345138

GUIDE D'ADMINISTRATION

Guide d'administration du commutateur administrable Cisco Small Business série 300 Version 1.3.5

Table des matières

Chapitre 1 : Mise en route 1

Démarrage de l'utilitaire Web de configuration 1
Configuration de l'appareil - Démarrage rapide 5
Conventions de nommage de l'interface 6
Navigation dans les fenêtres 7

Chapitre 2 : État et statistiques 12

Récapitulatif système 12
Affichage des interfaces Ethernet 12
Affichage des statistiques Etherlike 14
Affichage des statistiques GVRP 15
Affichage des statistiques EAP 802.1X 17
Affichage du taux d'utilisation TCAM 18
Intégrité 19
Gestion du contrôle à distance (RMON) 19
Afficher le journal 28

Chapitre 3 : Administration : Journal système 29

Définition des paramètres de journalisation système 29
Définition des paramètres de journalisation distante 31
Affichage des journaux de la mémoire 33

Chapitre 4 : Administration : Gestion de fichiers 35

Fichiers système 35
Mettre à niveau/sauvegarder micrologiciel/langue 39
Image active 43
Télécharger/sauvegarder configuration/journal 44
Propriétés des fichiers de configuration 50

Copier/enregistrer la configuration 51
Configuration automatique via DHCP 53

Chapitre 5 : Administration 60

Modèles de périphériques 61
Paramètres système 63
Paramètres de console (prise en charge du débit de bauds automatiques) 67
Interface de gestion 67
Comptes d'utilisateur 68
Définition du délai d'expiration en cas de session inactive 68
Paramètres de l'heure 68
Journal système 69
Gestion de fichiers 69
Redémarrage du périphérique 69
Ressources de routage 71
Intégrité 72
Diagnostic 74
Détection - Bonjour 74
Détection - LLDP 74
Détection - CDP 74
Ping 74
Traceroute 76

Chapitre 6 : Administration : Paramètres horaires 78

Options d'heure système 79
Modes SNTP 80
Configuration de l'heure système 81

Chapitre 7 : Administration : Diagnostic 92

Test des ports cuivre 92

Affichage de l'état des modules optiques 94
Configuration de la mise en miroir des ports et de VLAN 96
Affichage de l'utilisation du CPU et fonction Secure Core Technology (SCT) 98

Chapitre 8 : Administration : Détection 99

Bonjour 99
LLDP et CDP 101
Configuration de LLDP 103
Configuration de CDP 124

Chapitre 9 : Gestion des ports 134

Configuration des ports 134
Définition de la configuration des ports 135
Agrégation de liaisons 140
UDLD 148
PoE 148
Configuration de Green Ethernet 149

Chapitre 10 : Gestion des ports : Unidirectional Link Detection 158

Vue d'ensemble de la fonction UDLD 158
Fonctionnement de UDLD 159
Instructions d'utilisation 162
Dépendances envers les autres fonctions 163
Configuration et paramètres par défaut 163
Avant de commencer 163
Tâches UDLD courantes 164
Configuration de UDLD 164

Chapitre 11 : Port intelligent 169

Vue d'ensemble 169
Qu'est-ce qu'un port intelligent ? 170

Types de port intelligent 171
Macros Port intelligent 173
Échec de la macro et opération de réinitialisation 175
Fonctionnement de la fonction Port intelligent 176
Port intelligent automatique 177
Gestion des erreurs 181
Configuration par défaut 181
Relations avec les autres fonctions et compatibilité descendante 181
Tâches courantes de port intelligent 182
Configuration de port intelligent à l'aide de l'interface Web 184
Macros Port intelligent intégrées 190

Chapitre 12 : Gestion des ports : fonctionnalité PoE 202

PoE sur l'appareil 202
Configuration des propriétés PoE 205
Configuration des paramètres de la fonctionnalité PoE 207

Chapitre 13 : Gestion des VLAN 210

VLAN 210
Configuration des paramètres VLAN par défaut 213
Création d'un VLAN 215
Configuration des paramètres d'interface VLAN 216
Définition de l'appartenance VLAN 217
Paramètres GVRP 220
Groupes VLAN 222
VLAN voix 227
Accès VLAN TV port multidiffusion 241
VLAN TV port client multidiffusion 245

Chapitre 14 : Arbre recouvrant 248

Types de STP 248

Configuration de l'état STP et des paramètres globaux 249
Définition des paramètres d'interface du Spanning Tree 251
Configuration des paramètres Rapid Spanning Tree 254
Multiple Spanning Tree 256
Définition des propriétés MSTP 257
Mappage des VLAN à une instance MSTP 258
Définition des paramètres d'instance MSTP 259
Définition des paramètres de l'interface MSTP 260

Chapitre 15 : Gestion des tables d'adresses MAC 263

Configuration d'adresses MAC statiques 264
Gestion des adresses MAC dynamiques 265
Définition d'adresses MAC réservées 266

Chapitre 16 : Multidiffusion 267

Transfert de multidiffusion 267
Définition des propriétés de multidiffusion 271
Ajout d'une adresse MAC de groupe 272
Ajout d'adresses IP de groupe de multidiffusion 275
Configuration de la surveillance de trafic IGMP 276
Surveillance MLD 280
Interrogation du groupe de multidiffusion IP IGMP/MLD 282
Définition des ports de routeur de multidiffusion 283
Définition de la multidiffusion Tout transférer 284
Définition des paramètres de multidiffusion non enregistrée 285

Chapitre 17 : Configuration IP 287

Vue d'ensemble 287
IPv4 Management and Interfaces (Interfaces et gestion IPv4) 291
Serveur DHCP 313
IPv6 Management and Interfaces (Interfaces et gestion IPv6) 323

Nom de domaine 339

Chapitre 18 : Sécurité 345

Définition d'utilisateurs 346
Configuration de TACACS+ 350
Configuration de RADIUS 355
Méthode d'accès de gestion 360
Authentification de l'accès de gestion 366
Gestion sécurisée des données confidentielles 367
Serveur SSL 367
Serveur SSH 370
Client SSH 370
Configuration des services TCP/UDP 370
Définition du contrôle des tempêtes 372
Configuration de la sécurité des ports 373
802.1X 376
Prévention du déni de service 376
Surveillance DHCP 387
Protection de la source IP 387
Inspection ARP 391
Sécurité du premier saut 397

Chapitre 19 : Sécurité : Authentification 802.1X 398

Présentation de 802.1X 398
Présentation de l'authentificateur 400
Tâches courantes 411
Configuration de 802.1X via l'interface utilisateur graphique (GUI) 413
Définition des périodes 425
Prise en charge des méthodes d'authentification et des modes de port 425

Chapitre 20 : Sécurité : Sécurité du premier saut IPv6 428

Présentation de la Sécurité du premier saut 429
Protection Router Advertisement 433
Inspection Neighbor Discovery 433
Protection DHCPv6 434
Intégrité de la liaison de voisin 435
Protection contre les attaques 437
Stratégies, paramètres globaux et valeurs par défaut du système 439
Tâches courantes 441
Configuration et paramètres par défaut 443
Avant de commencer 443
Configuration de la Sécurité du premier saut via l'interface utilisateur graphique Web 444

Chapitre 21 : Sécurité : Gestion sécurisée des données confidentielles 457

Introduction 457
Règles SSD 458
Propriétés SSD 464
Fichiers de configuration 467
Canaux de gestion SSD 473
Interface de ligne de commande (CLI) et récupération du mot de passe 474
Configuration de SSD 474

Chapitre 22 : Sécurité : Client SSH 478

Secure Copy (SCP) et SSH 478
Méthodes de protection 479
Authentification du serveur SSH 481
Authentification du client SSH 482
Avant de commencer 483
Tâches courantes 483

Configuration du client SSH via l'interface utilisateur graphique (GUI) 485

Chapitre 23 : Sécurité : Serveur SSH 490

Vue d'ensemble 490
Tâches courantes 491
Pages de configuration du serveur SSH 492

Chapitre 24 : Contrôle d'accès 495

Listes de contrôle d'accès 495
Définition d'ACL basées sur MAC 498
ACL basées sur IPv4 500
ACL basées sur IPv6 505
Définition d'une liaison ACL 508

Chapitre 25 : Qualité de service 511

Fonctions et composants QoS 511
Configuration de la QoS - Général 515
Mode de base de QoS 525
Mode de QoS avancé 528
Gestion des statistiques de QoS 541

Chapitre 26 : SNMP 545

Versions et flux de travail SNMP 545
ID d'objet du modèle 549
ID de moteur SNMP 551
Configuration de vues SNMP 553
Création de groupes SNMP 554
Création d'utilisateurs SNMP 556
Définition de communautés SNMP 558
Définition de paramètres d'interceptions 561
Destinataires de notifications 561
Filtres de notification SNMP 566

1

Mise en route

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

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

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

Connexion

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

REMARQUE Si vous n'avez pas encore choisi la langue de l'interface utilisateur graphique, la page de connexion s'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), la première langue intégrée dont le code de la langue correspond est sélectionnée (sans code de pays correspondant, par exemple : fr_CA).

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

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

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

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

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

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

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

Si vous avez saisi un nom d'utilisateur ou un mot de passe erroné, un message d'erreur apparaît et la page Connexion reste affichée sur la fenêtre. Si vous rencontrez des problèmes pour vous connecter, reportez-vous à la section **Lancement de l'utilitaire de configuration** du Guide d'administration pour obtenir des informations supplémentaires.

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

HTTP/HTTPS

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

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 :

- 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 **Définition du délai d'expiration en cas de session inactive**.

AVERTISSEMENT 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 appareil, comme un téléphone IP (voir **Qu'est-ce qu'un port intelligent ?**), il configure le port de manière adéquate. Ces commandes de configuration sont écrites dans le fichier de Configuration d'exécution. L'icône Enregistrer se met alors à clignoter lorsque vous vous connectez, même si vous n'avez apporté aucune modification à la configuration.

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

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

En cas d'expiration du délai ou si vous vous déconnectez intentionnellement du système, un message apparaît et la page Connexion signalant l'état de déconnexion s'ouvre. 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 qui apparaît est la page Récapitulatif système.

Configuration de l'appareil - Démarrage rapide

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

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

Catégorie	Nom du lien (sur la page)	Page correspondante
	Configuration de sauvegarde de l'appareil	Page Télécharger/ sauvegarder configuration/ journal
	Créer une ACL basée sur MAC	Page ACL basée sur MAC
	Créer une ACL basée sur IP	Page ACL basée sur IPv4
	Configurer la QoS	Page Propriétés de QoS
	Configurer la mise en miroir des ports	Page Mise en miroir des ports et VLAN

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

Conventions de nommage de l'interface

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

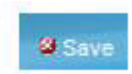
- **Type de l'interface** : les types suivants d'interface se retrouvent dans divers types de périphériques :
  - **Fast Ethernet (10/100 bits)** : celles-ci sont désignées par **FE**.
  - **Ports Gigabit Ethernet (10/100/1 000 bits)** : celles-ci sont désignées par **GE**.
  - **LAG (PortChannel)**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

Navigation dans les fenêtres

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

En-tête d'application

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

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

Boutons de gestion

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

Nom du bouton	Description
	Servez-vous du menu déroulant pour configurer le nombre d'entrées par page.
	Indique un champ obligatoire.
Ajout	Cliquez sur ce bouton pour afficher la 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.
Effacer les compteurs de toutes les interfaces	Cliquez sur ce bouton pour effacer les compteurs de statistiques de toutes les interfaces.

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

Nom du bouton	Description
Actualiser	Cliquez sur **Actualiser** pour actualiser les valeurs de compteur.
Test	Cliquez sur **Tester** pour effectuer les tests liés.

2

État et statistiques

Cette section décrit comment afficher les statistiques du périphérique.

Elle couvre les rubriques suivantes :

- **Récapitulatif système**
- **Affichage des interfaces Ethernet**
- **Affichage des statistiques Etherlike**
- **Affichage des statistiques GVRP**
- **Affichage des statistiques EAP 802.1X**
- **Affichage du taux d'utilisation TCAM**
- **Intégrité**
- **Gestion du contrôle à distance (RMON)**
- **Afficher le journal**

Récapitulatif système

Reportez-vous à la section **Paramètres système**.

Affichage des interfaces Ethernet

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

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

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

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

ÉTAPE 2 Saisissez les paramètres.

- **Interface** : sélectionnez le type d'interface et l'interface spécifique pour laquelle les statistiques Ethernet doivent être affichées.
- **Taux d'actualisation** : sélectionnez la durée qui s'écoule avant l'actualisation des statistiques Ethernet de l'interface. Les options disponibles sont les suivantes :
  - *Aucune actualisation* : les statistiques ne sont pas actualisées.
  - *15 s* : les statistiques sont actualisées toutes les 15 secondes.
  - *30 s* : les statistiques sont actualisées toutes les 30 secondes.
  - *60 s* : les statistiques sont actualisées toutes les 60 secondes.

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

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

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

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

Pour effacer ou afficher les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs de l'interface affichée.
- Cliquez sur **Voir les statistiques de toutes les interfaces** pour visualiser l'ensemble des ports sur une seule et même page.

Affichage des statistiques Etherlike

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

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

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

ÉTAPE 2 Saisissez les paramètres.

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

Les champs sont affichés pour l'interface sélectionnée.

- **Erreurs FCS (Frame Check Sequence)** : trames reçues ayant échoué aux contrôles de redondance cyclique (CRC).
- **Trames de collisions individuelles** : trames impliquées dans une collision individuelle, mais ayant été transmises avec succès.
- **Collisions tardives** : collisions ayant été détectées après les 512 premiers octets de données.
- **Collisions excessives** : nombre de transmissions rejetées dues à des collisions excessives.

- **Paquets de taille excessive** : paquets de plus de 2 000 octets reçus.
- **Erreurs de réception MAC internes** : trames rejetées en raison d'erreurs de destination.
- **Trames de pause reçues** : trames de pause de contrôle de flux reçues.
- **Trames de pause transmises** : trames de pause de contrôle de flux transmises à partir de l'interface sélectionnée.

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs sélectionnés.
- Cliquez sur **Voir les statistiques de toutes les interfaces** pour visualiser l'ensemble des ports sur une seule et même page.

Affichage des statistiques 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 Niveau 2 basé sur des normes permettant la configuration automatique des informations VLAN sur les commutateurs. Il a été défini dans l'amendement 802.1ak apporté à la norme 802.1Q-2005.

Les statistiques GVRP d'un port ne s'affichent que si GVRP est activé globalement et sur le port. Reportez-vous à la page 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.
- **Taux d'actualisation** : sélectionnez la durée qui s'écoule avant l'actualisation de la page des statistiques GVRP.

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

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

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

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

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs sélectionnés.
- Cliquez sur **Voir les statistiques de toutes les interfaces** pour visualiser l'ensemble des ports sur une seule et même page.

Affichage des statistiques EAP 802.1X

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

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

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

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

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

Les valeurs sont affichées pour l'interface sélectionnée.

- **Trames EAPOL reçues** : trames EAPOL valides reçues sur le port.
- **Trames EAPOL transmises** : trames EAPOL valides transmises par le port.
- **Trames EAPOL de début reçues** : affiche le nombre de trames EAPOL de début qui ont été reçues sur le port.
- **Trames EAPOL de déconnexion reçues** : affiche le nombre de trames EAPOL de déconnexion qui ont été reçues sur le port.
- **Trames ID/de réponse EAP reçues** : trames ID/de réponse EAP reçues sur le port.
- **Trames de réponse EAP reçues** : trames de réponse EAP reçues par le port (autres que les trames ID/de réponse).
- **Trames ID/de demande EAP transmises** : trames ID/de demande EAP transmises par le port.
- **Trames de demande EAP transmises** : trames de demande EAP transmises par le port.
- **Trames EAPOL non valides reçues** : affiche le nombre de trames EAPOL non reconnues qui ont été reçues sur ce port.
- **Trames d'erreur de longueur EAP reçues** : trames EAPOL avec une longueur de corps de paquet non valide reçues sur ce port.
- **Version de la dernière trame EAPOL** : numéro de version de protocole associé à la dernière trame EAPOL reçue.

- **Source de la dernière trame EAPOL** : adresse MAC source associée à la dernière trame EAPOL reçue.

Pour effacer les compteurs de statistiques :

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

Affichage du taux d'utilisation TCAM

L'architecture du périphérique utilise une mémoire TCAM (Ternary Content Addressable Memory) pour prendre en charge les actions des paquets à vitesse filaire.

La mémoire TCAM contient les règles produites par d'autres applications, telles que les règles ACL (Access Control Lists, listes de contrôle d'accès), les règles QoS (Qualité de service), 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 TCAM**.

La page Utilisation de TCAM répertorie les champs suivants :

- **Nombre maximum d'entrées TCAM pour les règles IPv4 et les règles non IP** : nombre maximum d'entrées TCAM disponibles.
- **Routage IPv4**
  - **Utilisée** : nombre d'entrées TCAM utilisées pour le routage IPv4.
  - **Maximum** : nombre d'entrées TCAM disponibles pouvant être utilisées pour le routage IPv4.

- **Règles non-IP**
  - **Utilisée** : nombre d'entrées TCAM utilisées pour les règles non IP.
  - **Maximum** : nombre d'entrées TCAM disponibles pour une utilisation par les règles non IP.

Intégrité

Reportez-vous à la section **Intégrité**.

Gestion du contrôle à distance (RMON)

RMON (Remote Networking Monitoring) est une spécification SNMP qui 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 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 (étant donné que 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, tels que « a atteint un certain nombre de collisions tardives » (définit l'alarme), puis définir l'action à mettre en œuvre lorsque cet événement se produit (journal, interception, ou journal et interception).

Affichage des statistiques RMON

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

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

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

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

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

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

Les statistiques sont affichées pour l'interface sélectionnée.

- **Octets reçus** : nombre d'octets reçus, y compris les paquets erronés et les octets FCS, mais sans les bits de synchronisation.
- **Événements d'abandon** : nombre de paquets ayant été abandonnés.
- **Paquets reçus** : nombre de paquets corrects reçus, dont les paquets de multidiffusion et de diffusion.
- **Paquets de diffusion reçus** : nombre de paquets de diffusion corrects reçus. Ce nombre n'inclut pas les paquets de multidiffusion.
- **Paquets de multidiffusion reçus** : nombre de paquets de multidiffusion corrects reçus.
- **Erreurs d'alignement et CRC** : nombre d'erreurs d'alignement et CRC qui se sont produites.
- **Paquets de taille insuffisante** : nombre de paquets de taille insuffisante (moins de 64 octets) reçus.
- **Paquets de taille excessive** : nombre de paquets de taille excessive (plus de 2 000 octets) reçus.

- **Fragments** : nombre de fragments (paquets de moins de 64 octets, à l'exception des bits de synchronisation, mais incluant les octets FCS) reçus.
- **Jabbers** : nombre total de paquets reçus ayant une longueur supérieure à 1 632 octets. Ce nombre exclut les bits de synchronisation, mais inclut les octets FCS qui comportaient une séquence FCS (Frame Check Sequence) erronée avec un nombre entier d'octets (Erreur FCS) ou une séquence FCS erronée avec un nombre non entier d'octets (Erreur d'alignement). Un paquet de jabotage est défini en tant que trame Ethernet respectant les critères suivants :
  - La longueur des données du paquet est supérieure à la MRU.
  - Le paquet a un CRC non valide.
  - Un événement d'erreur de réception (Rx) n'a pas été détecté.
- **Collisions** : nombre de collisions reçues. Si les trames Jumbo sont activées, le seuil des trames de jabotage est augmenté de façon à correspondre à la taille maximale des trames Jumbo.
- **Trames de 64 octets** : nombre de trames de 64 octets reçues.
- **Trames de 65 à 127 octets** : nombre de trames de 65 à 127 octets reçues.
- **Trames de 128 à 255 octets** : nombre de trames de 128 à 255 octets reçues.
- **Trames de 256 à 511 octets** : nombre de trames de 256 à 511 octets reçues.
- **Trames de 512 à 1 023 octets** : nombre de trames de 512 à 1 023 octets reçues.
- **Trames de 1 024 octets ou plus** : nombre de trames de 1 024 à 2 000 octets et de trames Jumbo reçues.

Pour effacer les compteurs de statistiques :

- Cliquez sur **Effacer les compteurs de l'interface** pour effacer les compteurs sélectionnés.
- Cliquez sur **Voir les statistiques de toutes les interfaces** pour visualiser l'ensemble des ports sur une seule et même page.

Configuration de l'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 Table de contrôle de l'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 dans la page Ajouter un historique RMON ci-dessous. Le seul champ de cette page qui n'est pas défini dans 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.
- **Nombre maximum d'échantillons à conserver** : saisissez le nombre d'échantillons à stocker.
- **Intervalle d'échantillonnage** : saisissez la durée (en secondes) pendant laquelle des échantillons sont collectés au niveau des ports. La plage du champ est comprise entre 1 et 3 600.
- **Propriétaire** : saisissez l'utilisateur ou la station RMON ayant demandé les informations RMON.

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** pour afficher les statistiques réelles.

Affichage de la table d'historique RMON

La page Table d'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 **Table d'historique**.

ÉTAPE 3 Dans la liste **N° d'entrée d'historique**, sélectionnez 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 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.
- **Paquets de multidiffusion** : 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 incluant les octets FCS.
- **Jabbers** : 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.

Définition du 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 d'interceptions.
- **Page Alarmes** : 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.

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 d'interceptions (facultatif). Veuillez noter que la communauté doit être définie à l'aide des pages **Définition de destinataires de notifications SNMPv1,2** ou **Définition de destinataires de notification SNMPv3** pour que l'interception 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.
- **Type de notification** : sélectionnez le type d'action résultant de cet événement. Les valeurs possibles sont :
  - *Aucun* : aucune action ne se produit lorsque l'alarme s'arrête.
  - *Journal (Table journal d'événements)* : ajoutez une entrée de journal à la table du journal d'événements lorsque l'alarme se déclenche.
  - *Interception (gestionnaire SNMP et serveur SYSLOG)* : permet d'envoyer une interception 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.
- **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.)
- **Propriétaire** : 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).

Affichage des journaux d'événements RMON

La page Table du journal d'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 de l'événement est réalisée lorsque l'événement est associé à une alarme (reportez-vous à la page Alarmes) et que les conditions de déclenchement de l'alarme sont remplies.

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

ÉTAPE 2 Cliquez sur **Table du journal d'événements**

Cette page affiche les champs suivants :

- **N° d'entrée d'événement** : numéro d'entrée dans le journal de l'événement.
- **N° de journal** : numéro du journal (au sein de l'événement).
- **Heure de journalisation** : heure à laquelle l'entrée a été enregistrée dans le journal.
- **Description** : description de l'événement qui a déclenché l'alarme.

Définition des alarmes RMON

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

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

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

Pour entrer des alarmes RMON :

ÉTAPE 1 Cliquez sur **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.
- **Nom du compteur** : sélectionnez la variable MIB qui indique le type d'occurrence mesuré.
- **Type d'échantillon** : sélectionnez la méthode d'échantillonnage pour générer une alarme. Les options sont les suivantes :
  - *Absolu* : si le seuil est franchi, une alarme est générée.
  - *Différentiel* : 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 Événements.
- **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.
- **Alarme de démarrage** : sélectionnez le premier événement à partir duquel lancer la génération d'alarmes. La hausse est définie en franchissant le seuil en partant d'un seuil de faible valeur vers un seuil de valeur plus importante.
  - *Alarme de hausse* : une valeur 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.

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

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

Afficher le journal

Reportez-vous à la section **Affichage des journaux de la mémoire**.

3

Administration : Journal système

Cette section décrit la fonction Journal 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 :

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

Définition des paramètres de journalisation système

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

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

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

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

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

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

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

Pour définir des paramètres de journalisation globaux :

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

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* : le nom d'hôte système est ajouté 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 sévérité des messages à journaliser dans la RAM.
- **Journalisation de la mémoire Flash** : sélectionnez les niveaux de sévérité des messages à journaliser dans la mémoire Flash.

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

Définition des paramètres de journalisation distante

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

Pour définir les serveurs SYSLOG :

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

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.

ÉTAPE 3 Cliquez sur **Ajouter**.

ÉTAPE 4 Saisissez les paramètres.

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

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

Affichage des journaux de la mémoire

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.

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

En haut de la page se trouve un bouton qui vous permet de Désactiver le clignotement de l'icône d'alerte. Pour activer ou désactiver cette fonction, **cliquez** sur ce bouton.

Cette page comporte les champs suivants :

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

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

Mémoire Flash

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

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

Cette page comporte les champs suivants :

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

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

4

Administration : Gestion de fichiers

Cette section se concentre sur la gestion des fichiers système.

Les sujets suivants sont traités :

- **Fichiers système**
- **Mettre à niveau/sauvegarder micrologiciel/langue**
- **Image active**
- **Télécharger/sauvegarder configuration/journal**
- **Propriétés des fichiers de configuration**
- **Copier/enregistrer la configuration**
- **Configuration automatique via DHCP**

Fichiers système

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

Vous pouvez effectuer diverses actions avec ces fichiers, par exemple : sélectionner le fichier du micrologiciel à partir duquel 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 externe.

Les méthodes de transfert de fichiers disponibles sont les suivantes :

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

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

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

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

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

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

Fichiers et types de fichiers

Les fichiers de configuration et fichiers opérationnels correspondant aux types suivants sont présents sur l'appareil :

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

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

  Pour conserver toutes les modifications apportées 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 sur la Configuration miroir. Vous pouvez toutefois copier la Configuration miroir vers d'autres types de fichiers ou sur un autre appareil.

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

Actions des fichiers

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

- Mettre à niveau le micrologiciel ou le code de démarrage, ou remplacer une langue, comme décrit dans la section **Mettre à niveau/sauvegarder micrologiciel/langue**
- Afficher l'image du micrologiciel actuellement utilisée ou sélectionner l'image à utiliser lors du redémarrage suivant, comme décrit à la section **Image active**.
- Enregistrer les fichiers de configuration de l'appareil dans un répertoire situé sur un autre appareil, comme décrit à la section **Télécharger/ sauvegarder configuration/journal**
- Effacer les types de fichiers de Configuration de démarrage ou de Configuration de sauvegarde, comme décrit dans la section **Propriétés des fichiers de configuration**
- Copier un type de fichier de configuration dans un autre type de fichier de configuration, comme décrit dans la section **Copier/enregistrer la configuration**
- Télécharger automatiquement un fichier de configuration depuis un serveur DHCP vers l'appareil, comme décrit à la section **Configuration automatique via DHCP**

Cette rubrique aborde les points suivants :

- **Mettre à niveau/sauvegarder micrologiciel/langue**
- **Image active**
- **Télécharger/sauvegarder configuration/journal**
- **Propriétés des fichiers de configuration**
- **Copier/enregistrer la configuration**
- **Configuration automatique via DHCP**

Mettre à niveau/sauvegarder micrologiciel/langue

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

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

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

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

Lorsqu'un nouveau fichier de langue est chargé sur l'appareil, la langue y correspondant peut être sélectionnée dans le menu déroulant. Notez que redémarrer l'appareil n'est pas nécessaire.

Deux images du micrologiciel 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 niveau du micrologiciel, la nouvelle image remplace toujours celle identifiée comme étant l'image inactive.

Même après avoir téléchargé le nouveau micrologiciel sur l'appareil, ce dernier continue de démarrer en utilisant l'image active (l'ancienne version) jusqu'à ce que vous activiez la nouvelle image, en vous conformant à la procédure décrite à la section **Image active**. Démarrez ensuite l'appareil.

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

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

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

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

- Si vous avez sélectionné **TFTP**, passez à l'**ÉTAPE 3**.
- Si vous avez sélectionné **via HTTP/HTTPS**, passez à l'**ÉTAPE 4**.
- Si vous avez sélectionné **via SCP**, passez à l'**ÉTAPE 5**.

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

Sélectionnez l'une des **actions d'enregistrement** suivantes :

- **Mettre à niveau** : spécifie que le type de fichier présent sur l'appareil doit être remplacé par sa nouvelle version, laquelle version est située sur un serveur TFTP.
- **Sauvegarder** : spécifie qu'une copie du type de fichier doit être enregistrée dans un fichier situé sur un autre appareil.

Renseignez les champs suivants :

- **Type de fichier** : sélectionnez le type de fichier de destination. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)
- **Définition du serveur TFTP** : indiquez si vous souhaitez spécifier le serveur TFTP par son adresse IP ou son nom de domaine.
- **Version IP** : indiquez si l'adresse utilisée est de type IPv4 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 uniquement des hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe FE80, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.

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

- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée)
- **Adresse IP/Nom serveur TFTP** : saisissez l'adresse IP ou le nom de domaine du serveur TFTP.
- **(Pour une mise à niveau) Nom du fichier source** : saisissez le nom du fichier source.
- **(Pour une sauvegarde) Nom du fichier de destination** : saisissez le nom du fichier de sauvegarde.

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

- **Type du fichier** : sélectionnez l'un des types de fichiers suivants :
  - *Image du micrologiciel* : sélectionnez cette option pour mettre à niveau l'image du micrologiciel.
  - *Langue* : sélectionnez cette option pour mettre à niveau le fichier de langue.
- **Nom du fichier** : cliquez sur **Parcourir** pour sélectionner un fichier ou saisissez le chemin et le nom du fichier source à utiliser pour le transfert.

ÉTAPE 5 Si vous avez sélectionné via **SCP (sur SSH),** consultez la section **Authentification du client SSH** pour obtenir de plus amples instructions. Renseignez ensuite les champs suivants : Notez que seuls les champs uniques sont décrits, pour les autres, consultez les descriptions ci-dessus.

- **Authentification du serveur SSH distant** : pour activer l'authentification du serveur SSH (qui est désactivée par défaut), cliquez sur **Modifier.** Vous êtes redirigé vers la page **Authentification du serveur SSH**, où vous pourrez configurer le serveur SSH, puis vous reviendrez vers 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.

  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.

Sélectionnez l'une des **actions d'enregistrement** suivantes :

- **Mettre à niveau** : spécifie que le type de fichier présent sur l'appareil doit être remplacé par sa nouvelle version, laquelle version est située sur un serveur TFTP.
- **Sauvegarder** : spécifie qu'une copie du type de fichier doit être enregistrée dans un fichier situé sur un autre appareil.

Renseignez les champs suivants :

- **Type de fichier** : sélectionnez le type de fichier de destination. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)
- **Définition du serveur SCP** : 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 uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.

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

- **Interface de liaison locale** : sélectionnez dans la liste de liaison locale.
- **Adresse IP/Nom serveur SCP** : saisissez l'adresse IP ou le nom de domaine du serveur SCP.
- **(Pour une mise à niveau) Nom du fichier source** : saisissez le nom du fichier source.
- **(Pour une sauvegarde) Nom du fichier de destination** : saisissez le nom du fichier de sauvegarde.

ÉTAPE 6 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.

Image active

Deux images du micrologiciel sont conservées sur l'appareil. Une des images est identifiée en tant qu'*image active* et l'autre en tant qu'*image inactive*. L'appareil démarre à partir de l'image que vous avez définie en tant qu'*image active*. Vous pouvez changer en *image active* l'image identifiée en tant qu'*image inactive*. Notez que vous pouvez redémarrer l'appareil en utilisant le processus décrit à la section **Interface de gestion**.

Pour sélectionner l'image active :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion de fichiers** > **Image active**.

Cette page affiche les éléments suivants :

- **Image active** : affiche le fichier image actuellement actif sur l'appareil.
- **Numéro de version de l'image active** : affiche la version du micrologiciel de l'image active.

- **Image active après redémarrage** : affiche l'image active après le redémarrage.
- **Numéro de version de l'image active après redémarrage** : affiche la version du micrologiciel de l'image active utilisée après redémarrage.

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

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

Télécharger/sauvegarder configuration/journal

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

- 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.

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

Lorsque vous restaurez un fichier de configuration vers la Configuration de démarrage ou un fichier de configuration de sauvegarde, 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 **Interface de gestion**.

Compatibilité descendante du fichier de configuration

Lors de la restauration des fichiers de configuration depuis un périphérique externe vers l'appareil, les problèmes de compatibilité suivants sont susceptibles de se présenter :

- **Modification du mode du système** : lorsque le fichier de configuration contient un mode système identique à celui actuellement utilisé sur l'appareil où le fichier est téléchargé, cette information n'est pas prise en compte. En cas de modification du mode système, les situations suivantes peuvent se présenter :
  - Lorsque le téléchargement du fichier de configuration sur l'appareil s'effectue à l'aide de la page Télécharger/sauvegarder configuration/journal, cette opération est annulée et un message s'affiche indiquant que le mode système doit être modifié sur la page Paramètres système.
  - Lorsque le téléchargement du fichier de configuration fait partie d'un processus de configuration automatique, le fichier de configuration de démarrage est supprimé et l'appareil redémarre automatiquement en exécutant le nouveau mode système. Lorsqu'un fichier de configuration vide est utilisé pour la configuration de l'appareil, Reportez-vous à la section **Configuration automatique via DHCP**.

Téléchargement ou sauvegarde d'un fichier de configuration ou d'un journal

Pour sauvegarder ou restaurer le fichier de configuration système :

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

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

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

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

Mode d'enregistrement Télécharger : indique que le type de fichier de l'appareil est remplacé par le type de fichier d'un autre appareil. Renseignez les champs suivants :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sélectionnez l'**Enregistrement**.

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

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

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

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

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

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

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

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

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

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

ÉTAPE 5 Si vous avez sélectionné **via SCP (sur SSH)**, reportez-vous à la section **Configuration du client SSH via l'interface utilisateur graphique (GUI)** pour plus d'instructions. 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 le 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 SCP** : 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 uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste de liaison locale.
- **Adresse IP/Nom serveur SCP** : saisissez l'adresse IP ou le nom de domaine du serveur SCP.

Si le **Mode d'enregistrement** est défini sur *Télécharger* (remplacement du fichier de l'appareil par une nouvelle version provenant d'un autre périphérique), renseignez les champs suivants :

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

Si le **Mode d'enregistrement** est défini sur *Sauvegarder* (copie d'un fichier vers un autre périphérique), renseignez les champs suivants (en plus de ceux répertoriés ci-dessus) :

- **Type du fichier source** : sélectionnez le type de fichier de configuration. Seuls les types de fichiers valides s'affichent. (Les types de fichiers sont décrits dans la section **Fichiers et types de fichiers**.)
- **Données confidentielles** : choisissez comment les données sensibles doivent être incluses dans le fichier de sauvegarde. Les options suivantes sont disponibles :
  - *Exclure* : ne pas inclure les données sensibles à la sauvegarde.
  - *Chiffré* : inclure les données sensibles dans la sauvegarde, mais en les cryptant.
  - *Texte en clair* : inclure les données sensibles dans la sauvegarde sous forme de texte en clair.

  REMARQUE : les options disponibles relatives aux données confidentielles sont déterminées par les règles SSD de l'utilisateur actuel. Pour en savoir plus, consultez la page Gestion sécurisée des données confidentielles > Règles SSD.
- **Nom du fichier de destination** : nom du fichier vers lequel vous copiez des données.

ÉTAPE 6 Cliquez sur **Appliquer**. Le fichier est mis à niveau ou sauvegardé.

Propriétés des fichiers de configuration

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

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

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

Cette page affiche les champs suivants :

- **Nom du fichier de configuration** : type de fichier système.
- **Heure de création** : date et heure de modification du fichier.

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

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

Copier/enregistrer la configuration

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. Pour conserver les paramètres de la Configuration d'exécution, celle-ci doit être copiée sur un autre type de configuration ou enregistrée sur un autre appareil.

AVERTISSEMENT 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 la Configuration de secours

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

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

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

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

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

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

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

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

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

Configuration automatique via DHCP

Le processus de configuration automatique DHCP permet de transférer les informations de configuration vers les hôtes d'un réseau TCP/IP. La fonctionnalité de configuration automatique s'appuyant sur ce protocole permet à l'appareil de télécharger des fichiers de configuration provenant d'un serveur TFTP/SCP.

Pour utiliser cette fonction, l'appareil doit être configuré comme client DHCPv4 auquel cas la configuration automatique depuis un serveur DHCPv4 est prise en charge et/ou comme client DHCPv6 auquel cas la configuration automatique depuis un serveur DHCPv6 est prise en charge.

Par défaut, en cas d'activation de la fonctionnalité de configuration automatique via DHCP, l'appareil est activé comme client DHCP.

Le processus de configuration automatique prend également en charge le téléchargement de fichiers de configuration contenant des informations sensibles telles que des clés de serveur RADIUS et 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 à la section **Sécurité : Gestion sécurisée des données confidentielles**.

La configuration automatique via DHCPv4 se déclenche dans les cas suivants :

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

La configuration automatique via DHCPv6 se déclenche dans les cas suivants :

- 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.

Options de serveur DHCP

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

Les informations de secours (adresse/nom du serveur de configuration et nom/chemin du fichier de configuration) peuvent être configurées sur la page de configuration automatique. Ces informations sont utilisées lorsque les messages DHCPv4 ne les contiennent pas (elles ne sont en revanche pas utilisées par DHCPv6).

Protocole de téléchargement de la configuration automatique (TFTP ou SCP)

Le protocole de téléchargement de la configuration automatique peut être configuré 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.

- **TFTP uniquement** : le téléchargement est effectué via TFTP peu importe l'extension de fichier du nom du fichier de configuration.

- **SCP uniquement** : le téléchargement est effectué via SCP (sur SSH) peu importe l'extension de fichier du nom du fichier de configuration.

Paramètres d'authentification du client 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 autoriser uniquement des connexions depuis des serveurs répertoriés dans la liste des serveurs sécurisés.

Les paramètres d'authentification du client SSH sont obligatoires pour que le client (soit 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 Notez que les paramètres d'authentification du client SSH peuvent également être utilisés lors du téléchargement manuel d'un fichier (c.-à-d., téléchargement effectué sans exploiter la fonctionnalité de configuration automatique DHCP).

Processus de configuration automatique

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

- Le serveur DHCP est sollicité pour permettre l'acquisition du nom/de l'adresse du serveur TFTP/SCP ainsi que du nom/du chemin du fichier de configuration (options DHCPv4 : 66,150 et 67, options DHCPv6 : 59 et 60).
- Si le serveur DHCP n'est pas en mesure de fournir ces informations :
  - **Pour DHCPv4 :** C'est le nom du fichier de configuration de secours défini par l'utilisateur qui est utilisé.
  - **Pour DHCPv6 :** Le processus est en revanche interrompu.
- Si le serveur DHCP n'est pas en mesure de fournir ces informations et que le paramètre d'adresse du serveur TFTP/SCP de secours est vide :
  - **Pour DHCPv4 :**

    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 automatique.

- **Pour DHCPv6 :** le processus de configuration automatique est interrompu.

- Si le nom du fichier de configuration a été communiqué par le serveur DHCP (DHCPv4 : option 67, DHCPv6 : option 60), c'est le protocole de copie (SCP/TFTP) qui est alors sélectionné, comme décrit à la section **Protocole de téléchargement de la configuration automatique (TFTP ou 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. Notez que, 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 serveur TFTP/SCP est sollicité et le téléchargement du fichier s'effectue à partir de ce serveur.

  Le téléchargement est réalisé seulement si le nouveau nom de fichier de configuration est différent du nom actuel (même si le fichier de configuration actuel est vide).
- Un message SYSLOG est généré pour confirmer que la configuration automatique a été effectuée avec succès.

Paramétrage de la configuration automatique DHCP

Flux de travail

Pour paramétrer la configuration automatique DHCP :

1. Configurez les serveurs DHCPv4 et/ou DHCPv6 de sorte qu'ils transmettent les informations requises à l'appareil. Cette procédure n'est pas décrite dans le présent guide.
2. Définition des paramètres de configuration automatique.
3. Définissez l'appareil comme client DHCPv4 sur la page **Définition d'une interface IPv4 en mode système Couche 2** ou **Définition d'une interface IPv4 en mode système Couche 3** et/ou définissez l'appareil comme client DHCPv6 sur la page **Interface IPv6**.

Configuration Web

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

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

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

- Un fichier de configuration placé sur le serveur TFTP/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.
- Dans IPv4, pour s'assurer que la configuration des appareils fonctionne comme prévu et en raison de l'allocation d'adresses IP différentes pour chaque cycle de renouvellement DHCP, il est conseillé de lier les adresses IP à des adresses MAC dans la table des serveurs DHCP. Cela permet de garantir que chaque appareil dispose de sa propre adresse IP réservée ainsi que d'autres informations appropriées.

Pour paramétrer la configuration automatique :

ÉTAPE 1 Cliquez sur **Administration** > **Gestion de fichiers** > **Configuration automatique 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 à la configuration automatique d'utiliser 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.
- **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 dans la page Authentification du client SSH.

ÉTAPE 3 Renseignez les informations facultatives suivantes à utiliser si aucun nom de fichier de configuration n'a été fourni par le serveur DHCP.

- **Définition du serveur de secours** : sélectionnez **Par adresse IP** ou **Par nom** pour configurer le serveur.
- **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 uniquement des hôtes sur une liaison de réseau unique. Une adresse de liaison locale possède le préfixe FE80, ne peut pas être routée et ne peut être utilisée pour la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - **Global** : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée)
- **Adresse IP/Nom du serveur de secours** : saisissez l'adresse IP ou le nom du serveur à utiliser si aucune adresse IP de serveur n'a été spécifiée dans le message DHCP.
- **Nom du fichier de configuration de sauvegarde** : saisissez le chemin et le nom du fichier à utiliser si aucun nom de fichier de configuration n'a été spécifié dans le message DHCP.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres sont copiés dans le fichier de Configuration d'exécution.

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 de périphériques**
- **Paramètres système**
- **Paramètres de console (prise en charge du débit de bauds automatiques)**
- **Interface de gestion**
- **Comptes d'utilisateur**
- **Définition du délai d'expiration en cas de session inactive**
- **Paramètres de l'heure**
- **Journal système**
- **Gestion de fichiers**
- **Ressources de routage**
- **Intégrité**
- **Diagnostic**
- **Détection - Bonjour**
- **Détection - LLDP**
- **Détection - CDP**
- **Ping**
- **Traceroute**

Modèles de périphériques

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

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

Lorsque le périphérique fonctionne en mode système Couche 3, les gestionnaires de stratégie de limite du débit VLAN et de QoS ne sont pas opérationnels. Les autres fonctionnalités du Mode avancé de QoS sont quant à elles opérationnelles.

REMARQUE Les conventions de port suivantes sont utilisées :

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

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

Nom du modèle	ID du produit (PID)	Description des ports de l'appareil	Puissance dédiée au PoE	Nbre de ports gérant PoE
SG300-10	SRW2008-K9	8 ports GE et 2 ports combinés spécifiques (GE/SFP)	N/A	N/A
SG300-10MP	SRW2008MP-K9	8 ports GE et 2 ports combinés spécifiques (GE/SFP)	124 W	8
SG300-10P	SRW2008P-K9	8 ports GE et 2 ports combinés spécifiques (GE/SFP)	62 W	8
SG300-20	SRW2016-K9	16 ports GE et 4 ports spécifiques - 2 liaisons montantes et 2 ports combo	N/A	N/A
SG300-28	SRW2024-K9	24 ports GE et 4 ports spécifiques - 2 liaisons montantes et 2 ports combinés	N/A	N/A
SG300-28P	SRW2024P-K9	24 ports GE et 4 ports spécifiques - 2 liaisons montantes et 2 ports combinés	180 W	24
SG300-52	SRW2048-K9	48 ports GE et 4 ports spécifiques - 2 liaisons montantes et 2 ports combinés	N/A	N/A

Nom du modèle	ID du produit (PID)	Description des ports de l'appareil	Puissance dédiée au PoE	Nbre de ports gérant PoE
SF300-08	SRW208-K9	8 ports FE	N/A	N/A
SF302-08	SRW208G-K9	8 ports FE plus 2 ports GE	N/A	N/A
SF302-08MP	SRW208MP-K9	8 ports FE plus 2 ports GE	124 W	8
SF302-08P	SRW208P-K9	8 ports FE plus 2 ports GE	62 W	8
SG300-10PP	SG300-10PP-K9	Commutateur administrable PoE 10/100 à 8 ports	62 W	8
SG300-10MPP	SG300-10MPP-K9	Commutateur administrable PoE Gigabit à 10 ports	124 W	8
SF300-24	SRW224G4-K9	24 ports FE plus 4 ports GE spécifiques - 2 liaisons montantes et 2 ports combo	N/A	N/A
SF300-24P	SRW224G4P-K9	24 ports FE plus 4 ports GE spécifiques - 2 liaisons montantes et 2 ports combo	180 W	24
SF300-24PP	SF300-24PP-K9	Commutateur administrable PoE 10/100 à 24 ports	180 W	24
SG300-28PP	SG300-28PP-K9	Commutateur administrable PoE Gigabit à 28 ports	180 W	24
SF300-48	SRW248G4-K9	48 ports FE plus 4 ports GE spécifiques - 2 liaisons montantes et 2 ports combo	N/A	N/A
SF300-48P	SRW248G4P-K9	48 ports FE plus 4 ports GE spécifiques - 2 liaisons montantes et 2 ports combo	375 W	48
SF300-48PP	SF300-48PP-K9	Commutateur administrable PoE 10/100 à 48 ports	375 W	48
SG300-52MP	SG300-52MP-K9	Commutateur administrable PoE Gigabit à 52 ports	740 W	48
SG300-10SFP	SG300-10SFP-K9	Commutateur SFP administrable Gigabit à 10 ports	N/A	N/A
SF300-24MP	SF300-24M-K9	Commutateur administrable PoE 10/100 à 24 ports	375 W	24

Nom du modèle	ID du produit (PID)	Description des ports de l'appareil	Puissance dédiée au PoE	Nbre de ports gérant PoE
SG300-28MP	SRW2024P-K9	Commutateur administrable PoE Gigabit à 28 ports	375 W	24
SF302-08PP		Commutateur administrable PoE 10/100 à 8 ports	62 W	8
SF302-08MPP		Commutateur administrable PoE 10/100 à 8 ports	124 W	8
ESW2-350G-52	ESW2-350G-52-K9	Commutateur administrable Gigabit à 52 ports	N/A	N/A
ESW2-350G-52DC	ESW2-350G-52DC-K9	Commutateur administrable Gigabit à 52 ports	N/A	N/A

Paramètres 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.

Affichage du récapitulatif du système

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

La page Récapitulatif du système contient les informations relatives au système et au matériel.

Informations système :

- **Description du système** : affiche une description du système.
- **Emplacement du système** : indique l'emplacement physique du périphérique. Cliquez sur **Modifier** pour accéder à la page Paramètres système, afin d'entrer cette valeur.

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

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

État des services TCP/UDP :

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

Autres informations générales :

- **Description du modèle** : description du modèle de périphérique.
- **Numéro de série** : numéro de série.
- **PID VID** : affiche la référence et l'identifiant de la version.
- **Version du micrologiciel (image active)** : numéro de version du micrologiciel de l'image active.
- **MD5 Checksum du micrologiciel (image active)** : MD5 Checksum de l'image active.

- **Version du micrologiciel (image non active)** : numéro de version du micrologiciel de l'image non active.
- **MD5 Checksum du micrologiciel (non active)** : MD5 Checksum de l'image non active.
- **Version de démarrage** : numéro de version de démarrage.
- **Total de contrôle MD5 de démarrage** : total de contrôle MD5 de la version de démarrage.
- **Paramètres régionaux** : paramètres régionaux de la première langue (il s'agit toujours de l'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.

Informations sur l'alimentation PoE :

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

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** : indiquez l'emplacement physique du périphérique.
- **Contact système** : saisissez le nom d'une 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).
- **Mode système** : sélectionnez le mode système de ce périphérique.

  REMARQUE : si vous changez de mode système après avoir cliqué sur **Appliquer**, le système devra être redémarré et le fichier de configuration de démarrage aura disparu après le démarrage.
  - *L2* : sélectionnez cette option pour passer en mode système Couche 2.
  - *L3* : sélectionnez cette option pour passer en mode système Couche 3.
- **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).

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

Paramètres de console (prise en charge du débit de 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.

En activant la détection automatique, le périphérique détecte automatiquement le débit de votre console pour vous éviter de le définir explicitement.

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 de 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 :

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

Interface de gestion

Reportez-vous à la section **IPv4 Management and Interfaces (Interfaces et gestion IPv4)**.

Comptes d'utilisateur

Reportez-vous à la section **Définition d'utilisateurs**.

Définition du délai d'expiration en cas de session inactive

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

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

Pour 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 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 de l'heure

Reportez-vous à la section **Administration : Paramètres horaires**.

Journal système

Reportez-vous à la section **Administration : Journal système**.

Gestion de fichiers

Reportez-vous à la section **Administration : Gestion de fichiers**.

Redémarrage du périphérique

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 **Appliquer** n'a pas pour effet d'enregistrer la configuration dans la Configuration de démarrage. Pour plus d'informations sur les fichiers et les types de fichiers, reportez-vous à la section **Fichiers système**.

Vous pouvez sauvegarder la configuration en utilisant *Administration > Gestion de fichiers > Copier/enregistrer la configuration* ou en cliquant sur **Enregistrer** en haut de la fenêtre. Vous pouvez également charger la configuration depuis un périphérique distant. Reportez-vous à la section **Télécharger/sauvegarder configuration/journal**.

Dans certains cas, vous pouvez préférer régler le redémarrage à une heure ultérieure. Cela peut se produire notamment dans l'un des cas suivants :

- Vous effectuez des actions sur un périphérique distant et ces actions peuvent provoquer une perte de connexion à ce périphérique distant. La pré-planification d'un redémarrage restaure la configuration fonctionnant et permet la restauration de la connexion au périphérique distant. Si ces actions sont réussies, le redémarrage retardé peut être annulé.
- 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** > **Redémarrer**.

ÉTAPE 2 Cliquez sur l'un des boutons de **Redémarrage** 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.

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

- **Redémarrer avec les paramètres d'origine** : redémarre le périphérique en utilisant sa configuration d'origine. Ce processus efface le fichier de Configuration de démarrage et le fichier de configuration de sauvegarde.

  Le fichier de configuration miroir n'est pas supprimé lorsque vous restaurez les paramètres d'origine.

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

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

Ressources de routage

Utilisez la page Ressources du routeur pour afficher l'allocation TCAM et modifier la taille totale TCAM. Les entrées TCAM sont divisées en groupes, spécifiés ci-dessous :

- **Entrées IP** : entrées TCAM réservées pour les acheminements statiques IP, les adresses IP sur le périphérique et les hôtes IP. Chaque type génère le nombre d'entrées TCAM suivant :
  - Acheminements statiques IPv4 : une seule entrée par acheminement.
  - Adresses IP : deux entrées par adresse IP
  - Hôtes IP : une entrée par hôte.
- **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.

Pour afficher et modifier les ressources du routeur :

ÉTAPE 1 Cliquez sur **Administration** > **Ressources du routeur**.

