (pour les 15 dernières secondes) des connexions du réseau.

Les connexions et liaisons s'affichent selon un code couleur, en fonction du volume du trafic qui y circule dans les deux sens.

Par défaut, voici les couleurs correspondant aux différents seuils :

- De 0 % à 69 % : couleur inchangée
- De 70 % à 89 % : jaune
- De 90 % à 100 % : rouge

Les connexions entre les périphériques de la vue de la topologie sont affichées en couleur, selon la liaison individuelle la plus utilisée au sein de la connexion. Lorsque vous consultez l'explorateur de connexion, chaque liaison affiche sa propre utilisation dans les deux sens.

L'utilisation pour chaque sens de circulation au sein d'une liaison est calculée en comptabilisant la quantité d'informations de part et d'autre, si la liaison relie des périphériques prenant en charge le système SNA. C'est la valeur la plus élevée qui est retenue en tant que valeur d'utilisation.

Par exemple, si une liaison relie le port 1 du périphérique A et le port 2 du périphérique B, le calcul de l'utilisation dans un sens s'effectue en comparant la valeur de transmission du port 1 et la valeur de réception du port 2. La valeur la plus élevée détermine la valeur de l'utilisation pour cette liaison.

Lorsqu'un seul des deux éléments reliés par la liaison est un périphérique prenant en charge le système SNA, l'utilisation de la liaison est exclusivement déterminée par les informations fournies par le périphérique prenant en charge le système SNA.

Pour le calcul de la liaison la plus utilisée dans le cas d'un affichage agrégé sur la carte de topologie, chaque sens de circulation dans une liaison est pris en compte comme une liaison distincte. Par exemple, si la circulation dans un sens de la liaison est utilisée à 5 % et l'autre à 92 %, la connexion agrégée s'affiche en rouge sur la carte de topologie, puisque l'utilisation la plus élevée est de 92 %.

Informations PoE

La superposition PoE affiche l'état de l'alimentation et de la consommation électrique des éléments du réseau.

Cette superposition modifie la couleur des liaisons en fonction de la quantité d'énergie fournie par la liaison pour alimenter les périphériques selon leur quantité d'énergie restante. Cette superposition met également en évidence les périphériques ne recevant pas le niveau d'alimentation électrique nécessaire à leur bon fonctionnement. L'utilisateur peut sélectionner les seuils auxquels ces couleurs changent pour chaque type de données, ainsi que les couleurs à utiliser dans chaque cas.

Une icône est ajoutée aux commutateurs fournissant de l'électricité. Elle s'affiche dans une couleur indiquant le budget de consommation électrique des commutateurs.

- Périphérique fournissant de 0 à 80 % de sa capacité d'alimentation : couleur inchangée
- Périphérique fournissant de 81 à 95 % de sa capacité d'alimentation : jaune
- Périphérique fournissant de 96 à 100 % de sa capacité d'alimentation : rouge

Les périphériques alimentés via une connexion PoE sont entourés d'un halo lumineux.

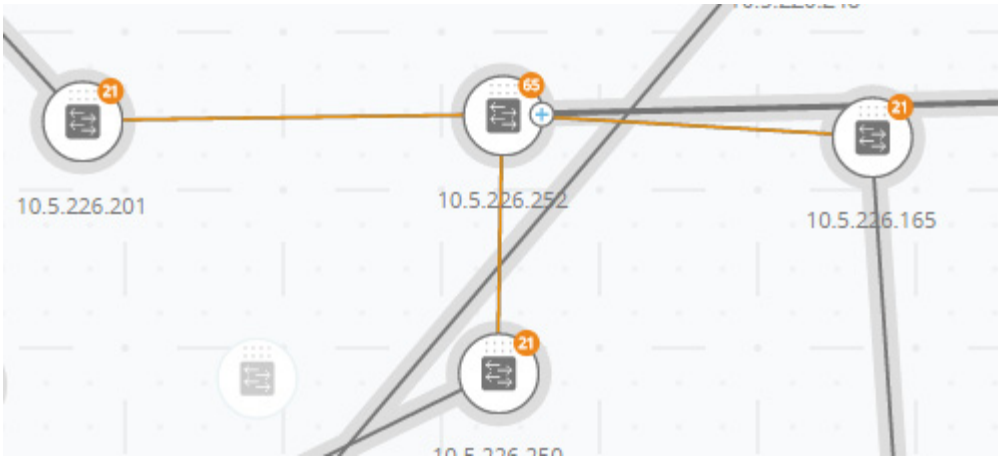
Les connexions contenant au moins une liaison fournissant de l'alimentation électrique sont mises en évidence dans la carte de topologie.

Dans l'explorateur de connexion, chaque lien transférant de l'énergie indique qu'il alimente un périphérique, ainsi que le sens dans lequel l'alimentation circule. Cette indication s'affiche pour chaque port, même si la liaison fait partie d'un LAG. Il est possible que certaines liaisons d'un LAG assurent l'alimentation de périphériques alors que d'autres non.

Appartenance VLAN

Cette superposition permet d'afficher les appartenances VLAN de divers ports et périphériques dans le réseau.

Par exemple, dans la figure ci-dessous, les lignes jaunes présentent des connexions asymétriques. Cela signifie que l'une des extrémités de la liaison fait partie du VLAN sélectionné, tandis que l'autre non.



Lorsque vous activez cette superposition, une liste des VLAN existants dans le réseau s'affiche (classés par ID de VLAN). Lorsque vous sélectionnez un VLAN, les nœuds appartenant à ce VLAN sont mis en évidence.

Les liaisons entre les périphériques s'affichent selon l'un des états suivants :

- Une liaison entre des périphériques SNA, où aucune des interfaces connectées des deux périphériques ne fait partie d'un VLAN, s'affiche sans modification.
- Une liaison entre un périphérique SNA et un périphérique non SNA, si l'interface du périphérique SNA n'appartient pas au VLAN, s'affiche sans modification.
- Une liaison entre des périphériques SNA où les interfaces connectées des deux périphériques appartiennent au VLAN est mise en évidence dans une couleur la désignant comme appartenant à ce VLAN.
- Une liaison entre un périphérique SNA et un périphérique non SNA, si l'interface du périphérique SNA appartient VLAN, est mise en évidence.
- Une liaison asymétrique entre deux périphériques SNA où l'une des interfaces connectées appartient au VLAN et pas l'autre ne s'affiche pas en jaune.

La connexion associant une agrégation de liaisons (LAG) entre des périphériques de la carte de topologie est identifiée conformément aux règles suivantes :

- Si au moins une liaison est mise en évidence, la connexion l'est également.
- Si au moins une liaison crée une connexion asymétrique, la connexion s'affiche en jaune.

Dans l'explorateur de connexion, chaque liaison peut être affichée individuellement. Quand un lien se trouve dans une configuration asymétrique, il s'affiche en jaune et l'explorateur de connexion indique l'extrémité du lien n'appartenant pas au VLAN.

Informations sur le fournisseur de téléphonie Internet (ITSP)

Cette superposition affiche la topologie active du réseau. Quand cette superposition est activée, une indication s'ajoute au périphérique racine spanning tree et à toutes les connexions. Cette indication permet de visualiser les liaisons bloquées par le spanning tree commun

Lorsque vous affichez un explorateur de connexion, toutes les liaisons bloquées sont mises en évidence.

Lorsqu'une liaison est bloquée, l'explorateur de connexion spécifie l'extrémité de la liaison connectée à l'interface bloquée.

Balises

Les balises permettent d'identifier les périphériques dans la vue de la topologie en indiquant leurs attributs ou leurs noms définis par l'utilisateur. Elles permettent également de sélectionner rapidement plusieurs éléments en recherchant une balise particulière. Par exemple, vous pouvez rechercher tous les nœuds du réseau affectés de la balise téléphone IP.

Les balises peuvent être prédéfinies ou définies par l'utilisateur.

- **Balises prédéfinies** : ces balises s'appliquent automatiquement aux nœuds en fonction des informations fournies par les protocoles de détection. Reportez-vous à la section Balises prédéfinies.
- **Balises définies par l'utilisateur** : ces balises sont ajoutées manuellement et affectées aux nœuds de la carte de topologie. Reportez-vous à la section Balises définies par l'utilisateur.

Les balises prédéfinies et définies par l'utilisateur s'affichent de façon distincte.

Balises prédéfinies

Ces balises s'appliquent automatiquement aux nœuds dès qu'ils sont ajoutés à la topologie. Elles peuvent être persistantes ou changer en fonction de l'état de chaque nœud. Tant que la balise s'applique au périphérique, elle ne peut en être supprimée. Voici une liste des balises prédéfinies :

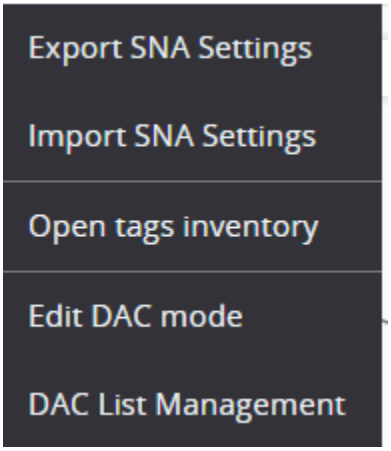
Balises	Méthodes pour attribuer une balise
Système SNA	Selon les données internes SNA
SNA partiel	Selon les données internes SNA
Hors ligne	Selon les données internes SNA
Commutateur	Selon les données annoncées via les protocoles de détection
Routeur	Selon les données annoncées via les protocoles de détection
Point d'accès	Selon les données annoncées via les protocoles de détection
Téléphone IP	Selon les données annoncées via les protocoles de détection
PC	Selon les données annoncées via les protocoles de détection (hôte)
Notifications	Selon les données internes SNA Selon l'état, s'affiche si des notifications non lues sont disponibles pour le périphérique
PoE PSE	Selon les données internes SNA, s'affiche si un périphérique peut fournir une alimentation via PoE (même si aucune alimentation n'est fournie)
PD PoE	Selon les données internes SNA Cec s'affiche si un périphérique peut être alimenté via PoE (même si aucune alimentation n'est fournie via PoE)