Les champs suivants sont affichés :

- **Voisins—Nombre** est le nombre de voisins enregistrés sur le périphérique et **Entrées TCAM** est le nombre total d'entrées TCAM utilisées pour les voisins.
- **Interfaces—Nombre** est le nombre d'adresses IP sur les interfaces du périphérique et **Entrées TCAM** est le nombre total d'entrées TCAM utilisées pour les adresses IP.
- **Acheminements—Nombre** est le nombre d'acheminements enregistrés sur le périphérique et **Entrées TCAM** est le nombre total d'entrées TCAM utilisées pour les acheminements.
- **Total** : affiche le nombre d'entrées TCAM actuellement utilisées.

- **Entrées maximales** : sélectionnez l'une des options suivantes :
  - *Valeurs par défaut* : le nombre d'entrées TCAM disponibles pour les entrées IP est de 25 % de la taille TCAM.
  - *Défini par l'utilisateur* : saisissez une valeur.

Vous devez enregistrer votre configuration actuelle avant de modifier les paramètres d'allocation TCAM.

REMARQUE : un récapitulatif des entrées TCAM réellement en utilisation et disponibles est affiché au bas de cette page. Pour une explication de ces champs, reportez-vous à **Affichage du taux d'utilisation TCAM**.

ÉTAPE 2 Enregistrez les nouveaux paramètres en cliquant sur **Appliquer**. Le système vérifie si l'allocation TCAM est possible. Si l'opération est incorrecte, un message d'erreur s'affiche. Si l'opération est correcte, l'allocation est enregistrée dans le fichier de Configuration d'exécution et un redémarrage est effectué.

Intégrité

La page Intégrité affiche l'état du ventilateur sur tous les périphériques équipés de ventilateurs. Selon le modèle, un périphérique possède un ou plusieurs ventilateurs. Certains modèles ne possèdent aucun ventilateur.

Pour les périphériques équipés d'un capteur de température, dans le but d'établir leur protection matérielle, les actions suivantes sont conduites par ces périphériques en cas de surchauffe et pendant la période de refroidissement qui accompagne la surchauffe :

Événement	Action
Au moins un capteur de température dépasse le seuil d'avertissement	Les actions suivantes sont générées : ▪ Message SYSLOG ▪ Message « trap » SNMP

Événement	Action
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.
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.

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

La rubrique Intégrité affiche les champs suivants :

- **État du ventilateur** : état du ventilateur. Les valeurs suivantes sont possibles :
  - OK : le ventilateur fonctionne normalement.
  - Échec : le ventilateur ne fonctionne pas correctement.
  - S/O : l'ID du ventilateur n'est pas applicable au modèle en question.
- **Direction du ventilateur** : (sur les périphériques concernés) la direction du fonctionnement des ventilateurs est (par exemple : de l'avant vers l'arrière).

Diagnostic

Reportez-vous à la section **Administration : Diagnostic**.

Détection - Bonjour

Reportez-vous à la section **Bonjour**.

Détection - LLDP

Reportez-vous à la section **Configuration de LLDP**.

Détection - CDP

Reportez-vous à la section **Configuration de CDP**.

Ping

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

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

Pour envoyer une requête Ping à un hôte :

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

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.
- **Type d'adresse IPv6 de destination** : sélectionnez Liaison locale ou Global comme type d'adresse IPv6 à saisir en tant qu'adresse IP de destination.
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, 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 autre message est ajouté à la liste des messages, indiquant le résultat de l'opération Ping.

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

Traceroute

Traceroute détecte les routes IP et indique également les paquets qui ont été transférés 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.

  REMARQUE : Si l'option Auto est sélectionnée, le système génère l'adresse source en fonction de l'adresse de destination.

- **Type d'adresse IPv6 de destination** : sélectionnez Liaison locale ou Global comme type d'adresse IPv6 à saisir.
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, sélectionnez son lieu de réception.
- **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 que cette valeur est atteinte. Pour utiliser la valeur par défaut (30), sélectionnez **Valeurs par défaut**.
- **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** *(1-3)* : affiche la durée de l'aller-retour en ms pour la trame 1/3 et l'état de l'opération 1/3.

6

Administration : Paramètres horaires

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

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

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

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

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

Options d'heure système

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

Dans le cadre du processus de démarrage, le 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 (Heure)

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

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

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

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

  Cette méthode de réglage de l'heure fonctionne avec les connexions HTTP et HTTPS.
- **SNTP** : l'heure peut être reçue à partir de serveurs de temps SNTP. SNTP garantit une synchronisation 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).

Configuration de l'heure système

Sélection de la source d'heure système

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

AVERTISSEMENT 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 sont affichés :

- **Heure actuelle (statique)** : 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 a été extraite pour la dernière fois.

ÉTAPE 2 Saisissez les paramètres suivants :

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

- **Source d'horloge principale (serveurs SNTP)** : si vous activez cette option, l'heure système est obtenue à partir d'un serveur SNTP. Pour utiliser cette fonctionnalité, vous devez également configurer une connexion à un serveur SNTP sur la page Paramètres d'interface SNTP. Vous pouvez

également appliquer l'authentification des sessions SNTP via la page Authentification SNTP.

- **Source d'horloge alternative (ordinateur via des sessions HTTP/HTTPS actives)** : sélectionnez cette option pour définir la date et l'heure depuis l'ordinateur effectuant la configuration via le protocole HTTP.

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

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

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

Paramètres de fuseau horaire : l'heure locale est utilisée via 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, *vous devez également activer le client DHCP 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 de fuseau horaire** : saisissez un nom défini par l'utilisateur représentatif du fuseau horaire que vous avez configuré. L'acronyme s'affiche dans le champ **Heure actuelle**.

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

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

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

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

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

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

Ajout d'un serveur de monodiffusion SNTP

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, activez la case à cocher **Client SNTP monodiffusion**.

Pour ajouter un serveur de monodiffusion SNTP :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres d'heure** > **Monodiffusion SNTP**.

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* : le serveur SNTP est actuellement recherché par le périphérique.
  - *En cours* : se produit lorsque le serveur SNTP n'a pas entièrement approuvé son propre serveur de temps (c'est-à-dire lors du premier démarrage du serveur SNTP).
- **Dernière réponse** : date et heure de la dernière réponse reçue de la part de ce serveur SNTP.
- **Décalage** : décalage estimé entre l'horloge du serveur et l'horloge locale, en millisecondes. L'hôte détermine la valeur de ce décalage à l'aide de l'algorithme décrit au sein de la RFC 2030.
- **Écart** : temps estimé d'un aller-retour de transmission entre l'horloge du serveur et l'horloge locale sur le chemin du réseau, en millisecondes. L'hôte détermine la valeur de cet écart à l'aide de l'algorithme décrit au sein de la RFC 2030.
- **Source** : configuration du serveur SNTP, par exemple : manuelle 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.**

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 :

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

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

- **Interface de liaison locale** : sélectionnez dans la liste l'interface de liaison locale (si la liaison locale du type d'adresse IPv6 est sélectionnée)

- **Adresse IP du serveur SNTP** : saisissez l'adresse IP du serveur SNTP. Le format dépend du type d'adresse sélectionné.

- **Serveur SNTP** : sélectionnez le nom du serveur SNTP à partir d'une liste de serveurs NTP connus. Si **autre** est choisi, saisissez le nom du serveur SNTP dans le champ adjacent.

- **Intervalle d'interrogation** : sélectionnez cette option afin d'activer l'interrogation du serveur SNTP pour les informations d'heure système. Tous les serveurs NTP enregistrés pour l'interrogation sont interrogés et l'horloge est sélectionnée à partir du serveur accessible qui dispose du niveau de strate le plus faible (distance par rapport à l'horloge de référence). Le serveur disposant de la strate la plus faible est considéré comme étant le serveur principal. Le serveur disposant de la strate la deuxième plus faible est un serveur secondaire et ainsi de suite. Si le serveur principal est inactif, le 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 (Vous pouvez créer des clés d'authentification sur la page Authentification SNTP.)

ÉTAPE 6 Cliquez sur **Appliquer**. Le serveur SNTP est ajouté et vous retournez à la page principale.

Configuration du mode SNTP

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 multidiffusion/ pluridiffusion**.

ÉTAPE 2 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 3 Si le système est en mode système Couche 3, cliquez sur **Ajouter** pour sélectionner l'interface de réception et de transmission SNTP.

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

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

Définition de l'authentification SNTP

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

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

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

Flux de travail

ÉTAPE 1 Activez l'authentification sur la page Authentification SNTP.

ÉTAPE 2 Créez une clé sur la page Authentification SNTP.

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 le périphérique à jour.

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** : saisissez la clé utilisée pour l'authentification (huit caractères maximum). 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.

Période

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 802.1X
- État des ports
- PoE basé sur le temps

Les deux types de périodes 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, le processus qui lui est associé n'est activé que si l'heure de début absolue et la période récurrente ont été atteintes. Le processus est désactivé une fois l'une des périodes atteintes.

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 **Chapitre 9, « Configuration des ports »** et **Chapitre 9, « Configuration des paramètres des LAG »**).
- 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 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.

7

Administration : Diagnostic

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

Elle couvre les rubriques suivantes :

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

Test des ports cuivre

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

VCT réalise deux types de tests :

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

Conditions préalables à l'exécution du test des ports cuivre

Avant d'exécuter le test, procédez comme suit :

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

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

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

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

Pour tester les câbles en cuivre reliés aux ports :

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

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

ÉTAPE 3 Cliquez sur **Test cuivre**.

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

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

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

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

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

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

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

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

Affichage de l'état des modules optiques

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

SFP compatibles MSA

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

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

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

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

Pour afficher les résultats des tests optiques, cliquez sur **Administration** > **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.
- **Intensité** : consommation de courant du SFP.
- **Puissance de sortie** : puissance optique transmise.
- **Puissance d'entrée** : puissance optique reçue.
- **Défaillance du transmetteur** : le SFP distant indique une perte de signal. Les valeurs sont Vrai, Faux et A/S (Aucun signal).
- **Perte de signal** : le SFP local indique une perte de signal. Les valeurs sont Vrai et Faux.
- **Données prêtes** : le SFP est opérationnel. Les valeurs sont Vrai et Faux.

Configuration de la mise en miroir des ports et de VLAN

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

Huit sources maximum peuvent être mises en miroir.

Un paquet reçu sur un port réseau affecté à un VLAN soumis à une mise en miroir est mis en miroir sur le port de l'analyseur même si le paquet a été intercepté ou abandonné. Les paquets envoyés par 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 n'est pas active sur un VLAN qui n'a pas été créé manuellement. Par exemple, le VLAN 23 a été créé par GVRP et vous avez créé manuellement le VLAN 34. Vous créez ensuite la mise en miroir des ports qui intègre le VLAN 23 et/ou le VLAN 34, et vous supprimez par la suite le VLAN 34. L'état de la mise en miroir des ports est alors défini sur **Pas prêt**, car le VLAN 34 ne se trouve plus dans la base de données et le VLAN 23 n'a pas été créé manuellement.

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

Pour activer la mise en miroir :

ÉTAPE 1 Cliquez sur **Administration** > **Diagnostics** > **Mise en miroir des ports et VLAN**.

Les champs suivants sont affichés :

- **Port de destination** : port sur lequel le trafic doit être copié ; port de l'analyseur.

- **Interface source** : interface, port ou VLAN à partir duquel le trafic est envoyé au port de l'analyseur.
- **Type** : type de surveillance ; entrant sur le port (réception), sortant du port (émission) ou les deux.
- **État** : affiche l'une des valeurs suivantes :
  - *Actif* : les interfaces source et de destination sont actives et transfèrent le trafic.
  - *Pas prêt* : la source ou la destination est inactive (ou les deux) et ne transfère pas le trafic pour une raison quelconque.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un port ou un VLAN à mettre en miroir.

ÉTAPE 3 Configurez les paramètres suivants :

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

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

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

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

L'appareil gère les types de trafic suivants en plus du trafic de l'utilisateur final :

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

Un trafic excessif encombre le CPU et peut empêcher 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 l'appareil et ne peut pas être désactivée.

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

Pour afficher l'utilisation du CPU :

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

La page Utilisation du CPU s'affiche.

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

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

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

8

Administration : Détection

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

Elle couvre les rubriques suivantes :

- **Bonjour**
- **LLDP et CDP**
- **Configuration de LLDP**
- **Configuration de 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 Sécurité > Services TCP/UDP pour activer ou désactiver les services de périphérique.) Le périphérique peut être détecté par un système de gestion réseau ou autre application tierce. Par défaut, Bonjour est activé sur le VLAN de gestion. La console Bonjour détecte automatiquement le périphérique et l'affiche.

Bonjour en mode système Layer 2

Lorsque le périphérique fonctionne en mode système Couche 2, la détection Bonjour est activée au niveau global ; vous ne pouvez pas l'activer séparément pour chaque port ou chaque VLAN. Le périphérique annonce tous les services qui ont été activés par l'administrateur en fonction de la configuration définie sur la page Services.

Lorsque vous activez à la fois la découverte Bonjour et IGMP, l'adresse IP de multidiffusion de Bonjour apparaît sur la page Ajouter une adresse IP de groupe de multidiffusion.

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

Pour activer Bonjour globalement lorsque le système est en mode système Couche 2 :

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

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

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

Bonjour en mode système Couche 3

En mode système Layer 3, chaque interface (VLAN, port ou LAG) peut recevoir une adresse IP. Lorsque vous activez Bonjour, le périphérique peut envoyer des paquets de détection Bonjour vers toutes les interfaces dotées d'une adresse IP. La détection Bonjour peut être affectée individuellement pour chaque port et/ou chaque VLAN. Lorsque vous activez Bonjour, le périphérique peut envoyer 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. (Lorsque le périphérique est en mode système Layer 3, accédez à **Configuration IP** > **Interfaces de gestion et IP** > **Interface IPv4** pour configurer une adresse IP sur une interface.)

Si une interface (un VLAN, par exemple) est supprimée, des paquets Goodbye sont envoyés pour désenregistrer les services annoncés par le périphérique auprès de la table de cache de voisinage sur le réseau local. La table de contrôle des interfaces de détection Bonjour montre les interfaces dont les adresses IP sont associées à la fonction Bonjour. Toute notification Bonjour ne peut être diffusée que vers les interfaces qui sont mentionnées dans cette table. (Reportez-vous à la table de contrôle des interfaces de détection Bonjour sur la page Administration > Détection - Bonjour. Si les services disponibles changent, ces modifications sont annoncées, ce qui désenregistre les services désactivés et enregistre les services activés. Si vous modifiez une adresse IP, cette modification est annoncée.

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

Pour configurer Bonjour lorsque le périphérique fonctionne en mode système Layer 3 :

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

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

ÉTAPE 3 Cliquez sur **Appliquer** pour mettre à jour le fichier de Configuration d'exécution.

ÉTAPE 4 Pour activer Bonjour sur une interface, cliquez sur **Ajouter**.

ÉTAPE 5 Sélectionnez l'interface et cliquez sur **Appliquer**.

REMARQUE Cliquez sur **Supprimer** pour désactiver Bonjour sur une interface (le système effectue alors l'opération de suppression sans réaliser d'autres opérations, telles que 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 mutuellement leurs fonctionnalités. Par défaut, le périphérique envoie périodiquement une annonce LLDP/CDP à toutes ses interfaces, puis s'arrête et 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/désactivé globalement, ou activé/désactivé pour chaque port. La fonctionnalité CDP/LLDP d'un port ne s'applique que si CDP/LLDP est globalement activé.
- Si CDP/LLDP est globalement activé, le 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/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 aux sections VLAN voix et VLAN voix automatique.

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

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

Si le contrôle d'accès au port 802.1x est activé sur une interface, le 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, il est considéré comme étant inactif conformément à CDP/LLDP.

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

Configuration de LLDP

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

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

Présentation de LLDP

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

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

LLDP est un protocole de couche de liaison. Par défaut, le 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 de LLDP sont accessibles sous le menu **Administration > Détection - LLDP**.

1. Saisissez les paramètres globaux LLDP, tels que l'intervalle de temps pour l'envoi des mises à jour LLDP, via la page Propriétés LLDP.
2. Configurez LLDP pour chaque port à l'aide de la page Paramètres des ports. Sur cette page, 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 Port intelligent automatique doit détecter les fonctionnalités des périphériques LLDP, activez LLDP sur la page Propriétés des ports intelligents.
6. Affichez les informations de surcharge à l'aide de la page Surcharge LLDP.

Configuration des propriétés LLDP

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

Pour saisir des propriétés LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Propriétés**.

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 si le multiplicateur de conservation est 4, les paquets LLDP seront éliminés après 120 secondes.
- **Délai de réinitialisation** : saisissez l'intervalle en secondes qui sépare la désactivation et la réactivation de LLDP, suite à un cycle d'activation ou de désactivation de LLDP.
- **Délai de transmission** : saisissez le délai en secondes qui séparera deux transmissions de trames LLDP successives en cas de modification dans la MIB de systèmes locaux LLDP.
- **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 **Nombre de répétitions pour le démarrage rapide**, saisissez le nombre d'envois de paquets LLDP lors de l'initialisation du mécanisme de démarrage rapide LLDP MED. Cela se produit lorsqu'un nouveau périphérique d'extrémité établit une liaison au 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.

Modification des paramètres de port LLDP

La page Paramètres des ports 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 des paramètres de port LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Paramètres des ports**.

Cette page affiche les informations LLDP des ports.

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

Cette page contient les champs suivants :

- **Interface** : sélectionnez le port à modifier.
- **État administratif** : sélectionnez l'option de publication LLDP pour le port. Les valeurs disponibles sont les suivantes :
  - *Émission uniquement* : publication uniquement, pas de détection.
  - *Réception uniquement* : détection uniquement, pas de publication.
  - *Émission et réception* : publication et détection.
  - *Désactiver* : indique que LLDP est désactivé sur le port.
- **Notification 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 Intervalle de notification SNMP de changement de topologie de la page Propriétés LLDP. Définissez les destinataires des notifications SNMP en utilisant la page SNMP > Destinataires de notifications v1,2 et/ou SNMP > Destinataires de notifications v3.
- **TLV facultatives disponibles** : sélectionnez les informations que le périphérique doit publier en déplaçant la TLV voulue vers la liste **TLV facultatives sélectionnées**. Les TLV disponibles contiennent les informations suivantes :
  - *Description du port* : informations sur le port, notamment son fabricant, son nom de produit et la version du matériel/logiciel.
  - *Nom du système* : nom attribué au système, au format alphanumérique. Cette valeur est identique à l'objet sysName.
  - *Description du système* : description de l'entité réseau, au format alphanumérique. Inclut le nom du système et la version du matériel, le système d'exploitation et les logiciels réseau pris en charge par le 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.
- *MAC-PHY 802.3* : fonction duplex et débit, avec les paramètres duplex et de débit actuels du périphérique d'envoi. Indique également si les paramètres actuels sont obtenus par négociation automatique ou configuration manuelle.
- *Agrégation de liaisons 802.3* : indique s'il est possible d'agréger la liaison (associée au port sur lequel la PDU LLDP est transmise). Indique également si la liaison est actuellement agrégée et, dans ce cas, précise l'ID du port agrégé.
- *Taille de trame maximale 802.3* : capacité de taille maximale de trame de l'implémentation MAC/PHY.

Les champs suivants concernent l'adresse de gestion :

- **Mode d'annonce** : sélectionnez l'une des méthodes suivantes pour l'annonce de l'adresse IP de gestion au périphérique :
  - *Annonce automatique* : spécifie que le logiciel choisit automatiquement une adresse de gestion à annoncer parmi toutes les adresses IP du produit. En cas d'adresses IP multiples, le logiciel choisit l'adresse IP la plus basse parmi les adresses IP dynamiques. S'il n'y a pas d'adresses dynamiques, le logiciel choisit l'adresse IP la plus basse parmi les adresses IP statiques.
  - *Aucune* : aucune annonce de l'adresse IP de gestion.
  - *Annonce manuelle* : sélectionnez cette option et l'adresse IP de gestion à annoncer. Il est recommandé de choisir cette option lorsque le périphérique fonctionne en mode système Couche 3 et qu'il est configuré avec plusieurs adresses IP (toujours vrai avec les périphériques SG500X/ESW2-550X).
- **Adresse IP** : si vous avez sélectionné Annonce manuelle, sélectionnez l'adresse de gestion voulue dans la liste d'adresses IP fournie.

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

Stratégie réseau LLDP MED

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

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

Configuration d'une stratégie réseau LLDP MED

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

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

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

En outre, l'administrateur peut demander au 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 :

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

Configuration des paramètres des ports LLDP MED

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

REMARQUE Si la stratégie réseau LLDP-MED pour l'application vocale (page Stratégie réseau LLDP MED) est Automatique et que le VLAN voix automatique fonctionne, le 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 contient les paramètres LLDP MED, y compris les TLV activées, pour tous les ports.

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

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

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 disponibles** : sélectionnez les TLV que le périphérique peut publier en les déplaçant vers la liste *TLV facultatives sélectionnées*.
- **Règles de réseau disponibles** : sélectionnez les règles LLDP MED que LLDP va publier en les déplaçant dans la liste Règles de réseau sélectionnées. Elles ont été créées sur la page Stratégie réseau LLDP MED.

Pour inclure une ou plusieurs stratégies réseau définies par l'utilisateur dans l'annonce, vous devez aussi sélectionner *Stratégie réseau* dans les TLV facultatives disponibles.

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

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

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

Affichage de l'état des ports LLDP

La page Table d'état des ports LLDP 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**.

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

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

Informations globales d'état des ports LLDP

- **Sous-type de l'ID du châssis** : type d'ID de châssis (adresse MAC, par exemple).
- **ID du châssis** : identificateur du châssis. Si vous avez choisi l'adresse MAC comme sous-type d'ID de châssis, l'adresse MAC du périphérique s'affiche.
- **Nom du système** : nom du périphérique.

- **Description du système** : description du périphérique, au format alphanumérique.
- **Fonctionnalités système prises en charge** : fonctions principales du périphérique, comme Pont, Point d'accès WLAN ou Routeur.
- **Fonctionnalités système activées** : fonctions principales activées sur le périphérique.
- **Sous-type de l'ID du port** : type d'ID de port affiché.

Table d'état des ports LLDP

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

Affichage des informations LLDP locales

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

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Informations locales LLDP**.

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

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

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

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

Cette page affiche les champs suivants :

Globale

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

Adresse de gestion

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

- **Sous-type de l'adresse** : type de l'adresse IP de gestion affichée dans le champ Adresse de gestion. Par exemple, IPv4.
- **Adresse** : adresse renvoyée qui convient le mieux pour l'utilisation de la gestion, généralement, une adresse Couche 3
- **Sous-type de l'interface** : méthode de numérotation servant à définir le numéro de l'interface.
- **Numéro de l'interface** : interface spécifique associée à cette adresse de gestion.

Détails MAC/PHY

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

Détails 802.3

- **Taille de trame maximale 802.3** : taille maximale de trame IEEE 802.3 possible.

Agrégation de liaisons 802.3

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

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

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

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

Détails MED

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

Informations sur l'emplacement

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

Table des stratégies réseau

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

Affichage des informations LLDP des voisins

La page Informations de voisinage LLDP 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 sur le voisin**.

Cette page comporte les champs suivants :

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

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

ÉTAPE 2 Sélectionnez un port local puis cliquez sur **Détails**.

La page Informations 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** : identificateur du châssis du périphérique de voisinage réseau (LAN) 802.
- **Sous-type de l'ID du port** : type d'ID de port affiché.
- **ID du port** : identificateur du port.
- **Description du port** : informations sur le port, notamment son fabricant, son nom de produit et la version du matériel/logiciel.
- **Nom du système** : nom du système publié.
- **Description du système** : description de l'entité réseau, au format alphanumérique. Inclut le nom du système et la version du matériel, le système d'exploitation et les logiciels réseau pris en charge par le périphérique. Cette valeur est identique à l'objet sysDescr.
- **Fonctionnalités système prises en charge** : fonctions principales du périphérique. Les fonctionnalités sont indiquées par deux octets. Les bits 0 à 7 indiquent respectivement Autres, Répéteur, Pont, Point d'accès WLAN, Routeur, Téléphone, Système de câble DOCSIS et Station. Les bits 8 à 15 sont réservés.

- **Fonctionnalités système activées** : fonctions principales activées sur le périphérique.

Table des adresses de gestion

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

Détails MAC/PHY

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

Alimentation 802.3 via MDI

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

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

Détails 802.3

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

Agrégation de liaisons 802.3

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

802.3 Energy Efficient Ethernet (EEE)

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

Détails MED

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

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

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

VLAN et protocole 802.1

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

Table PPVID

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

ID VLAN

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

ID de protocole

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

Informations sur l'emplacement

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

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

Stratégies réseau

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

Accès aux statistiques LLDP

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

Pour afficher les statistiques LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Statistiques LLDP**.

Pour chaque port, les champs suivants sont affichés :

- **Interface** : identificateur d'interface.
- **Total de trames émises** : nombre des trames transmises.

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

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

Surcharge LLDP

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

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

Pour afficher les informations de surcharge LLDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - LLDP** > **Surcharge LLDP**.

Cette page contient les champs suivants, pour chaque port :

- **Interface** : identificateur de port.
- **Total (octets)** : nombre total d'octets d'informations LLDP dans chaque paquet.
- **Restant à envoyer (octets)** : nombre total d'octets disponibles restants pour des informations LLDP supplémentaires dans chaque paquet.
- **État** : indique si des TLV sont en cours de transmission ou si une surcharge est intervenue.

ÉTAPE 2 Pour afficher les détails de surcharge d'un port, sélectionnez-le et cliquez sur **Détails**.

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

- **TLV LLDP obligatoires**
  - *Taille (octets)* : taille totale des TLV obligatoires, en octets.
  - *État* : indique si un groupe de TLV obligatoires est en cours de transmission ou si une surcharge est intervenue.
- **Fonctionnalités LLDP MED**
  - *Taille (octets)* : taille totale des paquets de fonctionnalités LLDP MED, en octets.
  - *État* : indique si les paquets de fonctionnalités LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **Emplacement LLDP MED**
  - *Taille (octets)* : taille totale des paquets d'emplacement LLDP MED, en octets.
  - *État* : indique si les paquets d'emplacement LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **Stratégie réseau LLDP MED**
  - *Taille (octets)* : taille totale des paquets de stratégie réseau LLDP MED, en octets.
  - *État* : indique si les paquets de stratégie réseau LLDP MED ont été envoyés ou si une surcharge est intervenue.
- **Alimentation LLDP MED étendue via MDI**
  - *Taille (octets)* : taille totale des paquets d'alimentation LLDP MED étendue via MDI, en octets.
  - *État* : indique si les paquets d'alimentation LLDP MED étendue via MDI ont été envoyés ou si une surcharge est intervenue.
- **TLV 802.3**
  - *Taille (octets)* : taille totale des paquets de TLV 802.3 LLDP MED, en octets.

- *État* : indique si les paquets de TLV 802.3 LLDP MED ont été envoyés ou si une surcharge est intervenue.

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

Configuration de CDP

Cette section explique comment configurer CDP.

Elle couvre les rubriques suivantes :

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

Définition des propriétés CDP

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

Flux de travail de configuration de CDP

Vous trouverez ci-après un exemple de flux de travail 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.

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

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

Pour saisir les paramètres généraux CDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - CDP** > **Propriétés**.

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.
- **Version CDP** : sélectionnez la version du protocole CDP à utiliser.
- **Délai d'attente CDP** : durée de conservation des paquets CDP avant leur élimination, en multiples de l'intervalle d'annonce TLV. Par exemple, si l'intervalle d'annonce TLV est de 30 secondes et si le multiplicateur de conservation est 4, les paquets LLDP seront éliminés après 120 secondes. 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 l'élément annoncé par le périphérique local.
- **Non-concordance VLAN natif Syslog** : cochez cette option pour envoyer un message SYSLOG lorsqu'une non-concordance VLAN natif est détectée. Cela signifie que les informations de VLAN natif dans la trame entrante ne correspondent pas à l'élément annoncé par le périphérique local.
- **Non-concordance duplex Syslog** : cochez cette option pour envoyer un message SYSLOG lorsque les informations duplex ne correspondent pas. Cela signifie que les informations duplex dans la trame entrante ne correspondent pas à l'élément annoncé par le périphérique local.

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

Modification des paramètres d'interface CDP

La page Paramètres d'interface permet aux administrateurs d'activer/désactiver CDP sur chaque port. Les notifications peuvent aussi être déclenchées lors de l'apparition de conflits avec des voisins CDP. Le conflit peut être Données VLAN voix, 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 d'interface LLDP MED.

Pour définir les paramètres d'interface CDP :

ÉTAPE 1 Cliquez sur **Administration** > **Détection - CDP** > **Paramètres d'interface**.

Cette page contient les informations CDP suivantes pour chaque interface.

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

Quatre boutons sont disponibles en bas de la page :

- **Copier les paramètres** : sélectionnez ce bouton pour copier une configuration d'un port vers un autre.
- **Modifier** : les différents champs sont décrits à l'étape 2 ci-dessous.
- **Détails des informations locales CDP** : ouvre la page Administration > Détection - CDP > Informations locales CDP.
- **Détails des informations de voisinage CDP** : ouvre la page Administration > Détection - CDP > Informations de voisinage CDP.

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

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

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

Affichage des informations locales CDP

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

ÉTAPE 1 Cliquez sur **Administration** > **Détection - CDP** > **Informations locales CDP**.

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

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

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

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

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

L'interface passe à l'état Désactivé.

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

Affichage des 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**.

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

ÉTAPE 2 Sélectionnez un périphérique, puis cliquez sur **Détails**.

Cette page contient les champs suivants relatifs au voisin :

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

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

Affichage des statistiques CDP

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

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

Pour afficher les statistiques CDP :

ÉTAPE 1 Cliquez sur **Administration> Détection - CDP > Statistiques CDP**.

Les champs suivants sont affichés pour chaque interface :

Paquets reçus/transmis :

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

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

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

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

9

Gestion des ports

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

Elle couvre les rubriques suivantes :

- **Configuration des ports**
- **Définition de la configuration des ports**
- **Agrégation de liaisons**
- **UDLD**
- **Configuration de Green Ethernet**

Configuration des ports

Pour configurer des ports, procédez comme suit :

1. Configurez le port sur la page Paramètres des ports.
2. Activez/désactivez le protocole LACP (Link Aggregation Control Protocol), puis configurez les ports membres potentiels sur les LAG souhaités via la page Gestion des LAG. Par défaut, tous les LAG sont vides.
3. Configurez les paramètres Ethernet, comme le débit et la négociation automatique pour les LAG, via la page Paramètres des LAG.
4. Configurez les paramètres LACP des ports membres d'un LAG ou candidats à l'adhésion à un LAG dynamique, via la page LACP.
5. Configurez Green Ethernet et 802.3 Energy Efficient Ethernet par l'intermédiaire de la page Propriétés.
6. Configurez le mode d'économie d'énergie Green Ethernet et 802.3 Energy Efficient Ethernet pour chaque port, via la page Paramètres des ports.

7. Si la PoE (Power on Ethernet, alimentation sur Ethernet) est prise en charge pour le périphérique concerné, configurez ce dernier en suivant les instructions de la rubrique **Gestion des ports : fonctionnalité PoE**.

Définition de la configuration des ports

Les ports peuvent être configurés dans les pages suivantes.

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**.

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

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

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

ÉTAPE 4 Pour mettre à jour les paramètres des ports, sélectionnez le port voulu et cliquez sur **Modifier**.

ÉTAPE 5 Modifiez les paramètres suivants :

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

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

  REMARQUE : la fibre SFP est prioritaire dans les ports mixtes lorsque les deux ports sont utilisés.
- **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.
- **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. Si vous n'avez pas encore défini de période, cliquez sur **Modifier** ou accédez à la page Période.
- **Nom de période** : sélectionnez le profil qui spécifie la période.
- **État de période opérationnelle** : indique si la période est actuellement active ou inactive.
- **Réactiver le port suspendu** : sélectionnez cette option pour réactiver un port précédemment suspendu. Vous pouvez suspendre un port de diverses manières, notamment via l'option de sécurité de verrouillage des ports, de violation d'hôte unique dot1x, de détection de bouclage, de garde de bouclage STP ou des configurations d'ACL (Access Control List, liste de contrôle d'accès). L'opération de réactivation permet de réactiver le port sans tenir compte du motif de suspension du port.

- **Négociation automatique** : sélectionnez cette option pour activer la négociation automatique sur le port. La négociation automatique permet à un port d'annoncer sa vitesse de transmission, son mode duplex et ses fonctions de contrôle de flux à son partenaire de liaison.
- **Négociation automatique opérationnelle** : affiche l'état actuel de la négociation automatique sur le port.
- **Débit de port administratif** : configurez la vitesse du port. Le type de port détermine les vitesses disponibles. Vous ne pouvez choisir *Vitesse administrative* que si la négociation automatique est désactivée pour le port.
- **Débit de port opérationnel** : affiche le débit actuel du port, obtenu par négociation.
- **Mode duplex administratif** : sélectionnez le mode duplex du port. Ce champ ne peut être configuré que lorsque la négociation automatique est désactivée et que le débit du port est réglé sur 10M ou 100M. Lorsque le port a un débit de 1G, le mode est toujours Duplex intégral. Les options disponibles sont les suivantes :
  - *Duplex intégral* : l'interface prend en charge la transmission entre le périphérique et le client dans les deux directions simultanément.
  - *Semi-duplex* : l'interface prend en charge la transmission entre le périphérique et le client dans une seule direction à la fois.
- **Mode duplex opérationnel** : affiche le mode duplex actuel des ports.
- **Annonce automatique** : sélectionnez les fonctionnalités annoncées par la négociation automatique lorsqu'elle est activée. Les options sont les suivantes :
  - *Capacité maximale* : tous les débits de port et paramètres de mode duplex sont acceptés.
  - *10 Semi-duplex* : débit de 10 Mbits/s et mode Semi-duplex.
  - *10 Duplex intégral* : débit de 10 Mbits/s et mode Duplex intégral.
  - *100 Semi-duplex* : débit de 100 Mbits/s et mode Semi-duplex.
  - *100 Duplex intégral* : débit de 100 Mbits/s et mode Duplex intégral.
  - *1 000 Duplex intégral* : débit de 1 000 Mbits/s et mode Duplex intégral.

- **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*.
- **Annonce de voisin** : affiche les fonctionnalités publiées par le périphérique de voisinage réseau (partenaire de liaison).
- **Contre-pression** : sélectionnez le mode de contre-pression du port (utilisé en mode Semi-duplex) à appliquer pour ralentir la vitesse de réception des paquets en cas de surcharge du périphérique. Cela désactive le port distant, ce qui l'empêche d'envoyer des paquets en engorgeant le signal.
- **Contrôle de flux** : activez ou désactivez le contrôle de flux 802.3x ou activez la négociation automatique du contrôle de flux sur le port (uniquement en mode Duplex intégral).
- **MDI/MDIX** : état MDI (*Media Dependent Interface*, interface dépendant du support)/MDIX (*Media Dependent Interface with Crossover*, interface dépendant du support avec croisement) sur le port.

  Les options sont les suivantes :

  - *MDIX* : sélectionnez cette option pour permuter les paires d'émission et de réception.
  - *MDI* : sélectionnez cette option pour relier ce 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 ne peuvent être transférés que vers des ports de sortie non protégés. Les règles de filtrage des ports protégés s'appliquent également aux paquets transférés par logiciel, comme les applications de traçage.

- La protection des ports ne dépend pas de l'appartenance aux VLAN. Les périphériques connectés à des ports protégés ne peuvent pas communiquer entre eux, même s'ils sont membres du même VLAN.
- Les ports et les LAG peuvent être munis ou non d'une protection. Les LAG protégés sont décrits à la section **Configuration des paramètres des LAG**.

▪ **Membre du 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 récupération d'erreur

Cette page permet de réactiver automatiquement un port qui a été arrêté en raison d'une condition d'erreur.

Pour configurer les paramètres de récupération d'erreur :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Paramètres de récupération d'erreur**.

ÉTAPE 2 Renseignez les champs suivants :

▪ **Intervalle de récupération automatique** : sélectionnez cette option pour activer le mécanisme de récupération d'erreur pour l'état err-disable de la sécurité des ports.

▪ **Sécurité des ports** : sélectionnez cette option pour activer le mécanisme de récupération d'erreur pour l'état err-disable de la sécurité des ports.

▪ **Violation d'hôte unique 802.1x** : sélectionnez cette option pour activer le mécanisme de récupération d'erreur pour l'état error-disable de 802.1x.

▪ **Déni de service ACL** : sélectionnez cette option pour activer le mécanisme de récupération d'erreur pour l'état error-disable du déni de service ACL.

▪ **Protection BPDU STP** : sélectionnez cette option pour activer le mécanisme de récupération d'erreur pour l'état error-disable de la protection BPDU STP.

▪ **UDLD** : sélectionnez cette option pour activer le mécanisme de récupération d'erreur pour l'état d'arrêt UDLD.

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 récupération d'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**.

Agrégation de liaisons

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

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

Présentation de l'agrégation de liaisons

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

Deux types de LAG sont pris en charge :

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

- *Dynamique* : un LAG est dynamique si le protocole LACP est activé sur celui-ci. Les ports attribués à un LAG dynamique sont des ports candidats. Le protocole LACP détermine les ports candidats qui sont des ports membres actifs. Les ports candidats non actifs sont des ports *de réserve* prêts à remplacer n'importe quel port membre actif défaillant.

Équilibrage de charge

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

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

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

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

Gestion des LAG

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

Le périphérique prend en charge 32 LAG avec jusqu'à 8 ports par groupe de LAG.

Chaque LAG possède les caractéristiques suivantes :

- Tous les ports d'un LAG doivent disposer du même type de support.
- Pour que vous puissiez ajouter un port au LAG, il ne doit appartenir à aucun autre VLAN que le VLAN par défaut.
- Les ports d'un LAG ne doivent être affectés à aucun autre LAG.
- Il est impossible d'affecter plus de huit ports à un LAG statique. Il est également impossible de définir plus de 16 ports comme candidats à un LAG dynamique.

- Bien que cette fonction puisse être activée sur le *LAG*, vous devez désactiver la négociation automatique sur tous les *ports* d'un LAG.
- Lorsqu'un port est ajouté à un LAG, la configuration du LAG est appliquée au port. Lorsque vous retirez ce port du LAG, il reprend sa configuration d'origine.
- Les divers protocoles, comme Spanning Tree, considèrent tous les ports d'un LAG comme étant un port unique.

Configuration et paramètres par défaut

Les ports ne sont pas membres d'un LAG et ne sont pas candidats à devenir une partie d'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. Attribuez jusqu'à 16 ports candidats au LAG dynamique. Pour ce faire, sélectionnez les ports et déplacez-les de la **Liste des ports** vers la liste **Membres de LAG**, sur la page Gestion des LAG.
2. Configurez les divers aspects du LAG, comme la vitesse et le contrôle de flux, via la page Paramètres des LAG.
3. Configurez la priorité et le délai LACP des ports du LAG, via la page LACP.

Définition de la gestion des LAG

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

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

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Agrégation de liaisons** > **Gestion des LAG**.

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**.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

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

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

Configuration des paramètres des LAG

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

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

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **LAG** : sélectionnez l'ID du LAG.
- **Description** : saisissez le nom du LAG ou un commentaire.
- **Type de LAG** : affiche le type de port inclus dans le LAG.
- **État administratif** : définissez le LAG sélectionné comme étant démarré ou arrêté.
- **État opérationnel** : indique si le LAG est actuellement opérationnel.
- **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. Si vous n'avez pas encore défini de période, cliquez sur **Modifier** ou accédez à la page Période.
- **Nom de période** : sélectionnez le profil qui spécifie la période.
- **État de période opérationnelle** : indique si la période est actuellement active ou inactive.
- **Réactiver le LAG suspendu** : sélectionnez cette option pour réactiver un port si le LAG a été désactivé via l'option de sécurité de verrouillage des ports ou via des configurations ACL.

- **Négociation automatique administrative** : permet d'activer ou de désactiver la négociation automatique sur le LAG. La négociation automatique est un protocole établi entre deux partenaires de liaison qui permet à un LAG d'annoncer sa vitesse de transmission et son contrôle de flux à son partenaire (la valeur par défaut pour le contrôle de flux est *Désactivé*). Il est recommandé de maintenir la négociation automatique activée des deux côtés d'une liaison agrégée (ou de la désactiver des deux côtés), tout en s'assurant que les débits de liaison sont identiques.
- **Négociation automatique opérationnelle** : affiche le paramètre de négociation automatique.
- **Débit administratif** : sélectionnez le débit du LAG.
- **Débit de LAG opérationnel** : affiche le débit actuel de fonctionnement du LAG.
- **Annonce administrative** : sélectionnez les fonctionnalités que le LAG doit annoncer. Les options sont les suivantes :
  - *Capacité maximale* : tous les débits de LAG et modes duplex sont acceptés.
  - *10 Duplex intégral* : le LAG annonce un débit de 10 Mbits/s et le mode est Duplex intégral.
  - *100 Duplex intégral* : le LAG annonce un débit de 100 Mbits/s et le mode est Duplex intégral.
  - *1 000 Duplex intégral* : le LAG annonce un débit de 1 000 Mbits/s et le mode est Duplex intégral.
- **Annonce opérationnelle** : affiche l'état d'annonce administrative. Le LAG annonce ses fonctions à son voisin pour lancer le processus de négociation. Les options disponibles sont celles spécifiées dans le champ *Annonce administrative*.
- **Contrôle de flux administratif** : définissez le contrôle de flux à **Activer** ou **Désactiver**, ou activez la **négociation automatique** du contrôle de flux sur le LAG.
- **Contrôle de flux opérationnel** : affiche le paramètre de contrôle de flux actuel.
- **LAG protégé** : sélectionnez cette option pour définir ce LAG comme port protégé pour l'isolation Couche 2. Consultez la description de la configuration des ports dans **Définition de la configuration de base des ports** pour plus d'informations sur les ports et LAG protégés.

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

Configuration de LACP

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

Priorité et règles LACP

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

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

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

Un LAG dynamique peut comporter jusqu'à 16 ports Ethernet du même type. Huit ports (maximum) peuvent être actifs et jusqu'à huit ports peuvent être en mode de réserve. Si un LAG dynamique comprend plus de huit ports, le 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 le 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 dans un ou plusieurs ports mais que ces derniers restent sans réponse LACP de la part du partenaire de liaison, le premier port dont la liaison a été activée est ajouté au LAG LACP et devient actif (les autres ports deviennent non-candidats). Ainsi, le périphérique voisin peut, par exemple, obtenir son adresse IP via DHCP et obtenir sa configuration via la configuration automatique.

Configuration des paramètres LACP

Utilisez la page LACP pour configurer les ports candidats 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 Saisissez la priorité du système LACP. Reportez-vous à la section **Priorité et règles LACP**.

ÉTAPE 3 Sélectionnez un port et cliquez sur **Modifier**.

ÉTAPE 4 Saisissez les valeurs pour les 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. Reportez-vous à la section **Configuration des paramètres LACP**.
- **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

Reportez-vous à la section **Gestion des ports : Unidirectional Link Detection**.

PoE

Reportez-vous à la section **Gestion des ports : fonctionnalité PoE**.

Configuration de 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**
- **Définition des propriétés Green Ethernet globales**
- **Définition des propriétés Green Ethernet des ports**

Présentation de la fonction Green Ethernet

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

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

- **Mode Détection d'énergie** : sur une liaison inactive, le port passe en mode inactif, ce qui permet d'économiser l'énergie tout en maintenant le port à l'état administratif Démarré. La sortie de ce mode et le retour au mode entièrement opérationnel sont rapides, transparents et sans aucune perte de trame. Ce mode est pris en charge sur les ports GE comme sur les ports FE.
- **Mode Courte portée** : cette fonction permet d'économiser de l'énergie sur une courte longueur de câble. Une fois que la longueur du câble a été analysée, la consommation d'énergie est ajustée en fonction de cette longueur. Si la longueur de câble est inférieure à 50 mètres, le 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.

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

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

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

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

Les DEL 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 DEL allumées est un gaspillage d'énergie. La fonction Green Ethernet permet de désactiver les DEL des ports (liaison, vitesse et PoE) lorsqu'elles ne sont pas nécessaires et de les activer lorsqu'elles le sont (débogage, raccordement de périphériques supplémentaires, etc.).

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

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 DEL de port

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

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

Sur la page des Propriétés >Green Ethernet, le périphérique permet à l'utilisateur de désactiver les DEL des ports afin d'économiser l'énergie.

Fonction 802.3az Energy Efficient Ethernet

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

Elle couvre les rubriques suivantes :

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

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

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

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

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

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

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

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

Découverte de niveau de liaison pour 802.3az EEE

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

Disponibilité de 802.3az EEE

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

Configuration par défaut

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

Interactions entre les fonctions

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

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

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 Gestion des ports > Green Ethernet > Propriétés (elle est activée par défaut). Cette page indique également la quantité d'énergie qui a été économisée.

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

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

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

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

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

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

Définition des propriétés Green Ethernet globales

La page Propriétés affiche et active la configuration du mode Green Ethernet pour le 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 Saisissez les valeurs pour les champs suivants :

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

  REMARQUE si le mode Courte portée est activé, EEE doit être désactivé.

- **DEL des ports** : sélectionnez cette option pour activer les DEL des ports. Lorsque les DEL des ports sont désactivés, ils n'affichent pas l'état des liaisons, l'activité, etc.

- **Économies d'énergie** : affiche le pourcentage d'énergie économisé grâce aux modes Green Ethernet et Courte portée. Les économies d'énergie affichées ne concernent que l'énergie économisée grâce aux modes Courte portée et Détection d'énergie. Les économies d'énergie EEE sont de nature dynamique, étant donné qu'elles sont basées sur l'utilisation des ports et qu'elles ne sont par conséquent pas prises en compte. Le calcul d'économie d'énergie est effectué en comparant la consommation maximale sans économies d'énergie à la consommation actuelle.
- **Énergie totale économisée** : affiche la quantité d'énergie économisée depuis le dernier redémarrage du périphérique. Cette valeur est mise à jour à chaque événement qui affecte l'économie d'énergie.
- **802.3 Energy Efficient Ethernet (EEE)** : permet d'activer ou de désactiver globalement le mode EEE.

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

Définition des propriétés Green Ethernet des ports

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

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

Pour définir les paramètres Green Ethernet de chaque port :

ÉTAPE 1 Cliquez sur **Gestion des ports** > **Green Ethernet** > **Paramètres des ports**.

La page Paramètres des ports affiche les éléments suivants :

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

Pour chaque port, les champs suivants sont décrits :

- **Port** : numéro du port.

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

  REMARQUE : le mode Courte portée n'est pris en charge que sur les ports GE RJ45 ; il ne s'applique pas aux ports mixtes.
- **802.3 Energy Efficient Ethernet (EEE)** : état du port concernant la fonction EEE :
  - *Administratif* : indique si la fonction EEE est activée.
  - *Opérationnel* : indique si la fonction EEE est actuellement opérationnelle sur le port local. Vous savez ainsi si elle a été activée (État administratif), si elle a été activée sur le port local et si elle est opérationnelle sur le port local.
  - *LLDP administratif* : indique si l'annonce des compteurs EEE via LLDP est activée.
  - *LLDP opérationnel* : indique si l'annonce des compteurs EEE via LLDP est actuellement opérationnelle.
  - *Support EEE sur la distance* : indique si la fonction EEE est prise en charge sur le partenaire de liaison. La fonction EEE doit être prise en charge sur les partenaires de liaison local et distant.

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

ÉTAPE 2 Sélectionnez un **port** puis cliquez sur **Modifier**.

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

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

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

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

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

10

Gestion des ports : Unidirectional Link Detection

Cette section décrit la fonction Unidirectional Link Detection (UDLD).

Elle couvre les rubriques suivantes :

- **Vue d'ensemble de la fonction UDLD**
- **Fonctionnement de UDLD**
- **Instructions d'utilisation**
- **Dépendances envers les autres fonctions**
- **Configuration et paramètres par défaut**
- **Avant de commencer**
- **Tâches UDLD courantes**
- **Configuration de UDLD**

Vue d'ensemble de la fonction UDLD

UDLD est un protocole 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.

Fonctionnement de UDLD

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 la liaison est unidirectionnelle, le port est fermé.
  - Si la liaison est indéterminée, le port n'est pas fermé. Si l'état est changé en indéterminé et qu'une notification est envoyée.

- **Agressif**

  Si la liaison est unidirectionnelle ou indéterminée, le port est fermé.

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 de périphérique local** : l'état de liaison du port est défini sur bidirectionnel.

  - **Si le message du voisin ne contient pas l'ID de 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 de voisinage avant l'expiration du délai, l'état de liaison du port est défini sur indéterminé et le système fonctionne 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 sur la page Gestion des ports > Paramètres de récupération d'erreur. Pour 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. Les opérations effectuées par le périphérique sont différentes si le mode UDLD est défini sur normal ou agressif.

Mode UDLD incohérent dans un périphérique local et de voisinage

Il est possible de définir le périphérique local et son voisin sur un mode UDLD différent (normal, agressif). Le mode UDLD n'est pas contenu dans les messages UDLD, afin que le périphérique local ne connaisse pas le mode UDLD de son voisin et inversement.

Si les modes UDLD sont différents sur le périphérique local et le périphérique de voisinage, ils opèrent comme suit :

- Lorsque l'état UDLD de la liaison est bidirectionnel ou unidirectionnel, les deux périphériques ferment leurs ports.
- Lorsque l'état UDLD du port est indéterminé, le système défini en mode UDLD normal émet simplement une notification, alors que le système défini en mode UDLD agressif ferme le port.

Si les deux périphériques sont définis en mode normal, le port n'est pas fermé lorsque son état est 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 :

- **Automatiquement** : vous pouvez configurer le système pour qu'il réactive automatiquement les ports fermés par UDLD sur la page Gestion des ports > Paramètres de récupération d'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.
- **Manuellement** : vous pouvez réactiver un port sur la page Gestion des ports > Paramètres de récupération d'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 simplement davantage de trafic sur le port sans offrir aucun avantage.

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 si vous souhaitez fermer un port dès qu'il existe une possibilité que la liaison soit indéterminée.

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.

- Protocoles UDLD et Couche 2

  UDLD s'exécute sur un port indépendamment des autres protocoles 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 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 Gestion des ports > Paramètres globaux UDLD.

a. Saisissez le **Délai de message**.

b. Sélectionnez l'état UDLD global **Désactivé**, **Normal** ou **Agressif**.

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 **Gestion des ports > Paramètres globaux UDLD**.

a. Sélectionnez un port.

b. Sélectionnez l'état UDLD du port **Par défaut**, **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 :*

ÉTAPE 1 Ouvrez la page **Gestion des ports** > **Paramètres de récupération d'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 ou indéterminée.

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 vers les autres ports.

Pour configurer UDLD pour 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** : identifiant du port.
- **État UDLD** : les états possibles sont :
  - *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 ferme un port si la liaison est unidirectionnelle ou indéterminée.
- **État bidirectionnel** : sélectionnez la valeur de ce champ pour le port sélectionné. 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* : UDLD a été désactivé sur ce port.
  - *Fermer* : le port a été fermé car sa liaison au périphérique connecté est unidirectionnelle ou indéterminée en mode agressif.
- **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 **Par défaut**, le port reçoit la valeur de l'**État UDLD par défaut du port fibre** défini 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 :

ÉTAPE 1 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 de voisinage 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 au périphérique connecté est unidirectionnelle ou indéterminée en mode agressif.

- **Délai d'expiration du voisin (sec)** : indique le délai devant expirer avant la détermination de l'état UDLD du port. Il correspond à trois fois le délai de message.
- **Heure du message du voisin (sec)** : indique le délai entre les messages UDLD.

11

Port intelligent

Ce document décrit la fonction Port intelligent.

Il contient les rubriques suivantes :

- Vue d'ensemble
- Qu'est-ce qu'un port intelligent ?
- Types de port intelligent
- Macros Port intelligent
- Échec de la macro et opération de réinitialisation
- Fonctionnement de la fonction Port intelligent
- Port intelligent automatique
- Gestion des erreurs
- Configuration par défaut
- Relations avec les autres fonctions et compatibilité descendante
- Tâches courantes de port intelligent
- Configuration de port intelligent à l'aide de l'interface Web
- Macros Port intelligent intégrées

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

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

La fonction Port intelligent est constituée de plusieurs composants et opère conjointement avec d'autres fonctions 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 **Configuration de LLDP** et **Configuration de 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 toutes les configurations effectuées par « la macro » lorsque cette interface devient un autre 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. Le 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
Valeur par défaut	Non	Non
Imprimante	Non	Non
Bureau	Non	Non
Invité	Non	Non
Serveur	Non	Non
Hôte	Oui	Non
Caméra IP	Non	Non
Téléphone IP	Oui	Oui
Téléphone IP Bureau	Oui	Oui
Commutateur	Oui	Oui
Routeur	Oui	Non
point d'accès sans fil	Oui	Oui

Types de port intelligent spéciaux

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

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

- **Valeur par défaut**

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

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

- Une opération de désactivation/activation de la liaison est effectuée sur l'interface.
- 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 pour une durée spécifiée.

- **Inconnu**

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

  Pour obtenir des conseils de dépannage, reportez-vous à la zone de 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.

La source de la macro peut être trouvée en laissant exécuter la commande Show parser macro name [macro_name] en mode d'exécution privilégié de l'interface de ligne de commande (CLI) ou en cliquant sur le bouton **Afficher la source de la macro** de la page Paramètres de type de port intelligent.

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

Il y a deux types de macros Port intelligent :

- **Intégrée** : 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_macro-name (par exemple : no_printer)
- **Définie 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 Modifier le paramètre du type de port intelligent.

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 Port intelligent automatique opérationnel global, l'état Port intelligent automatique de l'interface et l'état Persistant sont tous **activés**, le Type de port intelligent est défini sur ce type dynamique.
  - Sinon, l'anti-macro correspondante est appliquée et l'état de l'interface est défini sur Par défaut.

Échec de la macro et opération de réinitialisation

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

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

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

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

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

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

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

- **Port intelligent statique**

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

- **Port intelligent automatique**

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

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

Port intelligent automatique

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

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

Activation du Port intelligent automatique

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

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

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

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

Identification du Type de port intelligent

Si le Port intelligent automatique est activé au niveau global (sur la page Propriétés) et sur une interface (sur la page Paramètres d'interface), 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.

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

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

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 :

Mappage des fonctionnalités CDP au Type de port intelligent

Nom de la fonctionnalité	Bit CDP	Type de port intelligent
Routeur	0x01	Routeur
Pont TB	0x02	Point d'accès sans fil
Pont SR	0x04	Ignorer
Commutateur	0x08	Commutateur
Hôte	0x10	Hôte
Filtrage conditionnel IGMP	0x20	Ignorer
Répéteur	0x40	Ignorer

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

Nom de la fonctionnalité	Bit CDP	Type de port intelligent
Téléphone VoIP	0x80	ip_phone
Appareil géré à distance	0x100	Ignorer
Port de téléphone CAST	0x200	Ignorer
Relais MAC à deux ports	0x400	Ignorer

Mappage des fonctionnalités LLDP au Type de port intelligent

Nom de la fonctionnalité	Bit LLDP	Type de port intelligent
Autres	1	Ignorer
Répéteur IETF RFC 2108	2	Ignorer
Pont MAC IEEE Std. 802.1D	3	Commutateur
Point d'accès WLAN IEEE Std. 802.11 MIB	4	Point d'accès sans fil
Routeur IETF RFC 1812	5	Routeur
Téléphone IETF RFC 4293	6	ip_phone
Système de câble DOCSIS IETF RFC 4639 et IETF RFC 4546	7	Ignorer
Station uniquement IETF RFC 4293	8	Hôte
Composant C-VLAN d'un pont VLAN IEEE Std. 802.1Q	9	Commutateur
Composant S-VLAN d'un pont VLAN IEEE Std. 802.1Q	10	Commutateur
Relais MAC à deux ports (TPMR) IEEE Std. 802.1Q	11	Ignorer
Réservé	12-16	Ignorer

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

Plusieurs appareils associés au port

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

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

Interface du Port intelligent automatique persistant

Si l'État persistant d'une interface est activé, son Type de port intelligent et la configuration qui est déjà appliquée dynamiquement par le Port intelligent automatique sont conservés sur l'interface, même si l'appareil en cours d'association est arrivé à expiration, l'interface a été désactivée et 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 à partir des pages Paramètres d'interface et Modifier les paramètres d'interface.

Configuration par défaut

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

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

Relations avec les autres fonctions et compatibilité descendante

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

REMARQUE Lors de la mise à niveau d'une version de micrologiciel qui ne prend pas en charge le Port intelligent automatique vers un niveau de micrologiciel qui prend en charge le Port intelligent automatique, le VLAN voix automatique est désactivé après la mise à niveau. Si le OUI de téléphonie a été activé avant la mise à niveau, le Port intelligent automatique est désactivé après la mise à niveau et le OUI de téléphonie reste activé.

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 Port intelligent automatique sur l'appareil, ouvrez la page Port intelligent > 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 Port intelligent automatique sur une ou plusieurs interfaces, ouvrez la page Port intelligent > Paramètres d'interface.

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

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

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

ÉTAPE 9 Cliquez sur **Appliquer**.

Flux de travail 2 : pour configurer une interface en tant que port intelligent statique, procédez comme suit:

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

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

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

ÉTAPE 4 Définissez les paramètres de macro souhaités.

ÉTAPE 5 Cliquez sur **Appliquer**.

Flux de travail 3 : pour définir les valeurs par défaut des paramètres de macro Port intelligent et/ou lier une paire de macros définie 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.

1. Ouvrez la page Port intelligent > Paramètres de type de port intelligent.
2. Sélectionnez le Type de port intelligent.
3. Cliquez sur **Afficher la source de la macro** pour afficher la macro Port intelligent actuelle qui est associée au Type de port intelligent sélectionné.
4. Cliquez sur **Modifier** pour ouvrir une nouvelle fenêtre 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.
5. Sur la page Modifier, modifiez les champs.
6. Cliquez sur **Appliquer** pour réexécuter la macro si les paramètres ont été modifiés ou sur **Restaurer les valeurs par défaut** pour restaurer si nécessaire les valeurs par défaut des paramètres dans les macros intégrées.

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 Inconnu.

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

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

ÉTAPE 4 Cliquez sur **Modifier.** Une nouvelle fenêtre s'ouvre. Cliquez sur **Réinitialiser** pour réinitialiser l'interface.

ÉTAPE 5 Revenez à la page principale et réappliquez la macro en utilisant **Réappliquer** (pour les appareils qui ne sont ni des commutateurs, ni des routeurs ni des points d'accès) ou **Réappliquer la macro de port intelligent** (pour les commutateurs, routeurs ou points d'accès) afin d'exécuter la macro Port intelligent sur l'interface.

Il existe une deuxième méthode de réinitialisation des interfaces uniques ou multiples inconnues :

ÉTAPE 1 Sur la page Paramètres d'interface, activez la case à cocher Type de port est égal à.

ÉTAPE 2 Sélectionnez *Inconnu* et cliquez sur **OK**.

ÉTAPE 3 Cliquez sur **Réinitialiser tous les ports intelligents inconnus**. Réappliquez ensuite la macro comme indiqué ci-dessus.

CONSEIL L'échec de la macro peut être dû à un conflit avec une configuration de l'interface qui a été effectuée avant l'application de la macro (le plus souvent rencontré dans les paramètres de sécurité et de contrôle des tempêtes), un type de port incorrect, une typo ou une commande incorrecte dans la macro définie par l'utilisateur ou encore une valeur de paramètre non valide. Les paramètres sont contrôlés, sans prise en compte du type ou de la limite, avant la tentative d'application de la macro. Par conséquent, une entrée incorrecte ou non valide pour une valeur de paramètre se soldera presque assurément par un échec lors de l'application de la macro.

Configuration de port intelligent à l'aide de l'interface Web

Vous pouvez configurer la fonction Port intelligent sur les pages Port intelligent > Propriétés, Paramètres de type de port intelligent et Paramètres d'interface.

Pour la configuration du VLAN vocal, reportez-vous à la section **VLAN voix**.

Pour la configuration de LLDP/CDP, reportez-vous respectivement aux sections **Configuration de LLDP** et **Configuration de CDP**.

Propriétés de port intelligent

Pour configurer la fonction Port intelligent de façon globale :

ÉTAPE 1 Cliquez sur **Port intelligent> Propriétés**.

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 du CDP. Activez CDP si le Port intelligent automatique doit détecter le Type de port intelligent à partir de l'annonce CDP.
- **État LLDP opérationnel** : affiche l'état opérationnel du LLDP. Activez LLDP si le Port intelligent automatique doit détecter le Type de port intelligent à partir de l'annonce LLDP/LLDP-MED.
- **Détection périphérique de port intelligent auto.** : sélectionnez chaque type d'appareil pour lequel le Port intelligent automatique peut attribuer des Types de port intelligent aux interfaces. Si vous ne cochez pas cette option, le Port intelligent automatique n'attribue ce Type de port intelligent à aucune interface.

ÉTAPE 3 Cliquez sur **Appliquer**. Vous appliquez ainsi les paramètres de Port intelligent globaux sur l'appareil.

Paramètres de type de port intelligent

Utilisez la page Paramètres de type de port intelligent pour modifier les paramètres de type de port intelligent et afficher la source de la macro.

Par défaut, chaque Type de port intelligent est associé à une paire de macros Port intelligent intégrées. Pour plus d'informations sur la macro et l'anti-macro, reportez-vous à la section **Types de port intelligent**. Vous pouvez aussi associer votre propre paire de macros définies par l'utilisateur avec 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 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.

  Vous pouvez restaurer les valeurs par défaut des paramètres en cliquant sur **Restaurer les valeurs par défaut**.

ÉTAPE 5 Cliquez sur **Appliquer** pour enregistrer les modifications dans la configuration d'exécution. Si la macro Port intelligent et/ou ses valeurs de paramètre associées au Type de port intelligent sont modifiées, le Port intelligent automatique réapplique automatiquement la macro aux interfaces qui sont actuellement attribuées avec le Type de port intelligent par le Port intelligent automatique. Le Port intelligent automatique n'applique pas les modifications aux interfaces auxquelles un Type de port intelligent a été attribué de façon statique.

REMARQUE Il n'existe aucune méthode permettant de valider les paramètres de macro, car ils n'ont aucune association de type. Toutefois, n'importe quelle entrée est valide à ce stade. Néanmoins, des valeurs de paramètre non valides peuvent entraîner des erreurs lorsque le Type de port intelligent est attribué à une interface appliquant la macro associée.

Paramètres d'interface de port intelligent

Utilisez la page Paramètres d'interface pour effectuer les tâches suivantes :

- Appliquez de manière statique un Type de port intelligent spécifique à une interface, avec des valeurs spécifiques à l'interface pour les paramètres de macro.
- Activez le Port intelligent automatique sur une interface.
- Diagnostiquez une macro Port intelligent dont l'application a échoué et a généré l'état Inconnu du Type de port intelligent.
- Réappliquez une macro Port intelligent après son échec pour l'un des types d'interface suivants : commutateur, routeur et point d'accès. Nous partons du principe que vous avez effectué les corrections nécessaires avant de cliquer sur **Réappliquer**. Pour obtenir des conseils de dépannage, reportez-vous à la zone de 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**.

Réappliquez la macro Port intelligent associée comme suit :

- Sélectionnez un groupe de Types de port intelligent (commutateurs, routeurs ou points d'accès) et cliquez sur **Réappliquer la macro de port intelligent.** Les macros sont appliquées à tous les types d'interface sélectionnés.
- Sélectionnez une interface UP et cliquez sur **Réappliquer** pour réappliquer la dernière macro qui a été appliquée à l'interface.

  L'action **Réappliquer** ajoute aussi l'interface à tous les VLAN nouvellement créés.

ÉTAPE 2 Diagnostic de port intelligent.

Si une macro Port intelligent échoue, le Type de port intelligent de l'interface est Inconnu. Sélectionnez une interface dont le type est inconnu, puis cliquez sur **Afficher les diagnostics**. Le système affiche la commande où l'application de la macro a échoué. Pour obtenir des conseils de dépannage, reportez-vous à la zone de 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.

- Activez la case à cocher *Type de port est égal à*.
- Sélectionnez *Inconnu* et cliquez sur **OK**.
- Cliquez sur **Réinitialiser tous les ports intelligents inconnus**. Réappliquez ensuite la macro comme indiqué ci-dessus. Cette opération réinitialise l'ensemble des interfaces de type Inconnu, ce qui signifie que le type Par défaut est réattribué à toutes les interfaces. Une fois que vous avez corrigé l'erreur dans la macro et/ou dans la configuration d'interface actuelle, vous pouvez appliquer une nouvelle macro.

REMARQUE La réinitialisation de l'interface de type inconnu ne réinitialise pas la configuration effectuée par la macro qui a échoué. Ce nettoyage doit être réalisé manuellement.

Pour attribuer un Type de port intelligent à une interface ou activer la fonction Port intelligent automatique sur l'interface :

ÉTAPE 1 Sélectionnez une interface et cliquez sur **Modifier**.

ÉTAPE 2 Renseignez les champs.

- **Interface** : sélectionnez le port ou LAG.
- **Type de port intelligent** : affiche le Type de port intelligent actuellement attribué au port/LAG.
- **Application de port intelligent** : sélectionnez le Type de port intelligent dans le menu déroulant Application de port intelligent.
- **Méthode d'application de port intelligent** : si le Port intelligent automatique est sélectionné, il attribue automatiquement le Type de port intelligent en fonction de l'annonce CDP et/ou LLDP reçue des appareils en cours de connexion, et applique la macro Port intelligent correspondante. Pour attribuer un Type de port intelligent de manière statique et appliquer la macro Port intelligent correspondante à l'interface, sélectionnez le Type de port intelligent souhaité.

- **État persistant** : sélectionnez cette option pour activer l'État persistant. S'il est activé, l'association d'un Type de port intelligent à une interface est conservée même si l'interface est désactivée ou que 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 elle a l'état Inconnu (en raison d'un échec d'application de macro). La macro peut être réappliquée sur la page principale.

ÉTAPE 4 Cliquez sur **Appliquer** pour mettre à jour les modifications et attribuer le Type de port intelligent à l'interface.

Macros Port intelligent intégrées

Vous trouverez ci-dessous une description de la paire de macros intégrées pour chaque Type de port intelligent. Pour chaque Type de port intelligent, une macro permet de configurer l'interface et une anti-macro permet de supprimer la configuration.

Le code de macro des Types de port intelligent suivants est indiqué ci-après :

- **desktop**
- **printer**
- **guest**
- **server**
- **host**
- **ip_camera**
- **ip_phone**