Afficher les balises

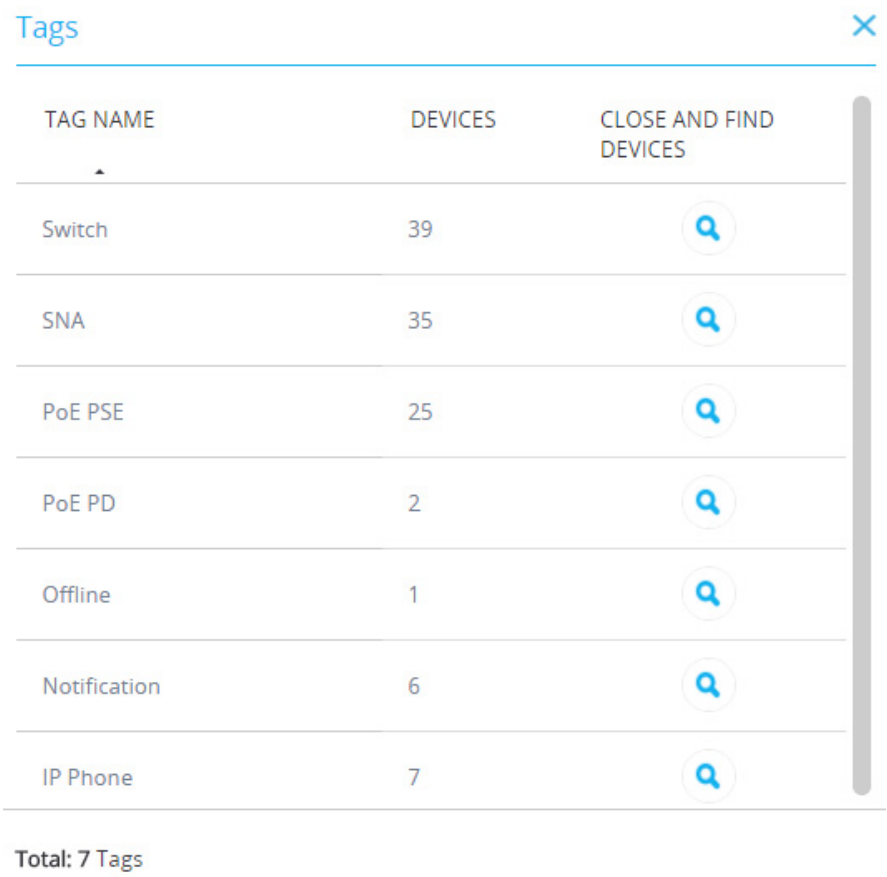
Voici comment afficher une liste de toutes les balises :

ÉTAPE 1 Cliquez sur le menu à trois barres horizontales situé à gauche de la vue de la topologie : ☰

Les informations suivantes s'affichent :



ÉTAPE 2 Sélectionnez **Ouvrir l'inventaire des balises**. Une liste des balises s'affiche, comme illustré ci-dessous :



ÉTAPE 3 Cliquez sur l'icône de recherche pour trouver une balise spécifique dans la colonne **Fermer et trouver des périphériques** pour afficher une liste des périphériques affectés de la balise sélectionnée.

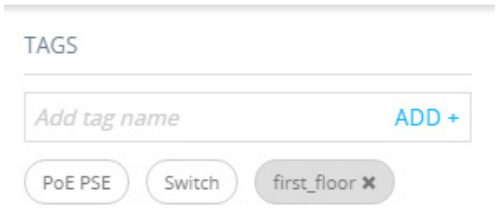
Balises définies par l'utilisateur

Vous pouvez créer des balises et les ajouter manuellement à des éléments sélectionnés dans la topologie dans la section Balises du panneau d'informations situé à droite.

Pour créer une nouvelle balise, procédez comme suit :

ÉTAPE 1 Dans la section Balises, cliquez sur le champ **Ajouter un nom de balise**, puis saisissez un nom de balise.

ÉTAPE 2 Cliquez sur **AJOUTER+**. Le nom de balise s'affiche alors. L'illustration ci-dessous montre que la balise **first_floor** a été créée.



Vous pouvez ajouter des balises portant les mêmes noms que des balises prédéfinies. Ces balises apparaissent sous la même forme que les balises définies par l'utilisateur et peuvent être supprimées à tout moment. Comme ces balises sont distinctes des balises prédéfinies, un même élément peut porter plusieurs balises portant le même nom à condition que l'une d'entre elles soit prédéfinie et l'autre définie par l'utilisateur.

Pour ajouter une balise à un périphérique, procédez comme suit :

ÉTAPE 1 Sélectionnez le périphérique.

ÉTAPE 2 Dans la section Balises, cliquez sur le champ **Ajouter un nom de balise**. La liste des balises s'affiche.

ÉTAPE 3 Sélectionnez la balise à appliquer au périphérique.

Recherche

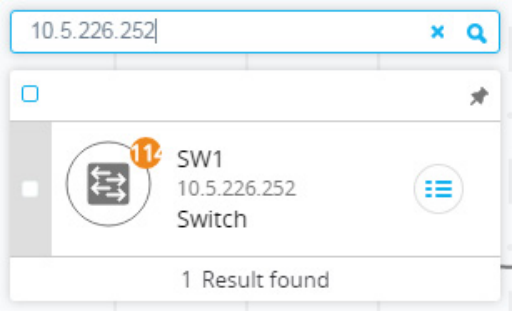
Utilisez la fonctionnalité de recherche pour trouver des périphériques spécifiques dans la vue de la topologie.

Le terme de recherche saisi est recherché dans les informations connues du système SNA.

Les champs suivants peuvent faire l'objet d'une recherche :

- Adresses IP
- Adresses MAC
- Nom d'hôte
- Nom de produit
- Description
- Balises

Les résultats de recherche s'affichent sous forme de liste de fiches d'identification sur lesquelles vous pouvez cliquer. Si vous cliquez sur une fiche d'identification, la carte de topologie effectue un zoom et se recentre sur l'élément correspondant.

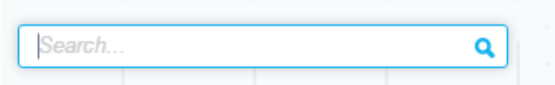


Vous pouvez préciser votre recherche en ajoutant des mots-clés afin de limiter ses champs concernés. Si vous saisissez un mot-clé suivi de deux-points et du terme recherché, le terme ne sera recherché que dans le champ précisé. Voici la liste des mots-clés pris en charge : **IP**, **MAC** et **Tag** (Balise).

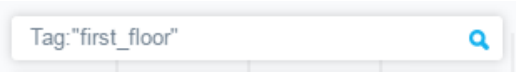
Si le terme recherché est saisi entre guillemets, seules les correspondances exactes seront trouvées.

Voici un exemple de recherche par balise :

ÉTAPE 1 Cliquez dans le champ de recherche :



ÉTAPE 2 Saisissez le mot-clé « Tag » (Balise) et le nom de cette balise, comme illustré ci-dessous :



ÉTAPE 3 Cliquez sur . Les résultats s'affichent.

Tableau de bord

Le tableau de bord du réseau est un écran distinct de la topologie, qui fournit à l'utilisateur des informations générales sur l'état du réseau.

Le tableau de bord comporte les sections suivantes :

Vue d'ensemble du réseau

Cette section affiche des informations générales sur le réseau. Toutes les informations affichées ici sont fournies par les périphériques SNA et SNA partiels du réseau.

Les informations suivantes sont indiquées :

- Alimentation PoE fournie par les périphériques PoE du réseau, exprimée en watts.
- Alimentation actuellement économisée par le mode Green Ethernet, exprimée sous forme de pourcentage et de valeur en watts (par exemple : 20 % ; 5 watts).
- Total de l'énergie économisée par le mode Green Ethernet, exprimé en watts-heures.
- Estimation projetée de l'énergie économisée annuellement par le mode Green Ethernet, exprimée en watts-heures.
- Énergie économisée actuellement grâce aux stratégies relatives à la gestion de l'alimentation, exprimée en watts.

- Total de l'énergie économisée grâce aux stratégies relatives à la gestion de l'alimentation, exprimé en watts.
- Estimation projetée de l'énergie économisée annuellement grâce aux stratégies relatives à la gestion de l'alimentation, exprimée en watts.

Alertes

Cette section affiche les dix alertes les plus récentes sur le réseau. Les alertes sont des notifications relevant d'une sévérité de niveau 1 (voir Section Notifications).

Elles s'affichent dans un tableau contenant les colonnes suivantes :

- Périphérique concerné

  Ceci n'apparaît que dans l'affichage des notifications agrégées. L'appareil concerné est identifié par la forme d'identification disponible la plus puissante, selon l'ordre de priorité suivant : Nom d'hôte ' Adresse IP ' Adresse MAC
- Horodatage
- Gravité
- Texte Syslog.

La liste peut être classée par périphérique, par date ou par niveau de sévérité. Elle peut être filtrée par périphérique ou par niveau de sévérité.

Par défaut, elle est classée par date, les notifications les plus récentes étant présentées en premier.

Bon fonctionnement du réseau

Cette section affiche des alertes si un problème d'intégrité est détecté sur un périphérique SNA du réseau.

Les alertes précisent le périphérique ou la connexion concernés, fournissent un lien permettant d'accéder à l'explorateur de ce périphérique ou de cette connexion et indiquent la nature du problème.

Elles s'affichent dans les cas suivants :

- Un ventilateur tombe en panne.
- Un capteur détecte une température anormalement élevée.

- Une surcharge est constatée au niveau de l'alimentation PoE (une demande d'alimentation PoE ne peut être satisfaite en raison d'une capacité dépassée).
- L'utilisation du trafic d'une connexion atteint ou dépasse les 70/90 %.
- L'utilisation du processeur d'un périphérique atteint ou dépasse les 96 %.

Cette section ne devrait pas s'afficher si l'intégrité du réseau n'est pas menacée.

Interfaces suspendues

Cette section affiche des informations sur tous les ports suspendus dans le réseau.

Les informations suivantes sont affichées pour chaque interface suspendue :

- ID de périphérique
- Nom de l'interface
- Motif de la suspension (chaîne d'une longueur maximale de 20 caractères)
- État de la reprise automatique (Activée/Désactivée)
- Un bouton pour tenter de réactiver l'interface (vous devez bénéficier de toutes les autorisations sur le système SNA)

Cette section ne devrait pas s'afficher si le réseau ne comporte pas d'interfaces suspendues.