- ip_phone_desktop
- switch
- router
- ap

desktop

```
[desktop]
#interface configuration, for increased network security and reliability when
connecting a desktop device, such as a PC, to a switch port. (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 ports : fonctionnalité PoE

La fonctionnalité PoE (Power over Ethernet) n'est disponible que sur les appareils basés sur PoE. Une liste de ces appareils vous est présentée à la section **Modèles de périphériques**.

Cette section décrit comment utiliser la fonctionnalité PoE.

Elle couvre les rubriques suivantes :

- **PoE sur l'appareil**
- **Configuration des propriétés PoE**
- **Configuration des paramètres de la fonctionnalité PoE**

PoE sur l'appareil

Un appareil PoE est un périphérique PSE (Power Sourcing Equipment) qui fournit une alimentation électrique à des appareils alimentés (PD, Powered Devices) sur des câbles en cuivre existants sans avoir à interférer avec le trafic réseau, à mettre à jour le réseau physique ni à modifier l'infrastructure réseau.

Consultez la section **Modèles de périphériques** pour en savoir plus sur la prise en charge PoE sur les différents modèles.

Fonctionnalités PoE

L'option PoE offre les fonctionnalités suivantes :

- Élimine le besoin de fournir une alimentation de 110/220 Vca à tous les appareils connectés à un LAN câblé.
- Supprime le besoin de placer tous les appareils réseau à proximité de sources d'alimentation.

- Élimine le besoin de déployer des systèmes à double câblage dans une entreprise et permet ainsi de réduire de façon significative les coûts d'installation.

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

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

Fonctionnement de PoE

Le processus de mise en œuvre de la fonctionnalité PoE comprend les étapes suivantes :

- Détection : envoie des impulsions spéciales sur le câble en cuivre. Lorsqu'un appareil PoE est situé à l'autre extrémité, cet appareil répond à ces impulsions.
- Classification : la négociation entre le PSE (Power Sourcing Equipment) et l'appareil alimenté (PD, Powered Device) débute après l'étape de détection. Au cours de la négociation, le PD spécifie sa classe, qui correspond à la puissance maximale qu'il consomme.
- Consommation électrique : une fois l'étape de classification terminée, le PSE fournit de la puissance au PD. Si ce dernier prend en charge PoE, il est considéré en l'absence d'une classification comme étant de classe 0 (le maximum). Si un PD essaie de consommer plus de puissance que ne l'autorise la norme, le PSE arrête d'alimenter le port.

PoE prend en charge deux modes :

- **Limite du port** : la puissance maximale que l'appareil accepte de fournir est limitée à la valeur configurée par l'administrateur système, ceci indépendamment du résultat de la classification.
- **Limite de classe** : la puissance maximale que l'appareil accepte de fournir est déterminée par les résultats obtenus à l'étape Classification. Cela signifie qu'elle est définie conformément à la demande du client.

Considérations relatives à la configuration de PoE

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

- la quantité de puissance que le PSE peut fournir ;
- la quantité de puissance que le PD essaie véritablement de consommer.

Vous pouvez décider :

- de la puissance maximale qu'un PSE est autorisé à fournir à un PD ;
- alors que l'appareil fonctionne, de changer le mode de Limite de classe en Limite du port et vice versa. de conserver les valeurs de puissance par port ayant été configurées pour le mode Limite du port ;

  REMARQUE : modifier le mode de Limite de classe à 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 Limite du port) ;
- de générer une interception lorsqu'un PD essaie de consommer trop de puissance et pour déterminer à quel pourcentage de la puissance maximale ce message est généré.

Le matériel PoE spécifique détecte automatiquement la classe du PD et sa limite de puissance en fonction de la classe de l'appareil connecté à chaque port spécifique (mode Limite de classe).

Si, à tout moment au cours de la connexion, un PD relié nécessite plus de puissance de la part du PSE que ce que permet l'allocation configurée (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 la fourniture de puissance au port PoE ;
- journalise le motif de l'arrêt de l'alimentation ;
- génère une interruption SNMP.

AVERTISSEMENT Tenez compte des éléments suivants lorsque vous connectez des commutateurs capables de fournir une alimentation PoE : les modèles PoE des séries Sx200, Sx300 et SF500 sont des appareils PSE (Power Sourcing Equipment) qui peuvent fournir une alimentation CC à des périphériques connectés (PD, Powered Devices). Ces derniers englobent notamment des téléphones VoIP, des caméras IP et des points d'accès sans fil. Les commutateurs PoE peuvent détecter et alimenter des périphériques connectés PoE existants pré-standard. En raison de la prise en charge du PoE hérité, un appareil PoE agissant en tant qu'appareil PSE peut détecter et alimenter à tort un appareil PSE connecté, y compris d'autres commutateurs PoE, en tant que PD hérité.

Même si les commutateurs PoE Sx200/300/500 sont des appareils PSE qui doivent bénéficier de courant alternatif, ils peuvent être alimentés en tant que PD hérité par un autre appareil PSE suite à une erreur de détection. Dans cette situation, l'appareil PoE risque de ne pas fonctionner correctement et peut également ne pas alimenter convenablement ses PD connectés.

Pour éviter toute erreur de détection, vous devez désactiver le PoE au niveau des ports des commutateurs PoE que vous utilisez pour vous connecter à des appareils PSE. Vous devez également d'abord alimenter un appareil PSE avant de le connecter à un appareil PoE. Lorsqu'un périphérique est considéré à tort comme un PD, vous devez déconnecter le périphérique du port PoE, puis l'alimenter avec du courant alternatif avant de reconnecter ses ports PoE.

Configuration des propriétés PoE

La page Propriétés PoE permet de sélectionner le mode PoE Limite du port ou Limite de classe et de spécifier les interceptions PoE à générer.

Ces paramètres sont saisis à l'avance. Lorsque le PD se connecte et consomme de la puissance, il peut consommer bien moins que la puissance maximale autorisée.

La puissance de sortie est désactivée lors du redémarrage, de l'initialisation et de la configuration système pour veiller à ne pas endommager les PD.

Pour configurer la fonctionnalité PoE sur l'appareil et surveiller la puissance consommée :

ÉTAPE 1 Cliquez sur **Gestion des ports > PoE > Propriétés**.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **Mode d'alimentation** : sélectionnez l'une des options suivantes :
  - *Limite du port* : la limite maximale de puissance par port est configurée par l'utilisateur.
  - *Limite de classe* : la limite maximale de puissance par port est déterminée par la classe de l'appareil, elle-même résultant de l'étape de Classification.

  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** : permettent 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.

Les compteurs suivants s'affichent :

- **Puissance nominale** : la quantité totale de puissance que l'appareil peut fournir à l'ensemble des PD connectés.
- **Consommation** : puissance actuellement consommée par les ports PoE.
- **Puissance disponible** : puissance nominale moins la quantité de puissance consommée.

ÉTAPE 3 Cliquez sur **Appliquer** pour enregistrer les propriétés PoE.

Configuration des paramètres de la fonctionnalité PoE

La page Paramètres PoE affiche les informations PoE système pour l'activation de PoE sur les interfaces et la surveillance de la consommation actuelle ainsi que de la limite maximale de puissance par port.

REMARQUE La fonctionnalité PoE de l'appareil peut être configurée pour un laps de temps limité. 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 spécifiés. Pour utiliser cette option de configuration, une période doit d'abord être définie à l'aide de la page **Période**.

Cliquez sur **Gestion des ports > PoE > Paramètres**.

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

- **Limite du port :** la puissance est limitée à une consommation en watts spécifique. Pour que ces paramètres soient actifs, le système doit être en mode Limite du port PoE. Vous pouvez configurer ce mode sur la page Propriétés PoE.

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

- **Limite de classe :** la puissance est limitée en fonction de la classe du PD connecté. Pour que ces paramètres soient actifs, le système doit être en mode Limite de classe PoE. Vous pouvez configurer ce mode sur la page Propriétés PoE.

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

Exemple de priorité PoE :

Supposition : un 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 1 440 watts, ce qui est bien trop. L'appareil ne peut pas fournir suffisamment de puissance à chaque port, il suit donc certaines priorités.

L'administrateur définit la priorité de chaque port, en lui allouant autant de puissance que possible.

Vous devez entrer ces priorités sur la page Paramètres PoE.

Reportez-vous à la section **Modèles de périphériques** 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 port PoE :

ÉTAPE 1 Cliquez sur **Gestion des ports > PoE > Paramètres**. La liste des champs ci-dessous correspond au mode d'alimentation Limite du port. Les champs peuvent légèrement différer si le mode d'alimentation est Limite de classe.

ÉTAPE 2 Sélectionnez un port et cliquez sur **Modifier.** La liste des champs ci-dessous correspond au mode d'alimentation Limite du port. Les champs peuvent légèrement différer si le mode d'alimentation est Limite de classe.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **Interface** : sélectionnez le port à configurer.
- **État administratif PoE** : permet d'activer ou de désactiver PoE sur le port.
- **Période** : sélectionnez cette option pour spécifier la période d'activation de la fonctionnalité PoE sur le port.
- **Nom de période** : si l'option Période est activée, choisissez la période à utiliser. Les périodes sont définies à l'aide de la page **Période**.
- **Niveau de priorité d'alimentation** : sélectionnez la priorité du port (faible, élevée ou critique) qui sera utilisée en cas de manque de puissance. Par exemple, si 99 % de la puissance disponible est consommée, et que le port 1 a une priorité élevée et le port 3 une priorité faible, le port 1 sera alimenté, contrairement au port 3.
- **Affectation de puissance administrative** : ce champ 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).
- **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.

- **Classe** : ce champ s'affiche uniquement si le mode d'alimentation Limite de classe est défini sur la page Propriétés PoE. La classe détermine le niveau de puissance :

Classe	Puissance maximale fournie par le port de l'appareil
0	15,4 W
1	4,0 W
2	7,0 W
3	15,4 W
4	30,0 W

- **Consommation électrique** : affiche la puissance (en milliwatts) affectée à l'appareil alimenté connecté à l'interface sélectionnée.
- **Nombre de surcharges** : affiche le nombre total d'occurrences de surcharges de courant.
- **Nombre de courts-circuits** : affiche le nombre total d'occurrences de courts-circuits électriques.
- **Nombre de refus** : affiche le nombre de fois où l'alimentation a été refusée pour l'appareil alimenté.
- **Nombre d'absences** : affiche le nombre de fois où l'alimentation de l'appareil alimenté a été arrêtée, l'appareil n'étant plus détecté.
- **Nombre de signatures non valides** : affiche le nombre de fois où une signature non valide a été reçue. L'appareil alimenté utilise des signatures pour s'identifier auprès du PSE. Ces signatures sont générées lors de la détection, la classification ou la maintenance de l'appareil alimenté.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres PoE du port sont consignés dans le fichier de Configuration d'exécution.

13

Gestion des VLAN

Cette section couvre les rubriques suivantes :

- VLAN
- Configuration des paramètres VLAN par défaut
- Création d'un VLAN
- Configuration des paramètres d'interface VLAN
- Définition de l'appartenance VLAN
- Paramètres GVRP
- Groupes VLAN
- VLAN voix
- Accès VLAN TV port multidiffusion
- VLAN TV port client multidiffusion

VLAN

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

Description des VLAN

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

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

Les VLAN traitent les problèmes de sécurité et d'extensibilité. Le trafic d'un VLAN reste à l'intérieur du VLAN et se termine à ses périphériques. Il facilite également la configuration réseau en connectant logiquement les périphériques sans les transférer physiquement.

Si une trame est balisée VLAN, une balise VLAN à 4 octets est ajoutée à chaque trame Ethernet. La balise contient un ID VLAN compris entre 1 et 4094 et une balise de priorité VLAN (VPT) comprise entre 0 et 7. Pour plus d'informations sur VPT, reportez-vous à **Qualité de service**.

Lorsqu'une trame entre dans un périphérique tenant compte du VLAN, elle est classée comme appartenant à un VLAN spécifique en vertu de sa balise VLAN à 4 octets au sein de la trame.

S'il n'existe aucune balise VLAN dans la trame ou si la trame comporte une balise de priorité, elle est catégorisée dans le VLAN selon le PVID (identificateur de port VLAN) configuré au port de réception de la trame.

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

Les trames appartenant à un VLAN restent dans le VLAN. Ceci s'applique en envoyant ou en transférant une trame uniquement à des ports de sortie membres du VLAN cible. Un port de sortie peut être un membre balisé ou non balisé d'un VLAN.

Le port de sortie :

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

Rôles du VLAN

Les réseaux VLAN fonctionnent au niveau de la couche 2. Tout le trafic VLAN (monodiffusion/diffusion/multidiffusion) demeure au sein de son réseau 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 raccordé.

Les VLAN sur un périphérique peuvent être créés statistiquement ou dynamiquement en vertu des informations GVRP échangées par les périphériques. Un VLAN peut être statique ou dynamique (via GVRP), mais pas les deux. Pour 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 plus d'informations, reportez-vous à la section VLAN voix.
- VLAN invité : défini sur la page Modifier l'authentification VLAN.
- VLAN par défaut : pour plus d'informations, reportez-vous à la section Configuration des paramètres VLAN par défaut.
- VLAN de gestion (dans des systèmes en mode système de couche 2) : pour plus d'informations, reportez-vous à la section Adressage IP couche 2.

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 le trafic sur le réseau. La balise S-tag permet de répartir le trafic entre plusieurs clients, tout en conservant les balises VLAN du client.

Le trafic du client est encapsulé avec une balise S-tag avec TPID 0x8100, peu importe s'il a été balisé en « c-tagged » ou non balisé au départ. La balise S-tag permet à ce trafic d'être traité comme un agrégat au sein d'un réseau de pont fournisseur, dans lequel le pontage est uniquement basé sur le VID S-tag (S-VID).

La balise S-Tag est conservée lorsque le trafic est transféré par le biais de l'infrastructure du fournisseur de services réseau ; elle est ensuite supprimée par un périphérique de sortie.

Un autre avantage de QinQ est qu'il n'est pas nécessaire de configurer les dispositifs de bordure du client.

Vous pouvez activer QinQ sur la page Gestion des VLAN > Paramètres d'interface.

Charge de travail de la configuration VLAN

Pour configurer les VLAN :

1. Dans la mesure où cela est requis, modifiez le VLAN par défaut en utilisant la section **Configuration des paramètres VLAN par défaut**.
2. Créez les VLAN requis à l'aide de la section **Création d'un VLAN**.
3. Définissez la configuration VLAN souhaitée pour les ports et activez QinQ sur une interface en suivant les indications de la section **Configuration des paramètres d'interface VLAN** .
4. Assignez des interfaces aux VLAN à l'aide de la section **Configuration de ports vers un VLAN** ou de la section **Configuration d'une appartenance VLAN**.
5. Affichez l'appartenance actuelle du port VLAN pour toutes les interfaces en suivant les indications de la section **Configuration d'une appartenance VLAN**.

Configuration des paramètres VLAN par défaut

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

Le VLAN par défaut comporte les caractéristiques suivantes :

- Il est distinct, non statique/non dynamique et tous les ports sont des membres non balisés par défaut.
- Il peut être supprimé.
- Il ne peut recevoir d'étiquette.
- Il ne peut pas être utilisé pour un rôle spécial tel qu'un VLAN non authentifié ou un VLAN voix. Cette option ne concerne que les VLAN voix définis sur OUI activé.

- Si un port n'est plus membre d'un VLAN, le 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 s'il 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.

Lorsque le VID du VLAN par défaut est modifié, le périphérique exécute les opérations suivantes sur tous les ports du VLAN après avoir enregistré la configuration et redémarré :

- Supprime l'appartenance VLAN des ports au VLAN par défaut d'origine (uniquement possible après le redémarrage).
- Remplace le PVID (identificateur de port VLAN) des ports par le VID du nouveau VLAN par défaut.
- L'ID du réseau VLAN par défaut d'origine est supprimé du périphérique. Il doit être recréé pour pouvoir être utilisé.
- Ajoute des ports en tant que membres VLAN non balisés du nouveau VLAN par défaut.

Pour changer le VLAN par défaut :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres VLAN par défaut**.

ÉTAPE 2 Saisissez les valeurs pour les champs suivants :

- **ID VLAN par défaut actuel** : affiche l'ID du réseau VLAN par défaut actuel.
- **ID VLAN par défaut après redémarrage** : saisissez un nouvel ID VLAN pour remplacer l'ID VLAN par défaut après le redémarrage.

ÉTAPE 3 Cliquez sur **Appliquer**.

ÉTAPE 4 Cliquez sur **Enregistrer** (dans le coin supérieur droit de la fenêtre) et enregistrez la Configuration d'exécution dans la Configuration de démarrage.

L'**ID VLAN par défaut après réinitialisation** devient l'**ID VLAN par défaut actuel** après le redémarrage du périphérique.

Création d'un VLAN

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

Le périphérique de la série 300 prend en charge jusqu'à 4 000 réseaux VLAN, y compris le VLAN par défaut.

Chaque VLAN doit être configuré avec un VID unique (ID VLAN) dont la valeur est comprise entre 1 et 4 094. Le périphérique conserve le VID 4 095 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**.

Cette page contient les champs suivants pour tous les VLAN :

- **ID VLAN** : ID VLAN défini par l'utilisateur.
- **Nom du VLAN** : nom du VLAN défini par l'utilisateur.
- **Initiateurs** : type de VLAN :
  - *GVRP* : le VLAN a été dynamiquement créé via le protocole GVRP (Generic VLAN Registration Protocol).
  - *Statique* : le VLAN a été défini par l'utilisateur.
  - *Défaut* : c'est le VLAN par défaut.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un nouveau VLAN.

La page permet la création d'un VLAN unique ou d'une plage de VLAN.

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

Pour créer une plage de VLAN, sélectionnez le bouton **Plage** et spécifiez la plage de VLAN à créer en saisissant le VID de départ et le VID de fin (ces valeurs sont comprises). Si vous utilisez la fonction **Plage**, le nombre maximal de VLAN que vous pouvez créer en une seule fois est 100.

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

Configuration des paramètres d'interface VLAN

La page Paramètres d'interface affiche et active la configuration des paramètres VLAN pour toutes les interfaces

Pour configurer les paramètres VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres d'interface**.

ÉTAPE 2 Sélectionnez un type d'interface (Port ou LAG) et cliquez sur **OK**. Les ports ou LAG et leurs paramètres VLAN s'affichent.

ÉTAPE 3 Pour configurer un port ou LAG, sélectionnez-le puis cliquez sur **Modifier**.

ÉTAPE 4 Saisissez les valeurs pour les champs suivants :

- **Interface** : sélectionnez un port/LAG.
- **Mode d'interface VLAN** : sélectionnez le mode d'interface du VLAN. Les options sont les suivantes :
  - *Général* : l'interface peut prendre en charge toutes les fonctions tel qu'elles sont définies dans les caractéristiques techniques IEEE 802.1q. Elle peut être un membre balisé ou non balisé d'un ou plusieurs VLAN.
  - *Accès* : l'interface est un membre non balisé d'un VLAN unique. Un port configuré dans ce mode est connu comme port d'accès.
  - *Liaison* : l'interface est un membre non balisé d'au moins un VLAN ainsi qu'un membre balisé de zéro ou plusieurs VLAN. Un port configuré dans ce mode est connu comme port de liaison.
  - *Client* : sélectionnez cette option pour mettre l'interface en mode QinQ. Vous pouvez ainsi appliquer votre propre agencement VLAN (PVID) sur le réseau du fournisseur. Le périphérique est en mode Q-in-Q lorsqu'il comporte un ou plusieurs ports client. Reportez-vous à la section **QinQ**.
- **PVID administratif** : saisissez l'ID VLAN du port (PVID) du VLAN dans lequel les trames non balisées entrantes et les trames balisées de priorité sont classées. Les valeurs possibles sont comprises entre 1 et 4094.
- **Type de trame** : sélectionnez le type de trame que l'interface peut recevoir. Les trames qui n'ont pas le type configuré sont abandonnées à l'entrée. Ces types de trames sont uniquement disponibles en mode Général. Les valeurs possibles sont :
  - *Tout admettre* : l'interface accepte tous les types de trames : trames non balisées, trames balisées et trames balisées de priorité.

- *Admettre balisées uniquement* : l'interface accepte uniquement les trames balisées.
- *Admettre non balisées uniquement* : l'interface accepte uniquement les trames de priorité et non balisées.

- **Filtrage d'entrée** (uniquement disponible en mode Général) : sélectionnez cette option pour activer le Filtrage d'entrée. Lorsqu'une interface est en mode Filtrage d'entrée, elle abandonne toutes les trames entrantes qui sont classées comme appartenant aux VLAN dont elle n'est pas membre. Le filtrage d'entrée peut être désactivé ou activé sur les ports généraux. Il est toujours activé sur les ports d'accès et les ports de liaison.

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

Définition de l'appartenance VLAN

Les pages Port vers VLAN et Appartenance VLAN des ports affichent les appartenances VLAN des ports dans diverses présentations. Vous pouvez les utiliser pour ajouter des appartenances aux VLAN ou en supprimer de ces derniers.

Lorsqu'un port est interdit d'appartenance au VLAN par défaut, il ne disposera d'aucune autorisation d'appartenance à aucun autre VLAN. Le VID interne 4095 est assigné au port.

Pour transférer correctement les paquets, les périphériques intermédiaires tenant compte du VLAN qui acheminent le trafic VLAN entre les nœuds d'extrémité doivent être configurés manuellement, ou doivent apprendre dynamiquement les VLAN ainsi que leurs appartenances de port via le protocole GVRP.

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

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

Configuration de ports vers un VLAN

Utilisez la page Port vers VLAN pour afficher et configurer les ports dans un VLAN spécifique.

Pour mapper les ports ou les LAG à un VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Port vers VLAN**.

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

Le mode de chaque port ou LAG s'affiche dans son état actuel (Accès, Liaison, Général ou Client). Vous pouvez le définir sur la page Paramètres d'interface.

Chaque port ou LAG s'affiche avec son enregistrement actuel sur le VLAN.

ÉTAPE 3 Modifiez l'enregistrement d'une interface au VLAN en sélectionnant l'option souhaitée dans la liste suivante :

- **Interdit** : l'interface n'est pas autorisée à rejoindre le VLAN même à partir de l'enregistrement GVRP. Lorsqu'un port n'est pas membre d'un autre VLAN, l'activation de cette option sur le port l'intègre au VLAN interne 4095 (VID réservé).
- **Exclu** : l'interface n'est actuellement pas membre du VLAN. C'est le paramètre par défaut pour tous les ports et LAG. Le port peut rejoindre le VLAN via un enregistrement GVRP.
- **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 de multidiffusion** : interface utilisée pour la TV numérique à l'aide d'IP de multidiffusion. Le port se connecte au VLAN avec une balise VLAN de VLAN TV multidiffusion. Pour plus d'informations, reportez-vous à la section **Accès VLAN TV port multidiffusion**.
- **PVID** : sélectionnez cette option pour définir le PVID de l'interface sur le VID du VLAN. Le PVID est un paramètre par port.

ÉTAPE 4 Cliquez sur **Appliquer**. Les interfaces sont attribuées au VLAN et écrites dans le fichier de Configuration d'exécution.

Vous pouvez continuer d'afficher et/ou de configurer l'appartenance de port à un autre VLAN en sélectionnant l'ID d'un autre VLAN.

Configuration d'une appartenance VLAN

La page Appartenance VLAN des ports affiche tous les ports du périphérique, ainsi qu'une liste des VLAN auxquels chaque port appartient.

Si la méthode d'authentification basée sur les ports pour une interface est 802.1x et que le Contrôle de port administratif est Auto, alors :

- Tant que le port n'est pas authentifié, il est exclu de tous les VLAN, à l'exception des VLAN invités et non authentifiés. Sur la page VLAN vers port, le port est marqué d'un « P » majuscule.
- Lorsque le port est authentifié, il reçoit l'appartenance dans le VLAN où il a été configuré.

Pour attribuer un port à un ou plusieurs VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Appartenance VLAN du port**.

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

- **Interface** : ID du port/LAG.
- **Mode** : mode VLAN d'interface qui a été sélectionné sur la page Paramètres d'interface.
- **VLAN administratifs** : liste déroulante qui affiche tous les VLAN dont l'interface peut être membre.
- **VLAN opérationnels** : liste déroulante qui affiche tous les VLAN dont l'interface est actuellement membre.
- **LAG** : si l'interface sélectionnée est Port, affiche le LAG dont elle est membre.

ÉTAPE 3 Sélectionnez un port et cliquez sur le bouton **Connecter le VLAN**.

ÉTAPE 4 Saisissez les valeurs pour les champs suivants :

- **Interface** : sélectionnez un port/LAG.
- **Mode** : affiche le mode VLAN du port qui a été sélectionné sur la page Paramètres d'interface.
- **Sélectionner le VLAN** : pour associer un port à un ou plusieurs VLAN, déplacez le ou les ID VLAN de la liste de gauche vers la liste de droite à l'aide des flèches. Le VLAN par défaut peut apparaître dans la liste de droite s'il est balisé. Il ne peut cependant être sélectionné.
- **Balisage** : sélectionnez une des options de PVID/balisage suivantes :
  - **Balisé** : sélectionnez cette option pour baliser le port. Cette option ne concerne pas les ports d'accès.
  - **Non balisé** : sélectionnez cette option pour que le port soit non balisé. Cette option ne concerne pas les ports d'accès.
  - **PVID** : le PVID du port est défini sur ce VLAN. Si l'interface est en mode Accès ou Liaison, le périphérique fait automatiquement de l'interface un membre non balisé du VLAN. Si l'interface est en mode général, vous devez configurer manuellement l'appartenance VLAN.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres sont modifiés et écrits dans le fichier de Configuration d'exécution.

Pour afficher les VLAN administratifs et opérationnels sur une interface, cliquez sur **Détails**.

Paramètres GVRP

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

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

Lorsqu'un port est connecté à un VLAN via GVRP, il est ajouté au VLAN en tant que membre dynamique, sauf si cette action a été expressément interdite 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 GVRP doit être activé globalement et sur chaque port. Lorsqu'il est activé, il transmet et reçoit des GPDU (GARP Packet Data Units). Les VLAN définis mais non actifs ne sont pas propagés. Pour propager le VLAN, il doit être actif au moins sur un port.

Par défaut, le protocole GVRP est désactivé globalement et sur les ports.

Définition des paramètres GVRP

Pour définir les paramètres GVRP pour une interface :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Paramètres GVRP**.

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

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

ÉTAPE 4 Sélectionnez un type d'interface (Port ou LAG), puis cliquez sur **Ok** 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 Saisissez les valeurs pour les champs suivants :

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

ÉTAPE 7 Cliquez sur **Appliquer**. Les paramètres GVRP sont modifiés et écrits dans le fichier de Configuration d'exécution.

Groupes VLAN

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 selon diverses classifications qui ont été configurées (comme des groupes VLAN).

Si plusieurs systèmes 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 MAC source au VLAN de l'interface d'entrée.
- **PVID :** le VLAN est extrait de l'ID VLAN par défaut du port.

Groupes 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.

Le tableau suivant décrit la disponibilité des groupes VLAN basés sur MAC dans diverses références :

Tableau 1 Disponibilité des groupes VLAN basés sur MAC

Référence	Mode système	Groupes VLAN basés sur MAC pris en charge
Sx300	**Couche 2**	Oui
	Couche 3	Non
Sx500, Sx500ESW2-550X	**Couche 2**	Oui
	Couche 3	Non

Référence	Mode système	Groupes VLAN basés sur MAC pris en charge
SG500X	**Natif**	Oui
	Hybride de base - Couche 2	Oui
	Hybride de base - Couche 3	Non
SG500XG	**Identique à Sx500**	Oui

Flux de travail

Pour définir un groupe 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. Attribuez 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.

Assignation de groupes VLAN 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 VLAN :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Groupes VLAN** > **Groupes basés sur MAC**.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

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

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

- **Masque** : saisissez l'une des informations suivantes :
  - *Hôte* : hôte source de l'adresse MAC

- *Longueur* : *préfixe* de l'adresse MAC

- **ID de groupe** : saisissez un numéro d'ID de groupe VLAN créé par l'utilisateur.

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

Mappage d'un groupe VLAN à un VLAN par interface

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 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 Saisissez les valeurs pour les champs suivants :

- **Type de groupe** : indique que le groupe est basé sur une adresse MAC.
- **Interface** : saisissez une interface générale (port/LAG) par laquelle le trafic est reçu.
- **ID de groupe** : sélectionnez un groupe VLAN, défini sur la page Groupes 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.

VLAN basés sur le 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 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 les protocoles**.

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 de 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**. La page Ajouter un groupe basé sur le protocole s'affiche.

ÉTAPE 3 Saisissez 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).
- **DSAP-SSAP :** entrez ces valeurs pour l'encapsulation LLC.
- **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.

Mappage de groupes basés sur 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 **Configuration des paramètres d'interface VLAN**).

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 protocole aux VLAN**.

Les mappages actuellement définis s'affichent.

ÉTAPE 2 Pour associer une interface à un groupe basé sur protocole au VLAN, cliquez sur **Ajouter**.

ÉTAPE 3 Renseignez les champs suivants.

- **Interface** : numéro de port ou LAG affecté au VLAN conformément au groupe basé sur protocole.
- **ID du groupe** : ID de groupe de protocoles
- **ID VLAN** : attache l'interface à un ID 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 rubrique aborde les points suivants :

- **Présentation du VLAN voix**
- **Configuration du VLAN voix**

Présentation du VLAN voix

Cette rubrique aborde les points suivants :

- **Modes VLAN voix dynamiques**
- **VLAN voix automatique, Port intelligent automatique, CDP et LLDP**
- **QoS VLAN voix**
- **Contraintes du VLAN voix**
- **Flux de travail de VLAN voix**

Vous trouverez ci-après des exemples de déploiement vocal classiques, accompagnés des configurations appropriées :

- **UC3xx/UC5xx hébergé :** tous les téléphones et points d'extrémité VoIP Cisco prennent en charge ce modèle de déploiement. Pour ce modèle (UC3xx/UC5xx), les téléphones et points d'extrémité VoIP Cisco résident sur le même VLAN voix. Par défaut, le VLAN voix de UC3xx/UC5xx est le VLAN 100.
- **PBX IP tiers hébergé :** les téléphones SBTG CP-79xx et SPA5xx ainsi que les points d'extrémité SPA8800 Cisco prennent en charge ce modèle de déploiement. Dans ce modèle, le VLAN utilisé par les téléphones est

déterminé par la configuration réseau. Il peut éventuellement y avoir des VLAN voix et données séparés. Les téléphones et points d'extrémité VoIP s'inscrivent sur un PBX IP sur site.

- **Centrex/ITSP IP hébergé :** les téléphones CP-79xx et SPA5xx ainsi que les points d'extrémité SPA8800 Cisco prennent en charge ce modèle de déploiement. Dans ce modèle, le VLAN utilisé par les téléphones est déterminé par la configuration réseau. Il peut éventuellement y avoir des VLAN voix et données séparés. Les téléphones et points d'extrémité VoIP s'inscrivent sur un proxy SIP hors site dans « le nuage ».

En ce qui concerne le VLAN, les modèles ci-dessus fonctionnent dans des environnements tenant compte du VLAN et ne tenant pas compte du VLAN. Dans l'environnement tenant compte du VLAN, le VLAN voix fait partie des nombreux VLAN configurés dans une installation. L'exemple ne tenant pas compte du VLAN est équivalent à un environnement tenant compte du VLAN avec un seul VLAN.

Le 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 le VLAN 1. Vous avez la possibilité de configurer manuellement un autre VLAN voix. Il peut aussi être appris dynamiquement lorsque la fonction VLAN voix automatique est activée.

Vous pouvez ajouter 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 ont des répercussions sur la façon dont le VLAN voix et/ou les appartenances VLAN des ports sont configurés. Les deux modes s'excluent mutuellement.

- **OUI de téléphonie**

  En mode OUI de téléphonie, le VLAN voix doit être un VLAN configuré manuellement et ne peut pas être le VLAN par défaut.

Lorsque le 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 **Configuration de l'OUI de téléphonie**.

- **VLAN voix automatique**

  En mode VLAN voix automatique, le VLAN voix peut être le VLAN voix par défaut manuellement configuré ou peut être appris à partir de périphériques externes comme UC3xx/5xx et de commutateurs qui annoncent le VLAN voix dans CDP ou VSDP. VSDP est un protocole défini par Cisco pour la détection des services vocaux.

  À la différence du mode OUI de téléphonie qui détecte les périphériques vocaux basés sur le mode OUI de téléphonie, le mode VLAN voix automatique dépend de la fonction Port intelligent automatique pour ajouter dynamiquement les ports au VLAN voix. Si elle est activée, la fonction Port intelligent automatique ajoute un port au VLAN voix lorsqu'elle détecte sur le port un périphérique en cours d'association qui s'annonce en tant que téléphone ou points d'extrémité de média, par l'intermédiaire de CDP et/ou LLDP-MED.

Points d'extrémité vocaux

Pour qu'un VLAN voix fonctionne correctement, les périphériques vocaux tels que les téléphones et points d'extrémité VoIP Cisco doivent être attribués au VLAN pouvant envoyer et recevoir leur trafic vocal. Voici quelques exemples possibles :

- Un téléphone/point d'extrémité peut être configuré de manière statique avec le VLAN voix.
- Un téléphone/point d'extrémité peut obtenir le VLAN voix dans le fichier de démarrage qu'il télécharge à partir d'un serveur TFTP. Un serveur DHCP peut spécifier le fichier de démarrage et le serveur TFTP lorsqu'il attribue une adresse IP au téléphone.
- Un téléphone/point d'extrémité peut obtenir les informations VLAN voix à partir des annonces CDP et LLDP-MED qu'il reçoit de ses systèmes vocaux et commutateurs voisins.

Le 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

Par défaut (paramètres d'usine), CDP, LLDP et LLDP-MED, le mode Port intelligent automatique et le mode de base de QoS avec DSCP de confiance sont activés sur le périphérique, et tous les ports sont membres du VLAN 1 par défaut, qui est aussi le VLAN voix par défaut.

En outre, le mode VLAN voix dynamique est la valeur par défaut du VLAN voix automatique avec activation basée sur le déclenchement, et la fonction Port intelligent automatique est la valeur par défaut à activer en fonction du VLAN voix automatique.

Déclenchements de VLAN voix

Lorsque le mode VLAN voix dynamique est activé sur VLAN voix automatique, cela signifie que le VLAN voix automatique ne devient opérationnel que si un ou plusieurs déclenchements se produisent. Les déclenchements possibles sont la configuration de VLAN voix statique, la réception d'informations VLAN voix dans une annonce de voisinage CDP et la réception d'informations VLAN voix dans le protocole VSDP (Voice VLAN Discovery Protocol). Si vous le souhaitez, vous pouvez rendre le mode VLAN voix automatique immédiatement opérationnel sans attendre de déclenchement.

Si la fonction Port intelligent automatique est activée en fonction du mode VLAN voix automatique, la fonction Port intelligent automatique est activée lorsque le mode VLAN voix automatique devient opérationnel. Si vous le souhaitez, vous pouvez activer la fonction Port intelligent automatique indépendamment du mode VLAN voix automatique.

REMARQUE La liste de configuration par défaut s'applique ici aux commutateurs dont la version du micrologiciel prend directement en charge le mode VLAN voix automatique. Elle s'applique également aux commutateurs non configurés qui ont été mis à niveau vers la version du micrologiciel prenant en charge le mode VLAN voix automatique.

REMARQUE Les déclenchements par défaut et de VLAN voix sont conçus pour n'avoir aucun effet sur les installations ne comportant pas de VLAN voix, ainsi que sur les commutateurs qui ont déjà été configurés. Vous pouvez désactiver et activer manuellement le mode VLAN voix automatique et/ou Port intelligent automatique en fonction de votre déploiement.

VLAN voix automatique

Le mode VLAN voix automatique permet de gérer le VLAN voix, mais dépend de la fonction Port intelligent automatique pour gérer l'appartenance des ports VLAN voix. Le mode VLAN voix automatique offre les fonctions suivantes lorsqu'il est opérationnel :

- Il détecte les informations VLAN voix dans les annonces CDP provenant des périphériques voisins à connexion directe.
- Si plusieurs commutateurs et/ou routeurs voisins, tels que des périphériques Cisco Unified Communication (UC), annoncent leur VLAN voix, le VLAN voix du périphérique ayant l'adresse MAC la plus basse est utilisé.

  REMARQUE : en cas de connexion du 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 de type de source, de la plus haute à la plus basse, sont la configuration VLAN statique, l'annonce CDP et la configuration par défaut basée sur le VLAN par défaut modifié, ainsi que le VLAN voix par défaut. Une adresse MAC numériquement basse a une priorité plus élevée qu'une adresse MAC numériquement haute.
- Il conserve le VLAN voix jusqu'à ce qu'un nouveau VLAN voix provenant d'une source de priorité plus élevée soit détecté ou jusqu'à ce que le mode VLAN voix automatique soit redémarré par l'utilisateur. Après le redémarrage, le 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 : si le périphérique est en mode système de couche 2, il peut uniquement se synchroniser avec les commutateurs compatibles VSDP situés dans le même VLAN de gestion. Si le périphérique est en mode système de couche 3, il peut se synchroniser avec les commutateurs compatibles VSDP, situés sur les sous-réseaux IP à connexion directe 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 le VLAN1 (VLAN par défaut).
- 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 de voix est accepté si l'adresse MAC peut être apprise par la FDB (Forwarding Database). (s'il n'existe aucun espace disponible dans la FDB, aucune action ne se produit).

Flux de travail 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 Gestion des VLAN > VLAN voix > Propriétés.

ÉTAPE 2 Sélectionnez l'ID du VLAN voix. Il ne peut pas être défini sur l'ID de VLAN 1 (cette étape n'est pas obligatoire pour le VLAN voix dynamique).

ÉTAPE 3 Sélectionnez **VLAN voix dynamique** pour activer le mode VLAN voix automatique.

ÉTAPE 4 Sélectionnez la méthode **Activation du VLAN voix automatique**.

REMARQUE : si le périphérique est actuellement en mode OUI de téléphonie, vous devez le désactiver pour pouvoir configurer le mode VLAN voix automatique.

ÉTAPE 5 Cliquez sur **Appliquer**.

ÉTAPE 6 Configurez les ports intelligents comme indiqué dans la section **Tâches courantes de port intelligent**.

ÉTAPE 7 Configurez LLDP/CDP comme décrit respectivement dans les sections **Configuration de LLDP** et **Configuration de CDP**.

ÉTAPE 8 Activez la fonction Port intelligent sur les ports appropriés par l'intermédiaire de la page Port intelligent > Paramètres d'interface.

REMARQUE : les étapes 7 et 8 sont facultatives, car elles sont activées par défaut.

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 OUI de téléphonie sur la page OUI de téléphonie.

ÉTAPE 3 Configurez l'appartenance VLAN OUI de téléphonie pour les ports sur la page Interface des OUI de téléphonie.

Configuration du VLAN voix

Cette section explique comment configurer le VLAN voix. Elle couvre les rubriques suivantes :

- **Configuration des propriétés du VLAN voix**
- **Affichage des Paramètres du VLAN voix automatique**
- **Configuration de l'OUI de téléphonie**

Configuration des propriétés du VLAN voix

Utilisez la page Propriétés du VLAN voix pour effectuer les tâches suivantes :

- Affichez les paramètres de configuration actuels du VLAN voix.
- Configurez l'ID de VLAN du VLAN voix.
- Configurez les paramètres QoS du VLAN voix.
- Configurez le mode VLAN voix (OUI de téléphonie ou VLAN voix automatique).
- Configurez la façon dont le VLAN voix automatique se déclenche.

Pour afficher et configurer les propriétés du VLAN voix :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **Propriétés**.

- 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 Saisissez les valeurs appropriées dans les champs suivants :

- **ID VLAN voix** : entrez le VLAN qui sera le VLAN voix.

  REMARQUE : les modifications apportées à l'ID du VLAN voix, CoS/802.1p et/ou DSCP obligent le 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 réseau de voix. Pour plus d'informations, reportez-vous à *Administration > Détection > LLDP > Stratégie réseau LLDP MED*.

- **DSCP** : sélection de valeurs DSCP utilisées par LLDP-MED en tant que stratégie réseau de voix. Pour plus d'informations, reportez-vous à *Administration > Détection > LLDP > Stratégie réseau LLDP MED*.
- **VLAN voix dynamique** : sélectionnez ce champ pour désactiver ou activer la fonction VLAN voix de l'une des manières suivantes :
  - *Activer le VLAN voix automatique* : active le VLAN voix dynamique en mode VLAN voix automatique.
  - *Activer OUI de téléphonie* : active le VLAN voix dynamique en mode OUI de téléphonie.
  - *Désactiver* : désactive le VLAN voix automatique ou le OUI de téléphonie.
- **Activation du VLAN voix automatique** : sélectionnez l'une des options suivantes pour activer le VLAN voix automatique :
  - *Immédiat* : le VLAN voix automatique 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.

Affichage des Paramètres du VLAN voix automatique

Si le mode VLAN voix automatique est activé, utilisez la page VLAN voix automatique pour afficher les paramètres globaux et d'interface appropriés.

Vous pouvez aussi utiliser cette page pour redémarrer manuellement le VLAN voix automatique, en cliquant sur **Redémarrer VLAN voix automatique**. Au bout de quelques instants, le système rétablit le VLAN voix par défaut, et relance la détection VLAN voix automatique et le processus de synchronisation sur tous les commutateurs du LAN pour lesquels le mode VLAN voix automatique est activé.

REMARQUE Cette opération rétablit uniquement le VLAN voix par défaut si le Type de source a l'état *Inactif*.

Pour afficher les paramètres VLAN voix automatique :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **VLAN voix automatique**.

Le bloc d'état opérationnel figurant sur cette page affiche des informations sur le VLAN voix actuel et sa source :

- **État de VLAN voix automatique** : indique si le VLAN voix automatique est activé.
- **ID du VLAN voix** : identificateur du VLAN voix actuel.
- **Type de source** : indique le type de source où le VLAN voix a été détecté par le périphérique racine.
- **CoS/802.1p** : affiche les valeurs CoS/802.1p utilisées par le LLDP-MED en tant que stratégie réseau de voix.
- **DSCP** : affiche les valeurs DSCP utilisées par le LLDP-MED en tant que stratégie réseau de voix.
- **Adresse MAC commutateur racine** : adresse MAC du périphérique racine VLAN voix automatique qui détecte ou est configuré avec le VLAN voix à partir duquel le VLAN voix est appris.
- **Adresse MAC du commutateur** : adresse MAC de base du périphérique. Si l'adresse MAC de commutateur du périphérique est l'adresse MAC commutateur racine, le périphérique est le périphérique racine VLAN voix automatique.
- **Heure de changement de l'ID VLAN voix** : dernière fois que le VLAN voix a été mis à jour.

ÉTAPE 2 Cliquez sur **Redémarrer VLAN voix automatique** pour rétablir le VLAN voix par défaut et relancer la détection VLAN voix automatique sur tous les commutateurs du LAN pour lesquels la fonction VLAN voix automatique est activée.

La Table locale VLAN voix affiche le VLAN voix configuré sur le 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 d'un UC à partir duquel la configuration de voix a été reçue.

- **Type de source** : type d'UC à partir duquel la configuration de voix a été reçue. Les options suivantes sont disponibles :
  - *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 le LLDP-MED en tant que stratégie réseau de voix
- **DSCP** : valeurs DSCP annoncées ou configurées qui sont utilisées par le LLDP-MED en tant que stratégie réseau de voix
- **Meilleure source locale** : indique si ce VLAN voix a été utilisé par le 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.

Configuration de l'OUI de téléphonie

Les OUI (Organizationally Unique Identifiers) sont attribués par l'autorité d'enregistrement intégrée IEEE (Institute of Electrical and Electronics Engineers). Étant donné que le numéro des fabricants de téléphone IP est limité et connu, les valeurs d'OUI connues entraînent l'affectation automatique au VLAN voix des trames appropriées et du port sur lequel elles sont détectées.

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

Cette rubrique aborde les points suivants :

- **Ajout de OUI à la Table des OUI de téléphonie**
- **Ajout d'interfaces au VLAN voix sur la base des OUI**

Ajout de OUI à la Table des OUI de téléphonie

Utilisez la page OUI de téléphonie pour configurer les propriétés QoS des OUI de téléphonie. Vous pouvez également configurer le Délai d'expiration d'appartenance automatique. Si la période expire sans aucune activité téléphonique, le port est supprimé du VLAN voix.

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

Pour configurer les OUI de téléphonie et/ou ajouter un nouveau OUI de VLAN voix :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **OUI de téléphonie**.

La page OUI de téléphonie contient les champs suivants :

- **État opérationnel OUI de téléphonie** : indique si les OUI sont utilisés pour identifier le trafic vocal.
- **CoS/802.1p** : sélectionnez la file d'attente CoS à attribuer au trafic vocal.
- **Remark CoS/802.1p** : sélectionnez cette option pour re-marquer le trafic sortant.
- **Délai d'expiration d'appartenance automatique** : entrez le délai à l'issue duquel un port doit être supprimé du VLAN vocal une fois que toutes les adresses MAC des téléphones détectés sur les ports ont expiré.

ÉTAPE 2 Cliquez sur **Appliquer** pour intégrer ces valeurs à la Configuration d'exécution du périphérique.

La Table des OUI de téléphonie s'affiche :

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

ÉTAPE 3 Cliquez sur **Restaurer les OUI par défaut** pour supprimer tous les OUI créés par l'utilisateur et conserver uniquement les OUI par défaut dans la table.

Pour supprimer tous les OUI, cochez la case du haut. Tous les OUI sont sélectionnés et peuvent être supprimés en cliquant sur **Supprimer**. Si vous cliquez ensuite sur **Restaurer les OUI par défaut**, le système récupère les OUI connus.

ÉTAPE 4 Pour ajouter un nouveau OUI, cliquez sur **Ajouter**.

ÉTAPE 5 Saisissez les valeurs pour les champs suivants :

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

ÉTAPE 6 Cliquez sur **Appliquer**. Le OUI est ajouté à la Table des OUI de téléphonie.

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

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

- **Tout** : les valeurs de qualité de service (QoS) configurées sur le VLAN voix sont appliquées à toutes les trames entrantes reçues sur l'interface et catégorisées comme VLAN voix.
- **Adresse MAC source de téléphonie** : les valeurs de QoS configurées pour le VLAN voix sont appliquées à toute trame entrante catégorisée comme VLAN voix et contenant un OUI dans l'adresse MAC source qui correspond à un OUI de téléphonie configuré.

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

Pour configurer l'OUI de téléphonie sur une interface :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **VLAN voix** > **Interface des OUI de téléphonie**.

La page Interface des OUI de téléphonie 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 Saisissez les valeurs pour les champs suivants :

- **Interface** : sélectionnez une interface.

- **Adhésion VLAN OUI de téléphonie** : si cette option est activée, l'interface est un port candidat du VLAN voix basé sur les OUI de téléphonie. Lorsque des paquets correspondant à l'un des OUI de téléphonie configurés sont reçus, le port est ajouté au VLAN voix.
- **Mode de QoS OUI de téléphonie** : 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 multidiffusion

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 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 statiquement comme suit :

- Type de port Liaison ou Général (voir **Configuration des paramètres d'interface VLAN**)
- Membre sur le VLAN TV de multidiffusion

Les ports récepteurs de l'abonné ne peuvent être associés au VLAN TV de multidiffusion que s'ils sont définis dans l'un des deux types suivants :

- Port d'accès
- Port client (voir **VLAN TV port client multidiffusion**)

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 **Configuration des paramètres d'interface VLAN**).

La configuration du VLAN TV de multidiffusion est définie pour chaque port. Les ports clients sont configurés pour être membres des VLAN TV de multidiffusion à l'aide de la page VLAN TV de multidiffusion.

IGMP Snooping

Un VLAN TV de multidiffusion s'appuie sur la surveillance IGMP, ce qui signifie les points suivants :

- 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

Caractéristiques des VLAN normaux et des VLAN TV de multidiffusion

	VLAN standard	VLAN TV multidiffusion
Membres du réseau VLAN	La source et tous les ports récepteurs doivent être 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

Flux de travail

Configurez un VLAN TV à l'aide des étapes suivantes :

1. Définissez un VLAN TV en associant un groupe de multidiffusion à un VLAN (à l'aide de la page Groupe 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 TV multidiffusion aux VLAN

Pour définir la configuration d'un VLAN TV de multidiffusion :

ÉTAPE 1 Cliquez sur **Gestion des VLAN** > **Accès VLAN TV port multidiffusion > Groupe multidiffusion aux VLAN.**

Les champs suivants sont affichés :

- **Groupe multidiffusion** : adresse IP du groupe de multidiffusion.
- **VLAN TV de multidiffusion** : VLAN auquel les paquets de multidiffusion sont affectés.

ÉTAPE 2 Cliquez sur **Ajouter** pour associer un groupe de multidiffusion à un VLAN. Vous pouvez sélectionner n'importe quel VLAN. Lorsqu'un VLAN est sélectionné, il devient un VLAN TV de multidiffusion.

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 le champ **VLAN TV de multidiffusion.**

ÉTAPE 3 La liste **Ports d'accès candidats** contient tous les ports d'accès configurés sur le périphérique. Déplacez les ports requis depuis le champ **Ports d'accès candidats** vers le champ **Ports d'accès membres.**

ÉTAPE 4 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
- 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 multidiffusion

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 Gestion des VLAN > 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 Gestion des VLAN > Paramètres d'interface).
3. Créez un VLAN TV de multidiffusion comportant un maximum de 4 094 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.

Mappage de VLAN CPE aux VLAN TV de multidiffusion

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 de multidiffusion du port client > 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 CPE du port multidiffusion

Les ports associés aux VLAN de multidiffusion doivent être configurés en tant que ports clients (voir **Configuration des paramètres d'interface VLAN**).

Utilisez la page Appartenance VLAN du port multidiffusion pour mapper ces ports aux VLAN TV de multidiffusion, comme décrit à la section **Appartenance VLAN du port multidiffusion**.

14

Arbre recouvrant

Cette section décrit le protocole STP (Spanning Tree Protocol) (IEEE802.1D et IEEE802.1Q) et couvre les rubriques suivantes :

- **Types de STP**
- **Configuration de l'état STP et des paramètres globaux**
- **Définition des paramètres d'interface du Spanning Tree**
- **Configuration des paramètres Rapid Spanning Tree**
- **Multiple Spanning Tree**
- **Définition des propriétés MSTP**
- **Mappage des VLAN à une instance MSTP**
- **Définition des paramètres d'instance MSTP**
- **Définition des paramètres de l'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 arrêtent de transférer des données d'utilisateur pendant un moment. Les liens sont automatiquement réactivés lorsque la topologie permet à nouveau le transfert de données.

Des boucles se produisent lorsque des routes alternatives existent entre les hôtes. Les boucles d'un réseau étendu peuvent utiliser des commutateurs pour acheminer indéfiniment le trafic, ce qui augmente la charge de ce dernier et diminue l'efficacité du réseau.

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

Le 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) : le protocole MSTP est basé sur le protocole 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 (Layer 2), il peut se produire une situation où une boucle se crée dans le VLAN A mais pas dans le VLAN B. Si les deux VLAN sont définis sur un port X et que STP souhaite réduire la boucle, le protocole stoppe le trafic sur tout le port, y compris celui du VLAN B.

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

Configuration de l'état STP et des paramètres globaux

La page État et paramètres globaux STP contient les paramètres permettant d'activer le protocole STP, RSTP ou MSTP.

Utilisez respectivement la page Paramètres d'interface STP, la page Paramètres d'interface RSTP et la page Propriétés MSTP pour configurer chaque mode.

Pour définir l'état et les paramètres globaux STP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **État STP et paramètres globaux**.

ÉTAPE 2 Saisissez les paramètres.

Paramètres globaux :

- **Spanning Tree State** : activez ou désactivez le protocole STP 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 sont utilisés pour transmettre des informations du Spanning Tree.
  - *Filtrage* : filtre les paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
  - *Inondation* : inonde les paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
- **Valeurs par défaut du coût de chemin** : sélectionne la méthode utilisée pour assigner des coûts de chemin par défaut aux ports STP. Le coût de chemin par défaut assigné à une interface varie selon la méthode sélectionnée.
  - *Court* : spécifie la plage de 1 à 65 535 pour les coûts de chemin des ports.
  - *Long* : spécifie la plage de 1 à 200 000 000 pour les coûts de chemin des ports.

Paramètres des ponts :

- **Priorité** : définit la valeur de priorité du pont. Après l'échange de BPDU, le périphérique de priorité inférieure devient le pont racine. Si tous les ponts utilisent la même priorité, leurs adresses MAC sont alors utilisées pour déterminer le pont racine. La valeur de priorité du pont est fournie par paliers de 4096. Par exemple 4096, 8192, 12 288, etc.
- **Délai Hello** : définissez le temps d'attente en secondes d'un pont racine entre deux messages de configuration.
- **Délai 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 durant laquelle le pont reste en mode d'apprentissage avant de transférer des paquets. Pour plus d'informations, reportez-vous à la section **Définition des paramètres d'interface du Spanning Tree**.

Racine désignée :

- **ID du pont** : la priorité du pont est concaténée avec l'adresse MAC du périphérique.
- **ID du pont racine** : la priorité du pont racine est concaténée avec l'adresse MAC du pont racine.
- **Port racine** : port proposant un chemin de coût inférieur entre ce pont et le pont racine. (Cette information est importante lorsque le pont n'est pas le pont racine.)
- **Coût d'acheminement vers la racine** : affiche le coût d'acheminement entre ce pont et le pont racine.
- **Nombre de changements de topologie** : nombre total des changements de topologie STP effectués.
- **Dernier changement de topologie** : intervalle de temps écoulé depuis le dernier changement de topologie. Cette durée s'affiche au format jours/heures/minutes/secondes.

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

Définition des paramètres d'interface du Spanning Tree

La page Paramètres d'interface STP vous permet de configurer 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 **Spanning Tree** > **Paramètres d'interface STP**.

ÉTAPE 2 Sélectionnez une interface et cliquez sur **Modifier**.

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.
- **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 sont utilisés pour transmettre des informations du Spanning Tree.
  - *Utiliser les paramètres globaux* : sélectionnez cette option pour utiliser les paramètres définis sur la page État et paramètres globaux STP.
  - *Filtrage* : filtre les paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
  - *Inondation* : inonde les paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
- **Coût de chemin** : définissez la contribution du port au coût du chemin racine ou utilisez le coût par défaut généré par le système.
- **Priorité** : définissez la valeur de priorité du port. La valeur de priorité influence le choix du port lorsqu'un pont dispose de deux ports connectés au sein d'une boucle. La priorité est une valeur comprise entre 0 et 240, et fonctionne par multiples de 16.
- **État du port** : affiche l'état STP actuel d'un port.
  - *Désactivé* : le protocole STP est actuellement désactivé sur le port. Le port transfère le trafic tout en apprenant les adresses MAC.
  - *Blocage* : le port est actuellement bloqué et ne peut ni transférer le trafic (à l'exception des données BPDU) ni connaître les adresses MAC.
  - *Écoute* : le port est en mode Écoute. Il ne peut ni transférer le trafic ni connaître les adresses MAC.
  - *Apprentissage* : le port est en mode Apprentissage. Il ne peut pas transférer le trafic mais il peut prendre connaissance de nouvelles adresses MAC.
  - *Transfert* : le port est en mode Transfert. Il peut réacheminer du trafic et apprendre de nouvelles adresses MAC.
- **ID du pont désigné** : affiche la priorité du pont et les adresses MAC du pont désigné.
- **ID du port désigné** : affiche la priorité et l'interface du port sélectionné.
- **Coût désigné** : affiche le coût du port participant à la topologie STP. Les ports de coûts inférieurs sont peu susceptibles d'être bloqués si STP détecte des boucles.

- **Transitions de transfert** : affiche le nombre de fois où le port est passé de l'état **Blocage** à l'état **Transfert**.
- **Vitesse** : affiche la vitesse du port.
- **LAG** : affiche le LAG auquel appartient le port. Si un port est membre d'un LAG, les paramètres du LAG remplacent ceux du port.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres d'interface sont écrits dans le fichier de Configuration d'exécution.

Configuration des paramètres Rapid Spanning Tree

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

La page Paramètres d'interface RSTP vous permet de configurer 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 **Spanning Tree** > **État STP et paramètres globaux**. Activez **RSTP**.

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

ÉTAPE 3 Sélectionnez un port.

REMARQUE : l'activation de la migration des protocoles est uniquement disponible après avoir sélectionné le port connecté au pont associé en cours de test.

ÉTAPE 4 Si un partenaire de lien est détecté via STP, cliquez sur **Activer la migration des protocoles** pour effectuer un test de migration des protocoles. Cette opération détecte si le lien associé utilisant le protocole STP existe toujours et, si c'est le cas, s'il a migré vers RSTP ou MSTP. S'il existe toujours en tant que lien STP, le périphérique continue de communiquer avec lui via STP. En revanche, s'il a migré vers RSTP ou MSTP, le périphérique communique avec lui via, respectivement, RSTP ou MSTP.

ÉTAPE 5 Sélectionnez une interface et cliquez sur **Modifier**.

ÉTAPE 6 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 du lien point à point. Les ports définis en tant que Full Duplex sont considérés comme liens de port point à point.
  - *Activer* : ce port devient un port de bordure RSTP lorsque cette option est activée et il est placé rapidement en mode Transfert (généralement en 2 secondes).
  - *Désactiver* : le port n'est pas considéré comme port point à point pour le RSTP ; par conséquent, STP fonctionne sur ce port à une vitesse normale et non à 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 afin de fournir des chemins STP. Les rôles possibles sont :
  - *Racine* : chemin de coût inférieur pour transférer des paquets au pont racine.
  - *Désigné* : interface par laquelle le pont est relié au LAN et qui fournit le chemin de coût inférieur depuis le LAN vers le pont racine.
  - *Secondaire* : fournit un chemin alternatif de l'interface racine au pont racine.
  - *Sauvegarde* : fournit un chemin de sauvegarde pour le chemin de port désigné vers les nœuds terminaux STP. Cela fournit une configuration dans laquelle deux ports sont reliés dans une boucle par un lien point à point. Des ports de secours sont également utilisés lorsqu'un LAN possède deux ou plusieurs connexions établies à un segment partagé.
  - *Désactivé* : le port ne participe pas au Spanning Tree.
- **Mode** : affiche le mode Spanning Tree actuel : RSTP ou STP classique.

- **État opérationnel Fast Link** : indique si Fast Link (port de bordure) est activé, désactivé ou automatique pour l'interface. Les valeurs disponibles sont les suivantes :
  - *Activé* : Fast Link est activé.
  - *Désactivé* : Fast Link est désactivé.
  - *Auto* : le mode Fast Link s'active quelques secondes après l'activation de l'interface.
- **État des ports** : affiche l'état RSTP sur le port spécifique.
  - *Désactivé* : le protocole STP est actuellement désactivé sur le port.
  - *Blocage* : le port est actuellement bloqué et ne peut ni transférer le trafic ni connaître les adresses MAC.
  - *Écoute* : le port est en mode Écoute. Il ne peut ni transférer le trafic ni connaître les adresses MAC.
  - *Apprentissage* : le port est en mode Apprentissage. Il ne peut pas transférer le trafic mais il peut prendre connaissance des nouvelles adresses MAC.
  - *Transfert* : le port est en mode Transfert. Il peut réacheminer du trafic et apprendre de nouvelles adresses MAC.

ÉTAPE 7 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Multiple Spanning Tree

Le protocole MSTP (Multiple Spanning Tree Protocol) est utilisé pour séparer l'état du port STP entre différents domaines (sur différents réseaux 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 Transfert dans une autre instance STP. La page Propriétés MSTP permet de définir les paramètres MSTP globaux.

Pour configurer MSTP :

1. Définissez le mode de fonctionnement STP sur MSTP comme décrit à la page **Configuration de l'état STP et des paramètres globaux** .
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 **Mappage des VLAN à une instance MSTP**.

3. Décidez quelle instance MSTP est active dans quel VLAN et associez ces instances MSTP aux VLAN en conséquence.
4. Pour configurer les attributs MSTP :
   - **Définition des propriétés MSTP**
   - **Définition des paramètres d'instance MSTP**
   - **Mappage des VLAN à une instance MSTP**

Définition des propriétés MSTP

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

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

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

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

Ce mappage peut être effectué sur la page VLAN vers instance MST.

Utilisez cette page si le système fonctionne en mode MSTP.

Pour définir MSTP :

ÉTAPE 1 Cliquez sur **Spanning Tree** > **État STP et paramètres globaux**. Activez MSTP.

ÉTAPE 2 Cliquez sur **Spanning Tree** > **MSTP Propriétés**.

ÉTAPE 3 Saisissez les paramètres.

- **Nom de région** : définissez un nom de région MSTP.
- **Révision** : définissez un nombre non affecté d'un signe à 16 octets qui identifie la révision de la configuration MST actuelle. Ce champ est compris entre 0 et 65535.
- **Sauts max.** : définissez le nombre total des sauts se produisant dans une région spécifique avant la désactivation du BPDU. Lorsque le BPDU est désactivé, les informations du port sont obsolètes. Ce champ est compris entre 1 et 40.
- **Maître IST** : affiche le maître de la région.

ÉTAPE 4 Cliquez sur **Appliquer**. Les propriétés MSTP sont définies et le fichier de Configuration d'exécution est mis à jour.

Mappage des VLAN à une 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.

Vous pouvez définir jusqu'à sept instances MST (prédéfinies de 1 à 7) sur les commutateurs de la série 300, en plus de l'instance zéro.

Le périphérique mappe automatiquement sur l'instance CIST (Core and Internal Spanning Tree) les réseaux VLAN qui ne sont pas explicitement mappés sur 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 **Spanning Tree** > **VLAN d'une instance MSTP**.

La page VLAN vers instance MSTP contient les champs suivants :

- **ID d'instance MST** : 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 Saisissez les paramètres.

- **ID d'instance MST** : sélectionnez l'instance MST.
- **VLAN** : définissez les VLAN à mapper sur 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.

Définition des 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 **Spanning Tree** > **Paramètres de l'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.
- **Sauts restants** : affiche le nombre de sauts restant jusqu'à la prochaine destination.

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

Définition des paramètres de l'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 **Spanning Tree** > **Paramètres d' interface MSTP**.

ÉTAPE 2 Saisissez les paramètres.

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

ÉTAPE 3 Cliquez sur **OK**. Les paramètres MSTP pour les interfaces de l'instance s'affichent.

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

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 spécifiée et l'instance MST.
- **Coût de chemin** : entrez la contribution du port au coût du chemin racine dans la zone de texte **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 connaître les adresses MAC.
  - *Écoute* : le port sur cette instance est en mode Écoute. Il ne peut ni transférer le trafic ni connaître les adresses MAC.
  - *Apprentissage* : le port sur cette instance est en mode Apprentissage. Il ne peut pas transférer le trafic mais 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 de limite. 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 vers cette interface fournit le chemin de coût inférieur pour transférer les paquets vers le périphérique racine.
  - *Désigné* : interface par laquelle le pont est relié au LAN et qui fournit le chemin de coût inférieur depuis le LAN vers le pont racine pour l'instance MST.
  - *Secondaire* : l'interface fournit un chemin alternatif de l'interface racine au périphérique racine.

- *Secours* : l'interface fournit un chemin de secours pour le chemin de port désigné vers les nœuds terminaux du Spanning Tree. Des ports de secours existent lorsque deux ports sont reliés dans une boucle par un lien point à point. Des ports de secours apparaissent également lorsqu'un LAN possède deux ou plusieurs connexions établies à un segment partagé.
- *Désactivé* : l'interface ne participe pas au Spanning Tree.
- *Limite* : le port sur cette instance est un port de limite. 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 de limite 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.
  - *Interne* : le port est un port interne.
- **ID de pont désigné** : affiche le numéro d'ID du pont qui connecte le lien ou le LAN partagé à la racine.
- **ID du port désigné** : affiche le numéro d'ID du port sur le pont désigné qui connecte le lien ou le LAN partagé à la racine.
- **Coût désigné** : affiche le coût du port participant à la topologie STP. Les ports de coûts inférieurs sont peu susceptibles d'être bloqués si STP détecte des boucles.
- **Sauts restants** : affiche le nombre de sauts restant jusqu'à la prochaine destination.
- **Transitions de transfert** : affiche le nombre de fois où le port est passé du mode Transfert au mode Blocage.

ÉTAPE 6 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

15

Gestion des tables d'adresses MAC

Cette section vous explique comment ajouter des adresses MAC au système. Elle couvre les rubriques suivantes :

- **Configuration d'adresses MAC statiques**
- **Gestion des adresses MAC dynamiques**
- **Définition d'adresses MAC réservées**

Types d'adresses MAC

Il existe deux types d'adresses MAC : statiques et dynamiques. En fonction de leur type, les adresses MAC sont stockées avec les informations relatives aux VLAN et aux ports soit dans la table des *adresses statiques*, soit dans la table des *adresses dynamiques*.

Les adresses statiques sont configurées par l'utilisateur et n'expirent donc jamais.

Une nouvelle adresse MAC source qui apparaît dans une trame reçue par le 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. On les appelle des trames de monodiffusion inconnue.

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

Configuration d'adresses MAC statiques

Les adresses MAC statiques sont affectées à une interface physique et à un VLAN spécifiques sur le périphérique. Si cette adresse est détectée sur une autre interface, elle est ignorée et n'est pas consignée dans la table des adresses.

Pour définir une adresse statique :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC > Adresses statiques**.

La page Adresses statiques affiche les adresses statiques actuellement définies.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **ID de VLAN** : sélectionnez l'ID de VLAN du port.
- **Adresse MAC** : saisissez l'adresse MAC de l'interface.
- **Interface** : sélectionnez une interface (port ou LAG) pour l'entrée.
- **État** : sélectionnez le mode de traitement de l'entrée. Les options sont les suivantes :
  - *Permanent* : le système ne supprime jamais cette adresse MAC. Si l'adresse MAC statique est enregistrée dans la Configuration de démarrage, elle est conservée après redémarrage.
  - *Suppr. à la réinitialisation* : l'adresse MAC statique est supprimée lorsque le périphérique est réinitialisé.
  - *Supprimer à l'expiration* : l'adresse MAC est supprimée à expiration du délai.
  - *Sécurisé* : l'adresse MAC est sécurisée lorsque l'interface est en mode verrouillé classique (voir **Configuration de la sécurité des ports**).

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

Gestion des adresses MAC dynamiques

La table des adresses dynamiques (table de pontage) contient les adresses MAC obtenues en surveillant les adresses source des trames entrant dans le périphérique.

Pour éviter de surcharger cette table et pour garder de l'espace pour de nouvelles adresses MAC, une adresse est supprimée si elle n'enregistre aucun trafic pendant une période donnée. Ce délai correspond au délai d'expiration.

Configuration du délai d'expiration d'adresses MAC dynamiques

Pour configurer le délai d'expiration des adresses dynamiques :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC > Paramètres des adresses dynamiques**.

ÉTAPE 2 Saisissez le **Délai d'expiration**. Le délai d'expiration est une valeur comprise entre la valeur configurée par l'utilisateur et deux fois cette valeur moins 1. Par exemple, si vous avez entré 300 secondes, le délai d'expiration sera compris entre 300 et 599 secondes.

ÉTAPE 3 Cliquez sur **Appliquer**. Le délai d'expiration est mis à jour.

Interrogation d'adresses dynamiques

Pour interroger la table des adresses dynamiques :

ÉTAPE 1 Cliquez sur **Tables d'adresses MAC> Adresses dynamiques**.

ÉTAPE 2 Dans le bloc *Filtre*, vous pouvez saisir les critères d'interrogation suivants :

- **ID de VLAN** : saisissez l'ID de VLAN pour lequel la table est interrogée.
- **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 Renseignez le champ **Clé de tri de la table des adresses dynamiques** en fonction duquel la table est triée. La table des adresses peut être triée en fonction de l'ID de VLAN, de l'adresse MAC ou de l'interface.

ÉTAPE 4 Cliquez sur **OK**. La Table des adresses MAC dynamiques est interrogée et les résultats s'affichent.

Cliquez sur **Effacer la table** pour supprimer toutes les adresses MAC dynamiques.

Définition d'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**. La page Adresses MAC réservées s'ouvre.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les valeurs pour les champs suivants :

- **Adresse MAC** : sélectionnez l'adresse MAC à réserver.
- **Type de trame** : sélectionnez un type de trame en fonction des critères suivants :
  - *Ethernet V2* : s'applique aux paquets Ethernet V2 avec l'adresse MAC spécifique.
  - *LLC* : s'applique aux paquets LLC (Logical Link Control) avec l'adresse MAC spécifique.
  - *LLC-SNAP* : s'applique aux paquets LLC-SNAP (Logical Link Control/ Sub-Network Access Protocol) avec l'adresse MAC spécifique.
  - *Tout* : s'applique à tous les paquets avec l'adresse MAC spécifique.
- **Action** : sélectionnez l'une des actions suivantes qui sera appliquée au paquet entrant correspondant aux critères sélectionnés :
  - *Abandonner* : supprime le paquet.
  - *Pont* : transfère le paquet à tous les membres du VLAN.

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

16

Multidiffusion

Cette section décrit la fonction de transfert de multidiffusion et couvre les rubriques suivantes :

- **Transfert de multidiffusion**
- **Définition des propriétés de multidiffusion**
- **Ajout d'une adresse MAC de groupe**
- **Ajout d'adresses IP de groupe de multidiffusion**
- **Configuration de la surveillance de trafic IGMP**
- **Surveillance MLD**
- **Interrogation du groupe de multidiffusion IP IGMP/MLD**
- **Définition des ports de routeur de multidiffusion**
- **Définition de la multidiffusion Tout transférer**
- **Définition des paramètres de multidiffusion non enregistrée**

Transfert de multidiffusion

Le transfert de multidiffusion permet la transmission d'informations en mode 1-à-n. Les applications de multidiffusion sont particulièrement utiles pour transmettre des informations à plusieurs clients lorsque ces clients n'ont pas besoin de l'intégralité du service disponible. Ceci est par exemple le cas dans le cadre d'une application de TV par câble où les clients peuvent contacter une chaîne au milieu d'une transmission et interrompre la connexion avant la fin.

Les données ne sont envoyées qu'aux ports pertinents. Le fait de ne transférer les données qu'aux ports concernés permet d'économiser de la bande passante et des ressources d'hôte sur la liaison.

Pour que le transfert de multidiffusion fonctionne sur des sous-réseaux IP, les nœuds et les routeurs doivent être compatibles avec la multidiffusion. Un nœud compatible avec la multidiffusion doit pouvoir :

- Envoyer et recevoir des paquets de multidiffusion
- Enregistrer les adresses de multidiffusion que le nœud écoute auprès des routeurs locaux afin que les routeurs locaux et distants puissent acheminer le paquet de multidiffusion vers les nœuds.

Configuration de multidiffusion typique

Alors que les routeurs de multidiffusion acheminent les paquets de multidiffusion d'un sous-réseau IP à un autre, les commutateurs Couche 2 compatibles avec la multidiffusion transfèrent les paquets de multidiffusion vers les nœuds enregistrés d'un LAN ou d'un VLAN.

La configuration typique inclut un routeur qui transfère les flux de multidiffusion d'un réseau IP privé et/ou public à l'autre, un périphérique doté de fonctions de traçage (Snooping) IGMP (Internet Group Membership Protocol, protocoles d'appartenance aux groupes Internet) ou MLD (Multicast Listener Discovery, détection des services d'écoute de multidiffusion) et un client de multidiffusion qui souhaite recevoir un flux de multidiffusion. Dans cette configuration, le routeur envoie des requêtes IGMP à intervalle régulier.

REMARQUE MLD pour IPv6 provient d'IGMP v2 pour IPv4. Même si la description de cette section concerne principalement IGMP, elle décrit également l'utilisation de MLD lorsque cela s'applique.

Ces requêtes atteignent le périphérique, qui répond en transmettant les requêtes au VLAN et en reconnaissant le port où réside un routeur de multidiffusion (Mrouter). Lorsqu'un hôte reçoit le message de requête IGMP, il répond en envoyant un message d'adhésion IGMP indiquant que l'hôte souhaite recevoir un flux de multidiffusion spécifique en provenance (facultatif) d'une source spécifique. Le périphérique avec fonction de traçage IGMP Snooping analyse les messages d'adhésion et apprend que le flux de multidiffusion demandé par l'hôte doit être transféré à ce port spécifique. Il transfère ensuite l'adhésion IGMP, uniquement vers le routeur Mrouter. De même, lorsque le routeur Mrouter reçoit un message d'adhésion IGMP, il apprend que l'interface à partir de laquelle il a reçu ce message souhaite recevoir un flux de multidiffusion spécifique. Le routeur Mrouter transfère le flux de multidiffusion demandé vers l'interface.

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 le périphérique possède une fonction de traçage IGMP/MLD Snooping et qu'il reçoit une trame de flux de multidiffusion, il la transfère à tous les ports enregistrés pour recevoir le flux de multidiffusion en question à l'aide de messages d'adhésion IGMP.

Le périphérique peut transférer des flux de multidiffusion sur la base de l'une des options suivantes :

- Adresse MAC de groupe de multidiffusion
- Adresse IP de multidiffusion de groupe (G)
- Combinaison de l'adresse IP source (S) et de l'adresse IP de multidiffusion de groupe (G) du paquet de multidiffusion

Vous ne pouvez configurer qu'une seule de ces options pour chaque VLAN.

Le système gère des listes de groupes de multidiffusion pour chaque VLAN. Ceci permet de gérer les informations de multidiffusion que chaque port doit recevoir. Les groupes de multidiffusion et les ports destinataires associés peuvent être configurés de manière statique ou appris de manière dynamique via le traçage de protocole IGMP Snooping ou MLD (Multicast Listener Discovery) Snooping.

L'enregistrement de multidiffusion est le processus qui consiste à écouter les protocoles d'enregistrement de multidiffusion et à y répondre. Les protocoles disponibles sont IGMP pour IPv4 et MLD pour IPv6.

Lorsque le traçage IGMP/MLD Snooping est activé sur le périphérique d'un VLAN, il analyse les paquets IGMP/MLD qu'il reçoit à partir du VLAN connecté au périphérique et à tous les routeurs de multidiffusion du réseau.

Lorsqu'un périphérique apprend qu'un hôte utilise des messages IGMP/MLD pour enregistrer un flux de multidiffusion, éventuellement à partir d'une source spécifique, ce périphérique ajoute l'enregistrement à sa base MFDB (Multicast Forwarding Data Base, base de données de transfert de multidiffusion).

Le traçage IGMP/MLD Snooping peut réduire le trafic de multidiffusion en provenance d'applications IP grosses consommatrices de bande passante de flux. Un périphérique qui utilise le traçage IGMP/MLD Snooping ne transfère le trafic de multidiffusion que vers les hôtes intéressés par ce trafic. Cette réduction du trafic de multidiffusion diminue la charge de traitement des paquets sur le périphérique et réduit la charge de travail des hôtes puisqu'ils n'ont pas besoin de recevoir tout le trafic de multidiffusion généré sur le réseau et de le filtrer.

Les versions suivantes sont prises en charge :

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

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

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.

Propriétés d'adresse de multidiffusion

Les adresses de multidiffusion possèdent les propriétés suivantes :

- Chaque adresse de multidiffusion IPv4 se trouve dans la plage d'adresses situées entre 224.0.0.0 et 239.255.255.255.
- L'adresse de multidiffusion IPv6 est FF00:/8.
- Pour mapper une adresse IP de multidiffusion de groupe sur une adresse de multidiffusion Couche 2 :
  - Pour IPv4, le mappage s'effectue en prenant les 23 bits de poids faible (de droite) de l'adresse IPv4 et en les ajoutant au préfixe 01:00:5e. Normalement, les neuf bits supérieurs de l'adresse IP sont ignorés et toutes les adresses IP qui diffèrent uniquement par ces bits supérieurs sont mappées sur la même adresse Couche 2 puisque les 23 bits inférieurs utilisés sont identiques. Par exemple, l'adresse 234.129.2.3 est mappée sur l'adresse MAC de groupe de multidiffusion 01:00:5e:01:02:03. Il est possible de mapper jusqu'à 32 adresses IP de multidiffusion de groupe sur une même adresse Couche 2.

- Pour IPv6, le processus de mappage utilise les 32 bits de poids faible (de droite) de l'adresse de multidiffusion et ajoute le préfixe 33:33. Par exemple, l'adresse de multidiffusion IPv6 FF00:1122:3344 est mappée sur l'adresse de multidiffusion Couche 2 33:33:11:22:33:44.

Définition des propriétés de multidiffusion

La page Propriétés permet de configurer l'état de filtrage multidiffusion par ponts.

Par défaut, toutes les trames de multidiffusion sont envoyées sur tous les ports du VLAN. Pour ne transférer les données, de façon sélective, que vers les ports concernés et filtrer (éliminer) le flux de multidiffusion sur les autres ports, activez le filtrage multidiffusion par ponts sur la page Propriétés.

Si le filtrage est activé, les trames de multidiffusion sont transférées vers un sous-ensemble des ports sur le VLAN concerné, comme il aura été défini dans la base MFDB (Multicast Forwarding Data Base, base de données de transfert de multidiffusion). Le filtrage multidiffusion s'exerce sur l'ensemble du trafic. Par défaut, ce type de trafic est envoyé à tous les ports concernés mais vous pouvez limiter le transfert à un sous-ensemble plus réduit.

L'une des méthodes couramment utilisées de représentation des membres de multidiffusion est la notation (S,G), où S représente la source (unique) qui envoie un flux de données de multidiffusion et G représente l'adresse IPv4 ou IPv6 de groupe. Si un client Multicast peut recevoir du trafic de multidiffusion à partir de n'importe quelle source d'un groupe de multidiffusion donné, celui-ci est enregistré sous (*,G).

Voici différentes méthodes de transfert des trames de multidiffusion :

- **Adresse MAC de groupe** : basée sur l'adresse MAC de destination dans la trame Ethernet.

  REMARQUE : comme indiqué précédemment, il est possible de mapper une ou plusieurs adresses IP de multidiffusion de groupe sur une seule adresse MAC de groupe. Le transfert basé sur une adresse MAC de groupe peut provoquer le transfert d'un flux de multidiffusion IP vers des ports qui ne possèdent aucun récepteur pour ce flux.

- **Adresse IP de groupe** : basée sur l'adresse IP de destination du paquet IP (*,G).
- **Adresse IP source de groupe** : basée à la fois sur l'adresse IP de destination et l'adresse IP source du paquet IP (S,G).

En sélectionnant le mode de transfert, vous pouvez définir la méthode utilisée par le matériel pour identifier le flux de multidiffusion à l'aide de l'une des options suivantes : Adresse MAC de groupe, Adresse IP de groupe ou Adresse IP source de groupe.

(S,G) est pris en charge par IGMPv3 et MLDv2 alors qu'IGMPv1/2 et MLDv1 ne prennent en charge que (*.G), qui inclut uniquement l'ID de groupe.

Le périphérique peut prendre en charge jusqu'à 256 adresses de groupe de multidiffusion statiques et dynamiques.

Pour activer le filtrage multidiffusion et sélectionner la méthode de transfert :

ÉTAPE 1 Cliquez sur **Multidiffusion > Propriétés**.

ÉTAPE 2 Saisissez les paramètres.

- **État du filtrage multidiffusion par ponts** : sélectionnez cette option pour activer le filtrage.
- **ID VLAN** : sélectionnez l'ID du VLAN voulu pour définir sa méthode de transfert.
- **Méthode de transfert pour IPv6** : choisissez l'une des méthodes de transfert suivantes pour les adresses IPv6 : Adresse MAC de groupe, Adresse IP de groupe ou Adresse IP source de groupe.
- **Méthode de transfert pour IPv4** : choisissez l'une des méthodes de transfert suivantes pour les adresses IPv4 : Adresse MAC de groupe, Adresse IP de groupe ou Adresse IP source de groupe.

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

Ajout d'une adresse MAC de groupe

Le périphérique prend en charge le transfert du trafic de multidiffusion entrant sur la base des informations de groupe de multidiffusion. Ces informations sont tirées des paquets IGMP/MLD reçus ou résultent d'une configuration manuelle. Elles sont stockées dans la base MFDB (Multicast Forwarding Database, base de données de transfert de multidiffusion).

Lorsque le système reçoit une trame d'un VLAN configuré pour transférer les flux de multidiffusion sur la base des adresses MAC de groupe et que l'adresse de destination est une adresse de multidiffusion Couche 2, la trame est transférée vers tous les ports membres de l'adresse MAC de groupe.

La page Adresse de groupe MAC offre les fonctions suivantes :

- Interrogation et affichage d'informations tirées de la base de données de filtrage multidiffusion concernant un ID de VLAN spécifique ou un groupe particulier d'adresses MAC. Ces données sont acquises de manière dynamique par traçage IGMP/MLD Snooping ou de manière statique par saisie manuelle.
- Ajout ou suppression d'entrées statiques dans la base MFDB, qui fournit des informations de transfert statiques basées sur les adresses MAC de destination.
- Affichage de la liste de tous les ports/LAG membres de chaque ID de VLAN ou adresse MAC de groupe, et indication précisant si le trafic doit ou non être transféré vers cette destination.

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

Pour définir et afficher des groupes de multidiffusion MAC :

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

ÉTAPE 2 Saisissez les paramètres.

- **ID VLAN est égal à** : saisissez l'ID de VLAN du groupe à afficher.
- **Adresse MAC de groupe égale à** : définissez l'adresse MAC du groupe de multidiffusion à afficher. Si aucune adresse MAC de groupe n'est indiquée, la page 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.

Le système affiche les entrées qui ont été créées sur cette page et sur la page Adresse IP de groupe de multidiffusion. Pour celles qui ont été créées sur la page Adresse IP de groupe de multidiffusion, les adresses IP sont converties en adresses MAC.

ÉTAPE 4 Cliquez sur **Ajouter** pour ajouter une adresse MAC de groupe statique.

ÉTAPE 5 Saisissez les paramètres.

- **ID VLAN** : définit l'ID de VLAN du nouveau groupe de multidiffusion.
- **Adresse de groupe MAC** : définit l'adresse MAC du nouveau groupe de multidiffusion.

ÉTAPE 6 Cliquez sur **Appliquer** et l'adresse MAC du groupe de multidiffusion est 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**.

Les informations contenues sur la page sont :

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

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

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

ÉTAPE 9 Sélectionnez la façon dont chaque interface est associée au groupe de multidiffusion :

- **Statique** : rattache l'interface au groupe de multidiffusion en tant que membre statique.
- **Dynamique** : indique que l'interface a été ajoutée au groupe de multidiffusion via le traçage IGMP/MLD Snooping.
- **Interdit** : spécifie que ce port n'est pas autorisé à rejoindre ce groupe sur ce VLAN.
- **Aucun** : spécifie que le port n'est actuellement pas membre de ce groupe de multidiffusion sur ce VLAN.

ÉTAPE10 Cliquez sur **Appliquer** ; le fichier de Configuration d'exécution est mis à jour.

REMARQUE : les entrées qui ont été créées sur la page Adresse IP de groupe de multidiffusion ne peuvent pas être supprimées sur cette page (même si elles sont sélectionnées).

Ajout d'adresses IP de groupe de multidiffusion

La page Adresse IP de groupe de multidiffusion est identique à la page Adresse de groupe MAC, à la seule différence que les groupes de multidiffusion y sont identifiés par leurs adresses IP.

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

Pour définir et afficher des IP de multidiffusion de groupes :

ÉTAPE 1 Cliquez sur **Multidiffusion > Adresse IP de multidiffusion de groupe**.

La page 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 multidiffusion de groupe égale à** : définissez l'adresse IP de multidiffusion du groupe à afficher. Cela s'applique uniquement lorsque le mode de transfert est (S,G).
- **Adresse IP source est égale à** : définissez l'adresse IP source du périphérique émetteur. Si le mode est (S,G), saisissez la valeur S (indiquant l'expéditeur). Combinée à l'adresse IP de groupe, cette valeur définit l'ID de multidiffusion du groupe (S,G) à afficher. Si le mode est (*.G), saisissez un astérisque (*) pour indiquer que le groupe de multidiffusion n'est défini que par sa destination.

ÉTAPE 3 Cliquez sur **OK**. Les résultats s'affichent dans le bloc inférieur. Lorsque vous activez à la fois Bonjour et IGMP sur un périphérique en mode système Couche 2, l'adresse IP de multidiffusion de Bonjour apparaît. Cliquez sur **OK**. Les résultats s'affichent dans le bloc inférieur.

ÉTAPE 4 Cliquez sur **Ajouter** pour ajouter une adresse IP de multidiffusion statique de groupe.

ÉTAPE 5 Saisissez les paramètres.

- **ID VLAN** : définit l'ID de VLAN du groupe à ajouter.
- **Version IP** : sélectionnez le type d'adresse IP approprié.

- **Adresse IP de multidiffusion de groupe** : définit l'adresse IP de multidiffusion du nouveau groupe.
- **Propre à la source** : indique que l'entrée contient une source spécifique et ajoute l'adresse correspondante dans le champ Adresse IP source. Dans le cas contraire, l'entrée est ajoutée sous la forme (*,G), c'est-à-dire une adresse IP de groupe associée à toutes les 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.
- **Interdit** : spécifie que ce port n'est pas autorisé à rejoindre ce groupe sur ce VLAN.
- **Aucun** : indique que le port n'est actuellement pas membre de ce groupe de multidiffusion sur ce VLAN. Cette option est définie par défaut tant que l'option Statique ou Interdit n'est pas sélectionnée.

ÉTAPE 9 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour.

Configuration de la surveillance de trafic IGMP

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

Par défaut, un périphérique Couche 2 transfère les trames de multidiffusion vers tous les ports du VLAN concerné, traitant en fait les trames comme s'il s'agissait de diffusions. Avec le traçage IGMP Snooping, le périphérique transfère les trames de multidiffusion vers les ports comportant des clients de multidiffusion enregistrés.

REMARQUE Le périphérique n'effectue le traçage IGMP Snooping que sur les VLAN statiques. Le traçage IGMP Snooping n'est pas pris en charge pour les VLAN dynamiques.

Lorsque vous activez le traçage IGMP Snooping, globalement ou sur un VLAN, tous les paquets IGMP sont transférés vers le CPU (l'unité centrale, l'UC). Le CPU analyse les paquets entrants et détermine les éléments suivants :

- Ports qui demandent à rejoindre tel ou tel groupe de multidiffusion sur un VLAN spécifique.
- Ports connectés aux routeurs de multidiffusion (Mrouters) qui génèrent des requêtes IGMP.
- Ports qui reçoivent les protocoles de requête PIM, DVMRP ou IGMP.

Ces informations sont affichées sur la page Traçage IGMP Snooping.

Les ports demandant à rejoindre un groupe de multidiffusion spécifique envoient un rapport IGMP qui spécifie le ou les groupes que l'hôte concerné souhaite rejoindre. Cela provoque la création d'une entrée de transfert dans la base de données de transfert de multidiffusion.

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

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

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 **Multidiffusion** > **IGMP Snooping**.

ÉTAPE 2 Activez ou désactivez l'état IGMP Snooping.

Lorsque le traçage IGMP Snooping est activé au niveau global, le périphérique qui surveille le trafic réseau peut détecter les hôtes qui ont demandé à recevoir le trafic de multidiffusion.

Le périphérique exécute uniquement le traçage IGMP Snooping si vous avez activé à la fois IGMP Snooping et le filtrage multidiffusion par ponts.

ÉTAPE 3 Sélectionnez un VLAN et cliquez sur **Modifier**.

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

ÉTAPE 4 Saisissez les paramètres.

- **ID VLAN** : sélectionnez l'ID du VLAN sur lequel le traçage IGMP Snooping est défini.
- **État IGMP Snooping** : active ou désactive la surveillance du trafic réseau pour le VLAN sélectionné.
- **État IGMP Snooping opérationnel** : affiche l'état actuel du traçage IGMP Snooping pour le VLAN sélectionné.
- **Apprentissage automatique des ports MRouter** : permet d'activer ou de désactiver l'apprentissage automatique des ports sur lesquels le routeur de multidiffusion (Mrouter) est connecté.
- **Robustesse des requêtes** : saisissez la valeur de la variable de robustesse à utiliser si ce périphérique est choisi comme émetteur de requêtes.
- **Robustesse des requêtes opérationnelles** : affiche la variable de robustesse envoyée par l'émetteur de requêtes choisi.
- **Intervalle de requête** : saisissez l'intervalle à appliquer entre deux requêtes générales si ce périphérique est choisi comme émetteur de requêtes.
- **Intervalle de requête opérationnelle** : intervalle en secondes qui sépare deux requêtes générales envoyées par l'émetteur de requêtes choisi.
- **Intervalle de réponse max aux requêtes** : saisissez la durée utilisée pour calculer le code de réponse maximal inséré dans les requêtes générales périodiques.
- **Intervalle de réponse max aux requêtes opérationnelles** : indique l'intervalle maximal de réponse aux requêtes inclus dans les requêtes générales envoyées par l'émetteur de requêtes choisi.

- **Nombre de requêtes du dernier membre** : indiquez le nombre de requêtes propres au groupe IGMP envoyées avant que le périphérique considère qu'il n'existe aucun autre membre pour le groupe, dans la mesure où ce périphérique a été choisi comme émetteur de requêtes.
- **Nombre de requêtes du dernier membre opérationnel** : affiche la valeur opérationnelle du compteur de requêtes du dernier membre.
- **Intervalle de requête du dernier membre** : saisissez le délai maximal de réponse aux requêtes à utiliser si le périphérique ne peut pas lire cette valeur dans les requêtes propres au groupe envoyées par l'émetteur de requêtes choisi.
- **Intervalle de requête du dernier membre opérationnel** : affiche l'intervalle de requête du dernier membre, envoyé par l'émetteur de requêtes choisi.
- **Sortie immédiate** : activez Sortie immédiate pour réduire la durée nécessaire au blocage d'un flux de multidiffusion envoyé à un port membre lorsque ce dernier reçoit un message de sortie de groupe IGMP.
- **État de l'émetteur de requêtes IGMP** : permet d'activer ou de désactiver l'émetteur de requêtes IGMP.
- **Adresse IP source de l'émetteur de requêtes administratif** : sélectionnez l'adresse IP source de l'émetteur de requêtes IGMP. Il peut s'agir de l'adresse IP du VLAN ou de l'adresse IP de gestion.
- **Adresse IP source de l'émetteur de requêtes opérationnel** : affiche l'adresse IP source de l'émetteur de requêtes choisi.
- **Version de l'émetteur de requêtes IGMP** : sélectionnez la version IGMP utilisée si le périphérique devient l'émetteur de requêtes choisi. Sélectionnez IGMPv3 s'il existe des commutateurs et/ou des routeurs de multidiffusion dans le VLAN qui réalise le transfert de multidiffusion IP propre à la source.

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

Surveillance MLD

Les hôtes emploient le protocole MLD pour signaler leur participation aux sessions de multidiffusion tandis que le périphérique utilise la surveillance MLD pour générer des listes de membres de multidiffusion. Ces listes servent à transmettre les paquets de multidiffusion uniquement aux ports du périphérique où existent des nœuds hôtes membres des groupes de multidiffusion. Le périphérique ne prend pas en charge l'émetteur de requêtes MLD.

Les hôtes emploient le protocole MLD pour signaler leur participation aux sessions de multidiffusion.

Le périphérique prend en charge deux versions du traçage MLD Snooping :

- Le traçage MLDv1 Snooping détecte les paquets de contrôle MLDv1 puis établit un pont pour le trafic sur la base d'adresses de multidiffusion de destination IPv6.
- Le traçage MLDv2 Snooping utilise des paquets de contrôle MLDv2 pour transférer le trafic sur la base de l'adresse IPv6 source et de l'adresse de multidiffusion de destination IPv6.

La version MLD réelle est sélectionnée par le routeur de multidiffusion sur le réseau.

Dans une approche semblable au traçage IGMP Snooping, les trames MLD font l'objet d'un traçage lorsqu'elles sont transférées par le périphérique des stations de travail vers un routeur de multidiffusion en amont et inversement. Cette fonction permet à un périphérique de déterminer :

- les ports sur lesquels il existe des stations de travail intéressées par l'adhésion à un groupe de multidiffusion particulier ;
- les ports sur lesquels résident les routeurs de multidiffusion qui envoient des trames de multidiffusion.

Ces connaissances servent à exclure des ports dénués d'intérêt (ceux sur lesquels aucune station de travail n'est enregistrée pour recevoir un groupe de multidiffusion spécifique) de l'ensemble de transfert d'une trame de multidiffusion entrante.

Si vous activez le traçage MLD Snooping en plus des groupes de multidiffusion configurés manuellement, cela crée une union entre les membres de groupes et de ports multidiffusions dérivés de la configuration manuelle et la détection dynamique par traçage MLD Snooping. Seules les définitions statiques sont conservées au redémarrage du système.

Pour activer le traçage MLD et le configurer sur un VLAN :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **MLD Snooping**.

ÉTAPE 2 Activez ou désactivez l'option **État MLD Snooping**. Lorsque le traçage MLD Snooping est activé au niveau global, le périphérique qui surveille le trafic réseau peut détecter les hôtes qui ont demandé à recevoir le trafic de multidiffusion. Le périphérique exécute uniquement le traçage MLD Snooping si vous avez activé à la fois MLD Snooping et le filtrage multidiffusion par ponts.

ÉTAPE 3 Sélectionnez un VLAN et cliquez sur **Modifier**.

ÉTAPE 4 Saisissez les paramètres.

- **ID VLAN** : sélectionnez l'ID du VLAN.
- **État MLD Snooping** : activez ou désactivez le traçage MLD Snooping sur le VLAN. Le périphérique surveille le trafic réseau pour déterminer les hôtes qui ont demandé à recevoir du 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.
- **État MLD Snooping opérationnel** : affiche l'état actuel du traçage MLD Snooping pour le VLAN sélectionné.
- **Apprentissage automatique des ports MRouter** : permet d'activer ou de désactiver l'apprentissage automatique pour le routeur de multidiffusion.
- **Robustesse des requêtes** : saisissez la valeur de la variable de robustesse à utiliser si le périphérique ne peut pas lire cette valeur dans les messages envoyés par l'émetteur de requêtes choisi.
- **Robustesse des requêtes opérationnelles** : affiche la variable de robustesse envoyée par l'émetteur de requêtes choisi.
- **Intervalle de requête** : saisissez la valeur d'intervalle de requête que le périphérique doit appliquer s'il ne peut pas extraire la valeur des messages envoyés par l'émetteur de requêtes choisi.
- **Intervalle de requête opérationnelle** : intervalle en secondes entre deux requêtes générales reçues de l'émetteur de requêtes choisi.
- **Intervalle de réponse max aux requêtes** : saisissez le délai maximal de réponse aux requêtes à utiliser si le périphérique ne peut pas lire cette valeur dans les requêtes générales envoyées par l'émetteur de requêtes choisi.

- **Intervalle de réponse max aux requêtes opérationnelles** : saisissez la durée utilisée pour calculer le code de réponse maximal inséré dans les requêtes générales.
- **Nombre de requêtes du dernier membre** : saisissez le nombre de requêtes du dernier membre à utiliser si le périphérique ne peut pas dériver cette valeur des messages envoyés par l'émetteur de requêtes choisi.
- **Nombre de requêtes du dernier membre opérationnel** : affiche la valeur opérationnelle du compteur de requêtes du dernier membre.
- **Intervalle de requête du dernier membre** : saisissez le délai maximal de réponse aux requêtes à utiliser si le périphérique ne peut pas lire cette valeur dans les requêtes propres au groupe envoyées par l'émetteur de requêtes choisi.
- **Intervalle de requête du dernier membre opérationnel** : intervalle de requête du dernier membre, envoyé par l'émetteur de requêtes choisi.
- **Sortie immédiate** : activez cette option pour réduire la durée nécessaire au blocage du trafic MLD inutile envoyé à un port du périphérique.

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

Interrogation du groupe de multidiffusion IP IGMP/MLD

La page Groupe de multidiffusion IP IGMP/MLD affiche l'adresse IPv4 et IPv6 des groupes appris à partir des messages IGMP/MLD.

Il y peut avoir une différence entre les informations affichées sur cette page et, par exemple, les informations affichées sur la page Adresse de groupe MAC. Supposez que le système comporte des groupes basés sur l'adresse MAC et qu'un port ait demandé à rejoindre les groupes de multidiffusion 224.1.1.1 et 225.1.1.1, tous deux mappés sur la même adresse MAC de multidiffusion (01:00:5e:01:01:01). Dans ce cas, la rubrique de multidiffusion MAC comporte une seule entrée mais la rubrique décrite ici en comporte deux.

Pour émettre une requête de recherche d'un groupe de multidiffusion IP :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **IP de multidiffusion de groupes IGMP/MLD**.

ÉTAPE 2 Définissez le type de groupe de traçage (Snooping) à rechercher : IGMP ou MLD.

ÉTAPE 3 Saisissez tout ou partie des critères de filtrage des requêtes suivants :

- **Adresse de groupe est égale à** : définit l'adresse MAC ou IP du groupe de multidiffusion à interroger.
- **Adresse source est égale à** : définit l'adresse d'expéditeur à interroger.
- **ID VLAN est égal à** : définit l'ID de VLAN à interroger.

ÉTAPE 4 Cliquez sur **OK**. Les champs suivants sont affichés pour chaque groupe de multidiffusion :

- **VLAN** : ID du VLAN.
- **Adresse de groupe** : adresse MAC ou IP du groupe de multidiffusion.
- **Adresse source** : adresse d'expéditeur pour tous les ports du groupe spécifié.
- **Ports inclus** : liste des ports de destination pour le flux de multidiffusion.
- **Ports exclus** : liste des ports qui ne sont pas inclus dans le groupe.
- **Mode de compatibilité** : version d'enregistrement IGMP/MLD la plus ancienne que le périphérique reçoit des hôtes à l'adresse IP du groupe.

Définition des ports de routeur de multidiffusion

Un port de routeur de multidiffusion (Mrouter) est un port qui se connecte à un routeur de multidiffusion. Le 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 ou afficher les ports dynamiquement détectés qui sont connectés au routeur de multidiffusion :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Port de routeur de multidiffusion**.

ÉTAPE 2 Saisissez tout ou partie des critères de filtrage des requêtes suivants :

- **ID VLAN est égal à** : sélectionnez l'ID de VLAN des ports de routeur qui sont décrits.

- **Version IP est égale à** : sélectionnez la version IP prise en charge par le routeur de multidiffusion.
- **Type d'interface est égal à** : choisissez d'afficher les ports ou les LAG.

ÉTAPE 3 Cliquez sur **OK**. Les interfaces répondant aux critères de requête sont affichées.

ÉTAPE 4 Sélectionnez le type d'association de chaque port ou LAG. Les options disponibles sont les suivantes :

- **Statique** : le port est configuré de manière statique en tant que port de routeur de multidiffusion.
- **Dynamique** : (affichage uniquement) le port est configuré de manière dynamique en tant que port de routeur de multidiffusion à l'aide d'une requête MLD/IGMP. Pour activer l'apprentissage dynamique des ports de routeurs de multidiffusion, accédez à la page **Multidiffusion** > **IGMP Snooping** et à la page **Multidiffusion** > **MLD Snooping**.
- **Interdit** : ce port ne doit pas être configuré en tant que port de routeurs de multidiffusion, même s'il reçoit des requêtes IGMP ou MLD. Si l'option Interdit est activée sur un port, l'apprentissage des ports MRouter n'a pas lieu sur ce port (ce qui signifie que l'option Apprentissage automatique des ports MRouter n'est pas activée sur ce port).
- **Aucun** : le port n'est actuellement pas un port de routeur de multidiffusion.

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

Définition de la multidiffusion Tout transférer

La page Tout transférer active et affiche la configuration des ports et/ou LAG qui doivent recevoir des flux de multidiffusion en provenance d'un VLAN spécifique. Cette fonction exige que vous activiez le filtrage multidiffusion par ponts sur la page Propriétés. Si cette fonction est désactivée, tout le trafic de multidiffusion est envoyé aux ports du 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 messages IGMP ou MLD ne sont pas transférés aux ports définis en mode *Tout transférer*.

REMARQUE Cette configuration affecte uniquement les ports membres du VLAN sélectionné.

Pour définir la multidiffusion Tout transférer :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Tout transférer**.

ÉTAPE 2 Définissez les éléments suivants :

- **ID VLAN est égal à** : ID du VLAN où les ports/LAG doivent être affichés.
- **Type d'interface est égal à** : choisissez d'afficher les ports ou les LAG.

ÉTAPE 3 Cliquez sur **OK**. L'état de tous les ports/LAG est affiché.

ÉTAPE 4 Sélectionnez le port/LAG à définir en mode Tout transférer à l'aide des méthodes suivantes :

- **Statique** : le port reçoit tous les flux de multidiffusion.
- **Interdit** : les ports ne peuvent pas recevoir de flux de multidiffusion, même si le traçage IGMP/MLD Snooping a désigné le port concerné comme devant rejoindre un groupe de multidiffusion.
- **Aucun** : le port n'est actuellement pas un port Tout transférer.

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

Définition des paramètres de multidiffusion non enregistrée

En général, les trames de multidiffusion sont transférées vers tous les ports du VLAN. Lorsque vous activez le traçage IGMP/MLD Snooping, le périphérique apprend l'existence des groupes de multidiffusion et surveille les ports membres de tel ou tel groupe. Les groupes de multidiffusion peuvent aussi être configurés de façon statique. Qu'ils aient été appris dynamiquement ou configurés de façon statique, ces groupes de multidiffusion sont considérés comme enregistrés.

Le périphérique transfère les trames de multidiffusion (depuis un groupe de multidiffusion enregistré) uniquement vers les ports enregistrés dans ce groupe de multidiffusion.

La page Multidiffusion non enregistrée permet de gérer les trames de multidiffusion appartenant à des groupes inconnus du périphérique (groupes de multidiffusion non enregistrés). En général, les trames de multidiffusion non enregistrées sont transférées vers tous les ports du VLAN.

Vous pouvez sélectionner un port pour qu'il reçoive les flux de multidiffusion non enregistrée ou pour qu'il les filtre. Cette configuration est valide pour tous les VLAN dont il est (ou sera) membre.

Cette fonction garantit que le client reçoit uniquement les groupes de multidiffusion demandés et non les autres groupes éventuellement transmis sur le réseau.

Pour définir des paramètres de multidiffusion non enregistrée :

ÉTAPE 1 Cliquez sur **Multidiffusion** > **Multidiffusion non enregistrée**.

ÉTAPE 2 Définissez les éléments suivants :

- **Type d'interface est égal à** : choisissez d'afficher tous les ports ou tous les LAG.
- **Port/LAG** : affiche l'ID de port ou de LAG.
- **Multidiffusion non enregistrée** : affiche l'état de transfert de l'interface sélectionnée. Ce champ peut prendre les valeurs suivantes :
  - *Transfert* : active le transfert des trames de multidiffusion non enregistrée vers l'interface sélectionnée.
  - *Filtrage* : active le filtrage (rejet) des trames de multidiffusion non enregistrée sur l'interface sélectionnée.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres sont enregistrés et le fichier de Configuration d'exécution est mis à jour.

17

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 rubrique aborde les points suivants :

- **Vue d'ensemble**
- **IPv4 Management and Interfaces (Interfaces et gestion IPv4)**
- **Serveur DHCP**
- **IPv6 Management and Interfaces (Interfaces et gestion IPv6)**
- **Nom de domaine**

Vue d'ensemble

Les périphériques Certaines fonctionnalités ne sont disponibles qu'en mode système Couche 2 ou Couche 3, comme décrit ci-dessous :

- En mode système Couche 2, le périphérique fonctionne en tant que périphérique reconnaissant les VLAN Couche 2, sans aucune fonction de routage.
- En mode système Couche 3, le périphérique possède des fonctions de routage IP en plus des fonctions du mode système Couche 2. En mode système, un port Couche 3 conserve la plupart des fonctionnalités de type Couche 2, comme le protocole STP (Spanning Tree Protocol) et l'appartenance VLAN.

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

Pour configurer le périphérique afin qu'il fonctionne dans l'un ou l'autre mode, reportez-vous à la page Administration >Paramètres système.

REMARQUE Pour passer d'un mode du système (Couche) à un autre (sur les périphériques Sx500), vous devez redémarrer, ce qui entraîne alors la suppression de la configuration de démarrage du périphérique.

Adressage IP Couche 2

En mode système Couche 2, le périphérique ne dispose que d'une adresse IPv4 et de deux interfaces IPv6 (soit interface « native », soit Tunnel) dans la gestion VLAN. Cette adresse IP et la passerelle par défaut peuvent être configurées manuellement ou par DHCP. Configurez l'adresse IP statique et la passerelle par défaut pour le mode système Couche 2 sur les pages Interface IPv4 et Interfaces IPv6. En mode système Couche 2, le périphérique utilise la passerelle par défaut (si elle existe) pour communiquer avec les périphériques qui ne se trouvent pas sur le même sous-réseau IP. Par défaut, VLAN 1 est le VLAN de gestion mais vous pouvez modifier ce paramètre. Lorsqu'il fonctionne en mode système Couche 2, le périphérique n'est accessible à l'adresse IP configurée que via son VLAN de gestion.

Le paramètre d'usine par défaut de la configuration de l'adresse IPv4 est *DHCPv4*. Cela signifie que le 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.

Lorsqu'un VLAN est configuré pour utiliser des adresses IPv4 dynamiques, le périphérique envoie des demandes DHCPv4 jusqu'à ce qu'un serveur DHCP lui attribue une adresse IPv4. En mode système Couche 2, seul le VLAN de gestion peut être configuré avec une adresse IP statique ou dynamique. En mode système Couche 3, vous pouvez configurer tous les types d'interfaces (ports, LAG et/ou VLAN) du périphérique avec une adresse IP statique ou dynamique.

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

- En mode système Couche 2, si le commutateur n'est pas configuré avec une adresse IP statique, il émet des requêtes DHCPv4 jusqu'à ce qu'il reçoive une réponse du serveur DHCP.
- 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 le périphérique revient à l'adresse IP par défaut.
- La DEL d'état du système s'allume en vert lorsque le serveur DHCP envoie une nouvelle adresse IP unique. Si une adresse IP statique a été définie, la DEL d'état du système s'allume également en vert. Cette DEL clignote pendant que le périphérique 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.

Adressage IP Couche 3

En mode système Couche 3, le périphérique peut posséder plusieurs adresses IP. Chaque adresse IP peut être affectée aux ports, LAG ou VLAN spécifiés. Ces adresses IP peuvent être configurées sur les pages Interface IPv4 et Interfaces IPv6 en mode système Couche 3. Cela offre davantage de souplesse réseau que le mode système Couche 2, qui ne permet de configurer qu'une seule adresse IP. Lorsqu'il fonctionne en mode système Couche 3, le périphérique est accessible à toutes ses adresses IP depuis les interfaces correspondantes.

Aucun acheminement prédéfini par défaut n'est fourni en mode système Couche 3. 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 qu'acheminements par défaut. De plus, vous pouvez définir manuellement des acheminements par défaut. Vous pouvez les définir sur les pages Acheminements statiques IPv4 et Acheminements IPv6.

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

Si les pages du mode Couche 2 et du mode Couche 3 sont différentes, les deux versions sont affichées.

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.

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.

Lorsque le commutateur est en mode système Couche 2, les règles suivantes sont prises en charge :

- Une seule interface de bouclage est prise en charge.
- Deux interfaces IPv4 peuvent être configurées : une sur un port VLAN ou Ethernet et une sur l'interface de bouclage.
- Si l'adresse IPv4 a été configurée sur le VLAN par défaut et que ce dernier a été changé, le commutateur déplace l'adresse IPv4 vers le nouveau VLAN par défaut.

Configuration d'une interface de bouclage

Pour configurer une interface de bouclage IPv4, procédez comme suit :

- En mode Couche 2, activez l'interface de bouclage et configurez son adresse sur la page Administration > Interface de gestion > Interface IPv4.
- En mode Couche 3, ajoutez une interface de bouclage en Configuration IP > IPv4 Management and Interfaces (Interfaces et gestion IPv4) > Interface IPv4.

Pour configurer une interface de bouclage IPv6, procédez comme suit :

- En mode Couche 2, ajoutez une interface de bouclage sur la page Administration > Interface de gestion > Interfaces IPv6. Configurez l'adresse IPv6 de cette interface sur la page Administration > Interface de gestion > Adresses IPv6. Cette page n'est pas disponible sur les périphériques SG500X, ESW2-550X et SG500XG.
- En mode Couche 3, ajoutez une interface de bouclage en Configuration IP > IPv6 Management and Interfaces (Interfaces et gestion IPv6) > Interface IPv6. Configurez l'adresse IPv6 de cette interface sur la page Configuration IP > IPv6 Management and Interfaces (Interfaces et gestion IPv6) > Adresses IPv6.

IPv4 Management and Interfaces (Interfaces et gestion IPv4)

Interface IPv4

Les interfaces IPv4 peuvent être définies sur le périphérique lorsque celui-ci se trouve en mode système Couche 2 ou Couche 3.

Définition d'une interface IPv4 en mode système Couche 2

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 du périphérique peut être configurée manuellement ou reçue automatiquement depuis un serveur DHCP.

Pour configurer une adresse IPv4 pour le périphérique :

ÉTAPE 1 Cliquez sur **Administration > Interface de gestion > Interface IPv4**.

ÉTAPE 2 Saisissez les valeurs appropriées dans les champs suivants :

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

  REMARQUE : l'option 12 DHCP (option Nom d'hôte) est prise en charge lorsque le périphérique est un client DHCP. Si l'option 12 DHCP est reçue d'un serveur DHCP, elle est enregistrée en tant que nom d'hôte du serveur. L'option 12 DHCP ne sera pas demandée par le périphérique. Le serveur DHCP doit être configuré pour envoyer l'option 12 indépendamment de ce qui est demandé afin de pouvoir utiliser cette fonctionnalité.

Pour définir une adresse IP statique, configurez les champs suivants.

- **Adresse IP** : saisissez l'adresse IP et configurez l'un des champs **Masque** suivants :
  - **Masque réseau** : sélectionnez et saisissez le masque d'adresse IP.
  - **Longueur du préfixe** : sélectionnez et saisissez la longueur du préfixe d'adresse IPv4.
- **Interface de bouclage** : sélectionnez cette option pour activer la configuration d'une interface de bouclage (voir **Interface de bouclage**).
- **Adresse IP de bouclage** : saisissez l'adresse IPv4 de l'interface de bouclage.

  Renseignez l'un des champs suivants pour l'interface de bouclage :
  - *Masque de bouclage* : saisissez le masque de l'adresse IPv4 de l'interface de bouclage.
  - *Longueur du préfixe* : saisissez la longueur du préfixe de l'adresse IPv4 de l'interface de bouclage.

- **Passerelle par défaut administrative** : sélectionnez **Défini par l'utilisateur** et saisissez l'adresse IP de la passerelle par défaut. Vous pouvez aussi sélectionner **Aucun** pour supprimer de l'interface l'adresse IP de passerelle par défaut sélectionnée.
- **Passerelle opérationnelle par défaut** : indique l'état de la passerelle par défaut actuelle.

  REMARQUE : si aucune passerelle par défaut n'est configurée pour le périphérique, ce dernier ne peut pas communiquer avec les périphériques qui ne font pas partie du même sous-réseau IP.

Si le système récupère une adresse IP dynamique auprès du serveur DHCP, parmi les champs suivants, sélectionnez ceux que vous souhaitez activer :

- **Renouveler l'adresse IP maintenant** : l'adresse IP dynamique du périphérique peut être renouvelée à tout moment après son affectation par un serveur DHCP. Remarque : selon la configuration de votre serveur DHCP, le périphérique peut recevoir une nouvelle adresse IP après le renouvellement, ce qui nécessite le paramétrage de l'utilitaire de configuration Web à la nouvelle adresse IP.
- **Configuration automatique via DHCP** : affiche l'état de la fonction Configuration automatique. Vous pouvez configurer cette fonction à l'aide de l'option *Administration > Gestion de fichiers > Configuration automatique DHCP*.

ÉTAPE 3 Cliquez sur **Appliquer**. Les paramètres d'interface IPv4 sont modifiés et écrits dans le fichier de Configuration d'exécution.

Définition d'une interface IPv4 en mode système Couche 3

Utilisez la page Interface IPv4 lorsque le périphérique fonctionne en mode système Couche 3. Ce mode permet de configurer plusieurs adresses IP pour la gestion du périphérique et fournit des services de routage.

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

Lorsqu'il fonctionne en mode Couche 3, le périphérique achemine le trafic entre les sous-réseaux IP à connexion directe configurés sur le périphérique. Le périphérique continue à servir de pont pour le trafic entre les périphériques appartenant au même VLAN. Vous pouvez configurer des acheminements IPv4 supplémentaires pour le routage vers des sous-réseaux sans connexion directe sur la page Acheminements statiques IPv4.

REMARQUE : le logiciel de périphérique consomme 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 4094.

Pour configurer des adresses IPv4 :

ÉTAPE 1 Cliquez sur **Configuration IP** > **IPv4 Management and Interfaces (Interfaces et gestion IPv4)**> **Interface IPv4.**

Cette page affiche les champs suivants dans la table des interfaces IPv4 :

- **Interface** : interface pour laquelle l'adresse IP est définie.
- **Type d'adresse IP** : adresse IP définie comme statique ou DHCP.
  - *Adresse IP dynamique* : reçue du serveur DHCP.
  - *Statique* : saisie manuellement.
- **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 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Sélectionnez l'un des champs suivants :

- **Interface** : sélectionnez Port, LAG ou 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 4 Sélectionnez **Adresse dynamique ou Adresse statique**.

ÉTAPE 5 Si vous avez sélectionné **Adresse statique**, entrez l'adresse IP pour cette interface, puis saisissez l'un des éléments suivants :

- **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.

Routes IPv4

Lorsque le périphérique fonctionne en mode système Couche 3, cette page vous permet de configurer et d'activer des acheminements 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.

Pour définir un acheminement IP statique :

ÉTAPE 1 Cliquez sur **Configuration IP** > **IPv4 Management and Interfaces (Interfaces et gestion IPv4)**> **Acheminements IPv4.**

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 et saisissez des informations dans l'un des champs suivants :
  - **Masque de réseau** : préfixe d'acheminement IP pour l'adresse IP de destination.

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

- **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.
  - *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.

ÉTAPE 4 Cliquez sur **Appliquer**. L'acheminement statique IP est enregistré dans le fichier de Configuration d'exécution.

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 En mode Couche 2, le mappage adresse IP-adresse MAC de la table ARP permet de transférer le trafic en provenance du périphérique. En mode Couche 3, les informations de mappage servent au routage Couche 3 et au transfert du trafic généré.

Pour définir les tables ARP :

ÉTAPE 1 Cliquez sur **Configuration IP > IPv4 Management and Interfaces (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.

- **VLAN** : affiche dans la Couche 2 l'ID de VLAN de la gestion.