Notifications

Les notifications sont des événements qui se produisent sur le réseau et peuvent demander l'attention de l'administrateur système. Le mécanisme des notifications utilise la fonctionnalité SYSLOG des commutateurs SNA dans le réseau et affiche les notifications sur la carte de topologie.

Consulter les notifications

Lorsqu'un message SYSLOG est généré par un périphérique SNA, une indication s'affiche pour ce périphérique dans la vue de la topologie.

Les notifications sont créées à partir des journaux de la mémoire RAM des commutateurs SNA. Seuls les SYSLOG correspondant aux seuils de sévérité configurés pour les journaux de la mémoire RAM sont détectés par le système SNA.

Les notifications du système SNA sont séparées en fonction des catégories basées sur le niveau de sévérité SYSLOG. La couleur de la notification indique son niveau de sévérité :

- Niveau 1 (rouge) : Critique, Alerte ou Urgence.
- Niveau 2 (orange) : Avertissement ou Erreur.
- Niveau 3 (bleu) : Informatif ou Remarque.

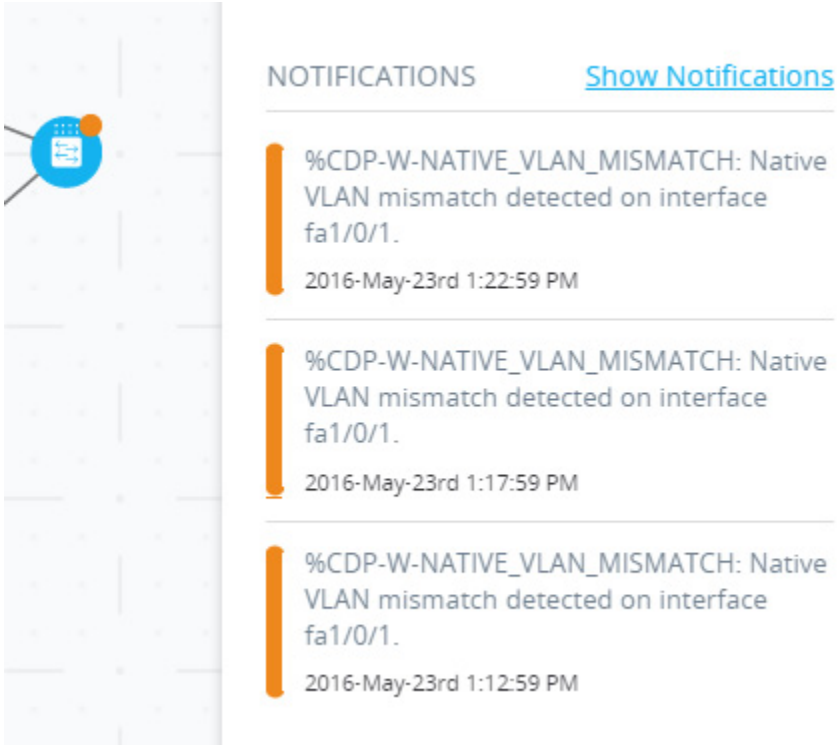
Quand un événement générant une notification se produit, une indication s'affiche sur le périphérique SNA correspondant, qui précise le nombre de nouvelles notifications sur l'appareil et le niveau de sévérité le plus élevé pour l'ensemble de ces notifications. Par exemple, 

indique que la notification la plus sévère est un Avertissement.

En outre, en cas de notification, celle-ci est signalée par une icône de notification générale qui s'affiche sur l'en-tête de l'application. Ces indications sont supprimées lorsque vous vous déconnectez, puis sont mises à jour de nouveau à mesure que des événements se produisent pendant le fonctionnement du système SNA.

Voici comment vous pouvez consulter les notifications :

- Sélectionnez un commutateur SNA ou géré. Les trois notifications les plus importantes, classées par niveau de sévérité et par date, s'affichent dans la section Notifications du panneau d'informations situé à droite.



- Cliquez sur **Afficher les notifications** pour développer la liste du panneau d'informations situé à droite pour afficher un tableau contenant les 100 dernières entrées SYSLOG enregistrées sur le périphérique. Cette option est disponible pour tous les commutateurs SNA et affiche les 100 dernières entrées SYSLOG, que celles-ci aient été enregistrées pendant que la session SNA était active ou pas.
- Cliquez sur  pour afficher le tableau contenant une liste agrégée des notifications pour l'ensemble du réseau. Ce tableau contient les 300 derniers événements enregistrés dans le réseau par les périphériques SNA ou SNA partiels.

Lorsque vous consultez les détails d'une notification, l'annotation de nouvelle notification est supprimée de la vue de la topologie, mais toutes les notifications restent disponibles sur le journal des notifications et les plus récentes demeurent dans le panneau latéral.

Lorsque vous consultez des notifications, les caractéristiques suivantes s'affichent :

- **Périphérique concerné** : ceci n'apparaît que dans l'affichage des notifications agrégées. L'appareil concerné est identifié par la forme d'identification disponible la plus puissante, selon l'ordre de priorité suivant : Nom d'hôte → Adresse IP → Adresse MAC
- **Horodatage**
- **Gravité**
- **Texte Syslog**

Fonctionnalité DAC (contrôle des autorisations des périphériques)

Utilisez la fonctionnalité DAC de contrôle des autorisations des périphériques pour configurer une liste des périphériques clients autorisés dans le réseau. La fonctionnalité DAC active les fonctionnalités 802.1x sur les périphériques SNA dans le réseau et un serveur RADIUS intégré (serveur RADIUS hôte) peut être paramétré sur l'un des périphériques SNA. L'autorisation des périphériques s'effectue via l'authentification MAC.

Flux de travail DAC

Le flux de travail DAC comprend les étapes suivantes :

ÉTAPE 1 Activez la fonctionnalité DAC. Reportez-vous à la section Accéder à la fonctionnalité DAC.

ÉTAPE 2 Configurez un périphérique serveur RADIUS et les périphériques clients. Reportez-vous à la section Préciser un serveur RADIUS et les clients.

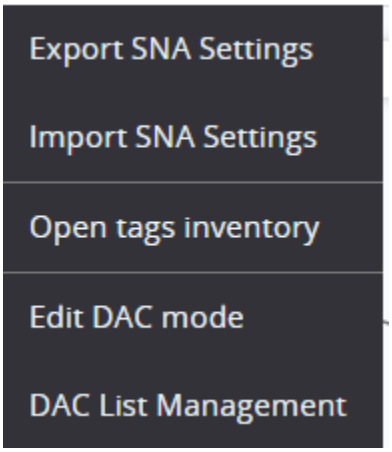
ÉTAPE 3 Ajoutez les périphériques clients à la liste blanche. Reportez-vous à la section Gestion de liste DAC.

Accéder à la fonctionnalité DAC

Pour accéder à la fonctionnalité DAC, effectuez les opérations suivantes :

ÉTAPE 1 Cliquez sur le menu d'options situé à gauche de la bannière : ☰

Les informations suivantes s'affichent :

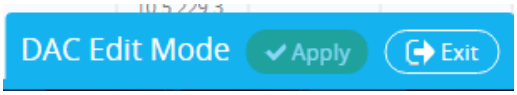


ÉTAPE 2 Sélectionnez **Mode de modification DAC**.

Préciser un serveur RADIUS et les clients

ÉTAPE 1 Cliquez sur **Mode de modification DAC** dans le menu Options ☰ .

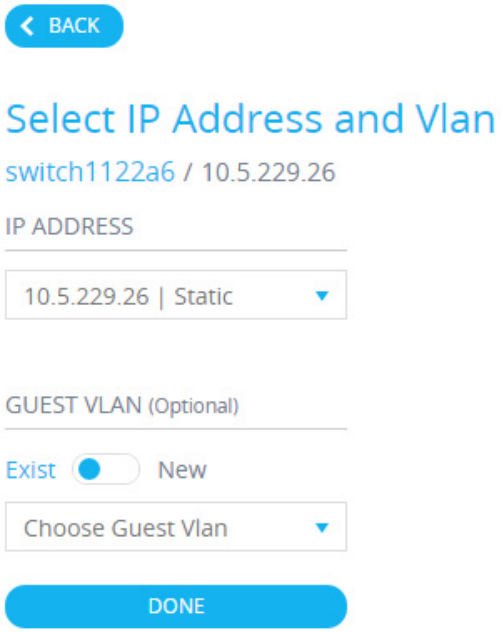
ÉTAPE 2 L'application lance le mode de modification de la fonctionnalité DAC (signalé par le cadre bleu autour de la carte de topologie et panneau de contrôle en base de l'écran).



ÉTAPE 3 Sélectionnez l'un des périphériques SNA, puis cliquez sur son menu .

ÉTAPE 4 Désignez-le en tant que serveur RADIUS pour le réseau en cliquant sur **+ Définir comme serveur DAC**.

Les informations suivantes s'affichent :



ÉTAPE 5 Si le périphérique a plus d'une seule adresse IP, sélectionnez l'une de ces adresses afin qu'elle soit utilisée par la fonctionnalité DAC. La liste d'adresses vous permet de savoir si l'interface IP est statique ou dynamique. Vous serez averti, si vous sélectionnez une interface dynamique, que l'adresse risque de ne pas être stable. Lorsque vous modifiez un serveur DAC existant, l'adresse utilisée par ses clients est présélectionnée.

ÉTAPE 6 Saisissez une chaîne de clé qui sera utilisée par le serveur RADIUS DAC avec l'ensemble de ses clients sur le réseau.

ÉTAPE 7 Cliquez sur **Terminé**.

Le serveur RADIUS DAC est mis en évidence dans la vue de la topologie.

ÉTAPE 8 Placez-vous sur le serveur, puis cliquez sur le menu ☰ du périphérique que vous souhaitez ajouter en tant que client. Cliquez sur **+Définir en tant que client**.

- Si un commutateur est déjà un client du serveur RADIUS DAC (son adresse IP figure dans la table NAS du serveur RADIUS et le serveur RADIUS est configuré dans son tableau de serveur RADIUS avec un type d'utilisation **802.1x** ou **Tous** et un niveau de priorité défini à 0), ce commutateur est présélectionné.
- Si un client est sélectionné et possède déjà un serveur RADIUS configuré pour une authentification 802.1x (autre que le serveur sélectionné précédemment), vous serez averti que cette sélection interrompra les opérations du serveur RADIUS actuel.
- Si un client est sélectionné et possède déjà un serveur RADIUS configuré pour une authentification 802.1x avec un niveau de priorité défini sur 0 (autre que le serveur sélectionné précédemment), un message d'erreur s'affiche et la fonctionnalité DAC ne sera pas configurée sur ce client.
- Sélectionnez au moins un client pour le serveur RADIUS DAC. Si aucun client n'est sélectionné, vous ne pourrez pas appliquer les paramètres.

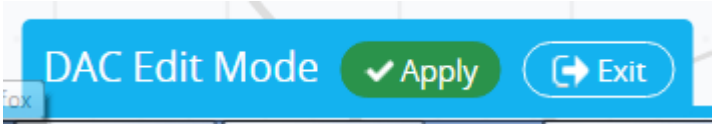
ÉTAPE 9 Lorsqu'un commutateur est sélectionné en tant que client, une fenêtre présentant ses ports s'affiche. Sélectionnez les ports du commutateur client sur lesquels vous souhaitez appliquer l'authentification 802.1x.

Le système SNA présente une liste de tous les ports de bordure suggérés (c'est-à-dire tous les ports qui ne sont pas reconnus comme connectés à d'autres commutateurs ou clouds). Vous pouvez sélectionner ces ports suggérés en cliquant sur :

Vous pouvez ajouter ou supprimer des ports dans la sélection. À ce stade, tous les ports disposant d'une configuration DAC complète (voir Tableau) s'affichent comme présélectionnés.

ÉTAPE 10 Cliquez sur **Terminé**.

ÉTAPE 11 Cliquez sur Appliquer dans le



Une fois la fonctionnalité DAC configurée, une alerte s'affiche à chaque fois qu'un périphérique ne figurant pas sur la liste noire est rejeté par le réseau via un serveur RADIUS où la fonctionnalité DAC est activée. Vous devez alors indiquer si vous souhaitez ajouter ce périphérique à la liste blanche ou à une liste noire afin de ne plus recevoir d'avertissements.

Lorsqu'il informe l'utilisateur de la présence de ce nouveau périphérique, le système SNA précise son adresse MAC, ainsi que périphérique et le port via lesquels ce périphérique tente d'accéder au réseau.

Si un rejet est signalé par un périphérique autre qu'un serveur RADIUS DAC, ce message est ignoré, ainsi que tous les messages suivants du même périphérique pendant les 20 minutes qui suivent. Après 20 minutes, le système SNA vérifie de nouveau si ce périphérique est un serveur RADIUS DAC. Si un utilisateur est ajouté à la liste blanche, ce périphérique est ajouté au groupe DAC de tous les serveurs DAC. Quand cette configuration est enregistrée, vous pouvez décider si vous souhaitez enregistrer ce paramètre immédiatement à la configuration de démarrage du serveur (cette option est activée par défaut).

Un périphérique ne peut pas accéder au réseau s'il n'a pas été ajouté à la liste blanche

Vous pouvez consulter et modifier la liste blanche ou la liste noire à tout moment pourvu qu'un serveur RADIUS DAC ait été défini et soit accessible.

Lorsque vous appliquez les paramètres DAC, vous, vous obtenez un rapport présentant les actions qui seront appliquées aux périphériques participants. Une fois les modifications approuvées, vous pouvez décider si les paramètres doivent également être copiés sur le fichier de configuration de démarrage des périphériques configurés (cette option est sélectionnée par défaut). Pour terminer, appliquez les paramètres.

Le rapport affiche les avertissements lorsque des étapes de la configuration DAC n'ont pas été respectées, et précise l'état des actions telles qu'elles sont gérées au niveau des périphériques.

Ce rapport contient les champs suivants :

Champ	Valeur	Commentaires
Appareil	Les identifiants du périphérique (Nom d'hôte, adresse IP)	
Action	Actions possibles pour le serveur DAC : • Activer le serveur RADIUS • Désactiver le serveur RADIUS • Mettre à jour la liste des clients • Créer un groupe de serveurs RADIUS • Supprimer un groupe de serveurs RADIUS Actions possibles pour le client DAC : • Ajouter une connexion à un serveur RADIUS • Mettre à jour une connexion à un serveur RADIUS • Supprimer une connexion à un serveur RADIUS • Mettre à jour les paramètres 802.1x • Mettre à jour les paramètres d'authentification de l'interface • Mettre à jour les paramètres de l'hôte et de la session pour l'interface	Il est possible (et probable) que plusieurs actions s'affichent pour chaque périphérique. Chaque action peut avoir son propre état.

Champ	Valeur	Commentaires
Avertissements.	Avertissements possibles pour le serveur DAC : • L'IP de l'interface sélectionnée est dynamique. Avertissements possibles pour les clients DAC : • Le périphérique est déjà client d'un autre serveur RADIUS. • Aucun port n'est sélectionné.	Les avertissements contiennent également des liens permettant d'accéder aux sections de la fonctionnalité DAC permettant de résoudre les problèmes détectés. Les modifications peuvent être appliquées lorsque des avertissements sont présents.
État	• En attente • Réussite • Échec	En cas d'état d'échec, le message d'erreur s'affiche pour l'action.

Gestion de liste DAC

Une fois que vous avez ajouté les périphériques clients et sélectionné les ports à authentifier, tous les périphériques non authentifiés détectés sur ces ports sont ajoutés à la liste de périphériques non authentifiés.

La fonctionnalité DAC prend en charge les listes de périphériques suivantes :

- **Liste blanche** : liste de tous les serveurs pouvant être authentifiés.
- **Liste noire** : liste des serveurs qui ne doivent en aucun cas être authentifiés.

Si vous souhaitez que des périphériques et leurs ports soient authentifiés, vous devez les ajouter aux listes blanches. Si vous ne souhaitez pas qu'ils soient authentifiés, aucune action n'est requise : ils sont ajoutés à la liste noire par défaut.

Voici comment ajouter ces périphériques à la liste blanche ou les supprimer de la liste noire :

ÉTAPE 1 Cliquez sur l'icône de périphérique non authentifié.

La page de gestion de liste DAC s'affiche avec la liste des périphériques non authentifiés.

ÉTAPE 2 Sélectionnez les périphériques que vous souhaitez ajouter à la liste blanche, puis cliquez sur **Ajouter à la liste blanche**.

ÉTAPE 3 Sélectionnez les périphériques que vous souhaitez ajouter à la liste noire, puis cliquez sur **Ajouter à la liste noire**.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paquets accédant aux ports du périphérique sont authentifiés sur le serveur RADIUS.

Pour gérer la liste blanche ou la liste noire, cliquez sur les onglets **Liste blanche** et **Liste noire**.

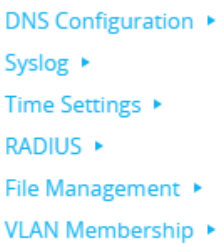
Vous pouvez effectuer les opérations suivantes dans ces pages :

- **Supprimer de la liste** : supprime les appareils sélectionnés de la liste.
- **Déplacer vers la liste noire ou Déplacer vers la liste blanche** : déplace les périphériques sélectionnés vers la liste choisie.
- **Ajouter un périphérique** : ajoutez un périphérique à la liste blanche ou à la liste noire en saisissant son adresse MAC, puis en appuyant sur **Ajouter+**.
- **Rechercher un périphérique avec une adresse MAC** : saisissez une adresse MAC, puis cliquez pour lancer la recherche. Vous obtenez la date et l'heure auxquelles un trafic émis par ce périphérique a été détecté (Dernière détection) et les ports ou périphériques via lesquels il a tenté d'accéder au réseau (Détecté à).

Services

Les services sont des configurations qui peuvent être activées sur plusieurs périphériques ou interfaces prenant en charge le système SNA de façon simultanée. Ils sont disponibles uniquement pour les périphériques offrant une prise en charge complète du système SNA ou pour les interfaces de ces périphériques.

Vous pouvez sélectionner ces services depuis le panneau d'informations situé à droite.



Pour appliquer un service, sélectionnez un ou plusieurs périphériques ou interfaces dans la vue de la topologie, soit de façon manuelle, dans la carte, ou les sélectionnant parmi les résultats de recherche. Vous pouvez activer tous les services correspondant aux éléments sélectionnés.

Lorsqu'un service a été sélectionné, une interface utilisateur correspondant à ce service s'affiche. Les réglages actuels pour la fonctionnalité applicable à l'ensemble des éléments sélectionnés s'affichent. Les paramètres spécifiques affichés pour chaque service sont décrits ci-dessous. Vous mettre à jour les paramètres sur certains périphériques ou certaines interfaces, ou sélectionner une entrée dans un périphérique afin de la copier et de l'appliquer à d'autres périphériques.

Vous pouvez également utiliser les réglages de l'un des périphériques ou de l'une des interfaces et les appliquer à l'ensemble des périphériques ou des interfaces de la sélection.

Pour la plupart des services, une page d'interface utilisateur présente les paramètres spécifiques pouvant être définis pour le service. Une fois que les paramètres ont été définis sur la page d'interface utilisateur et que toutes les validations côté client ont été effectuées, les paramètres sont envoyés aux périphériques ou interfaces sélectionnés. Un rapport s'affiche alors pour présenter les résultats du service au fil de leur réception. Pour chaque destinataire du service, un état s'affiche (envoi, réussite, échec). En cas d'erreur, le destinataire reçoit les détails du message correspondant.

Si une configuration échoue en raison d'une erreur de communication entre le système SNA et le périphérique configuré, une option s'affiche pour effectuer une nouvelle fois la configuration.

Par défaut, tous les services reprennent le fichier de configuration d'exécution pour le copier sur le fichier de configuration de démarrage une fois que la configuration est effectuée. Vous pouvez désactiver cette option.