  Pour les périphériques en mode Couche 2, il existe un seul sous-réseau IP à connexion directe, toujours situé sur le VLAN de gestion. Toutes les adresses statiques et dynamiques de la table ARP résident sur le VLAN de gestion.

  Interface : pour les périphériques en mode système Couche 3, vous pouvez configurer une interface IPv4 sur un port, un LAG ou un VLAN. Sélectionnez l'interface voulue dans la liste des interfaces IPv4 configurées sur le 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 le 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 > IPv4 Management and Interfaces (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.

UDP Relay/IP Helper (Relais UDP/Assistance IP)

La fonction UDP Relay/IP Helper (Relais UDP/Assistance IP) n'est disponible que lorsque le périphérique fonctionne en mode système Couche 3. En général, les commutateurs n'acheminent pas les paquets de diffusion IP d'un sous-réseau IP à un autre. Toutefois, cette fonction permet au périphérique de reCouche 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 > IPv4 Management and Interfaces (Interfaces et gestion IPv4)** > **UDP Relay/IP Helper (Relais UDP/Assistance IP)**.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Sélectionnez l'**Interface IP source** vers laquelle le périphérique doit reCouche 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 reCouche. 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.

Surveillance et relais DHCPv4

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 (dans la page Paramètres de l'interface de surveillance DHCP).

Relais DHCPv4

Le relais DHCP relaye les paquets DHCP vers le serveur DHCP.

DHCPv4 dans la Couche 2 et la Couche 3

En mode système Couche 2, le périphérique relaye les messages DHCP provenant de VLAN sur lesquels le relais DHCP a été activé.

En mode système Couche 3, le périphérique peut également reCouche les messages DHCP provenant de VLAN qui ne possèdent 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 le relais DHCP est activé sur un VLAN sans adresse IP ou si le périphérique n'est pas un routeur (périphérique Couche 2), vous devrez vous équiper d'un routeur externe.

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 quand le relais DHCP est activé.

	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

Vous découvrirez 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

	Relais DHCP VLAN avec adresse IP		Relais DHCP VLAN sans adresse IP	
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 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

Vous découvrirez 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

	Relais DHCP **VLAN avec adresse IP**		**Relais DHCP** **VLAN sans adresse IP**	
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

Vous découvrirez 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.

Cette base de données contient les informations 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

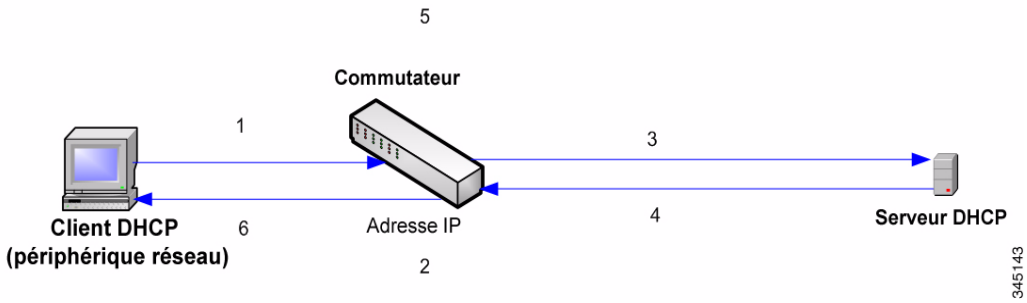
Les ports DHCP peuvent être sécurisés ou non sécurisés. Par défaut, tous les ports sont non sécurisés. Pour créer un port sécurisé, accédez à la page Paramètres de l'interface de surveillance DHCP. Les paquets transitant par ces ports sont automatiquement transférés. Les paquets passant par des ports 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.

Vous découvrirez 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.

Type de paquet	Arrivée via une interface d'entrée non sécurisée	Arrivée via une interface d'entrée sécurisée
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
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.

Options DHCP par défaut

Option	État par défaut
Surveillance DHCP	**Activé**
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 la surveillance DHCP et/ou le relais DHCP dans la page **Configuration IP > DHCP > Propriétés** ou dans la page **Sécurité > Surveillance DHCP > Propriétés**.

ÉTAPE 2 Définissez les interfaces sur lesquelles la surveillance DHCP est activée dans la page **Configuration IP > DHCP > Paramètres d'interface**.

ÉTAPE 3 Indiquez si les interfaces sont sécurisées ou non sécurisées dans la page **Configuration IP > DHCP > Interface de surveillance DHCP**.

ÉTAPE 4 Facultatif. Ajoutez des entrées à la base de données de liaison de surveillance DHCP dans la page **Configuration IP > DHCP > Base de données de liaison de surveillance DHCP**.

Surveillance/Relais DHCP

Cette section passe en revue l'implémentation des fonctionnalités de relais et de surveillance DHCP via l'interface Web.

Propriétés

Pour configurer le relais DHCP, la surveillance DHCP et l'option 82 :

ÉTAPE 1 Cliquez sur **Configuration IP** > **IPv4 Management and Interfaces (Interfaces et gestion IPv4)** > **Surveillance/Relais DHCP > Propriétés** ou **Sécurité** > **Surveillance DHCP**.

Renseignez les champs suivants :

- **Option 82 :** sélectionnez **Option 82** pour insérer des informations sur l'option 82 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. En cas d'activation de la surveillance DHCP, les options suivantes sont disponibles :
  - *Option 82 Pass Through* : sélectionnez cette option pour conserver des informations étrangères sur l'option 82 lors du transfert de paquets.
  - *Vérifier l'adresse MAC* : sélectionnez cette option pour vérifier que l'adresse MAC source de l'en-tête Couche 2 correspond à l'adresse matérielle du client telle qu'elle apparaît dans l'en-tête DHCP (partie de la charge 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.
  - *Intervalle d'actu. de base de données de secours* : indiquez la fréquence des sauvegardes de la base de données de liaison de surveillance DHCP (**si l'option Base de données de secours est sélectionnée**).

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

En mode Couche 2, la surveillance et le relais DHCP peuvent uniquement être activés sur des VLAN avec adresses IP.

En mode Couche 3, la surveillance et le relais DHCP peuvent être activés sur n'importe quelle interface avec adresse IP et sur des VLAN avec ou sans adresse IP.

Pour activer la surveillance ou le relais DHCP sur des interfaces spécifiques :

ÉTAPE 1 Cliquez sur **Configuration IP** > **IPv4 Management and Interfaces (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 DHCP**.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres sont consignés dans le fichier de Configuration d'exécution.

Interfaces sécurisées 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 (voir 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** > **IPv4 Management and Interfaces (Interfaces et gestion IPv4)** > **Surveillance/Relais DHCP > Interfaces sécurisées 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 d'exécution.

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 > IPv4 Management and Interfaces (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 et cliquez sur **OK**.

Les champs de la base de données de liaison de surveillance DHCP sont affichés. Ils sont décrits sur la page Ajouter, à l'exception du champ **Protection de la source IP** :

- **État :**
  - Actif **:** la protection de la source IP est active sur le périphérique.
  - Inactif **:** la 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 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

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. Cette opération s'effectue sur la page Groupes de réseaux.

Dépendances entre les fonctions

- Il est impossible de configurer en même temps le serveur DHCP et le client DHCP sur le système, à savoir : Si le client DHCP est activé sur une interface, il n'est pas possible d'activer le serveur DHCP globalement.
- 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 DHCP Server (Serveur DHCP) > 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 8 groupes d'adresses IP réseau à l'aide de la page Network Pools (Groupes réseau).

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 Groupes de réseaux. Le périphérique répond aux requêtes DHCP depuis cette interface IP. 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 Configuration IP > Interface 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.

Serveur DHCPv4

Pour configurer le périphérique en tant que serveur DHCPv4 :

ÉTAPE 1 Cliquez sur **Configuration IP** > **IPv4 Management and Interfaces (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, un ou plusieurs groupes d'adresses IP doivent être définis à partir desquels le périphérique attribuera les adresses IP aux clients. 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 au sous-réseau configuré sur l'interface IP du périphérique à partir duquel la demande DHCP a été reçue.
- **Client distant** : le périphérique prend une adresse IP du groupe de réseaux dont le premier sous-réseau de relais directement connecté au client correspond au sous-réseau configuré sur l'une des interfaces IP de commutateur.

Vous pouvez définir jusqu'à huit groupes de réseaux.

Pour créer un groupe d'adresses IP et définir leurs durées de bail :

ÉTAPE 1 Cliquez sur **Configuration IP** > **IPv4 Management and Interfaces (Interfaces et gestion IPv4)** > **DHCP Server (Serveur DHCP)** > **Network Pool (Groupe réseau)** pour afficher la page Network Pool (Groupe de réseaux).

Les groupes réseau précédemment définis s'affichent.

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.

- **Default Router IP Address (Option 3) (Adresse IP de routeur par défaut (option 3))** : saisissez le routeur par défaut pour le client DHCP.
- **Domain Name Server IP Address (Option 6) (Adresse IP de serveur de nom de domaines (option 6))** : sélectionnez l'un des serveurs DNS du périphérique (si déjà configuré) ou sélectionnez **Autre** et saisissez l'adresse IP du serveur DNS disponible pour le client DHCP.
- **Domain Name (Option 15) (Nom de domaine (option 15))** : saisissez le nom de domaine pour un client DHCP.
- **NetBIOS WINS Server (Option 44) (Serveur NetBIOS WINS (option 44))** : saisissez le serveur du nom NetBIOS WINS disponible pour un client DHCP.
- **NetBIOS Node Type (Option 46) (Type de nœud NetBIOS (option 46))** : sélectionnez comment 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.
- **SNTP Server IP Address (Option 4) (Adresse IP du serveur SNTP (option 4))** : sélectionnez l'un des serveurs DNS du périphérique (si déjà configuré) ou sélectionnez **Autre** et saisissez l'adresse IP du serveur horaire pour le client DHCP.
- **File Server IP Address (siaddr) (Adresse IP du serveur de fichiers (siaddr))** : saisissez l'adresse IP du serveur TFTP/SCP à partir duquel le fichier de configuration est téléchargé.

- **File Server Host Name (sname) (Nom d'hôte de serveur de fichier (sname))** : saisissez le nom du serveur TFTP/SCP.
- **Configuration File Name (file) (Nom du fichier de configuration (fichier))** : saisissez le nom du fichier utilisé comme fichier de configuration.

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** > **IPv4 Management and Interfaces (Interfaces et gestion IPv4)** > **DHCP Server (Serveur DHCP)** > **Excluded Addresses (Adresses exclues)** pour afficher la page Excluded Addresses (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.

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.

Pour attribuer manuellement une adresse IP permanente à un client spécifique :

ÉTAPE 1 Cliquez sur **Configuration IP** > **IPv4 Management and Interfaces (Interfaces et gestion IPv4)** > **DHCP Server (Serveur DCHP)** > **Static Hosts (Hôtes statiques)** pour afficher la page Static Hosts (Hôtes statiques).

Les hôtes statiques s'affichent.

ÉTAPE 2 Pour ajouter un hôte statique, cliquez sur **Ajouter** et 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.
- **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.
- **Default Router IP Address (Option 3) (Adresse IP de routeur par défaut (option 3))** : saisissez le routeur par défaut pour l'hôte statique.
- **Domain Name Server IP Address (Option 6) (Adresse IP de serveur de nom de domaines (option 6))** : sélectionnez l'un des serveurs DNS du périphérique (si déjà configuré) ou sélectionnez **Autre** etsaisissez l'adresse IP du serveur DNS disponible pour le client DHCP.
- **Domain Name (Option 15) (Nom de domaine (option 15))** : saisissez le nom de domaine pour l'hôte statique.
- **NetBIOS WINS Server (Option 44) (Serveur NetBIOS WINS (option 44))** : saisissez le serveur du nom NetBIOS WINS disponible pour l'hôte statique.
- **NetBIOS Node Type (Option 46) (Type de nœud NetBIOS (option 46))** : sélectionnez comment 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.

- **SNTP Server IP Address (Option 4) (Adresse IP du serveur SNTP (option 4))** : sélectionnez l'un des serveurs DNS du périphérique (si déjà configuré) ou sélectionnez **Autre** et saisissez l'adresse IP du serveur horaire pour le client DHCP.
- **File Server IP Address (siaddr) (Adresse IP du serveur de fichiers (siaddr))** : saisissez l'adresse IP du serveur TFTP/SCP à partir duquel le fichier de configuration est téléchargé.
- **File Server Host Name (sname) (Nom d'hôte de serveur de fichier (sname))** : saisissez le nom du serveur TFTP/SCP.
- **Configuration File Name (file) (Nom du fichier de configuration (fichier))** : saisissez le nom du fichier utilisé comme fichier de configuration.

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.

Les options spécifiquement configurées sur les pages Serveur DHCP > Groupes de réseaux et Serveur DHCP > Hôtes statiques (option 3-6, 15, 44, 46, 66, 67) ne peuvent pas être configurées par l'intermédiaire de la page Options DHCP.

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** > **IPv4 Management and Interfaces (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 et renseigner le champ :

- **Nom de groupe de serveurs DHCP :** sélectionnez l'un des groupes d'adresses réseau définis sur la page Groupes de réseaux.

ÉTAPE 3 Cliquez sur **Ajouter** et renseignez les champs :

- **Code :** entrez 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 entrer 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 entrer une adresse IP si elle est appropriée à l'option DHCP sélectionnée.
  - *Liste IP* **:** entrez 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, entrez la valeur à envoyer pour ce code.
- **Description :** saisissez une description à des fins de documentation.

Liaison d'adresses

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** > **IPv4 Management and Interfaces (Interfaces et gestion IPv4)** > **DHCP Server (Serveur DHCP)** > **Address Binding (Liaison d'adresses)** pour afficher la page Address Binding (Liaison d'adresses).

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.
- **MAC Address/Client Identifier (Adresse MAC/Identificateur de client)** :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 disponibles 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, sont 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.

IPv6 Management and Interfaces (Interfaces et gestion IPv6)

Internet Protocol version 6 (IPv6) est un protocole de couche réseau utilisé dans les communications entre réseaux à commutation de paquets. IPv6 a été conçu pour remplacer IPv4, le protocole Internet le plus souvent déployé.

IPv6 apporte davantage de souplesse dans l'affectation des adresses IP car la taille des adresses passe de 32 à 128 bits. Les adresses IPv6 sont constituées de huit groupes de quatre chiffres hexadécimaux, par exemple FE80:0000:0000:0000:0000:9C00:876A:130B. La forme abrégée, dans laquelle un groupe de zéros peut être ignoré et remplacé par « :: », est également admise. Exemple : ::-FE80::9C00:876A:130B.

Les nœuds IPv6 nécessitent un mécanisme de mappage intermédiaire pour communiquer avec d'autres nœuds IPv6 sur un réseau uniquement IPv4. Ce mécanisme, appelé tunnel, permet à des hôtes uniquement IPv6 de contacter des services IPv4, ainsi qu'à des hôtes et réseaux IPv6 isolés de contacter un nœud IPv6 sur une infrastructure IPv4.

La fonction de Tunneling utilise un mécanisme ISATAP ou manuel (reportez-vous à **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.

Configuration globale IPv6

Pour définir des paramètres IPv6 globaux et les paramètres de client DHCPv6 :

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

En mode système Couche 3, cliquez sur **Configuration IP** > **IPv6 Management and Interfaces (Interfaces et gestion IPv6)** > **Configuration globale IPv6**.

ÉTAPE 2 Saisissez les valeurs appropriées dans les champs suivants :

- **Intervalle de limites de débit ICMPv6** : saisissez la fréquence à laquelle les messages d'erreur ICMP sont générés.
- **Taille des cases de limite de débit ICMPv6** : saisissez le nombre maximal de messages d'erreur ICMP que le périphérique peut envoyer dans chaque intervalle.

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.

Interface IPv6

Vous pouvez configurer l'interface IPv6 sur un port, un LAG, un VLAN, une interface de bouclage ou un tunnel.

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

Pour définir une interface IPv6 :

ÉTAPE 1 En mode système Couche 2, cliquez sur **Administration** > **Interface de gestion** > **Interfaces IPv6**.
En mode système Couche 3, cliquez sur **Configuration IP** > **IPv6 Management and Interfaces (Interfaces et gestion IPv6)** > **Interfaces IPv6**.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter une nouvelle interface sur laquelle l'interface IPv6 est activée.

ÉTAPE 3 Renseignez les champs :

- **Interface IPv6** : sélectionnez un port, un LAG, un VLAN ou un tunnel ISATAP spécifique pour l'adresse IPv6.

ÉTAPE 4 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** :

- **Sans état** : sélectionnez cette option pour activer l'interface comme client DHCPv6 sans état. Cela permet la réception des informations de configuration à partir d'un serveur DHCP.
- **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 5 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.

  REMARQUE : le périphérique ne prend pas en charge la configuration automatique des adresses avec conservation d'état à partir d'un serveur DHCPv6.

- **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.

ÉTAPE 6 Cliquez sur **Appliquer** pour activer le traitement IPv6 sur l'interface sélectionnée. Pour les interfaces IPv6 standard, les adresses suivantes sont configurées automatiquement :

- Adresse de liaison locale, à l'aide de l'ID d'interface au format EUI-64, sur la base de l'adresse MAC d'un périphérique
- Toutes les adresses de multidiffusion de liaison locale des nœuds (FF02::1)
- Adresse de multidiffusion de nœud sollicité (au format FF02::1:FFXX:XXXX)

ÉTAPE 7 Cliquez sur **Table des adresses IPv6** pour affecter manuellement des adresses IPv6 à l'interface, si nécessaire. Cette page est décrite à la section **Définition d'adresses IPv6**.

ÉTAPE 8 Appuyez sur le bouton **Restart (Redémarrer)** pour lancer l'actualisation des informations sans état reçues du serveur DHCPv6.

Détails de client DHCPv6

Le bouton **DHCPv6 Client Details (Détails de client DHCPv6)** affiche les informations reçues sur l'interface 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) :

- **DHCPv6 Operational Mode (Mode de fonctionnement DHCPv6)** : permet d'afficher Enabled (Activé) lorsque les conditions suivantes sont remplies :
  - L'interface est active.
  - IPv6 y est activé.
  - Le client DHCPv6 sans état y est activé.
- **Stateless Service (Service sans état)** : configure si le client est défini comme sans état (il reçoit les informations d'un serveur DHCP) ou non.
- **DHCPv6 Server Address (Adresse du serveur DHCPv6)** : adresse du serveur DHCPv6.
- **DHCPv6 Server DUID (DUID du serveur DHCPv6)** : identificateur unique du serveur DHCPv6.
- **DHCPv6 Server Preference (Préférence du serveur DHCPv6)** : priorité de ce serveur DHCPv6.

- **Minimum Information Refresh Time (Intervalle minimal d'actualisation des informations)** : voir ci-dessus.
- **Information Refresh Time (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 possède une adresse IPv4 source et une adresse IPv4 de destination. Le paquet IPv6 est encapsulé entre ces adresses.

Tunnels ISATAP

Le type de tunnel pouvant être configuré sur le périphérique est nommé tunnel ISATAP (Intra-Site Automatic Tunnel Addressing Protocol, ou protocole d'adressage automatique de tunnel intrasite) qui peut être un tunnel point à 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. Notez les éléments suivants :

- 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.

Configuration des tunnels

REMARQUE Pour configurer un tunnel, configurez tout d'abord une interface IPv6 comme tunnel sur la page Interfaces IPv6.

Pour configurer un tunnel IPv6 :

ÉTAPE 1 En mode système Couche 2, cliquez sur **Administration > Interface de gestion > Tunnel IPv6**.

En mode système Couche 3, cliquez sur **Configuration IP> IPv6 Management and Interfaces (Interfaces et gestion IPv6) > Tunnel IPv6**.

ÉTAPE 2 Saisissez les valeurs appropriées dans les champs suivants :

- **Numéro du tunnel** : affiche le numéro de domaine du routeur de tunnel automatique.
- **Type du tunnel** : toujours ISATAP.
- **Adresse IPv4 source** : l'adresse IPv4 de l'interface sélectionnée sur le périphérique actuel utilisée pour constituer une partie de l'adresse IPv6.
  - *Auto* : sélectionne automatiquement l'adresse IPv4 la plus basse parmi toutes les interfaces IPv4 configurées sur le périphérique. Cette option est équivalente à l'option d'interface en mode Couche 3 car en mode Couche 2, il n'y a qu'une interface.

    REMARQUE : lorsque l'adresse IPv4 est modifiée, l'adresse locale de l'interface de tunnel est également modifiée.
  - *Aucun* : désactivez le tunnel.

- *Manuel* : saisissez l'adresse IPv4 source à utiliser. L'adresse IPv4 configurée doit être l'une des adresses IPv4 des interfaces IPv4 du périphérique.
- *Interface* : (Couche 3) sélectionnez l'interface IPv4 à utiliser.

- **ISATAP Router Name (Nom de routeur ISATAP)** : chaîne globale qui représente un nom de domaine de routeur de tunnel automatique spécifique. Il peut s'agir du nom par défaut (ISATAP) ou d'un nom défini par l'utilisateur.
- **Intervalle de sollicitation ISATAP** : nombre de secondes entre deux messages de sollicitation de routeur ISATAP, si aucun routeur ISATAP n'est actif. Il peut s'agir de l'intervalle par défaut ou d'une valeur d'intervalle définie par l'utilisateur.
- **Robustesse ISATAP** : permet de calculer l'intervalle des requêtes DNS ou de sollicitation de routeur. Plus la valeur est élevée, plus les requêtes sont fréquentes.

  REMARQUE : le tunnel ISATAP ne sera pas opérationnel si l'interface IPv4 sous-jacente n'est pas active.

ÉTAPE 3 Cliquez sur **Appliquer**. Le tunnel est enregistré dans le fichier de Configuration d'exécution.

Définition d'adresses IPv6

Pour affecter une adresse IPv6 à une interface IPv6 :

ÉTAPE 1 En mode système Couche 2, cliquez sur **Administration** > **Interface de gestion** > **Adresses IPv6**.
En mode système Couche 3, cliquez sur **Configuration IP** > **IPv6 Management and Interfaces (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.

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 locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : une adresse IPv6 qui est de type global IPV6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Adresse IPv6** : en mode Couche 2, le périphérique prend en charge une seule interface IPv6. Outre les adresses de liaison locale et de multidiffusion par défaut, le périphérique ajoute aussi automatiquement des adresses globales à l'interface sur la base des annonces de routeur qu'il reçoit. Le périphérique prend en charge un maximum de 128 adresses sur l'interface. Chaque adresse doit correspondre à une adresse IPv6 valide, spécifiée au format hexadécimal en utilisant des valeurs de 16 bits séparées par le caractère deux-points. Il est impossible de configurer des adresses IPv6 directement sur une interface de tunnel ISATAP.
- **Longueur du préfixe** : la longueur du préfixe IPv6 global est une valeur comprise entre 0 et 128 qui indique le nombre de bits contigus les plus significatifs de l'adresse dont se compose le préfixe (la partie réseau de l'adresse).
- **EUI-64** : sélectionnez cette option pour employer le paramètre EUI-64 afin d'identifier la portion de l'adresse IPv6 globale correspondant à l'ID d'interface en utilisant le format EUI-64 sur la base de l'adresse MAC d'un périphérique.

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

Liste des routeurs par défaut IPv6

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 En mode système Couche 2, cliquez sur **Administration > Interface de gestion > Liste des routeurs par défaut IPv6**.
En mode système Couche 3, cliquez sur **Configuration IP** > **IPv6 Management and Interfaces (Interfaces et gestion IPv6)** > **Liste des routeurs par défaut IPv6**.

Cette page affiche les champs suivants pour chaque routeur par défaut :

- **Adresse IPv6 du routeur par défaut** : adresse IP de liaison locale du routeur par défaut.
- **Interface** : interface IPv6 sortante où réside le routeur par défaut.
- **Type** : configuration du routeur par défaut qui inclut les options suivantes :
  - *Statique* : le routeur par défaut a été ajouté manuellement à cette table à l'aide du bouton **Ajouter**.
  - *Dynamique* : le routeur par défaut a été configuré de manière dynamique.

ÉTAPE 2 Cliquez sur **Ajouter** pour ajouter un routeur par défaut statique.

ÉTAPE 3 Renseignez les champs suivants :

- **Interface de liaison locale** : affiche l'interface Liaison locale sortante.
- **Adresse IPv6 du routeur par défaut** : adresse IP du routeur par défaut.

ÉTAPE 4 Cliquez sur **Appliquer**. Le routeur par défaut est enregistré dans le fichier de Configuration d'exécution.

Définition des informations sur les voisins IPv6

La page Voisins IPv6 vous permet de configurer et d'afficher la liste des voisins IPv6 sur l'interface IPv6. La table Voisins IPv6, également appelée Cache de détection du voisinage IPv6, affiche les adresses MAC des voisins IPv6 qui font partie du même sous-réseau IPv6 que le 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 En mode système Couche 2, cliquez sur **Administration > Interface de gestion > Voisins IPv6**.
En mode système Couche 3, cliquez sur **Configuration IP** > **IPv6 Management and Interfaces (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 Saisissez les valeurs appropriées dans les champs suivants :

▪ **Interface** : interface de voisinage IPv6 à ajouter.

▪ **Adresse IPv6** : saisissez l'adresse réseau IPv6 affectée à l'interface. Cette adresse doit être une adresse IPv6 valide.

▪ **Adresse MAC** : saisissez l'adresse MAC mappée sur l'adresse IPv6 spécifiée.

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

ÉTAPE 5 Pour remplacer le type d'une adresse IP **Dynamique** par **Statique**, 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 entrés, la plage est comprise entre les valeurs utilisées pour **Inférieur à** et **Supérieur à**.

Pour créer une liste de préfixes :

ÉTAPE 1 (En mode Couche 3) Cliquez sur **Configuration IP > IPv6 Management Interfaces (Interfaces et gestion IPv6) > Liste de préfixes IPv6**.

- ou

(En mode Couche 2) Cliquez sur **Administration > IPv6 Management Interfaces (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 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 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 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.

Affichage des tables de routage 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 :

Pour visualiser les entrées de routage IPv6 en mode système Couche 2 :

ÉTAPE 1 Cliquez sur **Administration > Interface de gestion > Acheminements IPv6**.

- ou

Pour visualiser les entrées de routage IPv6 en mode système Couche 3 : Cliquez sur **Configuration IP** > **IPv6 Management and Interfaces (Interfaces et gestion IPv6)** > **Routes IPv6**.

Cette rubrique affiche les champs suivants :

- **Adresse IPv6** : adresse du sous-réseau IPv6.
- **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** : interface utilisée pour transférer le paquet.
- **Saut suivant** : adresse vers laquelle le paquet est transféré. En général, il s'agit de l'adresse d'un routeur du voisinage. 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 locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : 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 :
  - *Local* : un réseau connecté directement dont le préfixe est dérivé de l'adresse IPv6 d'un périphérique configuré manuellement.

- *Dynamique* : la destination est une adresse de sous-réseau IPv6 attachée de façon indirecte (à distance). L'entrée a été obtenue de manière dynamique via le protocole ND ou ICMP.
- *Statique* : l'entrée a été configurée manuellement par un utilisateur.

Relais DHCPv6

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.

Global Destinations (Destinations globales)

Pour configurer une liste de serveurs DHCPv6 vers laquelle tous les paquets DHCPv6 sont relayés :

ÉTAPE 1 Cliquez sur **Configuration IP > IPv6 Management and Interfaces (Interfaces et gestion IPv6) > Relais DHCPv6 > Global Destinations (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.
- **Interface IPv6 de destination** : saisissez l'interface sur laquelle les paquets sont transmis lorsque le type d'adresse du serveur DHCPv6 est **Liaison locale** ou **Multidiffusion**.

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 > IPv6 Management and Interfaces (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.
- **Interface IPv6** : saisissez l'interface sur laquelle les paquets sont transmis lorsque le type d'adresse du serveur DHCPv6 est **Liaison locale** ou **Multidiffusion**.

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

Nom 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** > **Nom de domaine** > **Paramètres DNS**.

ÉTAPE 2 Saisissez les paramètres.

- **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).
  - **DHCP Domain Search List (Liste de recherche de domaine DHCP)** : cliquez sur **Détails** pour afficher la liste des serveurs DNS configurés sur le périphérique.

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

Table des serveurs DNS : Les champs suivants sont affichés 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 4 Vous pouvez définir jusqu'à huit serveurs DNS. Pour ajouter un serveur DNS, cliquez sur **Ajouter**.

Saisissez les paramètres.

- **Version IP** : sélectionnez Version 6 pour IPv6 ou Version 4 pour IPv4.

- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, 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 5 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 qui ont été configurés sur le périphérique :

ÉTAPE 1 Cliquez sur **Configuration IP** > **Nom 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 et 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.
- **Adresse IP** : adresse IP d'hôte.
- **Version IP** : 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'il s'agit d'une entrée dynamique, cette option indique combien de temps elle demeurera dans le cache.
- **Remaining TTL (TTL restante)** : s'il s'agit d'une entrée dynamique, cette option indique combien de temps supplémentaire elle demeurera 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 uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, sélectionnez l'interface de réception.
- **Nom d'hôte** : 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(s) IP** : saisissez une seule adresse ou jusqu'à huit adresses IP associées (IPv4 ou IPv6).

Vous pouvez sélectionner 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.

18

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 :

- **Définition d'utilisateurs**
- **Configuration de TACACS+**
- **Configuration de RADIUS**
- **Méthode d'accès de gestion**
- **Gestion sécurisée des données confidentielles**
- **Serveur SSL**

La protection contre les attaques visant le CPU du périphérique est décrite dans les sections suivantes :

- **Configuration des services TCP/UDP**
- **Définition du 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+**
- **Configuration de RADIUS**

- Configuration de la sécurité des ports
- 802.1X
- Définition des périodes

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
- Surveillance DHCP
- Serveur SSL
- Définition du contrôle des tempêtes
- Configuration de la sécurité des ports
- Protection de la source IP
- Inspection ARP
- Contrôle d'accès
- Sécurité du premier saut

Définition d'utilisateurs

Le nom d'utilisateur/mot de passe par défaut est **cisco/cisco**. Lors de votre première ouverture de session avec le nom d'utilisateur et le mot de passe par défaut, vous devez saisir un nouveau mot de passe. La complexité des mots de passe est activée par défaut. Si le mot de passe que vous choisissez n'est pas suffisamment complexe (les **Paramètres de complexité du mot de passe** peuvent être activés sur la page Sécurité du mot de passe), le système vous invite à créer un autre mot de passe.

Définition de comptes d'utilisateurs

La page Comptes d'utilisateur vous permet de saisir des utilisateurs supplémentaires autorisés à accéder au 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 d'utilisateurs**.

Cette page affiche les utilisateurs définis dans le système ainsi que leur niveau de privilèges.

ÉTAPE 2 Sélectionnez **Service de récupération du mot de passe** pour activer cette fonction. Lorsque cette fonction est activée, un utilisateur final disposant d'un accès physique au port de console du périphérique peut accéder au menu de démarrage et déclencher le processus de récupération du mot de passe. Lorsque le processus de démarrage du système est terminé, vous êtes autorisé à vous connecter au périphérique sans authentification de mot de passe. L'accès au périphérique est autorisé uniquement par le biais de la console et exclusivement lorsque la console est connectée au périphérique avec accès physique.

Lorsque le mécanisme de récupération du mot de passe est désactivé, l'accès au menu de démarrage est toujours autorisé et vous pouvez déclencher le processus de récupération du mot de passe. La différence est que dans ce cas, tous les fichiers de configuration et les fichiers des utilisateurs sont supprimés durant le processus de démarrage du système et un message de journal approprié est généré sur le terminal.

ÉTAPE 3 Cliquez sur **Ajouter** pour ajouter un nouvel utilisateur ou sur **Modifier** pour en modifier un.

ÉTAPE 4 Saisissez les paramètres.

- **Nom d'utilisateur** : saisissez un nouveau nom d'utilisateur comportant 20 caractères maximum. Les caractères UTF-8 sont interdits.
- **Mot de passe** : saisissez un mot de passe (les caractères UTF-8 sont interdits). Si vous définissez la sécurité et la complexité du mot de passe, le mot de passe de l'utilisateur doit être conforme à la stratégie configurée à la section **Définition des règles de complexité du mot de passe**.
- **Confirmer le mot de passe** : saisissez à nouveau le mot de passe.
- **Mesure de la robustesse du mot de passe** : affiche le niveau de robustesse du mot de passe. Vous pouvez définir la stratégie de sécurité et de complexité du mot de passe sur la page Sécurité du mot de passe.

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

Définition de règles de complexité des mots de passe

Les mots de passe permettent d'authentifier les utilisateurs qui accèdent au périphérique. Les mots de passe simples constituent des risques de sécurité potentiels. Par conséquent, les exigences de complexité du mot de passe sont appliquées par défaut et peuvent être configurées si nécessaire. Vous pouvez configurer les exigences de complexité du mot de passe sur la page **Sécurité du mot de passe** accessible via le menu déroulant Sécurité. En outre, le délai d'expiration du mot de passe peut être configuré sur cette page.

Pour définir les règles de complexité des mots de passe :

ÉTAPE 1 Cliquez sur **Sécurité** > **Fiabilité du mot de passe**.

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 :

- **Longueur minimale du mot de passe** : saisissez le nombre minimum de caractères requis pour les mots de passe.

  REMARQUE : un mot de passe de longueur nulle (pas de mot de passe) est autorisé, et un délai d'expiration du mot de passe peut lui être attribué.

- **Répétition de caractères autorisée** : saisissez le nombre de fois qu'un caractère peut être répété.
- **Nombre minimum de classes de caractères** : saisissez le nombre de classes de caractères qui doivent être présentes dans un mot de passe. Les classes de caractères sont minuscules (1), majuscules (2), chiffres (3) et symboles ou caractères spéciaux (4).
- **Le nouveau mot de passe doit être différent de l'actuel** : si cette option est sélectionnée, lors de la modification du mot de passe, le nouveau mot de passe ne peut pas être identique au mot de passe actuel.

ÉTAPE 5 Cliquez sur **Appliquer**. Les paramètres de mot de passe sont écrits dans le fichier de Configuration d'exécution.

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)*.

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 :

Tableau 2:

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 les autres paramètres sur les pages TACACS+ et Ajouter un serveur 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.

Configuration d'un serveur 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 la comptabilité 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.
- **IPv4 source** : (en mode système de couche 3 uniquement) sélectionnez l'interface source IPv4 du périphérique à utiliser dans les messages envoyés pour les communications avec le serveur TACACS+.
- **IPv6 source** : (en mode système de couche 3 uniquement) 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.

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 uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : 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.
- **Adresse IP source** : (Pour périphériques SG500X et autres en mode système de couche 3). Vous pouvez utiliser l'adresse source du périphérique par défaut ou l'une des adresses IP du périphérique disponibles pour la communication avec le serveur TACACS+.
- **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 possédez pas de chaîne de clé chiffrée (à partir d'un autre périphérique), saisissez la chaîne de clé en mode Texte en clair et cliquez sur **Appliquer**. La chaîne de clé chiffrée est générée et affichée.

  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** : saisissez la durée 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** : 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 Pour afficher les données sensibles sous la forme de texte en clair dans le fichier de configuration, cliquez sur **Afficher les données sensibles en texte clair**.

ÉTAPE 8 Cliquez sur **Appliquer**. Le serveur TACACS+ est ajouté au fichier de Configuration d'exécution du périphérique.

Configuration de RADIUS

Les serveurs RADIUS (Remote Authorization Dial-In User Service) offrent un contrôle d'accès réseau basé sur MAC ou 802.1X centralisé. Le périphérique est un client RADIUS pouvant utiliser un serveur RADIUS pour fournir une sécurité centralisée.

Une société peut établir un serveur RADIUS (Remote Authorization Dial-In User Service, service d'authentification à distance des utilisateurs) pour fournir un contrôle d'accès réseau basé MAC ou 802.1X centralisé à tous ses périphériques. 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 RADIUS utilisant 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.

Gestion de comptes utilisant un serveur RADIUS

L'utilisateur peut activer la gestion de comptes des sessions de connexion à l'aide d'un 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 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 > 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.

- **Tentatives** : saisissez le nombre de demandes transmises qui sont envoyées au serveur RADIUS avant que le système considère qu'une défaillance s'est produite.
- **Délai de réponse** : saisissez le nombre de secondes pendant lesquelles le 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 possédez pas de chaîne de clé chiffrée (à partir d'un autre périphérique), saisissez la chaîne de clé en mode Texte en clair et cliquez sur **Appliquer**. La chaîne de clé chiffrée est générée et affichée.

Cette clé remplace la chaîne de clé par défaut, si une telle clé a été définie.

- **IPv4 source** : (en mode système de couche 3 uniquement) sélectionnez l'interface source IPv4 du périphérique à utiliser dans les messages envoyés pour les communications avec le serveur RADIUS.
- **IPv6 source** : (en mode système de couche 3 uniquement) sélectionnez l'interface source IPv6 du périphérique à utiliser dans les messages envoyés 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** : indique que le type d'adresse IPv6 est Global.
- **Type d'adresse IPv6** : sélectionnez le type d'adresse IPv6 (en cas d'utilisation d'IPv6). Les options sont les suivantes :
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : 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.

- **Priorité** : 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** : 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 ont été effectuées. 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** : entrez le nombre de demandes envoyées au serveur RADIUS avant qu'un échec soit avéré. Si l'option **Valeurs par défaut** est sélectionnée, le périphérique utilise la valeur par défaut du nombre de tentatives.
- **Délai d'inactivité** : saisissez le nombre de minutes qui doivent s'écouler avant qu'un serveur RADIUS non réactif soit contourné pour les demandes de services. Si l'option **Valeurs par défaut** est sélectionnée, le 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 Pour afficher les données sensibles sous la forme de texte en clair dans le fichier de configuration, cliquez sur **Afficher les données sensibles en texte clair**.

ÉTAPE 7 Cliquez sur **Appliquer**. La définition du serveur RADIUS est ajoutée au fichier de Configuration d'exécution du périphérique.

Méthode d'accès de gestion

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
  - Telnet sécurisé (SSH)
  - Hypertext Transfer Protocol (HTTP)
  - HTTPS (Secure HTTP)
  - SNMP (Simple Network Management Protocol)
  - Tous les éléments ci-dessus
- **Action** : permet d'autoriser ou de refuser l'accès à une interface ou à une adresse source.
- **Interface** : ports, LAG ou VLAN, autorisés à accéder à l'utilitaire de configuration Web ou interdits d'accès à celui-ci.

- **Adresse IP source** : adresses IP ou sous-réseaux. 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 actif

La page Profils d'accès affiche les profils d'accès définis et permet de sélectionner un profil d'accès en tant que profil actif.

Lorsqu'un utilisateur tente d'accéder au 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 **Définition de règles de profils**.

Utilisez la page Profils d'accès pour créer un profil d'accès et ajouter sa première règle. Si le profil d'accès ne contient qu'une seule règle, vous avez terminé. Pour ajouter des règles supplémentaires au profil, utilisez la page Règles de profils.

ÉTAPE 1 Cliquez sur **Sécurité** > **Méthode d'accès de gestion** > **Profils d'accès**.

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.

- **Priorité des règles** : saisissez la priorité des règles. Lorsque le paquet est mis en correspondance avec une règle, les groupes d'utilisateurs se voient accorder ou refuser l'accès au 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. Le 1 correspond à la priorité la plus élevée.
- **Méthode de gestion** : sélectionnez la méthode de gestion pour laquelle la règle est définie. Les options sont les suivantes :
  - *Tout* : affecte toutes les méthodes de gestion à la règle.
  - *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.
- **S'applique à l'interface** : sélectionnez l'interface rattachée à la règle. Les options sont les suivantes :
  - *Tout* : s'applique à tous les ports, VLAN et LAG.
  - *Défini par l'utilisateur* : s'applique à l'interface sélectionnée.
- **Interface** : entrez le numéro d'interface si l'option Défini par l'utilisateur a été sélectionnée.
- **S'applique à l'adresse IP source** : sélectionnez le type d'adresse IP source auquel le profil d'accès s'applique. Le champ *Adresse IP source* est valide pour un sous-réseau. Sélectionnez l'une des valeurs suivantes :
  - *Tout* : s'applique à tous les types d'adresses IP.
  - *Défini par l'utilisateur* : s'applique uniquement aux types d'adresses IP définis dans les champs.
- **Adresse IP** : saisissez l'adresse IP source.
- **Masque** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs suivants :
  - *Masque de réseau* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Longueur du préfixe* : sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l'adresse IP source.

ÉTAPE 7 Cliquez sur **Appliquer.** Le profil d'accès est écrit dans le fichier de Configuration d'exécution. Vous pouvez à présent sélectionner ce profil d'accès en tant que profil d'accès actif.

Définition de règles de profils

Les profils d'accès peuvent comporter jusqu'à 128 règles afin de déterminer qui est autorisé à gérer le 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 profils**.

ÉTAPE 2 Sélectionnez le champ Filtre et un profil d'accès. Cliquez sur **OK**.

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.
- **Priorité des règles** : saisissez la priorité des règles. Lorsque le paquet est mis en correspondance avec une règle, les groupes d'utilisateurs se voient accorder ou refuser l'accès au 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.
- **Méthode de gestion** : sélectionnez la méthode de gestion pour laquelle la règle est définie. Les options sont les suivantes :
  - *Tout* : affecte toutes les méthodes de gestion à la règle.
  - *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 Telnet 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 **Autoriser** pour autoriser les utilisateurs qui essaient d'accéder au périphérique en utilisant la méthode d'accès configurée depuis l'interface et la source IP définies dans cette règle. Ou sélectionnez **Refuser** pour refuser l'accès.
- **S'applique à l'interface** : sélectionnez l'interface rattachée à la règle. Les options sont les suivantes :
  - *Tout* : s'applique à tous les ports, VLAN et LAG.
  - *Défini par l'utilisateur* : s'applique uniquement au port, VLAN ou LAG sélectionné.
- **Interface** : entrez le numéro d'interface.
- **S'applique à l'adresse IP source** : sélectionnez le type d'adresse IP source auquel le profil d'accès s'applique. Le champ *Adresse IP source* est valide pour un sous-réseau. Sélectionnez l'une des valeurs suivantes :
  - *Tout* : s'applique à tous les types d'adresses IP.
  - *Défini par l'utilisateur* : s'applique uniquement aux types d'adresses IP définis dans les champs.
- **Version IP** : sélectionnez la version IP prise en charge pour l'adresse source : IPv6 ou IPv4.
- **Adresse IP** : saisissez l'adresse IP source.

- **Masque** : sélectionnez le format du masque de sous-réseau pour l'adresse IP source et saisissez une valeur dans l'un des champs :
  - *Masque de réseau* : sélectionnez le sous-réseau auquel l'adresse IP source appartient et saisissez le masque de sous-réseau en utilisant un format décimal séparé par des points.
  - *Longueur du préfixe* : sélectionnez la longueur du préfixe et saisissez le nombre d'octets compris dans le préfixe de l'adresse IP source.

ÉTAPE 5 Cliquez sur **Appliquer**. La règle est ajoutée au profil d'accès.

Authentification de l'accès de gestion

Vous pouvez attribuer des méthodes d'authentification aux différentes méthodes d'accès de gestion, telles que SSH, console, Telnet, HTTP et HTTPS. L'authentification peut être effectuée localement ou sur un serveur TACACS+ ou 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.

L'authentification de l'utilisateur s'effectue en fonction de l'ordre de sélection des méthodes d'authentification. Si la première méthode d'authentification n'est pas disponible, la méthode suivante sera utilisée. Par exemple, si les méthodes d'authentification sélectionnées sont RADIUS et Local, et que tous les serveurs RADIUS configurés sont interrogés en vertu de leur ordre de priorité et qu'ils ne répondent pas, l'utilisateur sera authentifié au niveau local.

Si une méthode d'authentification échoue ou si le niveau de privilège d'un utilisateur est insuffisant, ce dernier se voit refuser l'accès au périphérique. En d'autres termes, si l'authentification échoue au niveau d'une méthode d'authentification, le périphérique n'essaie pas d'utiliser la méthode d'authentification suivante et s'arrête.

Pour définir les méthodes d'authentification d'une méthode d'accès :

ÉTAPE 1 Cliquez sur **Sécurité** > **Authentification de l'accès de gestion**.

ÉTAPE 2 Sélectionnez une méthode d'accès dans la liste **Application**.

ÉTAPE 3 Utilisez les flèches pour déplacer la méthode d'authentification entre les colonnes Méthodes facultatives et Méthodes sélectionnées. La première méthode sélectionnée correspond à celle qui sera utilisée en premier.

- *RADIUS* : l'utilisateur est authentifié sur un serveur RADIUS. Vous devez avoir configuré un ou plusieurs serveurs RADIUS.
- *TACACS+* : l'utilisateur est authentifié sur le serveur TACACS+. Vous devez avoir configuré un ou plusieurs serveurs TACACS+.
- *Aucun* : l'utilisateur est autorisé à accéder au périphérique sans avoir été authentifié.
- *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 **Aucun** doit toujours être sélectionnée en dernier. Toutes les méthodes d'authentification sélectionnées après **Local** ou **Aucun** sont ignorées.

ÉTAPE 4 Cliquez sur **Appliquer**. Les méthodes d'authentification sélectionnées sont associées à la méthode d'accès.

Gestion sécurisée des données confidentielles

Reportez-vous à la section **Sécurité : Gestion sécurisée des données confidentielles**.

Serveur SSL

Cette section décrit la fonctionnalité SSL (Secure Socket Layer).

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.

Configuration et paramètres par défaut

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 concernant les certificats 1 et 2 apparaissent dans la Table de clés de serveur SSL. Ces champs sont définis sur la page **Modifier**, excepté pour les champs suivants :

- **Valide du** : spécifie la date à partir de laquelle le certificat est valide.
- **Valide jusqu'au** : spécifie la date jusqu'à laquelle le certificat est valide.
- **Source du certificat** : spécifie si le certificat a été généré par le système (Autogénéré) ou l'utilisateur (Défini par l'utilisateur).

ÉTAPE 2 Sélectionnez un certificat actif.

ÉTAPE 3 Cliquez sur **Générer une demande de certificat**.

ÉTAPE 4 Renseignez les champs suivants :

- **Regénérer une clé RSA** : sélectionnez-le pour regénérer la clé RSA.
- **Longueur de clé** : entrez la longueur de la clé RSA à générer.
- **Nom courant** : spécifie l'adresse IP ou l'URL complète de l'appareil. Si elle n'est pas indiquée, le système utilisera l'adresse IP la plus basse de l'appareil (lors de la génération du certificat).
- **Unité organisationnelle** : spécifie l'unité organisationnelle ou le nom du service.
- **Nom de l'organisation** : spécifie le nom de l'organisation.
- **Lieu** : spécifie l'emplacement ou le nom de la ville.
- **État** : spécifie le nom de l'état ou de la province.
- **Pays** : spécifie le nom du pays.
- **Durée** : spécifie le nombre de jours de validité d'une certification.

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).

Pour importer 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.
- **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 **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).

ÉTAPE 5 Cliquez sur **Appliquer** pour appliquer les modifications dans la Configuration d'exécution.

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.

Serveur SSH

Reportez-vous à la section **Sécurité : Serveur SSH**.

Client SSH

Reportez-vous à la section **Sécurité : Client SSH**.

Configuration des 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.

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.)

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

Définition du contrôle des tempêtes

Lorsque des trames de Diffusion (Broadcast), Multidiffusion (Multicast) ou Monodiffusion inconnue (Unknown Unicast) sont reçues, elles sont dupliquées et une copie est envoyée à tous les ports de sortie possibles. Cela signifie dans la pratique qu'elles sont envoyées à tous les ports appartenant au VLAN approprié. De cette manière, une seule trame d'entrée est convertie en plusieurs trames, ce qui peut potentiellement occasionner une tempête de trafic.

La protection contre les tempêtes vous permet de limiter le nombre de trames entrant dans le 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.

Pour définir le contrôle des tempêtes :

ÉTAPE 1 Cliquez sur **Sécurité** > **Contrôle des tempêtes**.

Tous les champs de cette page sont décrits sur la page Modifier le contrôle des tempêtes, excepté pour le **Seuil de débit de contrôle des tempêtes (%)**. Il affiche le pourcentage de la bande passante totale disponible pour les paquets de Monodiffusion inconnue (Unknown Unicast), Multidiffusion (Multicast) et Diffusion (Broadcast) avant que le contrôle des tempêtes ne soit appliqué sur le port. La valeur par défaut est 10 % du débit maximal du port. Vous pouvez la définir sur la page Modifier le contrôle des tempêtes.

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

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez le port pour lequel activer le contrôle des tempêtes.
- **Contrôle des tempêtes** : sélectionnez cette option pour activer le contrôle des tempêtes.

- **Seuil de débit de contrôle des tempêtes** : saisissez le débit maximum auquel les paquets inconnus peuvent être transmis. La valeur par défaut de ce seuil est 10 000 pour les appareils FE et 100 000 pour les appareils GE.
- **Mode de contrôle des tempêtes** : sélectionnez l'un des modes suivants.
  - *Monodiffusion inconnue, multidiffusion et diffusion* : intègre le trafic de Monodiffusion inconnue (Unknown Unicast), Diffusion (Broadcast) et Multidiffusion (Multicast) au sein du seuil de la bande passante.
  - *Multidiffusion et diffusion* : intègre le trafic de Diffusion (Broadcast) et Multidiffusion (Multicast) au sein du seuil de la bande passante.
  - *Diffusion uniquement* : intègre uniquement le trafic de diffusion au sein du seuil de la bande passante.

ÉTAPE 4 Cliquez sur **Appliquer**. Le contrôle des tempêtes est modifié et le fichier de Configuration d'exécution est mis à jour.

Configuration de la sécurité des ports

Vous pouvez accroître la sécurité réseau en limitant l'accès à un port pour des utilisateurs disposant d'adresses MAC spécifiques. Les adresses MAC peuvent être apprises de façon dynamique ou configurées de manière statique.

La sécurité des ports surveille les paquets reçus et appris. L'accès aux ports verrouillés est limité aux utilisateurs disposant d'adresses MAC spécifiques.

La sécurité des ports dispose de quatre modes :

- **Verrouillage classique** : toutes les adresses MAC apprises sur le port sont verrouillées et le port n'apprend aucune nouvelle adresse MAC. Les adresses apprises ne sont pas soumises à un délai d'expiration ni à un réapprentissage.
- **Verrouillage dynamique limité** : le 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.

REMARQUE Pour utiliser 802.1X sur un port, il doit être en mode Hôtes multiples ou Sessions multiples. La sécurité des ports ne peut pas être définie sur un port si ce dernier est un mode unique (reportez-vous à la page 802.1x, Authentification hôtes et sessions).

Pour configurer la sécurité des ports :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité des ports**.

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.

- **Mode d'apprentissage** : sélectionnez le type de verrouillage du port. L'État de l'interface doit être déverrouillé pour que ce champ puisse être configuré. Le champ Mode d'apprentissage est uniquement activé si le champ *État de l'interface* est verrouillé. Pour modifier le Mode d'apprentissage, État de l'interface doit être désactivé. Une fois ce mode modifié, vous pouvez rétablir l'état de l'interface. Les options sont les suivantes :
  - *Verrouillage classique* : verrouille immédiatement le port, quel que soit le nombre d'adresses ayant déjà été apprises.
  - *Verrouillage dynamique limité* : verrouille le port en supprimant les adresses MAC dynamiques actuellement associées au port. Le port apprend au maximum le nombre d'adresses autorisées sur le port. Le réapprentissage et le délai d'expiration des adresses MAC sont activés.
  - *Sécurisé en permanence* : conserve les adresses MAC dynamiques actuellement associées au port et apprend au maximum le nombre d'adresses autorisées sur le port (défini par l'option **Nombre max. d'adresses autorisées**). Les opérations de réapprentissage et de délai d'expiration sont activées.
  - *Suppression sécur. à la réinitialisation* : supprime les adresses MAC dynamiques actuellement associées au port après la réinitialisation. Les nouvelles adresses MAC peuvent être apprises en tant qu'adresses supprimées à la réinitialisation (Delete-On-Reset) jusqu'au nombre d'adresses autorisées sur le port. Les opérations de réapprentissage et de délai d'expiration sont désactivées.
- **Nombre max. d'adresses autorisées** : saisissez le nombre maximum d'adresses MAC pouvant être apprises sur le port dans la mesure où le mode d'apprentissage *Verrouillage dynamique limité* est sélectionné. Le chiffre 0 indique que seules les adresses statiques sont prises en charge dans l'interface.
- **Action en cas de violation** : sélectionnez l'action à appliquer aux paquets qui arrivent sur un port verrouillé. Les options sont les suivantes :
  - *Abandonner* : abandonne les paquets en provenance d'une source non apprise.
  - *Transférer* : transfère les paquets en provenance d'une source inconnue sans apprendre l'adresse MAC.
  - *Arrêter* : abandonne les paquets en provenance d'une source non apprise et ferme le port. Le port reste fermé jusqu'à ce qu'il soit réactivé ou jusqu'à ce que le périphérique soit réinitialisé.

- « **Trap** » : sélectionnez cette option pour activer les interceptions 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 interception(s)** : saisissez la durée minimale qui s'écoulera entre deux interceptions.

ÉTAPE 4 Cliquez sur **Appliquer**. La sécurité des ports est modifiée et le fichier de Configuration d'exécution est mis à jour.

802.1X

Reportez-vous au chapitre **Sécurité : Authentification 802.1X** pour obtenir de plus amples informations sur l'authentification 802.1x. Il traite également de l'authentification MAC et Web.

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 dénis de service (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 CPU du périphérique.

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 l'appareil 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 CPU.

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

La fonction SCT peut être contrôlée sur la page Déni de service > Prévention du déni de service > Paramètres de la suite de sécurité (bouton **Détails**).

Types de dénis de service (DoS)

Les types de paquets suivants, ou d'autres stratégies, peuvent être impliqués dans un 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 nouvelle 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 dénis de service (DoS)

*La fonctionnalité Prévention du déni de service (Do*S) permet à l'administrateur système de résister à ces attaques 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.
- Blocage de paquets contenant des adresses martiennes (page Adresses martiennes)
- Empêcher les connexions TCP à partir d'une interface spécifique (page Filtrage SYN) et limiter le débit des paquets (page Protection du débit SYN)
- Configuration du blocage de certains paquets ICMP (page Filtrage ICMP)
- Abandon des paquets IP fragmentés issus d'une interface spécifique (page Filtrage de fragments IP)

- Empêchez 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.

Configuration de la prévention du déni de service (DoS)

Les pages suivantes sont utilisées pour configurer cette fonctionnalité.

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**. La page *Paramètres de la suite de sécurité* s'affiche.

Mécanisme de protection CPU : Activé indique que la fonction SCT est activée.

ÉTAPE 2 Cliquez sur **Détails** en regard de **Utilisation du CPU** pour accéder à la page Utilisation du CPU et afficher les informations d'utilisation des ressources du CPU.

ÉTAPE 3 Cliquez sur **Modifier** en regard de **Protection TCP SYN** pour accéder à la page Protection SYN et activer cette fonctionnalité.

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.

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 **Appliquer**. Les paramètres de la suite de sécurité de prévention du déni de service sont écrits dans le fichier de Configuration d'exécution.

- Si la Protection de niveau interface est sélectionnée, cliquez sur le bouton **Modifier** approprié pour configurer la protection souhaitée.

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 CPU compte les paquets SYN entrant par seconde par chaque port de réseau vers le CPU.

Si le nombre est supérieur au nombre spécifique, le seuil défini par l'utilisateur, un SYN de déni avec une règle MAC-to-me est appliqué sur le port. Cette règle est supprimée de l'intervalle défini par l'utilisateur du port (période de protection SYN).

Pour configurer 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 sur **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 supprimé du port).