Services au niveau des périphériques

Les services suivants sont disponibles pour les commutateurs :

- Configuration de client RADIUS
- Configuration de client DNS
- Configuration du SYSLOG server
- Configuration des paramètres d'heure
- Gestion des fichiers
- Stratégies relatives à la gestion de l'alimentation (au niveau du périphérique)
- Appartenance VLAN (au niveau du périphérique)

Pour chacun des services proposés au niveau des périphériques, les tickets affichant les configurations actuelles des périphériques sélectionnés contiennent les informations d'identification suivantes, en plus des paramètres spécifiques au service :

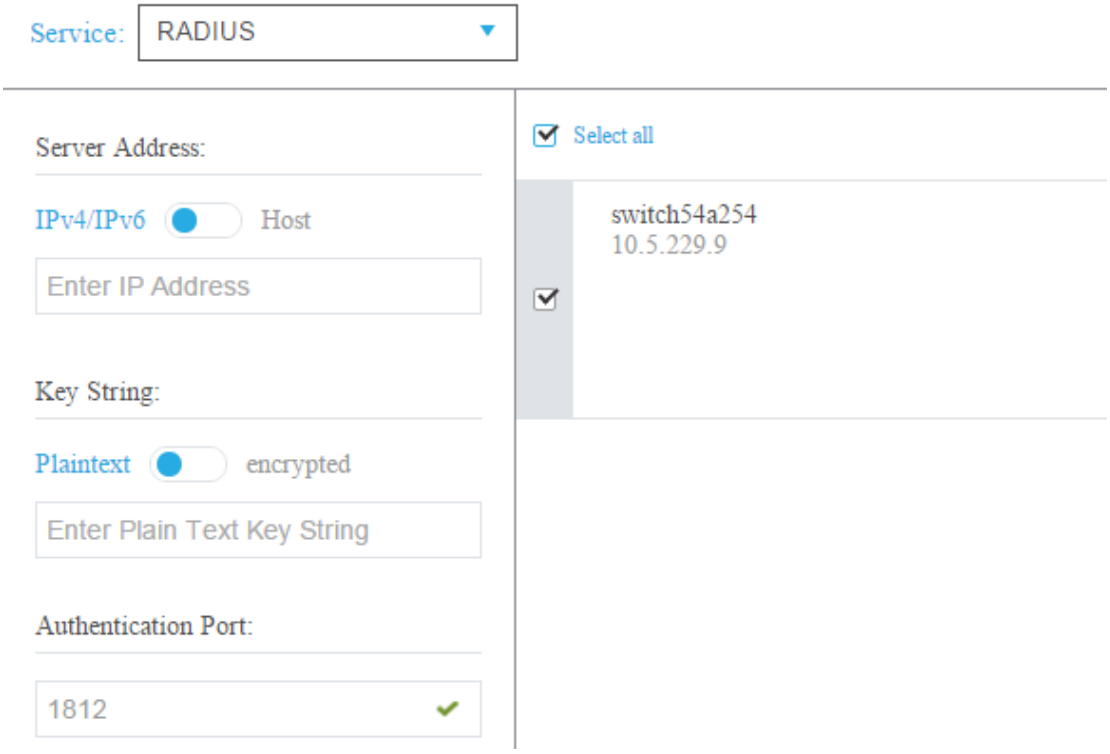
- Nom d'hôte du périphérique.
- Adresse IP : si plus d'une adresse IP existe pour le périphérique, c'est celle que le système SNA utilise pour accéder au périphérique qui s'affiche.
- Modèle du périphérique : chaîne alphanumérique représentant le modèle du périphérique. Par exemple : SG350XG-2F10.

Configuration de client RADIUS

Ce service vous permet de configurer un ou plusieurs périphériques en tant que clients RADIUS en définissant le serveur RADIUS qu'ils utilisent pour la connexion.

Configuration actuelle

Pour chaque périphérique sélectionné, la configuration actuelle affiche le serveur RADIUS avec le type d'utilisation **Connexion** ou **Tous** du niveau de priorité le plus bas configuré sur cet élément sur le panneau d'informations situé à droite.



S'il existe plus d'un serveur RADIUS correspondant au niveau de priorité le plus bas, un serveur unique s'affiche, dans cet ordre :

- Premier serveur RADIUS (par ordre alphabétique), défini par nom d'hôte
- Serveur RADIUS ayant l'adresse IPv4 la plus basse
- Serveur RADIUS ayant l'adresse IPv6 la plus basse

L'entrée créée par le service a un niveau de priorité de 0 et le type d'utilisation **Connexion**.

Si une entrée a déjà la même adresse IP ou nom d'hôte que la nouvelle entrée, avec le niveau de priorité 0 et le type d'utilisation **802.1x**, l'entrée existante est mise à jour et son type d'utilisation devient **Tous**.

Si une entrée ayant une adresse IP ou un nom d'hôte différent existe déjà, celle-ci s'affiche et si son type d'utilisation est **Connexion**, elle est remplacée par la nouvelle entrée. Si le type d'utilisation était **Tous**, il devient **802.1x**.

Si une entrée ayant la même adresse IP ou nom d'hôte existe déjà avec un niveau de priorité inférieur à 0, la priorité de cette entrée passe à 0, et le type d'utilisation **Connexion** lui est ajouté, si nécessaire.

Paramètres affichés/modifiables

Pour configurer les périphériques sélectionnés en tant que clients pour un autre serveur RADIUS que celui qui est configuré actuellement, renseignez les champs suivants :

- **Adresse du serveur** : adresse IPv4 ou IPv6 du serveur RADIUS.
- **Chaîne de clé** : chaîne de clé utilisée pour le serveur RADIUS (jusqu'à 128 caractères).

Ce paramètre s'affiche, le cas échéant, sous forme chiffrée. Vous pouvez saisir la chaîne de clé sous forme chiffrée ou en clair.

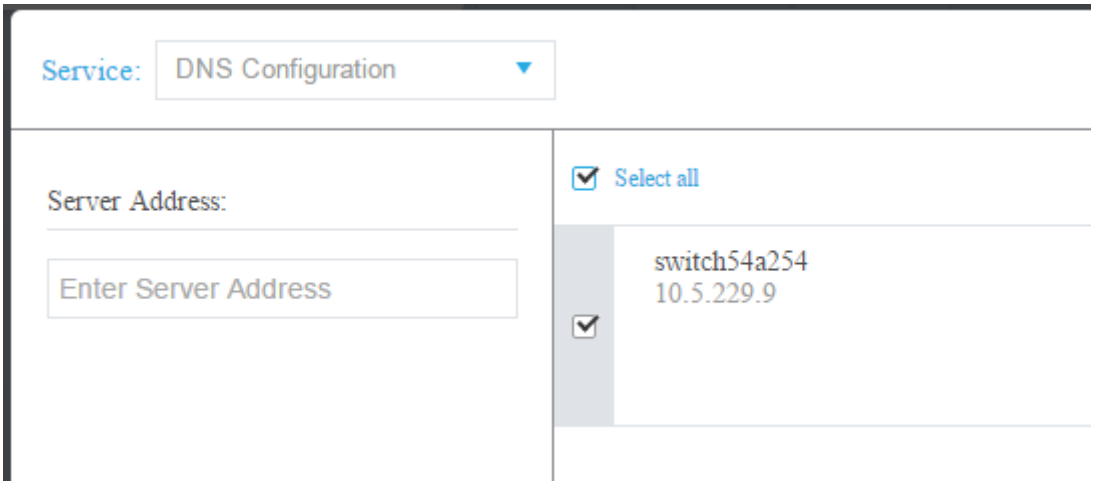
- **Port d'authentification** : numéro du port d'authentification.
- **Méthodes d'authentification** : liste des méthodes d'authentification utilisées pour chaque appareil par le canal utilisé par le système SNA (HTTP ou HTTPS). Les valeurs habituelles pour ce paramètre sont **Local** ou **RADIUS, Local**. Si la valeur actuelle pour un périphérique est différente, l'option de copie ne sera pas disponible pour ce périphérique. Lorsque vous copiez des paramètres, la valeur RADIUS, Local est associée à la case d'option Méthode d'authentification RADIUS Primaire.
- **Méthode d'authentification primaire** : paramètre en écriture seule apparaissant dans la section de configuration. Il s'agit d'un choix entre deux valeurs : **Base de données locale**, **RADIUS**. Si RADIUS est sélectionné, la valeur configurée pour tous les canaux sera en fait **RADIUS, Local**.

Configuration de client DNS

Le service de configuration de client DNS permet de définir le serveur DNS utilisé par les périphériques sélectionnés.

Configuration actuelle

Pour chaque périphérique sélectionné, la configuration actuelle affiche le serveur DNS actuel en utilisant la préférence 1 du côté droit. Si plusieurs serveurs DNS sont présents, le serveur défini de façon statistique s'affiche.



Si le serveur affiche est une entrée dynamique, un message s'affiche pour vous en avertir et vous empêcher de le supprimer.

L'entrée créée par le service aura la préférence 1. Si une entrée statique de préférence 1 existe déjà et s'affiche, le serveur statique est remplacé par la nouvelle entrée.

Paramètres affichés/modifiables

Pour définir un nouveau serveur DNS, saisissez son adresse IPv4 ou IPv6.

Configuration du SYSLOG server

Ce service permet de définir le SYSLOG server utilisé par les périphériques sélectionnés.

Configuration actuelle

Pour chaque périphérique sélectionné, le SYSLOG server ayant l'indice le plus bas dans la table SYSLOG s'affiche.

Si une entrée statique existait déjà et était affichée, la nouvelle entrée créée par le service remplace l'entrée préexistante.

Paramètres affichés/modifiables

Pour définir un nouveau SYSLOG server, saisissez son adresse IPv4 ou IPv6.

Étant donné que le nom d'hôte n'est pas enregistré, le système SNA effectue une résolution d'adresse IP dans le cadre de l'envoi de l'adresse du serveur. Par conséquent, l'adresse de serveur figurant sur le ticket s'affiche toujours sous forme d'adresse IP.

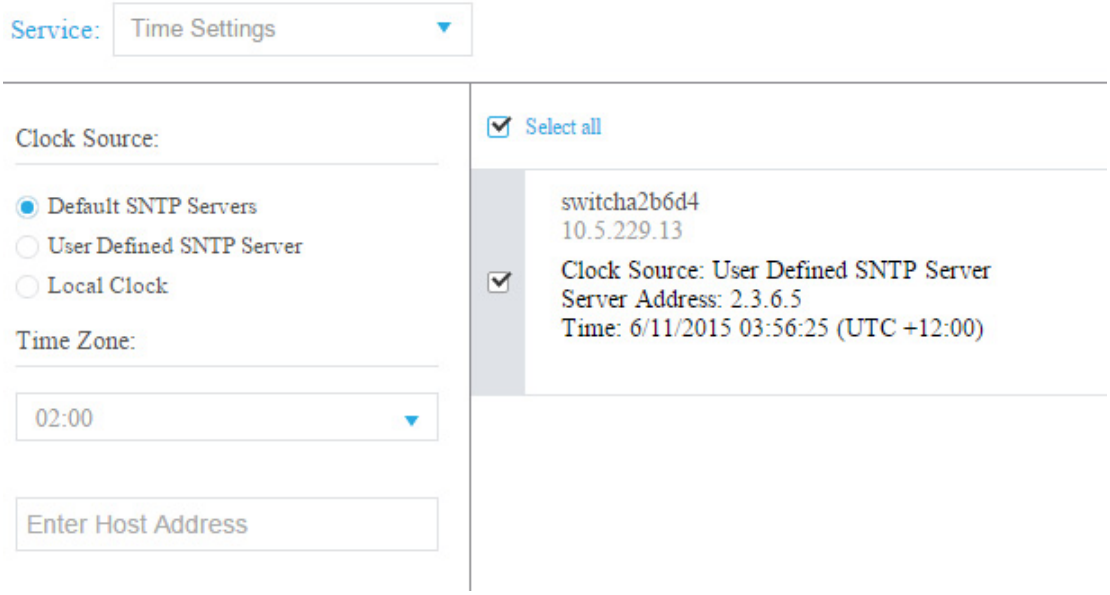
Configuration des paramètres d'heure

Ce service permet de définir la source d'heure et l'heure système des périphériques sélectionnés.

REMARQUE Nous vous conseillons vivement d'exécuter ce service afin de synchroniser les paramètres d'heure entre tous les périphériques du réseau. C'est particulièrement recommandé lorsque vous consultez des informations statistiques historiques sur plusieurs périphériques.

Configuration actuelle

Pour chaque périphérique sélectionné, la configuration actuelle s'affiche :



La source d'horloge actuelle, avec l'option suivante, s'affiche :

- **Serveurs SNTP par défaut** : serveurs s'affichant par défaut si la source d'horloge est SNTP.

- **Serveur SNTP défini par l'utilisateur** : cette option s'affiche si la source d'horloge est SNTP et la configuration actuelle comprend au moins un serveur SNTP défini par l'utilisateur. Dans ce cas, le serveur SNTP supérieur s'affiche selon l'ordre de priorité suivant :
  - Premier serveur SNTP (par ordre alphabétique), défini par nom d'hôte
  - Serveur SNTP ayant l'adresse IPv4 la plus basse
  - Serveur SNTP ayant l'adresse IPv6 la plus basse
- **Horloge locale** : cette option s'affiche si la source d'horloge est locale.
- **Heure actuelle** : affiche l'heure actuelle et le décalage du fuseau horaire.

Paramètres modifiables

Pour modifier la source d'horloge, sélectionnez l'une des options suivantes :

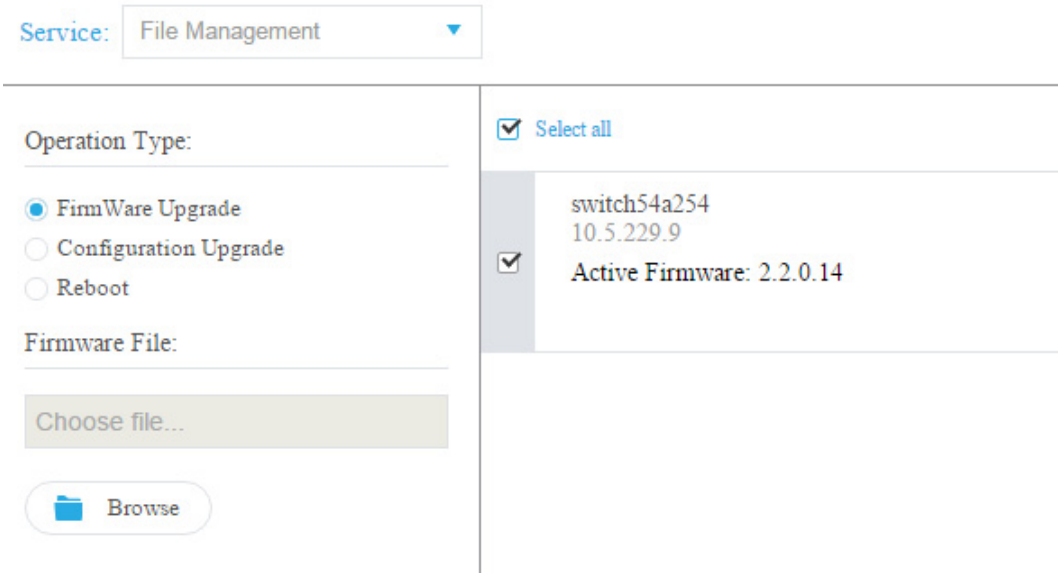
- **Serveur SNTP par défaut** : supprime tous les serveurs SNTP configurés et recrée trois nouveaux serveurs par défaut.
- **Serveur SNTP défini par l'utilisateur** : ajoutez l'adresse du serveur SNTP en saisissant son nom d'hôte ou son adresse IPv4 ou IPv6. Lorsque vous appliquez le serveur, tous les serveurs existants configurés sont supprimés et le serveur 1 est ajouté. **Fuseau horaire** : le fuseau horaire doit être configuré avec cette option.
- **Horloge locale** : remplace la source d'horloge du périphérique par l'horloge locale. La date, l'heure et le fuseau horaire doivent être renseignés.
- **Définir la date et l'heure** : date et heure si l'horloge locale est configurée.
- **Fuseau horaire** : décalage du fuseau horaire si un serveur SNTP défini par l'utilisateur ou une heure locale sont configurés.

Gestion des fichiers

Contrairement aux services évoqués plus haut, le service de gestion des fichiers ne modifie pas directement la configuration des périphériques sélectionnés. Il effectue plutôt une opération sur l'ensemble des périphériques sélectionnés. Utilisez ce service pour télécharger de nouvelles versions de microprogramme ou de fichiers de configuration vers des périphériques sélectionnés ou pour les redémarrer.

Configuration actuelle

La configuration actuelle affiche la version active du microprogramme comme suit :



Opérations

Les opérations suivantes sont disponibles avec ce service :

- Téléchargement du microprogramme via HTTP

  Permet de télécharger un nouveau fichier de microprogramme. Dans le système de fichier local, accédez au fichier de microprogramme, puis sélectionnez-le. Ce fichier est alors téléchargé sur tous les périphériques inclus dans le service.

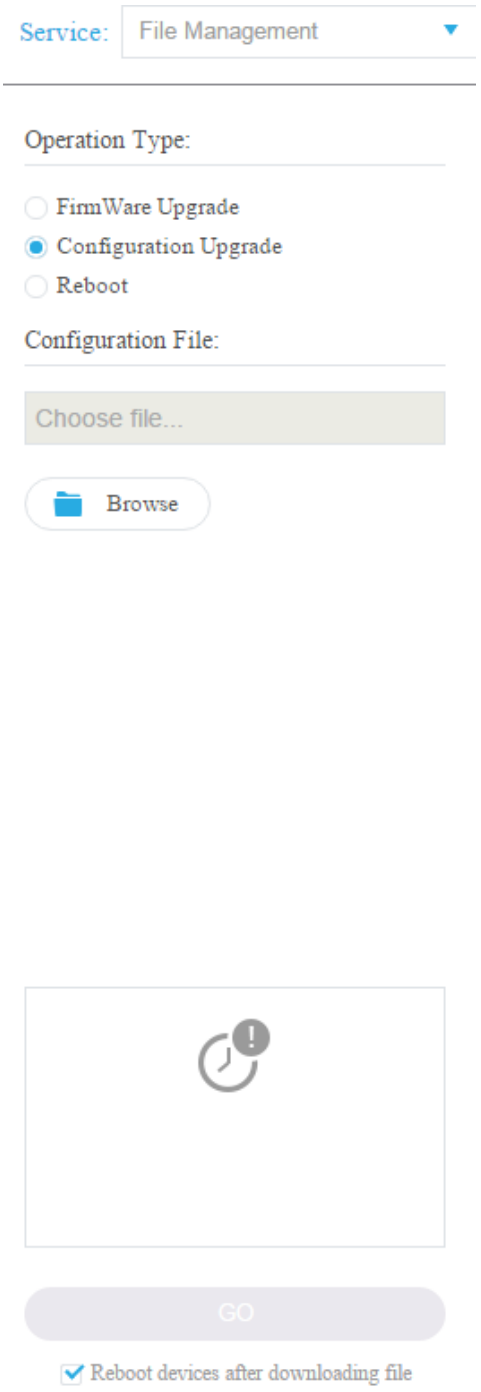
  Une fois le nouveau microprogramme téléchargé, le périphérique le définit automatiquement comme la version active du microprogramme.

Lorsque vous sélectionnez cette opération, vous pouvez également exiger que tous les périphériques ayant terminé le téléchargement redémarrent automatiquement afin de finaliser leur mise à jour (cette option est sélectionnée par défaut).

- Téléchargement de la configuration via HTTP

  Permet de télécharger un nouveau fichier de configuration. Dans le système de fichier local, accédez au fichier de configuration, puis sélectionnez-le. Ce fichier est alors téléchargé sur la configuration de démarrage de tous les périphériques inclus dans le service.

Lorsque vous activez ce téléchargement, vous pouvez exiger le redémarrage de tous les périphériques ayant téléchargé la configuration afin d'activer les nouvelles configurations.



- Redémarrage :

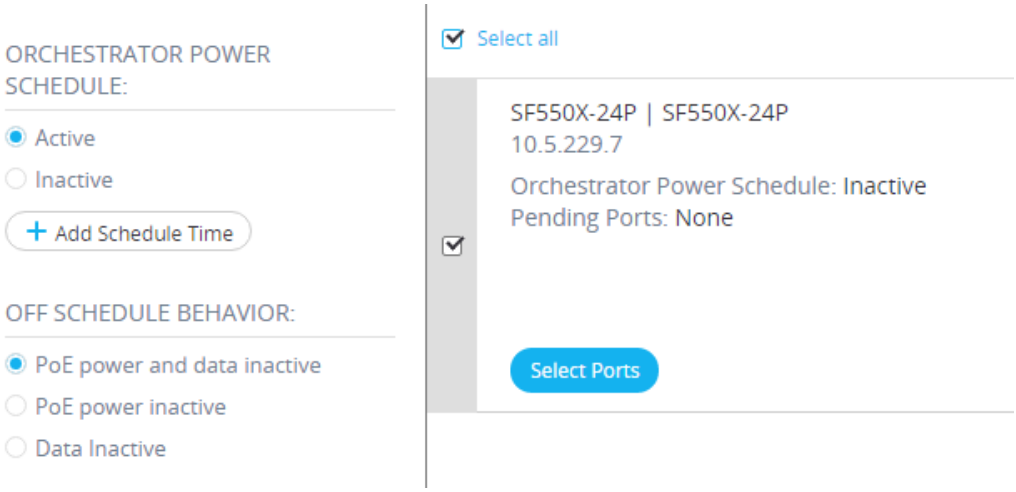
  Cliquez sur **Aller à** pour redémarrer les périphériques sans effectuer d'autres actions.