ÉTAPE 3 Cliquez sur **Appliquer**. La protection SYN est défini et le fichier de Configuration d'exécution est mis à jour.

Table d'interface de protection SYN affiche les champs suivants pour chaque port ou LAG (en fonctions 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 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 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.
- **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 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.

Cette fonction est uniquement disponible lorsque le périphérique est en mode système de couche 2.

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 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 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.

Surveillance DHCP

Reportez-vous à la section **Surveillance et relais DHCPv4**.

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.

Interactions avec les autres fonctions

Les points suivants sont importants 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).

Configuration du workflow de la protection de la source IP

Pour configurer la protection de la source IP :

ÉTAPE 1 Activez la surveillance DHCP à la page >Configuration IP > DHCP Propriétés ou à la page Sécurité > Surveillance DHCP > Propriétés.

ÉTAPE 2 Définissez les VLAN sur lesquels la surveillance DHCP est activée à la page Configuration IP > DHCP > Paramètres d'interface.

ÉTAPE 3 Indiquez si les interfaces sont sécurisées ou non sécurisées dans la page Configuration IP > DHCP > Interface de surveillance DHCP.

ÉTAPE 4 Activez la protection de la source IP à la page >Sécurité > Protection de la source IP Propriétés.

ÉTAPE 5 Activez la protection de la source IP sur les interfaces non sécurisées, comme requis, à la page Sécurité > Protection de la source IP > Paramètres d'interface.

ÉTAPE 6 Affichez les entrées de la base de données de liaison à la page Sécurité > Protection de la source IP > Base de données de liaison.

Activation de la protection de la source IP

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.

Configuration de la protection de la source IP sur des interfaces

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 **Surveillance et relais DHCPv4**.

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 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.

Pour afficher un sous-ensemble de ces entrées, saisissez les critères de recherche appropriés et cliquez sur **OK**.

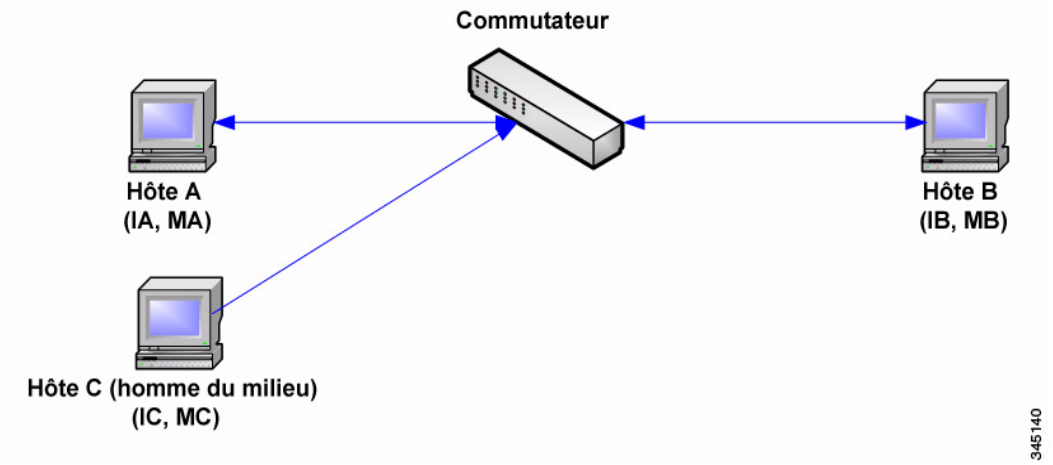
Inspection ARP

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 transférer le trafic intercepté vers ces hôtes en utilisant l'adresse MAC correcte en guise de destination. L'hôte C s'est par conséquent inséré dans le flux de trafic situé entre l'hôte A et l'hôte B, exécutant ainsi une attaque classique dite de l'homme du milieu.

Comment ARP peut empêcher l'empoisonnement de cache

La fonction d'inspection ARP s'applique aux interfaces sécurisées ou non (reportez-vous à la page Sécurité > Inspection ARP > 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 sécurisées. Les paquets ARP qui sont reçus sur une interface sécurisée sont simplement transférés.

La logique suivante est appliquée lors de l'arrivée de paquets sur des interfaces non sécurisées :

- 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 la surveillance DHCP est activée pour le VLAN du paquet, le système recherche la paire <VLAN - adresse IP> du paquet dans la base de données de liaison de surveillance DHCP. Si la paire <VLAN - adresse IP> a été trouvée et si l'adresse MAC ainsi que l'interface dans la base de données correspondent à l'adresse MAC et à l'interface d'entrée du paquet, alors le paquet est valide.
- Si l'adresse IP du paquet est introuvable dans les règles de contrôle d'accès ARP ou dans la base de données de liaison de surveillance DHCP, le paquet n'est pas valide et il est supprimé. Un message SYSLOG est alors généré.
- Lorsqu'un paquet est valide, il est transféré et le cache ARP est mis à jour.

Si l'option 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 multidiffusion IP.

Les paquets contenant des liaisons d'inspection ARP non valides sont journalisés 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 la surveillance DHCP

Si la surveillance DHCP est activée, l'inspection ARP utilise la base de données de liaison de surveillance DHCP en plus des règles de contrôle d'accès ARP. Si la surveillance DHCP n'est pas activée, 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 configurez diverses options à la page Sécurité > Inspection ARP > Propriétés.

ÉTAPE 2 Configurez les interfaces en tant qu'interfaces ARP sécurisées ou non à la page Sécurité > Inspection ARP > Paramètres d'interface.

ÉTAPE 3 Ajoutez des règles à la page Sécurité > Inspection ARP > Contrôle d'accès ARP et 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 à la page Sécurité > Inspection ARP > Paramètres VLAN.

Définition des propriétés d'inspection ARP

Pour configurer 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 suivantes :
  - **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 multidiffusion IP.
- **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.

Définition des paramètres des interfaces d'inspection ARP dynamique

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.

Définition du contrôle d'accès d'inspection 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 MAC** : adresse MAC du paquet.
- **Adresse IP** : adresse IP du paquet.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres sont définis et le fichier de Configuration d'exécution est mis à jour.

Définition des règles de contrôle d'accès d'inspection 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.

ÉTAPE 2 Pour ajouter des règles supplémentaires à un groupe, cliquez sur **Ajouter**.

ÉTAPE 3 Sélectionnez un groupe de contrôle d'accès et renseignez les champs suivants :

- **Adresse MAC** : adresse MAC du paquet.
- **Adresse IP** : adresse IP du paquet.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres sont définis et le fichier de Configuration d'exécution est mis à jour.

Définition des paramètres VLAN d'inspection ARP

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 groupe **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

19

Sécurité : Authentification 802.1X

Cette section décrit l'authentification 802.1X.

Elle couvre les rubriques suivantes :

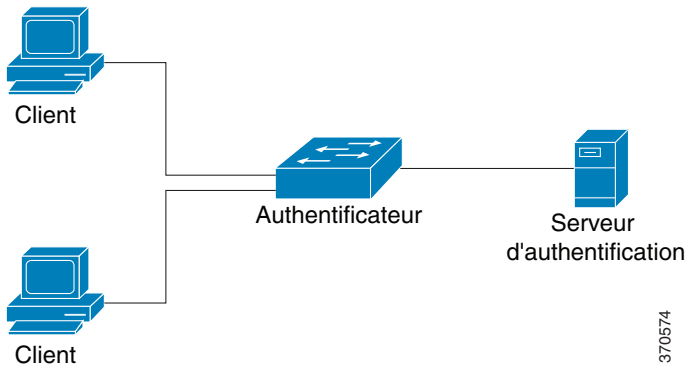
- **Présentation de 802.1X**
- **Présentation de l'authentificateur**
- **Tâches courantes**
- **Configuration de 802.1X via l'interface utilisateur graphique (GUI)**
- **Définition des périodes**
- **Prise en charge des méthodes d'authentification et des modes de port**

Présentation de 802.1X

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 modes d'authentification suivants sur les ports sont pris en charge (vous pouvez définir ces modes dans Sécurité > Authentification MAC/Web 802.1X > Hôte et Authentification) :

- **Hôte unique** : prend en charge l'authentification basée sur les ports avec un seul client par port.
- **Hôtes multiples** : prend en charge l'authentification basée sur les ports avec plusieurs clients par port.

- **Sessions multiples** : prend en charge l'authentification basée sur les clients avec plusieurs clients par port.

Pour plus d'informations, reportez-vous à la section **Modes hôte de port**.

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.

Dans l'authentification 802.1x, l'authentificateur extrait les messages EAP des messages 802.1x (trames 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.

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.

Présentation de l'authentificateur

États d'authentification administrative du port

L'état administratif du port détermine si le client a accès au réseau.

L'état administratif du port peut être configuré sur la page Sécurité > Authentification 802.1X/MAC/Web > Authentification des ports.

La 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 **Définition de l'authentification des hôtes et sessions**. Le commutateur envoie les paquets EAP 802.1x qui intègrent les message d'erreur EAP lorsqu'il reçoit les messages de démarrage EAPOL 802.1x.

- **auto**

  Active les authentifications 802.1 x conformément au mode hôte de port configuré et aux méthodes d'authentification configurées sur le port.

Modes hôte de port

Les ports peuvent être définis dans les modes hôte de port suivants (configurés sur la page Sécurité > Authentification 802.1X/MAC/Web > Hôte et Authentification) :

- **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 Sécurité > Authentification 802.1X/MAC/Web > 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. Ce mode requiert une recherche TCAM. Puisque les commutateurs du mode Couche 3 (voir **Prise en charge du mode Sessions multiples**) n'ont pas de recherche TCAM allouée pour le mode Sessions multiples, ils prennent en charge une forme limitée de mode Sessions multiples, qui n'autorise pas les attributs VLAN invité et VLAN RADIUS. Le nombre maximal d'hôtes autorisés sur le port doit être configuré sur la page Authentification des ports.

  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.

  Si un hôte autorisé se voit attribuer un VLAN par un serveur RADIUS, tout son trafic balisé et non balisé n'appartenant pas aux VLAN non authentifiés est ponté via le VLAN ; si le VLAN n'est pas attribué, tout son trafic est ponté en fonction de la configuration du port d'appartenance au VLAN statique.

Le Sx300 en mode routeur Couche 3 prend en charge le mode Sessions multiples sans attribution de VLAN invité et VLAN RADIUS :

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.

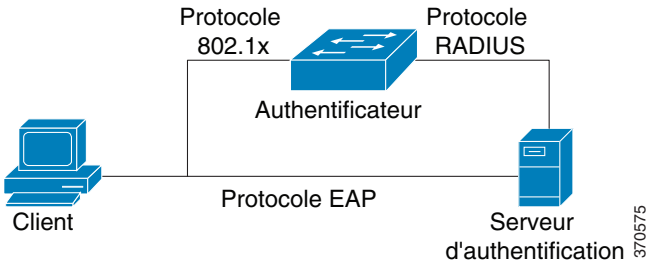
Lorsqu'une méthode d'authentification s'exécute avec succès pour un client authentifié par une méthode d'authentification ayant une priorité plus basse, les attributs de la nouvelle méthode d'authentification sont appliqués. Lorsque la nouvelle méthode échoue, le client continue à être autorisé pour 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

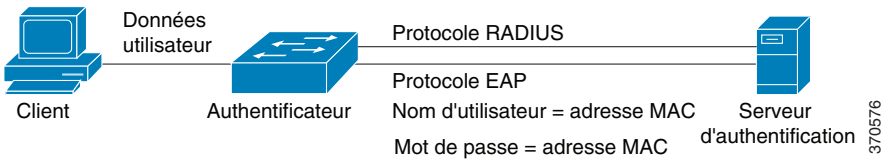


Authentification MAC

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



La 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 des clients non autorisés vers le port, à l'exception des paquets ARP, DHCP, DNS et NETBIOS. 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.

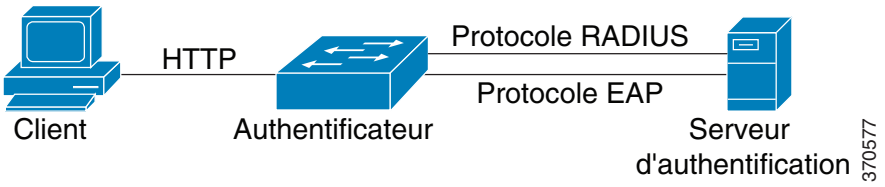
Tous les paquets HTTP/HTTPS sur IPv4 issus des clients non autorisés sont interceptés par le processeur sur le commutateur. Lorsqu'un utilisateur demande l'accès au réseau, si l'authentification Web est activée sur le port, une page de connexion apparaît avant que la page demandée ne s'affiche. L'utilisateur 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 **Tableau 1 Modes de port et méthodes d'authentification**.

Lorsque l'authentification est terminée, le commutateur transfère tout le trafic provenant du client sur le port, comme indiqué 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 via la page Sécurité > Authentification 802.1X/MAC/Web > Personnalisation de l'authentification Web.

Vous pouvez prévisualiser chacune des pages personnalisées. La configuration est enregistrée dans le fichier de Configuration d'exécution.

Le tableau suivant indique les références qui prennent en charge l'authentification Web et dans quels modes système :

Référence	Mode système	WBA pris en charge
Sx300	**Couche 2**	Oui
	Couche 3	Non
Sx500, Sx500ESW2-550X	**Couche 2**	Oui
	Couche 3	Non
SG500X	**Natif**	Oui
	Hybride de base - Couche 2	Oui
	Hybride de base - Couche 3	Non
SG500XG	**Identique à Sx500**	Oui

REMARQUE

- Si l'authentification Web n'est pas prise en charge, VLAN invité et DVA ne peuvent pas être configurés en mode Sessions multiples.
- Si l'authentification Web est prise en charge, VLAN invité et DVA peuvent être configurés en mode Sessions multiples.

VLAN non authentifiés et VLAN invité

Les VLAN non authentifiés et le VLAN invité fournissent l'accès aux services qui ne nécessitent pas que les ports ou appareils d'abonnement disposent d'une authentification et d'une autorisation basées sur MAC ou 802.1X.

Le VLAN invité est le VLAN attribué à un client non autorisé. Vous pouvez configurer le VLAN invité et un ou plusieurs VLAN pour qu'ils soient non authentifiés via la page Sécurité > Authentification 802.1X/MAC/Web > 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 **« Tableau 3 Prise en charge de l'attribution VLAN invité et 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 en Couche 2**

  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.

- **Mode Sessions multiples en Couche 3**

  Le mode ne prend pas en charge le VLAN invité.

Affectation VLAN RADIUS ou Affectation VLAN dynamique

Un client autorisé peut se voir attribuer un VLAN par le serveur RADIUS si cette option est activée sur la page Authentification des ports. Elle porte le nom de Dynamic VLAN Assignment (DVA) ou VLAN affecté par RADIUS. Dans ce guide, le terme VLAN affecté par RADIUS est utilisé.

Lorsqu'un port est en mode Sessions multiples et que la fonction VLAN affecté par RADIUS est activée, le périphérique ajoute automatiquement le port en tant que membre non balisé du VLAN qui est attribué par le serveur RADIUS lors du processus d'authentification. Le périphérique classe les paquets non balisés pour le VLAN attribué si les paquets proviennent des appareils ou ports qui sont authentifiés et autorisés.

Pour plus d'informations sur le comportement des différents modes lorsque la fonction VLAN affecté par RADIUS est activée sur le périphérique, reportez-vous au **Tableau 3 Prise en charge de l'attribution VLAN invité et VLAN RADIUS** and **Le tableau suivant décrit la façon dont le trafic authentifié et non authentifié est traité dans diverses situations.**.

REMARQUE .En mode Sessions multiples, l'affectation VLAN RADIUS est uniquement prise en charge lorsque le périphérique est en mode système Couche 2.

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 Affectation VLAN RADIUS sur 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.

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 complet**

  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.

- **Mode Sessions multiples en mode système Couche 3**

  Ce mode ne prend pas en charge la fonction VLAN affecté par RADIUS,

Le tableau suivant décrit la prise en charge de l'attribution VLAN invité et VLAN RADIUS en fonction de la méthode d'authentification et du mode de port.

Méthode d'authentification	Hôte unique	Hôtes multiples	Sessions multiples	
			Périphérique en L3	Périphérique en L2
802.1x	†	†	N/C	†
MAC	†	†	N/C	†
WEB	N/C	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. Cette opération 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 source 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.

Tâches courantes

Flux de travail 1 : activer l'authentification 802.1x sur un port

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X/MAC/Web > Propriétés**.

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/MAC/Web> > Authentification 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/MAC/Web > Authentification des ports**.

ÉTAPE 10 Sélectionnez un port et cliquez sur **Modifier**.

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/MAC/Web** > **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 Web

ÉTAPE 1 Cliquez sur **Sécurité > Authentification 802.1X/MAC/Web > 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 **Définition de l'authentification des ports 802.1X**.

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/MAC/Web > Authentification des ports**.

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

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/MAC/Web**> **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/MAC/Web** > **Propriétés**.

ÉTAPE 2 Sélectionnez un VLAN et 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.

Configuration de 802.1X via l'interface utilisateur graphique (GUI)

Définition des propriétés 802.1X

La page Propriétés 802.1X permet d'activer 802.1X globalement et de définir la façon dont les ports sont authentifiés. Pour que 802.1X puisse fonctionner, il doit être activé à la fois globalement et individuellement sur chaque port.

Pour définir l'authentification basée sur les ports :

ÉTAPE 1 Cliquez sur **Sécurité** > **Authentification 802.1X/MAC/Web** > **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, l'authentification 802.1X, MAC et Web est désactivée.

- **Méthode d'authentification** : sélectionnez les méthodes d'authentification des utilisateurs. Les options sont les suivantes :

  - *RADIUS, aucune* : effectue tout d'abord l'authentification des ports en utilisant le serveur RADIUS. Si aucune réponse n'est reçue de ce serveur (par exemple s'il n'est pas actif), aucune authentification n'est réalisée et la session est autorisée. 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.

- **ID du VLAN invité** : sélectionnez le VLAN invité dans la liste des VLAN.

- **Délai d'expiration VLAN invité** : définissez une période :
  - Une fois la connexion établie, si le logiciel ne détecte pas le demandeur 802.1X ou si l'authentification a échoué, le port est ajouté au VLAN invité 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.
- **Interceptions** : pour activer les interceptions, sélectionnez une ou plusieurs 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 si l'authentification MAC échoue.
  - *Interceptions de réussite d'authentification MAC* : sélectionnez cette option pour générer une interception si l'authentification MAC réussit.
- Lorsque le commutateur est en mode commutateur Couche 2 :
  - *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.

Lorsque le périphérique est en mode routeur Couche 3, 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.

Définition de l'authentification des ports 802.1X

La page Authentification des ports permet de définir les paramètres 802.1X pour chaque port. Puisque certaines modifications de la configuration ne sont possibles que si le port a l'état Autorisation forcée (par exemple, l'authentification des hôtes), il est recommandé de changer le contrôle du port en Autorisation forcée avant d'effectuer des modifications. Une fois la configuration terminée, rétablissez l'état précédent du contrôle de port.

REMARQUE Un port sur lequel 802.1X est défini ne peut pas devenir membre d'un LAG.

Pour définir l'authentification 802.1X :

ÉTAPE 1 Cliquez sur **Sécurité** > **Authentification 802.1X/MAC/Web** > **Authentification des ports**.

Cette page affiche les paramètres d'authentification de tous les ports.

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

ÉTAPE 3 Saisissez les paramètres.

- **Interface** : sélectionnez un port.
- **Contrôle de port actuel** : affiche l'état actuel de l'autorisation du port. Si l'état est *Autorisé*, le port est authentifié ou le *Contrôle de port administratif* est en *Autorisation forcée*. À l'inverse, si l'état est *Non autorisé*, le port est non authentifié ou le *Contrôle de port administratif* est en *Non-autorisation forcée*.
- **Contrôle de port administratif** : affiche l'état d'autorisation du port administratif. Les options sont les suivantes :
  - *Non-autorisation forcée* : refuse l'accès à l'interface en passant cette dernière en mode non autorisé. Le 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 indiquer que l'utilisation d'un VLAN invité précédemment défini est activée pour le périphérique. Les options sont les suivantes :
  - *Sélectionné* : permet d'utiliser un VLAN invité pour les ports non autorisés. Si un VLAN invité est activé, le port non autorisé rejoint automatiquement le VLAN sélectionné dans le champ ID du VLAN invité de la page Authentification des ports 802.1X.
    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.
  - *Supprimé* : désactive le VLAN invité sur le port.
- **Authentification 802.1X** : l'authentification 802.1X est la seule méthode d'authentification exécutée sur le port.
- **Authentification MAC** : le port est authentifié 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.
- **Authentification Web** : cette fonction est uniquement disponible en mode commutateur Couche 2. Sélectionnez cette option pour activer l'authentification Web sur le commutateur.
- **Réauthentification périodique** : sélectionnez cette option pour autoriser les tentatives de réauthentification du port une fois la Période de réauthentification spécifiée expirée.
- **Période de réauthentification** : saisissez le délai (en secondes) au bout duquel le port sélectionné est réauthentifié.
- **Réauthentifier maintenant** : sélectionnez cette option pour permettre la réauthentification immédiate du port.

- **État de l'authentificateur** : affiche l'état défini de l'autorisation du port. Les options sont les suivantes :
  - *Initialiser* : processus de démarrage.
  - *Autorisation forcée* : l'état du port contrôlé est défini sur Autorisation forcée (le trafic est transféré).
  - *Non-autorisation forcée* : l'état du port contrôlé est défini sur Non-autorisation forcée (le trafic est abandonné).

    REMARQUE : si le port n'est pas en Autorisation forcée ou Non-autorisation forcée, il est en mode automatique et l'authentificateur affiche l'état de l'authentification en cours. Une fois le port authentifié, l'état indique Authentifié.
- **Période** : affecte une limite au temps d'autorisation d'utilisation du port spécifique si 802.1X a été activé (l'option Authentification basée sur les ports est cochée).
- **Nom de période** : sélectionnez le profil qui spécifie la période.
- **Nombre maximal de tentatives de connexion WBA** : cette fonction est uniquement disponible en mode commutateur Couche 2. Entrez le nombre maximal de tentatives de connexion autorisées dans l'interface. Sélectionnez **Infini** pour ne spécifier aucune limite ou **Défini par l'utilisateur** pour spécifier une limite.
- **Période de silence WBA maximale** : cette fonction est uniquement disponible en mode commutateur Couche 2. Entrez la durée maximale de la période silencieuse autorisée dans 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 le délai (en secondes) pendant lequel le périphérique reste en état silencieux après l'échec d'un échange d'authentification.
- **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.

- **Demandes EAP max.** : saisissez le nombre maximum de demandes EAP pouvant être envoyées. Si aucune réponse n'est reçue après la période définie (délai pour demandeur), le processus d'authentification est relancé.
- **Délai pour demandeur** : saisissez le nombre de secondes qui s'écoulent avant que les demandes EAP soient renvoyées au demandeur.
- **Délai pour serveur** : saisissez le nombre de secondes qui s'écoulent avant que le périphérique renvoie une demande au serveur d'authentification.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres des ports sont écrits dans le fichier de Configuration d'exécution.

Définition de l'authentification des hôtes et sessions

La page Authentification hôtes et sessions permet de définir le mode de fonctionnement de 802.1X sur le port, ainsi que l'action à réaliser si une violation a été détectée.

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/MAC/Web** > **Authentification hôtes et sessions**.

Les paramètres d'authentification 802.1X sont décrits pour tous les ports. Tous les champs à l'exception des suivants sont décrits sur la page Modifier l'authentification hôte et session.

- **Nombre de violations d'hôte unique** : 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.
- **Authentification des hôtes** : sélectionnez l'un des modes. Ces modes sont décrits ci-dessus dans la rubrique **Modes hôte de port**.

Les champs suivants ne sont pertinents que si vous sélectionnez Individuelle dans le champ Authentification des hôtes.

Paramètres de violation d'hôte unique :

- **Action en cas de violation** : sélectionnez l'action à appliquer aux paquets arrivant en mode session unique/hôte unique en provenance d'un hôte dont l'adresse MAC ne correspond pas à celle du demandeur. Les options sont les suivantes :
  - *Protéger (Abandonner)* : abandonne les paquets.
  - *Restreindre (Transférer)* : transfère les paquets.
  - *Arrêter* : abandonne les paquets et ferme le port. Les ports restent fermés jusqu'à ce qu'ils soient réactivés ou jusqu'à ce que le périphérique soit réinitialisé.
- **Interceptions** (en cas de violation d'hôte unique) : sélectionnez cette option pour activer les interceptions.
- **Fréquence des interruptions (en cas de violation d'hôte unique)** : définit la fréquence d'envoi des interceptions à l'hôte. Ce champ ne peut être défini que si plusieurs hôtes sont désactivés.
- **Nombre de violations** : affiche le nombre de violations (nombre de paquets en mode Session unique/Hôte unique provenant d'un hôte dont l'adresse MAC n'est pas l'adresse MAC du demandeur.

ÉTAPE 4 Cliquez sur **Appliquer**. Les paramètres sont consignés dans le fichier de Configuration d'exécution.

Affichage des hôtes authentifiés

Pour afficher des informations détaillées sur les utilisateurs authentifiés :

ÉTAPE 1 Cliquez sur **Sécurité** > **Authentification 802.1X/MAC/Web** > **Hôtes authentifiés**.

Cette page affiche les champs suivants :

- **Nom d'utilisateur** : nom des demandeurs authentifiés sur chaque port.
- **Port** : numéro du port.
- **Heure de session (JJ:HH:MM:SS)** : durée pendant laquelle le demandeur a été connecté au port.

- **Méthode d'authentification** : méthode utilisée pour l'authentification de la dernière session.
- **Serveur d'authentification** : serveur RADIUS.
- **Adresse MAC** : affiche l'adresse MAC du demandeur.
- **ID 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/MAC/Web**> **Client verrouillé**.

Les champs suivants sont affichés :

- **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 (secondes)** : 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/MAC/Web**> **Personnalisation de l'authentification Web**.

ÉTAPE 2 Cliquez sur **Ajouter**.

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 :

ÉTAPE 1 Cliquez sur **Sécurité** > **Authentification 802.1X/MAC/Web**> **Personnalisation de l'authentification Web.**

Cette page affiche les langues pouvant être personnalisées.

ÉTAPE 2 Cliquez sur **Modifier la page de connexion**.

Figure 4 La page suivante s'affiche :

ÉTAPE 3 Cliquez sur **Modifier1**. Les champs suivants sont affichés :

- **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 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** : sélectionnez 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 **Modifier2**. Les champs suivants sont affichés :

▪ **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 **Modifier3**. Les champs suivants sont affichés :

- **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 **Modifier4**. Les champs suivants sont affichés :

- **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.

ÉTAPE10 Cliquez sur **Appliquer**. Les paramètres sont enregistrés dans le fichier de Configuration d'exécution.

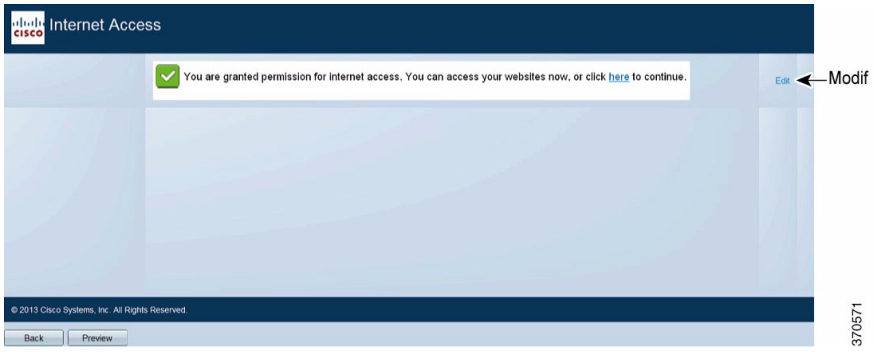
ÉTAPE11 Cliquez sur **Modifier5**. Les champs suivants sont affichés :

- **Copyright** : sélectionnez cette option pour activer l'affichage du texte de copyright.
- **Texte de copyright** : entrez le texte de copyright.

ÉTAPE12 Cliquez sur **Appliquer**. Les paramètres sont enregistrés dans le fichier de Configuration d'exécution.

ÉTAPE13 Cliquez sur **Modifier la page de réussite**.

Figure 5 La page suivante s'affiche :



ÉTAPE14 Cliquez sur le bouton **Modifier** sur le côté droit de la page.

ÉTAPE15 Saisissez le **Message de réussite**. Il s'agit du texte qui s'affichera si l'utilisateur réussit à se connecter.

ÉTAPE16 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 une des langues comme langue par défaut, cliquez sur **Définir la langue d'affichage par défaut**.

Définition des périodes

Pour obtenir une explication de cette fonctionnalité, reportez-vous à la section **Période**.

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.

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 L'authentification Web requiert la prise en charge TCAM pour la classification du trafic d'entrée. Elle est en outre uniquement prise en charge par le mode Sessions multiples complet. Vous pouvez simuler le mode Hôte unique en définissant le paramètre Nombre d'hôtes max. à 1 sur 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

20

Sécurité : Sécurité du premier saut IPv6

Cette section décrit le fonctionnement de la Sécurité du premier saut (First Hop Security, FHS) et la façon de configurer cette fonction dans l'interface utilisateur graphique.

Elle couvre les rubriques suivantes :

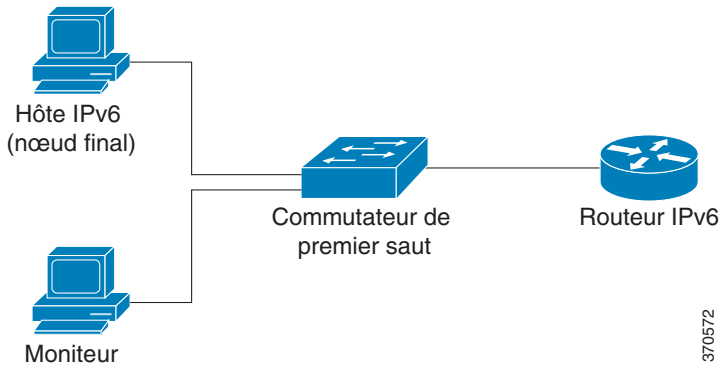
- **Présentation de la Sécurité du premier saut**
- **Protection Router Advertisement**
- **Inspection Neighbor Discovery**
- **Protection DHCPv6**
- **Intégrité de la liaison de voisin**
- **Protection contre les attaques**
- **Stratégies, paramètres globaux et valeurs par défaut du système**
- **Tâches courantes**
- **Configuration et paramètres par défaut**
- **Avant de commencer**
- **Configuration de la Sécurité du premier saut via l'interface utilisateur graphique Web**

Présentation de la Sécurité du premier saut

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 Couche 2 (comme indiqué à la **Figure 6**) filtre les messages Neighbor Discovery Protocol (NDP), les messages DHCPv6 et les messages de données utilisateur sur la base de différentes règles.

Figure 6 Configuration de la Sécurité du premier saut



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
FCFS-SAVI	First Come First Served - Source Address Validation Improvement
Message NA	Message Neighbor Advertisement
NDP	Neighbor Discovery Protocol
Message NS	Message Neighbor Solicitation

Nom	Description
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

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 en 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.

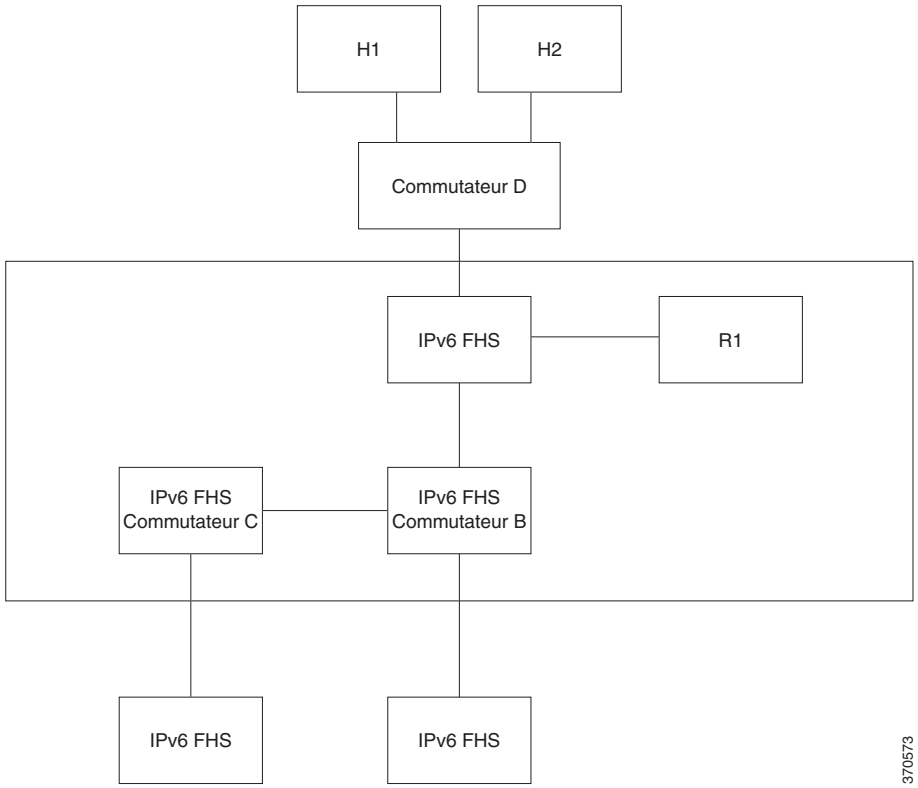
L'Intégrité de la liaison de voisin acquiert (apprend) les voisins à partir des messages reçus (messages NDP et DHCPv6) et les stocke dans la Table de liaisons de voisins. En outre, les entrées statiques peuvent être ajoutées manuellement. Une fois les adresses apprises, la fonction NBI transmet les 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, les liaisons SwitchC-H3, SwitchB-H4 et SwitchA-SwitchD de la **Figure 7** constituent le périmètre, alors que les liaisons SwitchA-SwitchB, SwitchB-SwitchC et SwitchA-R1 sont les liaisons internes situées à l'intérieur de de la zone protégée.

Figure 7 Périmètre de la Sécurité du premier saut IPv6



La commande **device-role** dans l'écran de configuration de stratégie 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 sur la page Sécurité > Sécurité du premier saut IPv6 > 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. Vous pouvez définir ces stratégies 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. Vous pouvez définir cette stratégie 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 sur la page Paramètres de protection DHCP.

- 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 de liaisons de voisins.

Présentation de la table de liaisons de voisins

Lorsqu'il n'y a pas d'espace disponible pour créer un nouvelle entrée, la nouvelle entrée remplace l'entrée dont la date de création est la plus ancienne.

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 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 par 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.

Stratégie d'intégrité de la liaison de voisin

De la même manière que les autre fonctions Sécurité du premier saut IPv6, le comportement Intégrité de la liaison de voisin sur une interface est spécifié par une stratégie d'intégrité de la liaison de voisin associée à une interface. Vous pouvez configurer ces stratégies sur la page Paramètres de liaison de voisin.

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 sans état.

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_RS qui l'annonce 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 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 à l'implémentation NDP, qui limite le nombre d'entrées autorisées à l'état INCOMPLET dans le cache Neighbor Discovery, fournit la protection requise.

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 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, port ou LAG par l'intermédiaire des pages 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, port ou LAG par l'intermédiaire des pages 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, port ou LAG par l'intermédiaire des pages 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, port ou LAG par l'intermédiaire des pages 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, port ou LAG par l'intermédiaire des pages 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.

Avant de commencer

Aucune tâche préalable n'est requise.

Configuration de la Sécurité du premier saut via l'interface utilisateur graphique Web

Paramètres de la Sécurité du premier saut IPv6 commune

Utilisez la page Paramètres FHS pour activer la fonction Paramètres de la Sécurité du premier saut IPv6 commune sur un groupe de VLAN spécifique, mais aussi pour définir la valeur de configuration globale pour la journalisation des abandons de paquets. 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 configurer la Sécurité du premier saut IPv6 commune sur des ports ou LAG :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut** > **Paramètres FHS**.

ÉTAPE 2 Renseignez les champs de configuration globale suivants :

- **Liste des VLAN FHS** : entrez un ou plusieurs VLAN sur lesquels la Sécurité du premier saut est activée.
- **Journalisation des abandons de paquets** : sélectionnez cette option pour créer un SYSLOG lorsqu'un paquet est abandonné par une fonction de Sécurité du premier saut. Il s'agit de la valeur globale par défaut si aucune stratégie n'est définie.

ÉTAPE 3 Si nécessaire, créez une stratégie FHS en cliquant sur **Ajouter**.

Renseignez les champs suivants :

- **Nom de la stratégie** : saisissez un nom de stratégie défini par l'utilisateur.
- **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.
  - *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.

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 protection RA sur les ports ou les LAG :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut** > **Paramètres de protection RA**.

ÉTAPE 2 Renseignez les champs de configuration globale suivants :

- **Liste VLAN de protection RA** : entrez un ou plusieurs VLAN sur lesquels la protection RA est activée.
- **Limite de saut minimale** : ce champ indique si la stratégie Protection RA contrôle la limite de saut minimale du paquet reçu.
  - *Limite de saut minimale* : vérifie que la limite de nombre de sauts est supérieure ou égale à cette valeur.
  - *Aucune vérification* : désactive la vérification de la limite inférieure pour la limite de nombre de sauts.
- **Limite de saut maximale** : ce champ indique si la stratégie Protection RA contrôle la limite de saut maximale du paquet reçu.
  - *Limite de saut maximale* : 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.
  - *Aucune vérification* : désactive la vérification de la limite supérieure pour la limite de nombre de sauts.
- **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.
  - *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.

- **Autre drapeau de configuration** : ce champ spécifie la vérification du drapeau Autre configuration annoncé au sein d'une stratégie Protection RA IPv6.
  - *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.
- **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 au sein de la stratégie Protection RA.
  - *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 suivantes sont acceptées : faible, moyenne et élevée (voir RFC4191).
  - *Moyenne* : spécifie la valeur minimale Préférence de routeur par défaut annoncée autorisée. Les valeurs suivantes sont acceptées : faible, moyenne et élevée (voir RFC4191).
  - *Élevée* : spécifie la valeur minimale Préférence de routeur par défaut annoncée autorisée. Les valeurs suivantes sont acceptées : faible, moyenne et élevée (voir RFC4191).
- **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 au sein de la stratégie Protection RA.
  - *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 suivantes sont acceptées : faible, moyenne et élevée (voir RFC4191).
  - *Moyenne* : spécifie la valeur maximale Préférence de routeur par défaut annoncée autorisée. Les valeurs suivantes sont acceptées : faible, moyenne et élevée (voir RFC4191).
  - *Élevée* : spécifie la valeur maximale Préférence de routeur par défaut annoncée autorisée. Les valeurs suivantes sont acceptées : faible, moyenne et élevée (voir RFC4191).

Pour créer une stratégie Protection RA ou pour configurer les stratégies par défaut définies par le système, cliquez sur **Ajouter** et entrez les paramètres ci-dessus.

Si nécessaire, cliquez sur **Associer la stratégie au VLAN** ou **Associer la stratégie à l'interface**.

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 protection DHCPv6 sur les ports ou les LAG :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut** > **Paramètres de protection DHCPv6**.

ÉTAPE 2 Renseignez les champs de configuration globale suivants :

- **Liste de VLAN de protection DHCPv6** : entrez un ou plusieurs VLAN sur lesquels la protection DHCPv6 est activée.
- **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.
- **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 Si nécessaire, cliquez sur **Ajouter** pour créer une stratégie DHCPv6.

ÉTAPE 4 Renseignez les champs suivants :

- **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 rôle du périphérique est hôte.
- **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.
- **Préférence minimale** : voir ci-dessus.
- **Préférence maximale** : voir ci-dessus.

ÉTAPE 5 Si nécessaire, cliquez sur **Associer la stratégie au VLAN** ou **Associer la stratégie à l'interface**.

Paramètres d'inspection Neighbor Discovery

Utilisez la page Paramètres d'inspection ND pour activer la fonction Inspection ND 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 Inspection ND par défaut, définies par le système, sur cette page.

Pour configurer l'inspection ND sur les ports ou les LAG :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut** > **Paramètres d'inspection ND**.

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.
- **Abandonner 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.
- **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.

ÉTAPE 3 Si nécessaire, cliquez sur **Ajouter** pour créer une stratégie Inspection ND.

ÉTAPE 4 Renseignez les champs suivants :

- **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 l'inspection ND.
  - *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 rôle du périphérique est hôte.
- **Abandonner non sûr** : voir ci-dessus.
- **Niveau de sécurité minimal** : voir ci-dessus.

- **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 5 Si nécessaire, cliquez sur **Associer la stratégie au VLAN** ou **Associer la stratégie à l'interface**.

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 liaison de voisin sur les ports ou les LAG :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut** > **Paramètres de liaison de voisin**.

ÉTAPE 2 Renseignez les champs de configuration globale suivants :

- **Liste de VLAN de liaison de voisins** : entrez un ou plusieurs VLAN sur lesquels la Liaison de voisin est activée.
- **Liaison de voisin manuelle** : sélectionnez cette option pour indiquer que les entrées peuvent être ajoutées manuellement à la Table de liaisons de voisins.
- **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** : ce champ indique si vous souhaitez activer la validation d'une adresse IPv6 liée en fonction de la table des préfixes de voisins et la journalisation des principaux événements de la table de liaisons.
- **Limites d'entrées de liaisons de voisins** : spécifie 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 numéro de VLAN.
  - *Entrées par interface* : spécifie la limite de liaisons de voisins par interface.
  - *Entrées par adresse MAC* : spécifie la limite de liaisons de voisins par adresse MAC.

ÉTAPE 3 Si nécessaire, cliquez sur **Ajouter** pour créer une stratégie de liaison de voisin.

ÉTAPE 4 Renseignez les champs suivants :

- **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 stratégie de liaison de voisin.
  - *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 rôle du périphérique est hôte.
- **Journalisation des liaisons de voisins** : voir ci-dessus.
- **Limites d'entrées de liaisons de voisins** : voir ci-dessus.

ÉTAPE 5 Si nécessaire, cliquez sur **Associer la stratégie au VLAN** ou **Associer la stratégie à l'interface**.

Association de stratégie (VLAN)

Pour associer une stratégie à un ou plusieurs VLAN :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut** > **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. Sélectionnez **Tous les VLAN** ou entrez une plage de VLAN.

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** > **Association de stratégie (Port)**.

Les stratégies qui sont déjà associées sont affichées sous forme de liste, avec le **Numéro d'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.
- **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. Sélectionnez **Tous les VLAN** ou entrez une plage de VLAN.

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

Table de liaisons de voisins

Pour ajouter ou modifier des entrées dans la table de liaisons de voisins :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut** > **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.

ÉTAPE 3 Cliquez sur **Ajouter** pour ajouter une nouvelle entrée dans la table.

ÉTAPE 4 Renseignez les champs suivants :

- **ID VLAN** : ID du VLAN de l'entrée.
- **Adresse IPv6** : adresse IPv6 source de l'entrée.
- **Nom de l'interface** : port sur lequel le paquet est reçu.
- **Adresse MAC** : adresse MAC du voisin du paquet.

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** > **État FHS**.

ÉTAPE 2 Sélectionnez un port, LAG ou VLAN pour lequel l'état FHS est indiqué.

ÉTAPE 3 Les champs suivants sont affichés 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**
  - *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.
  - *Drapeau de configuration gérée* : indique si la vérification du drapeau de configuration gérée est activée.
  - *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.
  - *Limite de saut minimale* : indique si la vérification de la limite de saut RA minimale est activée.
  - *Limite de saut maximale* : indique si la vérification de la limite de saut RA maximale est activée.
  - *Préférence de routeur minimale* : indique si la vérification de la préférence de routeur minimale est activée.
  - *Préférence de routeur maximale* : indique si la vérification de la préférence de routeur 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 protection DHCP**
  - *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.
  - *Trouver préfixes de rép. correspondants* : indique si la vérification des préfixes de réponse DHCP est activée.
  - *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.
  - *Préférence maximale* : indique si la vérification de la préférence maximale est activée.
- **État de la liaison de voisin**
  - *État de liaison de voisin sur le VLAN actuel* : indique si la fonction Liaison de voisin est activée sur le VLAN actuel.
  - *Rôle du périphérique* : rôle du périphérique Liaison de voisin.
  - *Liaison de journalisation* : indique si la journalisation des événements de la table de liaisons de voisins est activée.
  - *Entrées max par VLAN* : nombre maximal autorisé d'entrées de Table de liaisons de voisins dynamiques par VLAN.
  - *Entrées max par interface* : nombre maximal autorisé d'entrées de Table de liaisons de voisins par interface.
  - *Nombre d'entrées max. par adresse MAC* : nombre maximal autorisé d'entrées de Table de liaisons de voisins par adresse MAC.

Statistiques FHS

Pour afficher les statistiques FHS :

ÉTAPE 1 Cliquez sur **Sécurité** > **Sécurité du premier saut** > **Statistiques FHS**.

ÉTAPE 2 Les champs suivants sont affichés :

- **Messages NDP (Neighbor Discovery Protocol)** : le nombre de messages reçus et pontés est affiché pour les types de messages suivants :
  - *RA* : messages Router Advertisement
  - *CPA* : messages Certification Path Advertisement
  - *ICMPv6* : messages Internet Control Message IPv6 Protocol
  - *NS* : messages Neighbor Solicitation
  - *RS* : messages Router Solicitation
  - *CPS* : messages Certification Path Solicitation
- **Messages DHCPv6** : le nombre de messages reçus et pontés est affiché pour les différentes types de messages DHCPv6.

Les champs suivants sont affichés dans la Table de messages abandonnés FHS.

- **Protocole** : protocole des messages abandonnés
- **Type de message** : type de message abandonné
- **Nombre** : nombre de messages abandonnés
- **Motif** : motif d'abandon des messages

21

Sécurité : Gestion sécurisée des données confidentielles

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**
- **Règles SSD**
- **Propriétés SSD**
- **Fichiers de configuration**
- **Canaux de gestion SSD**
- **Interface de ligne de commande (CLI) et récupération du mot de passe**
- **Configuration de 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. Et les règles SSD, les propriétés SSD et les configurations d'authentification des utilisateurs sur l'appareil sont elles-mêmes des données protégées par SSD.

Gestion de SSD

La gestion SSD inclut un ensemble de paramètres de configuration qui définissent le traitement et la sécurité des données confidentielles. Les paramètres de configuration SSD eux-mêmes sont des données confidentielles et sont protégés par SSD.

Toute la configuration de SSD s'effectue via les pages SSD qui sont uniquement disponibles pour les utilisateurs disposant des autorisations appropriées (reportez-vous à la section **Règles SSD**).

Règles SSD

Les règles SSD définissent les autorisations en lecture et le mode de lecture par défaut attribués à une session utilisateur sur un canal de gestion.

Une règle SSD est identifiée de manière unique par son utilisateur et le canal de gestion SSD. Il peut y avoir différentes règles SSD pour le même utilisateur mais pour différents canaux. Inversement, il peut y avoir différentes règles pour le même canal, mais pour différents utilisateurs.

Les autorisations en lecture déterminent la façon dont les données confidentielles peuvent être affichées : sous forme chiffrée uniquement, sous forme de texte en clair uniquement, sous forme chiffrée ou de texte en clair, ou aucune autorisation d'afficher les données confidentielles. Les règles SSD elles-mêmes sont protégées en tant que données confidentielles.

Un appareil peut prendre en charge un total de 32 règles SSD.

Un appareil accorde à un utilisateur l'autorisation en lecture SSD de la règle SSD qui correspond le mieux à l'identité/aux informations d'identification de l'utilisateur et au type de canal de gestion à partir duquel l'utilisateur accède ou accédera aux données confidentielles.

À l'origine, un appareil comporte un ensemble de règles SSD par défaut. Un administrateur peut ajouter, supprimer et modifier des règles SSD comme il le souhaite.

REMARQUE Il se peut qu'un appareil ne puisse pas prendre en charge tous les canaux définis par SSD.

Éléments d'une règle SSD

Une règle SSD inclut les éléments suivants :

- **Type d'utilisateur** : les types d'utilisateur pris en charge dans l'ordre de préférence (de la plus haute à la plus basse) sont les suivants : (Si un utilisateur correspond à plusieurs règles SSD, la règle avec le Type d'utilisateur ayant la préférence la plus haute sera appliquée).
  - **Spécifique** : la règle s'applique à un utilisateur spécifique.
  - **Utilisateur par défaut (cisco)** : la règle s'applique à l'utilisateur par défaut (cisco).
  - **Niveau 15** : la règle s'applique aux utilisateurs ayant le niveau de privilège 15.
  - **Tous** : la règle s'applique à tous les utilisateurs.
- **Nom d'utilisateur** : si le type d'utilisateur est Spécifique, un nom d'utilisateur est requis.
- **Canal** type de canal de gestion SSD auquel la règle s'applique. Les types de canaux pris en charge sont :
  - **Sécurisé** : spécifie que la règle s'applique uniquement aux canaux sécurisés. Un appareil peut prendre en charge une partie ou l'ensemble des canaux sécurisés suivants : interface du port de console, SCP, SSH et HTTPS.

- **Non sécurisé** : spécifie que cette règle s'applique uniquement aux canaux non sécurisés. Un appareil peut prendre en charge une partie ou l'ensemble des canaux non sécurisés suivants : Telnet, TFTP et HTTP.
- **SNMP XML sécurisé** : spécifie que cette règle s'applique uniquement au XML sur HTTPS 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 changé sur la page Propriétés SSD si le nouveau mode de lecture n'enfreint pas l'autorisation en lecture.

REMARQUE Notez les éléments suivants :

- Le mode de lecture par défaut pour les canaux de gestion SNMP XML sécurisé et SNMP XML non sécurisé doit être identique à leur autorisation en lecture.
- L'autorisation en lecture 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 l'appareil :

Tableau 3

Clé de règle		Action de règle	
Utilisateur	**Canal**	**Autorisation en lecture**	**Mode de lecture par défaut**
Niveau 15	SNMP XML sécurisé	Texte en clair uniquement	Texte en clair
Niveau 15	Sécurisé	Les deux	Chiffré
Niveau 15	Non sécurisé	Les deux	Chiffré
Tous	SNMP XML non sécurisé	Exclure	Exclure
Tous	Sécurisé	Chiffré uniquement	Chiffré
Tous	Non sécurisé	Chiffré uniquement	Chiffré

Il est possible de modifier les règles par défaut, mais pas de les supprimer. Si les règles par défaut SSD ont été modifiées, elles peuvent être restaurées.

Remplacement du mode de lecture par défaut SSD de la session

Le système affiche les données confidentielles dans une session, sous forme chiffrée ou de texte en clair, en fonction de l'autorisation en lecture et du mode de lecture par défaut de l'utilisateur.

Le mode de lecture par défaut peut être temporairement remplacé tant que cela n'occasionne pas de conflit avec l'autorisation en lecture SSD de la session. Cette modification est effective immédiatement dans la session actuelle, jusqu'à ce que l'un des événements suivants se produise :

- L'utilisateur le change à nouveau.
- La session est terminée.
- L'autorisation en lecture de la règle SSD qui est appliquée à l'utilisateur de la session est modifiée et n'est plus compatible avec le mode de lecture actuel de la session. Dans ce cas, le mode de lecture de la session redevient le mode de lecture par défaut de la règle SSD.

Propriétés SSD

Les propriétés SSD sont un ensemble de paramètres qui, conjointement avec les règles SSD, définissent et contrôlent l'environnement SSD d'un appareil. L'environnement SSD comporte les propriétés suivantes :

- Contrôle de la façon dont les données confidentielles sont chiffrées.
- Contrôle du niveau de sécurité sur les fichiers de configuration.
- Contrôle de la façon dont les données confidentielles sont affichées dans la session en actuelle.

Mot de passe

Le mot de passe constitue la base du mécanisme de sécurité dans la fonction SSD. Il permet de générer la clé de cryptage et de décryptage des données confidentielles. Les commutateurs Sx200, Sx300, Sx500 et SG500X/SG500XG/ESW2-550X qui ont le même mot de passe peuvent décrypter mutuellement leurs données confidentielles qui ont été cryptées avec la clé générée à partir du mot de passe en question.

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.

AVERTISSEMENT Toute modification apportée à un fichier configuration dont l'intégrité est protégée est considérée comme une altération.

Un appareil détermine si l'intégrité d'un fichier de configuration est protégée en examinant la commande Contrôle de l'intégrité du fichier dans le bloc de contrôle SSD du fichier. Si la protection de l'intégrité est définie pour un fichier, mais qu'un appareil détecte que l'intégrité du fichier n'est pas intacte, l'appareil refuse le fichier. Sinon, le fichier est accepté pour traitement ultérieur.

Un appareil vérifie l'intégrité d'un fichier de configuration textuel lorsque le fichier est téléchargé ou copié vers le fichier de Configuration de démarrage.

Mode Lecture

Chaque session comporte un mode de lecture. Il détermine la façon dont les données confidentielles s'affichent. Le mode de lecture peut être Texte en clair, auquel cas les données confidentielles apparaissent en texte normal ou Chiffré, auquel cas les données confidentielles apparaissent sous forme chiffrée.

Fichiers de configuration

Un fichier de configuration contient la configuration d'un appareil. Un appareil comporte un fichier de Configuration d'exécution, un fichier de Configuration de démarrage, un fichier de Configuration miroir (facultatif) et un fichier de Configuration de secours. Un utilisateur peut charger et télécharger un fichier de configuration de et vers un serveur de fichiers distant. Un appareil peut télécharger automatiquement sa configuration de démarrage à partir d'un serveur de fichiers distant pendant l'étape de configuration automatique via DHCP. Les fichiers de configuration stockés sur des serveurs de fichiers distants sont appelés des fichiers de configuration à distance.

Un fichier de Configuration d'exécution contient la configuration actuellement utilisée par un appareil. La configuration dans un fichier de Configuration de démarrage devient la configuration d'exécution une fois le redémarrage effectué. Les fichiers de Configuration d'exécution et de Configuration de démarrage ont un format interne. Les fichiers de Configuration miroir, de secours et à distance sont des fichiers textuels qui sont généralement stockés à des fins d'archivage, d'enregistrement ou de récupération. Lors de la copie, du chargement et du téléchargement d'un fichier de configuration source, un appareil convertit automatiquement le contenu source dans le format du fichier de destination si les deux fichiers ont un format différent.

Indicateur SSD de fichier

Lors de la copie du fichier de Configuration d'exécution ou de démarrage dans un fichier de configuration textuel, l'appareil génère et place l'indicateur SSD de fichier dans le fichier de configuration textuel pour indiquer si le fichier contient des données confidentielles sous forme chiffrée, des données confidentielles sous forme de texte en clair, ou s'il exclut les données confidentielles.

- L'indicateur SSD, s'il existe, doit se trouver dans le fichier d'en-tête de configuration.

- Une configuration textuelle qui n'inclut pas d'indicateur SSD ne contient normalement pas de données confidentielles.
- L'indicateur SSD permet d'appliquer les autorisations en lecture SSD à des fichiers de configuration textuels, mais il est ignoré lors de la copie des fichiers de configuration vers le fichier de Configuration d'exécution ou de démarrage.

L'indicateur SSD dans un fichier est défini conformément à l'instruction de l'utilisateur, au cours de la copie, pour inclure les données confidentielles sous forme chiffrée ou de texte en clair, ou exclure les données confidentielles d'un fichier.

Bloc de contrôle SSD

Lorsqu'un appareil crée un fichier de configuration textuel à partir de son fichier de Configuration de démarrage ou d'exécution, il insère un bloc de contrôle SSD dans le fichier si un utilisateur demande que le fichier doit inclure les données confidentielles. Le bloc de contrôle SSD, qui est protégé contre toute altération, contient les règles SSD et les propriétés SSD de l'appareil qui crée le fichier. Un bloc de contrôle SSD commence et finit respectivement avec « ssd-control-start » et « ssd-control-end ».

Fichier de Configuration de démarrage

L'appareil prend actuellement en charge la copie depuis les fichiers de Configuration d'exécution, de secours, miroir et à distance vers un fichier de Configuration de démarrage. Les configurations définies dans la configuration de démarrage sont effectives et deviennent la configuration d'exécution une fois le redémarrage effectué. Un utilisateur peut récupérer les données confidentielles sous forme chiffrée ou de texte en clair à partir d'un fichier de Configuration de démarrage, sujet à l'autorisation en lecture SSD et au mode de lecture SSD actuel de la session de gestion.

L'accès en lecture aux données confidentielles dans la configuration de démarrage sous toutes ses formes est exclu si le mot de passe défini dans le fichier de Configuration de démarrage diffère du mot de passe local.

SSD ajoute les règles suivantes lors de la copie des fichiers de Configuration de secours, miroir et à distance vers le fichier de Configuration de démarrage :

- Une fois qu'un appareil a été réinitialisé à ses valeurs par défaut, toutes ses configurations y compris les règles et les propriétés SSD sont réinitialisées à leurs valeurs par défaut.

- Si un fichier de configuration source contient des données confidentielles chiffrées, mais pas de bloc de contrôle SSD, l'appareil refuse le fichier source et la copie échoue.
- S'il n'y a pas de bloc de contrôle SSD dans le fichier de configuration source, la configuration SSD définie dans le fichier de Configuration de démarrage est réinitialisée à ses valeurs par défaut.
- Si un mot de passe est présent dans le bloc de contrôle SSD du fichier de configuration source, l'appareil refuse le fichier source, et la copie échoue s'il y a des données confidentielles chiffrées dans le fichier qui ne sont pas chiffrées par la clé générée à partir du mot de passe dans le bloc de contrôle SSD.
- S'il y a un bloc de contrôle SSD dans le fichier de configuration source et que le fichier échoue lors du contrôle d'intégrité SSD et/ou lors du contrôle d'intégrité du fichier, l'appareil refuse le fichier source et la copie échoue.
- S'il n'y a aucun mot de passe dans le bloc de contrôle SSD du fichier de configuration source, toutes les données confidentielles chiffrées dans le fichier doivent être chiffrées soit par la clé générée à partir du mot de passe local, soit par la clé générée à partir du mot de passe par défaut, mais pas par les deux. Sinon, le fichier source est refusé et la copie échoue.
- L'appareil configure le mot de passe, le contrôle du mot de passe et l'intégrité du fichier le cas échéant à partir du bloc de contrôle SSD dans le fichier de configuration source vers le fichier de Configuration de démarrage. Il configure le fichier de Configuration de démarrage avec le mot de passe qui est utilisé pour générer la clé permettant de décrypter les données confidentielles dans le fichier de configuration source. Toutes les configurations SSD introuvables sont réinitialisées à leurs valeurs par défaut.
- S'il y a un bloc de contrôle SSD dans le fichier de configuration source et que le fichier contient des données confidentielles sous forme de texte en clair, à l'exclusion des configurations SSD dans le bloc de contrôle SSD, le fichier est accepté.

Fichier de Configuration d'exécution

Un fichier de Configuration d'exécution contient la configuration actuellement utilisée par l'appareil. Un utilisateur peut récupérer les données confidentielles sous forme chiffrée ou de texte en clair à partir d'un fichier de Configuration d'exécution, sujet à l'autorisation en lecture SSD et au mode de lecture SSD actuel de la session de gestion. L'utilisateur peut changer la configuration d'exécution en copiant les fichiers de Configuration de secours ou miroir, à travers d'autres actions de gestion via CLI, XML, 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 de fichiers > Propriétés des fichiers de configuration**.

Un utilisateur peut afficher, copier et charger les fichiers complets de Configuration miroir et de secours, sujets à l'autorisation en lecture SSD, au mode de lecture actuel dans la session et à l'indicateur SSD de fichier dans le fichier source comme suit :

- S'il n'y a pas d'indicateur SSD de fichier dans un fichier de configuration miroir ou de 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 cible contenant des données confidentielles. Elle ne nécessite pas de préconfigurer manuellement les appareils cible avec le mot de passe dont la clé permet de crypter les données confidentielles.

L'appareil prend actuellement en charge la Configuration automatique, qui est activée par défaut. Lorsque la Configuration automatique est activée sur un appareil et que l'appareil reçoit les options DHCP qui spécifient un serveur de fichiers et un fichier de démarrage, l'appareil télécharge le fichier de démarrage (fichier de configuration à distance) dans le fichier de Configuration de démarrage à partir d'un serveur de fichiers, puis redémarre.

> **REMARQUE :** le serveur de fichiers peut être spécifié par les champs bootp siaddr et sname, ainsi que l'option DHCP 150 et statiquement configuré sur l'appareil.

L'utilisateur peut en toute sécurité configurer automatiquement les appareils cible contenant des données confidentielles, en créant d'abord le fichier de configuration qui doit être utilisé dans la configuration automatique à partir d'un appareil qui contient les configurations. L'appareil doit être configuré et défini pour :

- Crypter les données confidentielles dans le fichier
- Assurer l'intégrité du contenu du fichier
- Inclure les règles SSD et les commandes de configuration d'authentification sécurisées qui contrôlent et sécurisent correctement l'accès aux appareils et aux données confidentielles