Stratégies relatives à la gestion de l'alimentation (au niveau du périphérique)

Ce service permet de définir des règles relatives à l'alimentation pour les périphériques sélectionnés.

Configuration actuelle

Pour chaque périphérique sélectionné, les paramètres de planification de l'alimentation en vigueur sont affichés, comme illustré ci-dessous :



Les paramètres suivants s'affichent :

- Planification de l'alimentation SNA (active/inactive).
- Détails de la planification de l'alimentation si elle est active.
- Indique si l'alimentation planifiée est active chaque jour, du lundi au dimanche.
- Comportement des ports en dehors de périodes planifiées Les options comprennent :
  - Alimentation PoE inactive
  - Données inactives
  - Alimentation PoE et données inactives

- Personnalisé : s'affiche si une planification créée par le système SNA ne s'applique pas de façon uniforme à tous les ports d'accès. Les ports d'accès sont ceux dont le mode VLAN est Accès.
- Ports configurés : une liste de tous les ports régis par la planification créée par le système SNA.

Paramètres modifiables

Vous pouvez créer une planification de l'alimentation (voir Définir une stratégie relative à la gestion de l'alimentation) et l'appliquer aux périphériques. Pour ce faire, sélectionnez une heure de démarrage et de fin d'activité pour chaque jour de la semaine, puis sélectionnez l'un des comportements suivants pour les périodes d'inactivité.

- Alimentation PoE inactive
- Données inactives
- Alimentation PoE et données inactives (option par défaut)

Pour activer correctement la planification sur les périphériques, vous devez sélectionner au moins un port par périphérique.

Vous devez sélectionner au moins un périphérique PoE pour sélectionner un comportement. Dans le cas contraire, la planification peut uniquement être créée ou supprimée.

La planification créée par ce service utilise un nom réservé (orch_power_sched). Les plages horaires portant d'autres noms seront ignorées par le système SNA.

Lorsque vous appliquez les paramètres, le comportement est imposé à tous les ports sélectionnés. Tous les ports non sélectionnés ne sont plus régis par la planification s'ils l'étaient auparavant.

Les ports non PoE ne sont affectés que si l'un des comportements, qui désactiverait les données, est sélectionné. Si un port sélectionné n'est pas affecté par le comportement sélectionné, une observation est ajoutée au message de réussite. Cette observation avertit l'utilisateur que certains ports ne sont pas concernés par la planification, car le comportement sélectionné ne s'applique pas à eux.

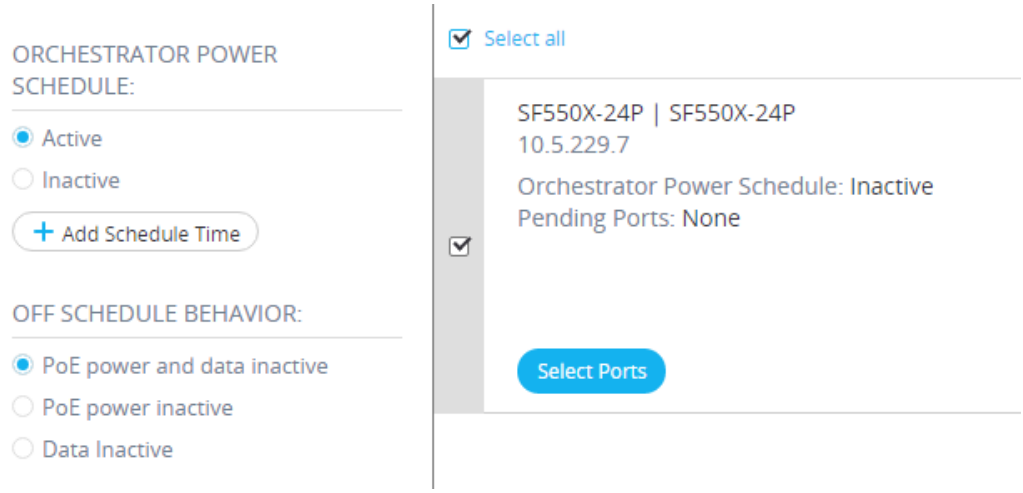
Définir une stratégie relative à la gestion de l'alimentation

Pour définir une stratégie relative à la gestion de l'alimentation, procédez comme suit :

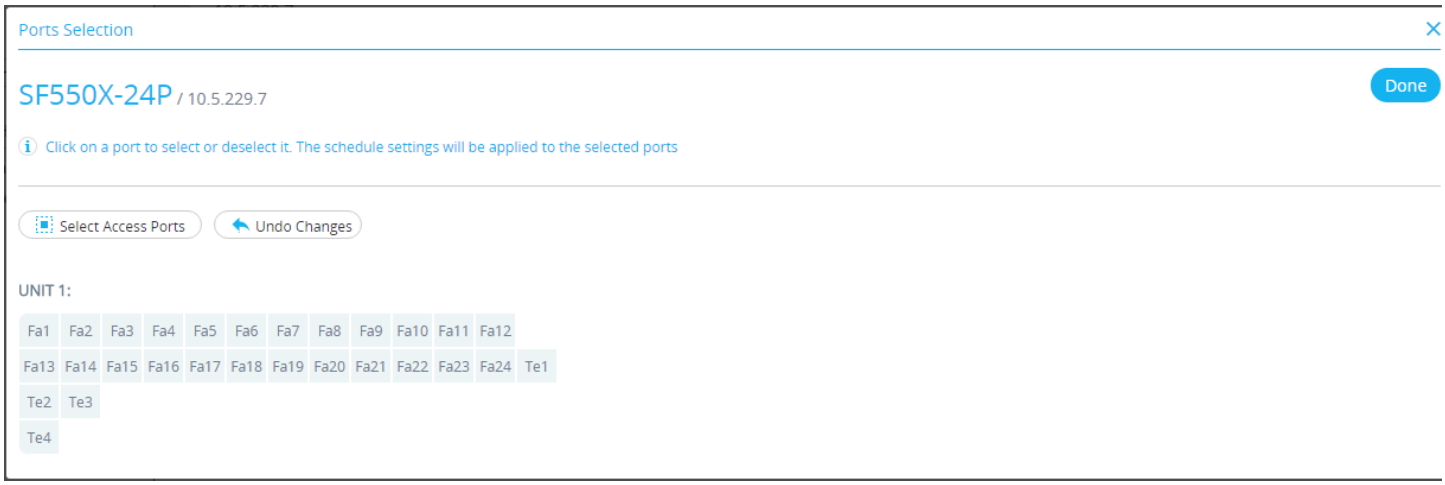
ÉTAPE 1 Cliquez sur un périphérique dans la vue de la topologie.

ÉTAPE 2 Sélectionnez le service **Gestion de l'alimentation** dans le panneau d'informations situé à droite.

Les éléments suivants s'affichent :

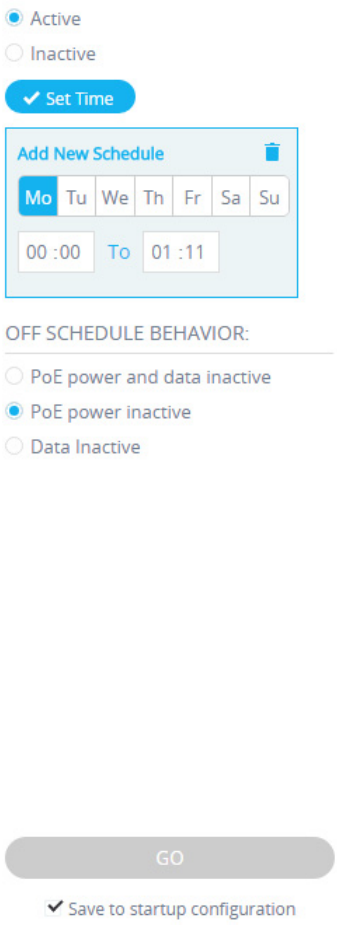


ÉTAPE 3 Cliquez sur **Sélectionner des ports**.



ÉTAPE 4 Sélectionnez un ou plusieurs ports, puis cliquez sur **Terminé**.

ÉTAPE 5 Cliquez sur **+Ajouter un horaire planifié**.



ÉTAPE 6 Complétez les champs (voir les descriptions plus haut), puis cliquez sur **Aller à**.

Vous venez de définir une stratégie relative à la gestion de l'alimentation.

Appartenance VLAN (au niveau du périphérique)

Ce service configure l'appartenance VLAN des interfaces pour plusieurs périphériques.

Configuration actuelle

Pour chaque périphérique, les paramètres suivants s'affichent :

- Ports d'accès : une liste des ports en mode VLAN d'accès. Cette liste est groupée par VLAN d'accès auxquels les ports appartiennent. Les plages consécutives de ports sont abrégées à l'aide de tirets.
- Ports de liaison : une liste des ports en mode VLAN de liaison. Cette liste est groupée par VLAN natifs auxquels les ports appartiennent. Les plages consécutives de ports sont abrégées à l'aide de tirets.

Paramètres modifiables

Lorsque vous modifiez les appartenances au VLAN, sélectionnez d'abord un VLAN sur lequel vous voulez intervenir. Cette sélection de VLAN vous permet d'obtenir une sélection de tous les VLAN existants dans le réseau, ainsi qu'une option de créer un nouveau VLAN.

Quand un VLAN est sélectionné, ouvrez un panneau de sélection des ports connectés à la fiche de chaque périphérique.

Dans ce panneau, tous les ports qui appartiennent au VLAN sélectionné sont marqués selon leur type d'appartenance :

- A : les ports d'accès qui appartiennent au VLAN, mais n'ont pas de balise.
- U : les ports de liaison qui appartiennent au VLAN, mais n'ont pas de balise (natifs).
- "*" : tous les autres états, soit n'appartenant pas au VLAN, soit appartenant au VLAN sous un mode VLAN différent.

Lorsque vous cliquez sur un port, vous basculez entre les états A et U (ou l'état "*" s'il s'agissait de l'état d'origine de ce port).

Les ports appartenant à des LAG affichent la marque correspondant à leur LAG, et lorsque vous cliquez sur un tel port, tous les membres du même LAG basculent simultanément.

Une fois l'appartenance modifiée et appliquée, le VLAN sera créé sur tous les périphériques ayant des ports qui lui appartiennent (si ce VLAN n'était pas déjà enregistré dans ces périphériques auparavant).

Services au niveau des interfaces

Certains services s'appliquent aux interfaces plutôt qu'aux périphériques. Lorsque vous les activez, sélectionnez une ou plusieurs interfaces, puis un service parmi ceux qui figurent dans la liste qui s'affiche.

Les services suivants sont disponibles pour les interfaces :

- **Paramètres de la gestion de l'alimentation (port)** : priorité PoE et comportement dans l'application de la planification. Reportez-vous à la section Réglages de la gestion de l'alimentation (au niveau de l'interface)
- **Appartenance VLAN (port/LAG)** : type Switchport (Accès et Liaison), appartenance pour Accès et Liaison. Reportez-vous à la section Appartenance VLAN (au niveau de l'interface)

Pour chacun de services, les tickets affichant les configurations actuelles des interfaces sélectionnées contiennent les informations d'identification suivantes, en plus des paramètres spécifiques au service :

- Nom de l'interface.
- Nom d'hôte du périphérique (du périphérique parent de l'interface).
- Adresse IP (du périphérique parent de l'interface) : si plus d'une adresse IP existe pour le périphérique, c'est celle que le système SNA utilise pour accéder au périphérique qui s'affiche.
- Modèle du périphérique (du périphérique parent de l'interface) : chaîne alphanumérique représentant le modèle du périphérique. Par exemple : SG350XG-2F10.

Réglages de la gestion de l'alimentation (au niveau de l'interface)

Ce service permet de configurer les réglages de l'alimentation sur des ports spécifiques. Il peut s'exécuter uniquement quand tous les ports sélectionnés appartiennent au même périphérique (ou à la même pile).

Paramètres affichés

- État administratif de l'alimentation PoE (Activée/Désactivée) : ce paramètre de s'affiche que pour les ports PoE.
- Priorité de l'alimentation des ports (Basse/Élevée/Critique) : ce paramètre ne s'affiche que pour les ports PoE.

- Planification de l'alimentation SNA (Appliquée/Non appliquée) : ce paramètre ne s'affiche que si le périphérique a une planification de l'alimentation créée par le système SNA.
- Comportement planifié : cette information ne s'affiche que si le port a une planification de l'alimentation définie par le système SNA. Ce champ peut prendre les valeurs suivantes :
  - Alimentation PoE inactive
  - Données inactives
  - Alimentation PoE et données inactives

Paramètres modifiables

- État administratif de l'alimentation PoE (Activée/Désactivée) : cette commande n'apparaît que si au moins l'un des ports PoE est sélectionné pour le service et ne s'applique qu'aux ports PoE.
- Priorité de l'alimentation des ports (Basse/Élevée/Critique) : cette commande n'apparaît que si au moins l'un des ports PoE est sélectionné pour le service et ne s'applique qu'aux ports PoE.
- Planification de l'alimentation SNA (Appliquée/Non appliquée) : cette commande ne s'affiche que si le périphérique a une planification de l'alimentation créée par le système SNA.
- Comportement planifié : cette commande ne s'affiche que si l'utilisateur souhaite appliquer la planification. Les valeurs possibles comprennent :
  - Alimentation PoE inactive
  - Données inactives
  - Alimentation PoE et données inactives

Si aucun port PoE n'est sélectionné, la planification peut uniquement être appliquée ou supprimée du port, et aucun comportement ne peut être sélectionné. Le fait d'appliquer la planification aux ports produit le même effet que de sélectionner l'option **Données inactives**.

Si des ports PoE et non PoE sont sélectionnés en même temps, lorsque vous appliquez les réglages aux ports PoE, l'option **Alimentation PoE et données inactives** est traitée comme s'il s'agissait de **Données inactives**, et l'option **Alimentation PoE inactive** est traitée comme si la planification n'était pas activée sur le port non Poe.

Appartenance VLAN (au niveau de l'interface)

Ce service configure l'appartenance VLAN des interfaces sélectionnées.

Paramètres affichés/modifiables

- Nom de l'interface (Écriture seule).
- Mode Switchport : pour l'affichage, il peut être défini sur Accès, Liaison, Général, Client, Hôte-Privé, Privé-De proximité. Lors de la configuration, l'utilisateur peut choisir Accès ou Liaison.
- VLAN d'accès : ne s'affiche qu'en mode Accès. Lorsque ce paramètre s'affiche, il présente l'ID du VLAN d'accès et permet la sélection du VLAN d'accès pendant la configuration.
- VLAN Natif (version 2.3 du système SNA) : ne s'affiche qu'en mode de liaison. Lorsque ce paramètre s'affiche, il présente l'ID du VLAN natif et permet la sélection du VLAN natif pendant la configuration.

La sélection des VLAN s'effectue dans une liste contenant tous les VLAN du réseau. Si le VLAN n'existe pas sur un périphérique auquel appartient l'interface sélectionnée, ce VLAN sera créé comme un élément inclus dans le fonctionnement du service.

L'utilisateur peut également sélectionner l'option d'ajouter un VLAN (1-4 094). Ce VLAN s'ajoutera à tous les commutateurs disposant d'interfaces sélectionnées pour le service.

Paramètres d'interface

Ce service configure les principaux paramètres des interfaces pour les ports ou les LAG.

Paramètres d'affichage

- État administratif : Actif/Inactif
- État actuel : Actif/Inactif/Suspendu Si le port est suspendu, le motif de cette suspension est précisé entre parenthèses. Par exemple : "Suspendu (ACL)".
- Négociation automatique – Activé/Désactivé
- Débit d'administration : ce paramètre ne s'affiche que si la Négociation automatique est désactivée.

  Les valeurs peuvent être 10 Mo, 100 Mo, 1 000 Mo, 2 500 Mo, 5 Go ou 10 Go.
- Débit actuel : 10 Mo, 100 Mo, 1 000 Mo, 2 500 Mo, 5 Go ou 10 Go.

- Mode duplex administratif : ce paramètre ne s'affiche que si la Négociation automatique est désactivée.

  Les valeurs peuvent être Semi-duplex ou Duplex intégral.

- Mode Duplex actuel : Semi-duplex ou Duplex intégral

Paramètres modifiables

- État administratif : Actif/Inactif
- Négociation automatique – Activé/Désactivé
- Débit : ce paramètre ne peut être modifié que si la Négociation automatique est désactivée. Les valeurs possibles pour le débit sont : 10 Mo, 100 Mo, 1 000 Mo, 2 500 Mo, 5 Go ou 10 Go. Différents types de ports peuvent présenter différents sous-groupes pour ces valeurs, et les options affichées dans le service varient selon les types de ports sélectionnés.
- Mode duplex : ce paramètre n'est disponible que si la Négociation automatique est désactivée et si le débit sélectionné est de 10 Mo ou 100 Mo.

Enregistrement des paramètres SNA

Toutes les modifications apportées au système SNA lui-même (sans utilisation des services) peuvent être enregistrées. Ils sont alors disponibles pour le lancement de la session SNA suivante sur le réseau. Ces informations enregistrées seront aussi disponibles lors de votre prochain accès au réseau depuis n'importe quel périphérique SNA connecté au même réseau ou depuis n'importe quel navigateur, à condition d'utiliser le même nom d'utilisateur lors de cette connexion.

Lorsque vous sauvez les paramètres, le système SNA tente d'enregistrer les modifications dans tous les périphériques SNA en ligne détectés (dans un dossier spécial **SNA** de la mémoire flash). S'il est impossible d'enregistrer une copie de ces paramètres, vous recevez une alerte d'échec.

Si l'opération d'enregistrement échoue sur l'un des périphériques ou sur tous, vous pouvez demander un rapport indiquant les périphériques pour lesquels les paramètres n'ont pas été enregistrés. Chaque périphérique cité dans le rapport affiche son ID et l'erreur constatée à son niveau.

Lorsque le système SNA est en cours de fonctionnement, si une nouvelle version des paramètres SNA est détectée sur l'un des appareils du réseau, vous recevrez une alerte vous l'indiquant (précisant sa date de création et le périphérique sur lequel elle a été créée), et serez invité à sélectionner la version des paramètres que le système SNA doit utiliser.

Les paramètres suivants peuvent être enregistrés :

- Position de tous les périphériques backbone dans le réseau.
- Tout périphérique client désigné comme un périphérique backbone conserve son état.
- Toute balise ajoutée manuellement aux éléments du réseau.
- Tout périphérique ajouté manuellement au réseau.
- Une chaîne de description pour les périphériques backbone.
- La liste noire utilisée par la fonctionnalité DAC.

Outre l'enregistrement des paramètres SNA dans le réseau, vous pouvez également exporter et importer des paramètres vers ou depuis un fichier externe pour bénéficier d'une sauvegarde supplémentaire.

L'importation d'un fichier ou l'acceptation d'un fichier plus récent détecté sur le réseau remplacera les paramètres SNA actuels. Une fois le fichier importé et la topologie mise à jour conformément aux nouveaux paramètres, vous êtes invité à faire le choix entre conserver ces modifications ou restaurer les paramètres précédents.

Si vous conservez les modifications, les nouveaux paramètres sont enregistrés dans tous les périphériques du réseau. Si vous restaurez les paramètres précédents, la topologie précédente est également restaurée conformément à ces paramètres.

Si vous sauvegardez manuellement les paramètres après avoir importé un nouveau fichier, vous ne bénéficiez plus de l'option de restaurer les anciens paramètres.

Détails techniques

Voici quelques détails techniques concernant la fonctionnalité SNA :

- Navigateurs pris en charge : IE10 et ultérieur, Chrome, Firefox
- Safari sur MAC OS : 6.1.2-7.0.2
- Systèmes d'exploitation pris en charge : Win 7, Win 8, Win 8.1, Linux 2.6, 3.11, MAC OSX version 10.7 et versions ultérieures.