Si le fichier de configuration a été généré avec un mot de passe utilisateur et que le contrôle du mot de passe du fichier SSD est Restreint, le fichier de configuration qui en résulte peut être configuré automatiquement pour les appareils cible souhaités. Néanmoins, pour que la configuration automatique réussisse avec un mot de passe défini par l'utilisateur, les appareils cible doivent être préconfigurés manuellement avec le même mot de passe que celui de l'appareil qui génère les fichiers, ce qui ne correspond donc pas à une configuration sans intervention.

Si l'appareil qui crée le fichier de configuration est défini sur le mode de contrôle du mot de passe Sans restriction, l'appareil inclut le mot de passe dans le fichier. Par conséquent, l'utilisateur peut configurer automatiquement les appareils cible, y compris les appareils neufs ou définis à leurs paramètres par défaut, avec le fichier de configuration sans devoir manuellement préconfigurer les appareils cible avec le mot de passe. Il s'agit là d'une configuration sans intervention, car les appareils cible apprennent le mot de passe directement à partir du fichier de configuration.

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 en différentes types en fonction de leur sécurité et/ou leurs protocoles : sécurisé, non sécurisé, SNMP XML sécurisé et SNMP XML non sécurisé.

Le tableau suivant indique si chaque canal de gestion est considéré par SSD comme sécurisé ou non sécurisé. S'il est non sécurisé, le tableau indique le canal sécurisé parallèle.

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.
- Vous pouvez définir les règles SSD sur la page Règles SSD.

Propriétés SSD

Seuls les utilisateurs qui disposent de l'autorisation en lecture SSD Texte en clair uniquement ou Les deux sont autorisés à définir les propriétés SSD.

Pour définir les propriétés SSD globales :

ÉTAPE 1 Cliquez sur **Sécurité** > **Gestion sécurisée des données confidentielles** > **Propriétés**. 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**).

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.

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.

ÉTAPE 2 Pour ajouter une nouvelle règle, cliquez sur **Ajouter**. Renseignez les champs suivants :

- **Utilisateur** : définit le ou les utilisateurs auxquels la règle s'applique : Sélectionnez une des options suivantes :
  - *Utilisateur spécifique* : sélectionnez et entrez le nom d'utilisateur spécifique auquel cette règle s'applique (cet utilisateur ne doit pas nécessairement être défini).
  - *Utilisateur par défaut (cisco)* : indique que cette règle s'applique à l'utilisateur par défaut.

- *Niveau 15* : indique que cette règle s'applique à tous les utilisateurs ayant le niveau de privilège 15.
- *Tous* : indique que cette règle s'applique à tous les utilisateurs.

- **Canal** : définit le niveau de sécurité du canal d'entrée auquel la règle s'applique : Sélectionnez une des options suivantes :
  - *Sécurisé* : indique que cette règle s'applique uniquement aux canaux sécurisés (console, 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 Les actions suivantes peuvent être effectuées :

- **Restaurer les valeurs par défaut** : rétablit les valeurs d'origine d'une règle par défaut qui a été modifiée par l'utilisateur.
- **Restaurer toutes les règles par défaut** : rétablit les valeurs d'origine de toutes les règles par défaut qui ont été modifiées par l'utilisateur et supprime toutes les règles définies par l'utilisateur.

22

Sécurité : Client SSH

Cette section décrit l'appareil lorsqu'il fonctionne en tant que client SSH.

Elle couvre les rubriques suivantes :

- **Secure Copy (SCP) et SSH**
- **Méthodes de protection**
- **Authentification du serveur SSH**
- **Authentification du client SSH**
- **Avant de commencer**
- **Tâches courantes**
- **Configuration du client SSH via l'interface utilisateur graphique (GUI)**

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.

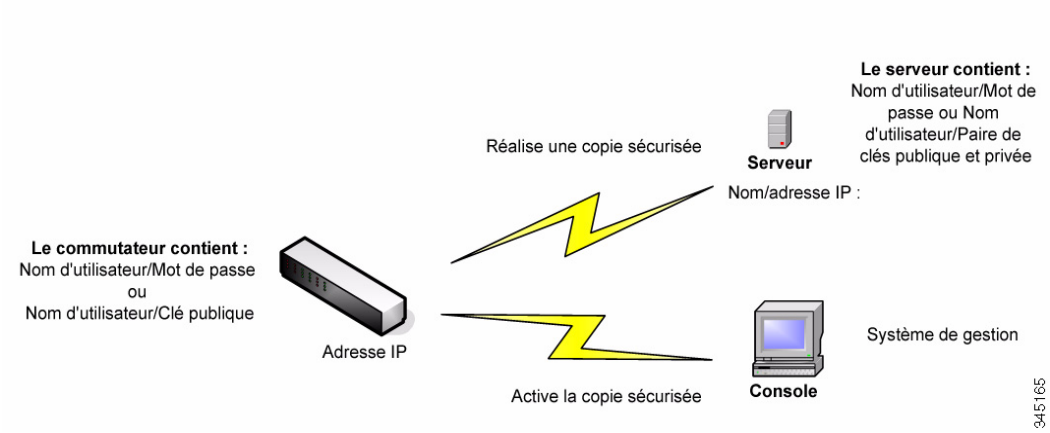
Lorsque des fichiers sont téléchargés via TFTP ou HTTP, les transfert des données n'est pas sécurisé.

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



Méthodes de protection

Lorsque des données sont transférées d'un serveur SSH vers un appareil (client), le serveur SSH utilise différentes méthodes pour l'authentification 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 des données sont transférées du serveur vers l'appareil, le nom d'utilisateur/mot de passe fourni par l'appareil 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 publique/privée

Pour utiliser la méthode de la clé publique/privée, créez un nom d'utilisateur et une clé publique sur le serveur SSH. Comme décrit ci-dessous, la clé publique est générée sur l'appareil, puis copiée vers le serveur. Les actions de création d'un nom d'utilisateur sur le serveur et de copie de la clé publique vers le serveur ne sont pas décrites dans 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 regénérées.

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 **Importer des clés**).

Importer des 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.

Authentification du serveur SSH

En tant que clients SSH, les appareils communiquent seulement avec les 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.
- L'appareil recherche l'adresseIP/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.

Authentification du client SSH

L'authentification du client 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.

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.

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-cbc
  - 3des-cbc
  - arcfour
  - aes192-cbc
  - aes256-cbc
- Algorithmes de code d'authentification de message
  - hmac-sha1
  - hmac-md5

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 quelques tâches courantes réalisées à l'aide du 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, procédez comme suit :

ÉTAPE 1 Choisissez 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 créez un mot de passe temporaire sur la page Mettre à niveau/sauvegarder micrologiciel/langue ou la page Télécharger/sauvegarder configuration/journal, au moment où vous activez le transfert de données sécurisé.

b. Mettez à niveau le micrologiciel, l'image d'amorçage ou le fichier de langue via SCP en sélectionnant l'option **via SCP (sur SSH)** de la page Mettre à niveau/sauvegarder micrologiciel/langue. Vous pouvez saisir le mot de passe directement dans cette page ou utiliser le mot de passe saisi à l'aide de la page Authentification des utilisateurs SSH.

c. Téléchargez/sauvegardez le fichier de configuration, via SCP, en sélectionnant l'option **via SCP (sur SSH)** sur la page Télécharger/sauvegarder configuration/journal. Vous pouvez saisir le mot de passe directement dans cette page ou utiliser le mot de passe saisi à l'aide de la page Authentification des utilisateurs SSH.

ÉTAPE 3 Configurez les nom d'utilisateur et mot de passe sur le serveur SSH ou modifiez le mot de passe existant, sur ce même serveur 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 micrologiciel ou le fichier de langue via SCP en sélectionnant l'option **via SCP (sur SSH)** de la page Mettre à niveau/sauvegarder micrologiciel/langue.

d. Téléchargez/sauvegardez le fichier de configuration, via SCP, en sélectionnant l'option **via SCP (sur SSH)** sur la page Télécharger/sauvegarder configuration/journal.

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, puis créez un nouveau mot de passe local sur la page Gestion sécurisée des données confidentielles > Propriétés.

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 appareil, puis 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 Modifier le 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.

Configuration du client SSH via l'interface utilisateur graphique (GUI)

Cette section décrit les pages utilisées pour configurer la fonction Client SSH.

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 **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 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.
- **Type d'adresse IP** : 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 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 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 4 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.
- **Type d'adresse IP** : 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 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 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.

23

Sécurité : Serveur SSH

Cette section décrit la façon d'établir une session SSH sur l'appareil.

Elle couvre les rubriques suivantes :

- **Vue d'ensemble**
- **Tâches courantes**
- **Pages de configuration du serveur SSH**

Vue d'ensemble

La fonction Serveur SSH permet aux utilisateurs de créer une session SSH sur l'appareil. Elle est similaire à la fonction permettant d'établir une session telnet, sauf que cette session est sécurisée.

Les clés publique et privée sont automatiquement générées sur l'appareil. Elles peuvent être modifiées par l'utilisateur.

Vous pouvez ouvrir une session SSH en utilisant une application client SSH spéciale, telle que PuTTY.

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 : pour vous connecter à l'appareil via SSH à l'aide de clé créée de manière automatique par ce dernier (option par défaut), procédez comme suit :

ÉTAPE 1 Activez le serveur SSH sur la page Services TCP/UDP, puis vérifiez que l'authentification des utilisateurs SSH par clé publique est désactivée sur la page Authentification des utilisateurs SSH.

ÉTAPE 2 Connectez-vous à l'application client SSH externe, telle que PuTTY, à l'aide de l'adresse IP de l'appareil (il n'est pas nécessaire d'utiliser un nom d'utilisateur ou une clé que l'appareil connaît déjà).

Flux de travail 2 : pour créer un utilisateur SSH et une connexion via SSH à l'appareil à l'aide de cet utilisateur, procédez comme suit :

ÉTAPE 1 Générez une clé RSA ou DSA sur une application client SSH externe, telle que PuTTY.

ÉTAPE 2 Activez l'authentification des utilisateurs SSH par clé publique ou mot de passe sur la page Authentification des utilisateurs SSH.

ÉTAPE 3 Activez l'option de connexion automatique si nécessaire (reportez-vous à la section **Connexion automatique** ci-dessous).

ÉTAPE 4 Ajoutez un utilisateur sur la page Authentification des utilisateurs SSH et copiez la clé publique générée en externe.

ÉTAPE 5 Connectez-vous à l'application client SSH externe, telle que PuTTY, à l'aide de l'adresse IP de l'appareil et du nom de l'utilisateur.

Flux de travail 3 : pour importer une clé RSA ou DSA de l'appareil A dans l'appareil B, procédez comme suit :

ÉTAPE 1 Sur l'appareil A, sélectionnez une clé RSA ou DSA sur la page Authentification du serveur SSH.

ÉTAPE 2 Cliquez sur **Détails**, puis copiez la clé publique du type de clé sélectionné dans Notepad ou une application d'édition de texte similaire.

ÉTAPE 3 Connectez-vous à l'appareil B, puis ouvrez la page Authentification du serveur SSH. Sélectionnez la clé RSA ou DSA, cliquez sur **Modifier**, puis collez la clé de l'appareil A.

Pages de configuration du serveur SSH

Cette section décrit les pages utilisées pour configurer la fonctionnalité **Serveur SSH**.

Authentification des utilisateurs SSH

Utilisez la page Authentification des utilisateurs SSH pour activer l'authentification connexe par clé publique et/ou mot de masse et ajouter (dans le cadre de l'authentification par clé publique) un utilisateur du client SSH qui permettra de créer une session SSH dans une application SSH externe (telle que PuTTY).

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**).

- **Désactiver** : 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 **Définition d'utilisateurs**).
- **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**. Reportez-vous à la section **Connexion automatique**.

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 3 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.

Authentification du serveur 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.
- **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.

ÉTAPE 4 Si de nouvelles clés ont été copiées à partir d'autres clés, cliquez sur **Appliquer**. Les clés sont stockées dans le fichier de Configuration d'exécution.

24

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 sont attribués 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 :

- **Listes de contrôle d'accès**
- **Définition d'ACL basées sur MAC**
- **ACL basées sur IPv4**
- **ACL basées sur IPv6**
- **Définition d'une liaison ACL**

Listes de contrôle d'accès

Une liste de contrôle d'accès (ACL, Access Control List) est une liste ordonnée d'actions et de filtres de classification. Chaque règle de classification, englobant l'action correspondante, est appelée élément de contrôle d'accès (ACE, Access Control Élément).

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.

L'appareil prend en charge un maximum de 512 ACL et de 512 ACE.

Lorsqu'un paquet correspond à un filtre ACE, l'action ACE est appliquée et le traitement de cette ACL est arrêté. Si le paquet ne correspond pas au filtre ACE, l'ACE suivant est traité. Si tous les ACE d'une ACL ont été traités sans trouver de correspondance et qu'il existe une autre ACL, celle-ci est traitée de manière similaire.

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.

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 (voir **Mode de QoS avancé**).

Création d'un flux de travail d'ACL

Pour créer des ACL et les associer à une interface, procédez comme suit :

1. Créez un ou plusieurs des types d'ACL suivants :
   a. ACL basée sur MAC via les pages ACL basée sur MAC et ACE basé sur MAC
   b. ACL basée sur IP via la page ACL basée sur IPv4 et la page ACE basé sur IPv4
   c. ACL basée sur IPv6 via la page ACL basée sur IPv6 et la page ACE basé sur IPv6
2. Associez l'ACL aux interfaces via la page Liaison ACL.

Modification d'un flux de travail d'ACL

Vous ne pouvez modifier une ACL que si elle n'est pas en cours d'utilisation. La procédure suivante décrit la suppression de la liaison d'une ACL, préalable nécessaire à sa modification :

1. Si l'ACL n'appartient pas à un mappage de classe Mode avancé de QoS, mais qu'elle a été associée à une interface, supprimez la liaison avec cette interface via la page Liaison ACL.
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.

Définition d'ACL basées sur MAC

Les ACL basées sur MAC sont utilisées pour filtrer le trafic basé sur les champs de la Couche 2. Ces ACL vérifient toutes les trames à la recherche d'une correspondance.

Vous pouvez définir les ACL basées sur MAC sur la page ACL basée sur MAC. Vous pouvez définir les règles sur la page ACE basé 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 **Nom de l'ACL**. 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.

Ajout de règles à une ACL basée 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 **OK**. Les ACE de l'ACL sont répertoriés.

ÉTAPE 3 Cliquez sur **Ajouter**.

ÉTAPE 4 Saisissez les paramètres.

- **Nom de l'ACL** : affiche le nom de l'ACL à laquelle un ACE est ajouté.
- **Priorité** : permet d'entrer la priorité de l'ACE. Les ACE disposant d'une priorité plus élevée sont traitées 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 des ports.
- **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 **Période**.
- **Adresse MAC de destination** : sélectionnez *Indiffér.* si toutes les adresses de destination sont possibles ou *Défini par l'utilisateur* pour entrer une adresse de destination ou une plage d'adresses de destination.
- **Valeur de l'adresse MAC de destination** : saisissez l'adresse MAC avec laquelle l'adresse MAC de destination sera mise en correspondance et saisissez également, le cas échéant, son masque.
- **Masque générique MAC de destination** : saisissez le masque pour définir une plage d'adresses MAC. Veuillez noter que ce masque est différent de ceux employés à d'autres fins comme un masque de sous-réseau. Ici, définir un octet avec **1** signifie « sans importance », et **0** implique masquer cette valeur.

  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 le suivant : 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.
- **Masque générique MAC source** : saisissez le masque afin de définir une plage d'adresses MAC.

- **ID VLAN** : saisissez la partie ID VLAN de la balise VLAN à mettre en correspondance.
- **802.1p** : sélectionnez **Inclure** pour utiliser 802.1p.
- **Valeur 802.1p** : saisissez la valeur 802.1p à ajouter à la balise VPT.
- **Masque 802.1p** : saisissez le masque générique à appliquer à la balise VPT.
- **Ethertype** : saisissez l'Ethertype de trame à mettre en correspondance.

ÉTAPE 5 Cliquez sur **Appliquer**. L'ACE basé sur MAC est consigné dans le fichier de Configuration d'exécution.

ACL basées sur IPv4

Les ACL basées sur IPv4 servent à vérifier les paquets Pv4. 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 (voir **Mode de QoS avancé**).

La page ACL basée sur IPv4 permet d'ajouter des ACL au système. Vous pouvez définir les règles sur la page ACE basé sur IPv4.

Vous pouvez définir les ACL basées sur IPv6 sur la page ACL basée sur IPv6.

Définition d'une ACL basée sur IPv4

Pour définir une ACL basée sur IPv4 :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACL basée sur IPv4**.

Cette page affiche toutes les ACL basées sur IPv4 actuellement définies.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez le nom de la nouvelle ACL dans le champ **Nom de l'ACL**. Les noms respectent la casse.

ÉTAPE 4 Cliquez sur **Appliquer**. L'ACL basée sur IPv4 est consigné dans le fichier de Configuration d'exécution.

Ajout de règles (ACE) à une ACL basée 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 **OK**. Toutes les ACE IP actuellement définies pour l'ACL sélectionnée s'affichent.

ÉTAPE 3 Cliquez sur **Ajouter**.

ÉTAPE 4 Saisissez les paramètres.

- **Nom de l'ACL** : affiche le nom de l'ACL.
- **Priorité** : permet d'entrer la priorité. Les ACE disposant d'une priorité plus élevée sont traitées 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 Gestion des ports.

- **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 **Période**.
- **Protocole** : choisissez de créer un ACE en fonction d'un protocole ou d'un ID de protocole spécifique. Sélectionnez *Tout (IPv4)* pour accepter tous les protocoles IP. Sinon, sélectionnez un des protocoles suivants dans la liste déroulante :
  - *ICMP* : Internet Control Message Protocol
  - *IGMP* : Internet Group Management Protocol
  - *IP in IP* : encapsulation IP in IP
  - *TCP* : Transmission Control Protocol
  - *EGP* : Exterior Gateway Protocol
  - *IGP* : Interior Gateway Protocol
  - *UDP* : User Datagram Protocol
  - *HMP* : Host Mapping Protocol
  - *RDP* : Reliable Datagram Protocol
  - *IDPR* : Inter-Domain Policy Routing Protocol
  - *IPV6* : tunnellisation IPv6 sur IPv4
  - *IPV6:ROUT* : fait correspondre les paquets appartenant à la route IPv6 sur IPv4 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.
- **Masque générique IP source** : 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 le suivant : 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.
- **Masque générique IP de destination** : saisissez le masque pour définir une plage d'adresses IP.
- **Port source** : sélectionnez une des options suivantes :
  - *Indiffér.* : correspond à tous les ports source.
  - *Unique* : saisissez un seul port TCP/UDP source avec lequel les paquets sont mis en correspondance. Ce champ n'est actif que si TCP ou UDP est sélectionné dans le menu déroulant Sélectionner dans la liste.

- *Plage* : sélectionnez une plage de ports source TCP/UDP avec lesquels le paquet est mis en correspondance. Huit plages de ports différentes peuvent être configurées (partagées entre les ports source et de destination). Les protocoles TCP et UDP disposent chacun de huit plages de ports.

- **Port de destination** : sélectionnez l'une des valeurs disponibles (identiques à celles du champ Port source décrit ci-dessus).

  REMARQUE : vous devez spécifier le protocole IP de l'ACE avant de pouvoir entrer le port source et/ou de destination.

- **Indicateurs TCP** : sélectionnez un ou plusieurs indicateurs TCP avec lesquels 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

  - *Priorité IP en correspondance* : 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.

  - *Sélectionner dans la liste* : permet de sélectionner le type de message en fonction de son nom.

  - *Type ICMP de mise en correspondance* : numéro du type de message à utiliser afin de filtrer.

- **Code ICMP** : les messages ICMP peuvent disposer d'un champ de code indiquant comment gérer le message. Sélectionnez l'une des options suivantes pour indiquer si le filtrage s'effectuera en fonction de ce code :

  - *Indiffér.* : tous les codes sont acceptés.

  - *Défini par l'utilisateur* : saisissez un code ICMP 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 :
  - *Indiffér.* : tous les types de message sont acceptés.
  - *Sélectionner dans la liste* : permet de sélectionner le type de message en fonction de son nom.
  - *Type IGMP de mise en correspondance* : numéro du type de message qui sera utilisé pour filtrer.

ÉTAPE 5 Cliquez sur **Appliquer**. L'ACE basé sur IPv4 est consigné dans le fichier de Configuration d'exécution.

ACL basées sur IPv6

La page ACL basée sur IPv6 affiche les ACL IPv6 contrôlant le pur trafic basé sur IPv6 et permet également leur création. Les ACL IPv6 ne vérifient pas les paquets IPv6 sur IPv4 ou ARP.

REMARQUE Les ACL sont également utilisées en tant qu'éléments de base pour les définitions de flux relatifs à la gestion de la QoS par flux (voir **Mode de QoS avancé**).

Définition d'une ACL basée sur IPv6

Pour définir une ACL basée sur IPv6 :

ÉTAPE 1 Cliquez sur **Contrôle d'accès** > **ACL basée sur IPv6**.

Cette fenêtre affiche la liste des ACL définies et leur contenu.

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez le nom de la nouvelle ACL dans le champ **Nom de l'ACL**. Les noms respectent la casse.

ÉTAPE 4 Cliquez sur **Appliquer**. L'ACL basée sur IPv6 est consigné dans le fichier de Configuration d'exécution.

Ajout de règles (ACE) à une ACL basée 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 **OK**. Toutes les ACE IP actuellement définies pour l'ACL sélectionnée s'affichent.

ÉTAPE 3 Cliquez sur **Ajouter**.

ÉTAPE 4 Saisissez les paramètres.

- **Nom de l'ACL** : affiche le nom de l'ACL à laquelle un ACE est ajouté.
- **Priorité** : permet d'entrer la priorité. Les ACE disposant d'une priorité plus élevée sont traitées 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 Gestion des ports.
- **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 **Période**.
- **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 seront transmis et reçus dans l'ordre dans lequel ils ont été envoyés.
  - *UDP* : User Datagram Protocol. Transmet les paquets mais ne garantit pas leur livraison.
  - *ICMP* : fait correspondre les paquets au protocole ICMP (Internet Control Message Protocol).

- **ID protocole de mise en correspondance** : saisissez l'ID du protocole avec lequel établir la correspondance.
- **Adresse IP source** : sélectionnez *Indiffér.* si toutes les adresses source sont acceptables ou *Défini par l'utilisateur* pour entrer une adresse source ou une plage d'adresses source.
- **Valeur de l'adresse IP source** : saisissez l'adresse IP avec laquelle l'adresse IP source sera mise en correspondance et saisissez également, le cas échéant, son masque.
- **Longueur du préfixe IP source** : saisissez la longueur du préfixe de l'adresse IP source.
- **Adresse IP de destination** : sélectionnez *Indiffér.* si toutes les adresses de destination sont acceptables ou *Défini par l'utilisateur* pour entrer une adresse de destination ou une plage d'adresses de destination.
- **Valeur de l'adresse IP de destination** : saisissez l'adresse IP avec laquelle l'adresse MAC de destination sera mise en correspondance et saisissez également, le cas échéant, son masque.
- **Longueur du préfixe IP de destination** : saisissez la longueur du préfixe de l'adresse IP.
- **Port source** : sélectionnez une des options suivantes :
  - *Indiffér.* : correspond à tous les ports source.
  - *Unique* : saisissez un seul port TCP/UDP source avec lequel les paquets sont mis en correspondance. Ce champ n'est actif que si 800/6-TCP ou 800/17-UDP est sélectionné dans le menu déroulant Protocole IP.
  - *Plage* : sélectionnez une plage de ports source TCP/UDP avec lesquels le paquet est mis en correspondance.
- **Port de destination** : sélectionnez l'une des valeurs disponibles. (Elles sont identiques à celles du champ Port source décrit ci-dessus.)

  REMARQUE : vous devez spécifier le protocole IPv6 de l'ACL avant de pouvoir configurer le port source et/ou de destination.
- **Indicateurs TCP** : sélectionnez un ou plusieurs indicateurs TCP avec lesquels 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.
  - Défini : une correspondance est établie si l'indicateur est Défini.

- Non défini : une correspondance est établie si l'indicateur est Non défini.
- Sans importance : ignore l'indicateur TCP.

- **Type de service** : type de service du paquet IP.
- **ICMP** : si l'ACL est basée sur ICMP, sélectionnez le type de message ICMP à utiliser afin de filtrer. Sélectionnez le type de message en fonction de son nom ou saisissez le numéro du type de message. Si tous les types de message sont acceptés, sélectionnez *Indiffér.*.
  - *Indiffér.* : tous les types de message sont acceptés.
  - *Sélectionner dans la liste* : permet de sélectionner le type de message en fonction de son nom dans la liste déroulante.
  - *Type ICMP de mise en correspondance* : numéro du type de message qui sera utilisé 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 :
  - *Indiffér.* : tous les codes sont acceptés.
  - *Défini par l'utilisateur* : saisissez un code ICMP à des fins de filtrage.

ÉTAPE 5 Cliquez sur **Appliquer**.

Définition d'une 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 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.

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 **OK**. Pour chaque type d'interface sélectionné, toutes les interfaces de ce type sont affichées avec la liste de leurs ACL actuelles :

- **Interface** : identificateur d'interface.
- **ACL MAC** : les ACL de type MAC qui sont liées à l'interface (le cas échéant).
- **ACL IPv4** : les ACL de type IPv4 qui sont liées à l'interface (le cas échéant).
- **ACL IPv6** : les ACL de type IPv6 qui sont liées à l'interface (le cas échéant).

REMARQUE Pour supprimer la liaison de toutes les ACL au niveau d'une interface, sélectionnez cette dernière puis cliquez sur **Supprimer**.

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

ÉTAPE 5 Sélectionnez l'une des options suivantes :

- **Sélectionner une ACL basée sur MAC** : sélectionnez une ACL basée sur MAC à lier à l'interface.
- **Sélectionner une ACL basée sur IPv4** : sélectionnez une ACL basée sur IPv4 à lier à l'interface.
- **Sélectionner une ACL basée sur IPv6** : sélectionnez une ACL basée sur IPv6 à lier à l'interface.
- **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.

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 :

- **Sélectionner une ACL basée sur MAC** : sélectionnez une ACL basée sur MAC à lier à l'interface.
- **Sélectionner une ACL basée sur IPv4** : sélectionnez une ACL basée sur IPv4 à lier à l'interface.
- **Sélectionner une ACL basée sur IPv6** : sélectionnez une ACL basée sur IPv6 à lier à l'interface.
- **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.

25

Qualité de service

La fonction QoS (Quality of Service, qualité de service) est appliquée à l'ensemble du réseau pour garantir que le trafic réseau est géré en fonction des critères fixés et que les données voulues reçoivent un traitement préférentiel.

Cette rubrique aborde les points suivants :

- **Fonctions et composants QoS**
- **Configuration de la QoS - Général**
- **Mode de base de QoS**
- **Mode de QoS avancé**
- **Gestion des statistiques de QoS**

Fonctions et composants QoS

La fonction QoS permet d'optimiser les performances du réseau.

La QoS fournit les éléments suivants :

- Classification du trafic entrant en différentes classes sur la base d'attributs, notamment :
  - Configuration du périphérique
  - Interface d'entrée
  - Contenu des paquets
  - Combinaison de ces attributs

La QoS inclut :

- **Classification du trafic** : permet de marquer chaque paquet entrant comme appartenant à un flux de trafic spécifique, sur la base du contenu de ce paquet et/ou du port. Cette classification est réalisée à l'aide d'une ACL (Access Control List, liste de contrôle d'accès). Seul le trafic répondant aux critères d'ACL est soumis à la classification CoS ou QoS.
- **Affectation à des files d'attente matérielles** : affecte les paquets entrants à des files d'attente de transfert. Les paquets sont envoyés à une file d'attente particulière pour gestion en tant que fonction de la classe de trafic à laquelle ils appartiennent. Reportez-vous à la section **Configuration de files d'attente de QoS**.
- **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 de confiance sur la page Paramètres globaux. Pour chaque valeur de ce champ, une file d'attente de sortie est désignée, indiquant la file d'attente choisie pour l'envoi de la trame sur la page CoS/802.1p vers file d'attente ou la page DSCP vers file d'attente (selon que le mode de confiance choisi est CoS/802.1p ou DSCP).

Modes QoS

Le mode QoS sélectionné s'applique à toutes les interfaces du système.

- **Mode De base** : CoS (Class of Service, classe de service).

  Tout le trafic d'une même classe reçoit un traitement identique, à savoir l'action unique de QoS consistant à déterminer la file d'attente de sortie sur le port de sortie, ceci sur la base de la valeur QoS indiquée dans la trame entrante. En mode Couche 2, il peut s'agir de la valeur VPT (VLAN Priority Tag, balise de priorité de VLAN) 802.1p. En mode Couche 3, le système utilise la valeur DSCP (Differentiated Service Code Point, point de code de service différencié) pour IPv4 et la valeur TC (Traffic Class, classe de trafic) pour IPv6. Lorsqu'il fonctionne en mode De base, le périphérique fait confiance à cette valeur de QoS affectée en externe. La valeur de QoS affectée en externe à un paquet détermine sa classe de trafic et la QoS.

Vous pouvez entrer le champ d'en-tête de confiance sur la page Paramètres globaux. Pour chaque valeur de ce champ, une file d'attente de sortie est désignée comme destinataire de l'envoi de la trame sur la page CoS/802.1p vers la file d'attente ou la page DSCP vers la file d'attente (selon que le mode de confiance choisi est CoS/802.1p ou DSCP).

- **Mode Avancé** : QoS (Quality of Service, qualité de service) pour chaque flux.

  En mode Avancé, la QoS de chaque flux est 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, les valeurs DSCP ou CoS/802.1p et les actions à appliquer au trafic hors profil (excédent).

- **Mode Désactivé** dans ce mode, tout le trafic est mappé sur une seule file d'attente de type « meilleur effort » (best effort) et aucun type de trafic n'est prioritaire sur les autres.

Vous ne pouvez activer qu'un seul mode à la fois. Lorsque le système est configuré pour fonctionner en mode de QoS avancé, les paramètres du mode de base de QoS sont inactifs, et inversement.

Lorsque vous changez de mode, les événements suivants se produisent :

- Lorsque vous passez du mode de QoS avancé à un autre mode, les définitions de profil de stratégie et les mappages de classe sont supprimés. Les ACL directement liées aux interfaces restent liées.
- Lorsque vous passez du mode de base de QoS au mode avancé, la configuration du mode de confiance QoS sur le mode De base n'est pas conservée.
- Lorsque vous désactivez la QoS, les paramètres de lissage (shaping) et de file d'attente (paramètre de bande passante WRR/SP) sont réinitialisés sur leurs valeurs par défaut.

Tous les autres éléments de configuration définis par l'utilisateur restent intacts.

Flux de travail de QoS

Pour configurer les paramètres de QoS généraux, procédez comme suit :

ÉTAPE 1 Choisissez le mode de QoS du système (De base, Avancé ou Désactivé, comme décrit à la section **« 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 (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 Si nécessaire (uniquement pour le trafic Couche 3), attribuez une file d'attente à chaque valeur DSCP/TC, via 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 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.

ÉTAPE 8 Configurez le mode sélectionné en réalisant l'une des opérations suivantes :

a. Configurez le mode De base, comme décrit à la section *Flux de travail de configuration du mode De base de QoS*.

b. Configurez le mode Avancé, comme décrit à la section *Flux de travail de configuration du mode Avancé de QoS*.

Configuration de la QoS - Général

La page Propriétés de QoS contient des champs permettant de définir le mode de QoS du système (De base, Avancé ou Désactivé, comme décrit à la section « Modes de QoS »). En outre, vous pouvez définir la priorité CoS par défaut de chaque interface.

Configuration des propriétés QoS

Pour sélectionner le mode de QoS :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Propriétés de QoS**.

ÉTAPE 2 Pour définir le mode de 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 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 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.

Sélectionnez **Restaurer les valeurs par défaut** pour rétablir le paramètre de CoS par défaut défini en usine pour cette interface.

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.

Configuration de files d'attente de QoS

L'appareil prend en charge 4 files d'attente par interface. La file d'attente numéro quatre est celle qui dispose de la priorité la plus élevée. La file d'attente numéro un est celle dont la priorité est la plus faible.

Il existe deux façons de déterminer le mode de gestion du trafic dans les files d'attente : Priorité stricte et WRR (Weighted Round Robin, technique du tourniquet pondéré).

- **Priorité stricte** : le trafic sortant émanant de la file d'attente de priorité la plus élevée est transmis en premier. Le trafic des files d'attente de priorité(s) plus faible(s) n'est traité qu'après transmission des files d'attente de priorité(s) supérieure(s), ce qui donne le niveau de priorité le plus élevé au trafic de la file d'attente portant le numéro le plus élevé.
- **Weighted Round Robin (WRR)** : en mode WRR, le nombre de paquets envoyés depuis la file d'attente est proportionnel à la pondération de cette file d'attente (plus la pondération est élevée, plus le nombre de trames transmises est important). Par exemple, 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 le mode de mise en file d'attente se fait par priorité stricte, l'ordre de priorité définit l'ordre de traitement des files d'attente, en commençant par la file d'attente 4 ou 8 (celle dont la priorité est la plus élevée), puis en passant à la file d'attente de niveau immédiatement inférieur à la fin du traitement de chaque file.

Lorsque la mise en file d'attente est de type WRR (Weighted Round Robin), chaque file d'attente est traitée jusqu'à ce que son quota soit atteint. Le système passe ensuite à une autre file d'attente.

Il est également possible d'affecter une WRR à certaines des files d'attente de priorité plus faible tout en maintenant le traitement 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.

- **File d'attente** : affiche le numéro de la file d'attente.
- **Méthode de planification :** Sélectionnez une des options suivantes :
  - *Priorité stricte* : la planification du trafic de la file d'attente sélectionnée et de toutes les files d'attentes supérieures est strictement basée sur la priorité de chaque file d'attente.
  - *WRR* : la planification du trafic de la file d'attente sélectionnée se base sur une WRR. Chaque période est divisée entre les files d'attente WRR qui ne sont pas vides (celles qui ont des descripteurs de sortie). Ceci ne s'applique que lorsque les files d'attente à priorité stricte sont vides.
  - *Pondération WRR* : si vous choisissez WRR, saisissez la 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.

Mappage CoS/802.1p vers une file d'attente

La page CoS/802.1p vers file d'attente mappe des priorités 802.1p sur des files d'attente de sortie. La table CoS/802.1p vers file d'attente détermine les files d'attente de sortie des paquets entrants sur la base de la priorité 802.1p figurant dans leurs 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 4 files d'attente sont utilisées :

Valeurs 802.1p (0 à 7, 7 étant la valeur la plus élevée)	File d'attente (4 files numérotées de 1 à 4, 4 étant la priorité la plus élevée)	Notes
0	1	Arrière-plan
1	1	Meilleur effort (Best effort)
2	2	Excellent effort
3	3	Application critique - SIP pour téléphone LVS
4	3	Vidéo
5	4	Voix - Valeur par défaut de téléphone IP Cisco
6	4	Contrôle de l'interfonctionnement - RTP pour téléphone LVS
7	4	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 vers 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 a la plus basse priorité et la file d'attente 4 ou 8 a la plus haute priorité.

Pour mapper des valeurs de CoS sur des files d'attente de sortie :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **CoS/802.1p vers file d'attente**.

ÉTAPE 2 Saisissez les paramètres.

- **802.1p** : affiche les valeurs de balise de priorité 802.1p à affecter à une file d'attente de sortie, où 0 est la priorité la plus faible et 7 la plus élevée.
- **File d'attente de sortie** : sélectionnez la file d'attente de sortie sur laquelle la priorité 802.1p est mappée. Le système prend en charge quatre 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**. Les valeurs de priorité 801.1 vers les files d'attente sont mappées et le fichier de Configuration d'exécution est mis à jour.

Mappage DSCP 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 vers file d'attente s'applique aux paquets IP si :

- Le périphérique est en mode de base de QoS et DSCP est en mode de confiance, ou
- 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 classés comme appartenant à la file d'attente Meilleur effort (Best effort).

Les tableaux suivants décrivent le mappage DSCP vers file d'attente par défaut pour un système à 4 files d'attente :

DSCP	63	55	47	39	31	23	15	7
File d'attente	3	3	4	3	3	2	1	1
DSCP	62	54	46	38	30	22	14	6
File d'attente	3	3	4	3	3	2	1	1
DSCP	61	53	45	37	29	21	13	5
File d'attente	3	3	4	3	3	2	1	1
DSCP	60	52	44	36	28	20	12	4
File d'attente	3	3	4	3	3	2	1	1
DSCP	59	51	43	35	27	19	11	3
File d'attente	3	3	4	3	3	2	1	1
DSCP	58	50	42	34	26	18	10	2
Filed'attente	3	3	4	3	3	2	1	1
DSCP	57	49	41	33	25	17	9	1
File d'attente	3	3	4	3	3	2	1	1
DSCP	56	48	40	32	24	16	8	0
File d'attente	3	3	4	3	3	2	1	1

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.

Configuration de la bande passante

La page Bande passante permet aux utilisateurs de définir deux valeurs (Limite de vitesse d'entrée et Taux de modelage en sortie), qui déterminent la quantité de trafic que le système peut recevoir et envoyer.

La limite de vitesse d'entrée indique le nombre de bits par seconde que l'interface d'entrée peut recevoir. La bande passante dépassant cette limite est éliminée.

Les valeurs suivantes sont entrées pour le lissage en sortie (egress shaping) :

- **L'option Débit minimal garanti (CIR)** définit la quantité moyenne maximale de données que le système est autorisé à envoyer à l'interface de sortie, en bits par seconde.
- **L'option Taille de rafale garantie (CBS)** indique la rafale de données que le système est autorisé à envoyer même au-delà de la valeur CIR. Cette valeur est exprimée en nombre d'octets de données.

Pour indiquer la limite de bande passante :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Bande passante**.

La page Bande passante affiche les informations de bande passante de chaque interface.

La colonne % indique la limite de débit entrant pour le port divisée par la quantité totale de bande passante du port.

ÉTAPE 2 Sélectionnez une interface et cliquez sur **Modifier**.

ÉTAPE 3 Sélectionnez le **port ou l'interface LAG**.

ÉTAPE 4 Remplissez les champs pour l'interface sélectionnée :

- **Limite de débit d'entrée** : sélectionnez cette option pour activer la limite de débit d'entrée, que vous définissez ensuite dans le champ situé au-dessous.
- **Limite de débit d'entrée** : saisissez la quantité maximale de bande passante autorisée sur l'interface.

  REMARQUE : les deux champs **Limite de vitesse d'entrée** ne s'affichent pas lorsque le type d'interface est LAG.
- **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.
- **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.

Configuration du lissage en 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 lissage (shaping) 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 le lissage en sortie (egress shaping) pour chaque file d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Modelage de sortie par file d'attente**.

La page Modelage de sortie par file d'attente affiche la limite de débit et la taille de rafale applicables à chaque file d'attente.

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

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 (kbits/s). Le CIR est la quantité maximale moyenne de données pouvant être envoyée.
- **Taille de rafale garantie (CBS)** : saisissez la taille maximale de rafale (CBS), en octets. Le CBS indique la taille maximale de rafale de données dont l'envoi est autorisé même si cela dépasse le CIR.

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

Limite de débit d'entrée VLAN

REMARQUE La fonction de limite de débit VLAN n'est disponible que lorsque le périphérique fonctionne en mode Couche 3.

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.

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 **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **ID VLAN** : sélectionnez un VLAN.
- **Débit minimal garanti (CIR)** : saisissez la quantité moyenne maximale de données qui peut être acceptée sur le VLAN, en kilo-octets par seconde.
- **Taille de rafale garantie (CBS)** : saisissez la taille maximale de rafale de données de l'interface de sortie, en octets. Cette quantité de données peut être envoyée même si cela provoque un dépassement temporaire de la limite de la bande passante autorisée. Cette valeur ne peut pas être saisie pour un LAG.

ÉTAPE 4 Cliquez sur **Appliquer**. La limite de débit VLAN est ajoutée et le fichier de Configuration d'exécution est mis à jour.

Évitement de l'encombrement 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 l'encombrement est dû au fait que plusieurs sources envoient des paquets munis de mêmes nombres d'octets.

Pour configurer l'évitement de l'encombrement TCP :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Général** > **Évitement de l'encombrement TCP**.

ÉTAPE 2 Cliquez sur **Activer** pour activer l'évitement de l'encombrement TCP, puis cliquez sur **Appliquer**.

Mode de base de QoS

En mode de base de QoS, vous pouvez définir un domaine spécifique du réseau en qualité de domaine de confiance. Dans ce domaine, les paquets sont marqués avec la priorité 802.1p et/ou DSCP afin de signaler le type de service qu'ils nécessitent. Les nœuds du domaine utilisent ces champs pour affecter les paquets à une file d'attente de sortie spécifique. La classification initiale des paquets et le marquage de ces champs s'effectuent dans les données d'entrée du domaine de confiance.

Flux de travail de configuration du mode de base de QoS

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 de confiance CoS/802.1p utilise la priorité 802.1p figurant dans la balise VLAN. Le mode de confiance 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 QoS sur ce port dans la page Paramètres d'interface.

Activez ou désactivez le mode de confiance sélectionné au niveau global sur les divers ports dans la page Paramètres d'interface. Si un port est désactivé sans mode de confiance, tous ses paquets d'entrée sont transférés en mode Meilleur effort (Best effort). Il est recommandé de désactiver le mode de confiance sur les ports où les valeurs CoS/802.1p et/ou DSCP des paquets entrants ne sont pas dignes de confiance. Dans le cas contraire, cela peut avoir un impact négatif sur les performances de votre réseau.

Configuration des paramètres globaux

La page Paramètres globaux contient des informations concernant l'activation du mode de confiance sur le périphérique (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 Meilleur effort (Best 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 d'autres, d'après la table de substitution DSCP. Lorsque la fonction Remplacer DSCP d'entrée est activée, le périphérique 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.

DSCP en entrée affiche la valeur DSCP du paquet entrant qui doit à nouveau être marqué d'une autre valeur.

ÉTAPE 5 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 QoS de l'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 **Modifier**.

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

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 Autoriser (transfert) sont considérés comme appartenant au même flux et sont soumis à la même QoS. Ainsi, une stratégie contient un ou plusieurs flux, chacun avec une QoS définie par l'utilisateur.
- La QoS d'un mappage de classe (flux) est exercée par le gestionnaire de stratégie associé. Il existe deux types de gestionnaire de stratégie : le gestionnaire de stratégie individuelle et le gestionnaire de stratégie d'agrégats. Chaque gestionnaire de stratégie est configuré avec une spécification de QoS. Le gestionnaire de stratégie individuelle applique la QoS à un seul mappage de classe, c'est-à-dire à un seul flux, en se fondant sur la spécification de QoS qu'il contient. Le gestionnaire de stratégie d'agrégats applique la QoS à un ou plusieurs mappages de classe (flux). Un gestionnaire de stratégie d'agrégats peut prendre en charge des mappages de classe issus de plusieurs stratégies.
- La QoS est appliquée à chaque flux par liaison des stratégies aux ports voulus. Vous pouvez lier une stratégie et ses mappages de classe à un ou plusieurs ports mais chaque port ne peut être lié qu'à une seule stratégie.

Remarques :

- Les gestionnaires de 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 Mappage 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.

Configuration des 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 avancé de QoS** > **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 Meilleur effort (Best 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 avancé de QoS**, 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 avancé de QoS > 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, le périphérique 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. Pour plus d'informations, reportez-vous à la page Table de substitution DSCP.

Configuration du mappage 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 qualité de service (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 est DSCP hors profil, le périphérique remappe la valeur DSCP d'origine des paquets IP hors profil sur une nouvelle valeur, sur la base de la table Mappage DSCP hors profil. Le 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 Mappage DSCP hors profil. Sinon, l'action est Null, car la valeur DSCP de la table remappe le paquet sur lui-même, selon les valeurs par défaut définies en usine.

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 de base de QoS. Une fois activés, ils s'appliquent à l'échelle globale.

Exemple : Supposez qu'il existe trois niveaux de service : Argent, Or et Platine et que les valeurs DSCP entrantes utilisées pour marquer ces niveaux soient respectivement 10, 20 et 30. Si ce trafic est transféré vers un autre fournisseur de services offrant les mêmes niveaux de service, mais que ce fournisseur emploie les valeurs DSCP 16, 24 et 48, le **mappage DSCP hors profil** remplace les valeurs entrantes au fur et à mesure qu'elles sont mappées sur les valeurs sortantes.

Pour mapper des valeurs DSCP :

ÉTAPE 1 Cliquez sur **Qualité de service > Mode de QoS avancé > Mappage DSCP hors profil**. Cette page permet de définir la valeur DSCP de remplacement du trafic qui entre sur le périphérique ou le quitte.

DSCP en entrée affiche la valeur DSCP du paquet entrant qui doit à nouveau être marqué d'une autre valeur.

ÉTAPE 2 Sélectionnez la valeur **DSCP en sortie** correspondant à l'endroit sur lequel la valeur entrante est mappée.

ÉTAPE 3 Cliquez sur **Appliquer**. Le fichier de Configuration d'exécution est mis à jour avec la nouvelle table Mappage DSCP.

Définition d'un mappage de classe

Un mappage de classe définit un flux de trafic doté d'ACL (Access Control List, Liste de contrôle d'accès). Vous pouvez combiner une ACL MAC, une ACL IP et une ACL IPv6 en un même mappage de classe. Les mappages de classe sont configurés pour mettre en correspondance des critères de paquet sur une base 1-à-1 ou une base 1-à-n. La correspondance est établie avec les paquets selon la méthode du « premier qui convient » : l'action associée au premier mappage de classe reconnu comme correspondant aux critères est appliquée par le système. Les paquets correspondant au même mappage de classe sont considérés comme appartenant au même flux.

REMARQUE La définition de mappages de classe n'a aucun effet sur la QoS ; il s'agit d'une étape intermédiaire nécessaire pour que les mappages de classe puissent être utilisés ultérieurement.

Si vous avez besoin d'ensembles de règles plus complexes, vous pouvez regrouper plusieurs mappages de classe en un grand groupe, appelé stratégie (reportez-vous à **Configuration d'une stratégie**).

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**.

Cette page affiche les mappages de classes déjà définis.

ÉTAPE 2 Cliquez sur **Ajouter**.

Vous ajoutez un nouveau mappage de classe en sélectionnant une ou plusieurs ACL et en attribuant un nom au mappage de classe. Si un mappage de classe inclut deux ACL, vous pouvez spécifier que les trames doivent correspondre à ces deux ACL ou bien demander qu'elles correspondent à au moins une des deux ACL sélectionnées.

ÉTAPE 3 Saisissez les paramètres.

- **Nom du mappage de classe** : saisissez le nom du nouveau mappage de classe.

- **Type d'ACL recherché** : critères qu'un paquet doit satisfaire pour être considéré comme appartenant au flux défini dans le mappage de classe. Les options 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 ou 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.

Gestionnaires de stratégie QoS

REMARQUE Les gestionnaires de stratégie QoS ne sont pas pris en charge lorsque les périphériques Sx500 fonctionnent en mode système Couche 3. Ils sont toujours pris en charge sur les périphériques SG500X.

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 :

- Débit maximal autorisé, appelé CIR (Committed Information Rate, débit minimal garanti), mesuré en kbits/s.
- Quantité de trafic, mesurée en octets, appelée CBS (Committed Burst Size, taille de rafale garantie). Il s'agit du trafic autorisé à transiter sous forme de rafale temporaire, même s'il dépasse le débit maximal défini.
- Action à appliquer aux trames qui dépassent les limites (appelées trafic hors profil), à savoir s'il faut transmettre ces trames telles quelles, les éliminer ou les transmettre, mais en les remappant sur une valeur DSCP qui les marque comme trames de priorité faible pour tous les traitements suivants sur le périphérique.

Vous affectez un gestionnaire de stratégie à un mappage de classe lorsque vous ajoutez ce mappage à une stratégie. Si vous choisissez un gestionnaire de stratégie d'agrégats, vous devez le créer sur la page Gestionnaire de stratégie d'agrégats.

Définition de gestionnaires de stratégie d'agrégats

Le gestionnaire de stratégie d'agrégats applique la QoS à un ou plusieurs mappages de classe, et donc à un ou plusieurs flux. Un gestionnaire de stratégie d'agrégats peut prendre en charge des mappages de classes issus de différentes stratégies et appliquer la QoS à tous les flux, de façon agrégée, sans tenir compte des stratégies ni des ports.

REMARQUE Le périphérique prend en charge les gestionnaires de stratégie individuelle et d'agrégats uniquement lorsqu'il fonctionne en mode Couche 2 sur les appareils qui prennent en charge un mode système Couche 2 séparé.

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 **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Nom du gestionnaire de stratégie d'agrégats** : saisissez le nom du gestionnaire de stratégie d'agrégats.
- **Débit minimal garanti en entrée** (CIR) : saisissez la bande passante maximale autorisée, en bits par seconde. Reportez-vous à la description 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 options disponibles sont les suivantes :
  - *Transférer* : les paquets qui dépassent la limite CIR définie sont transférés.
  - *Éliminer* : les paquets qui dépassent la limite CIR définie sont éliminés.
  - *DSCP hors profil* : les valeurs DSCP des paquets qui dépassent la limite CIR définie sont remappées sur d'autres, d'après la table Mappage DSCP hors profil.

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

Configuration d'une stratégie

La page Table des stratégies affiche la liste des stratégies de QoS avancé définies sur le système. Cette page vous permet également de créer et de supprimer des stratégies. Seules les stratégies liées à une interface sont actives (reportez-vous à la 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 **Table de mappages de classe de stratégie** pour afficher la page Mappages de classe de stratégies.
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 défini le type des paquets qui sont considérés comme appartenant au même flux de trafic.

REMARQUE Il est impossible de configurer un gestionnaire de stratégie sur un mappage de classe lorsque le périphérique fonctionne en mode Couche 3. Le périphérique ne prend en charge les gestionnaires de stratégie qu'en mode Couche 2.

Pour ajouter un mappage de classe à une stratégie :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Table des 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.

- **Nom de la stratégie** : indique la stratégie à laquelle vous ajoutez le mappage de classe.
- **Nom du mappage de classe** : sélectionnez le mappage de classe existant à associer à la stratégie. Vous 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.
  - *Utilisez le mode de confiance par défaut* : permet d'ignorer la valeur CoS/802.1p et/ou DSCP d'entrée. Les paquets concordants sont envoyés en mode Meilleur effort (Best effort).
  - *Toujours faire confiance* : si vous sélectionnez cette option, le périphérique fait confiance aux valeurs CoS/802.1p et DSCP du paquet concordant. S'il s'agit d'un paquet IP, le périphérique place le paquet dans la file d'attente de sortie en fonction de la valeur DSCP détectée et du contenu de la table DSCP vers la file d'attente. Sinon, la file d'attente de sortie du paquet dépend de la valeur CoS/802.1p de ce paquet et du contenu de la table CoS/802.1p vers file d'attente.
  - *Définir* : si vous sélectionnez cette option, le système utilise le contenu saisi dans le champ **Nouvelle valeur** afin de déterminer la file d'attente de sortie des paquets concordants comme suit :

Si la nouvelle valeur (0..7) est une priorité CoS/802.1p, utilisez la valeur de priorité ainsi que le contenu de la table CoS/802.1p vers file d'attente afin de déterminer la file d'attente de sortie de tous les paquets concordants.

Si la nouvelle valeur (0..63) est une valeur DSCP, utilisez la nouvelle valeur DSCP ainsi que le contenu de la table DSCP vers file d'attente afin de déterminer la file d'attente de sortie des paquets IP concordants.

Sinon, le système utilise la nouvelle valeur (1.0,8) comme numéro de file d'attente de sortie pour tous les paquets concordants.

- **Type de gest. de stratégie** : disponible uniquement en mode système Couche 2. Sélectionnez le type de gestionnaire de stratégie pour votre stratégie. Les options sont les suivantes :
  - *Aucun* : aucune stratégie n'est utilisée.
  - *Individuelle* : la stratégie est associée à un gestionnaire de stratégie individuelle.
  - *Agrégat* : la stratégie est associée à un gestionnaire de stratégie d'agrégats.
- **Gestionnaire de stratégie d'agrégats** : disponible uniquement en mode système Couche 2. Si **Type de stratégie** est configuré sur *Agrégat*, sélectionnez un gestionnaire de stratégie d'agrégats précédemment défini (sur la page Gestionnaire de stratégie d'agrégats).

Si **Type de gest. de stratégie** indique *individuelle*, saisissez les paramètres de QoS suivants :

- **Débit minimal garanti en entrée (CIR)** : saisissez la valeur CIR, en kilobits par seconde. Reportez-vous à la description 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 à appliquer aux paquets entrants qui dépassent le seuil CIR. Les options disponibles sont les suivantes :
  - *Aucun* : aucune action.
  - *Éliminer* : les paquets qui dépassent la limite CIR définie sont éliminés.

- *DSCP hors profil* : les paquets IP qui dépassent la limite CIR définie sont transférés avec une nouvelle valeur DSCP, tirée de la table Mappage DSCP hors profil.

ÉTAPE 5 Cliquez sur **Appliquer**.

Liaison de stratégies

La page Liaison de stratégies indique le profil de stratégie lié à chaque port. Lorsqu'un profil de stratégie est lié à un port spécifique, il est actif sur ce port. Vous ne pouvez configurer qu'un seul profil de stratégie sur chaque port mais il 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 en entrée qui correspond aux flux définis au sein de cette stratégie. La stratégie ne s'applique pas au trafic en sortie sur le même port.

Pour modifier une stratégie, vous devez d'abord la supprimer (annuler la liaison) de tous les ports auxquels elle est liée.

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 liaison de stratégie :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Mode de QoS avancé** > **Liaison de stratégies**.

ÉTAPE 2 Sélectionnez un **nom de stratégie** et un **type d'interface**, si nécessaire.

ÉTAPE 3 Cliquez sur **OK**. La stratégie est sélectionnée.

ÉTAPE 4 Sélectionnez les options suivantes pour la stratégie / l'interface :

- **Liaison** : sélectionnez cette option pour lier la stratégie à l'interface.
- **Tout autoriser** : sélectionnez cette option pour transfèrer 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 5 Cliquez sur **Appliquer**. La liaison de stratégie QoS est définie et le fichier de Configuration d'exécution est mis à jour.

Gestion des 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 de 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 **Ajouter**.

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.

Affichage des statistiques de file 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 afficher les statistiques de file d'attente :

ÉTAPE 1 Cliquez sur **Qualité de service** > **Statistiques de QoS** > **Statistiques de file 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 :
  - *Aucune actualisation* : les statistiques ne sont pas actualisées.
  - *15 s* : les statistiques sont actualisées toutes les 15 secondes.
  - *30 s* : les statistiques sont actualisées toutes les 30 secondes.
  - *60 s* : les statistiques sont actualisées toutes les 60 secondes.
- **Jeu de compteurs** : les options disponibles sont les suivantes :
  - *Jeu 1* : affiche les statistiques du jeu 1, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) élevée.
  - *Jeu 2* : affiche les statistiques du jeu 2, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) faible.
- **Interface** : interface à laquelle correspondent les statistiques de file d'attente affichées.
- **File d'attente** : file d'attente d'où proviennent les paquets transférés ou éliminés, la file étant pleine (tail drop).
- **Priorité d'élimination** : les paquets portant la priorité d'élimination la plus faible ont davantage de chances d'être conservés.
- **Nombre total de paquets** : nombre de paquets transférés ou éliminés, la file étant pleine (tail drop).
- **Paquets éliminés** : pourcentage de paquets éliminés, la file étant pleine (tail drop).

ÉTAPE 2 Cliquez sur **Ajouter**.

ÉTAPE 3 Saisissez les paramètres.

- **Jeu de compteurs** : sélectionnez le jeu voulu :
  - *Jeu 1* : affiche les statistiques du jeu 1, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) élevée.
  - *Jeu 2* : affiche les statistiques du jeu 2, qui inclut toutes les interfaces et files d'attente avec une valeur DP (Drop Precedence, priorité d'élimination) faible.
- **Interface** : sélectionnez les ports auxquels correspondent les statistiques affichées. Les options sont les suivantes :
  - *Port* : sélectionnez le port pour lequel vous voulez afficher les statistiques, pour le numéro d'unité sélectionné.
  - *Tous les ports* : l'écran affiche les statistiques pour tous les ports.
- **File d'attente** : sélectionnez la file d'attente pour laquelle vous voulez afficher les statistiques.
- **Priorité d'élimination** : saisissez la priorité d'élimination, c'est-à-dire la probabilité de suppression des paquets.

ÉTAPE 4 Cliquez sur **Appliquer**. Le compteur de statistiques de files d'attente est ajouté et le fichier de Configuration d'exécution est mis à jour.

26

SNMP

Cette section décrit la fonctionnalité SNMP (Simple Network Management Protocol), qui fournit une méthode de gestion des unités de réseau.

Elle couvre les rubriques suivantes :

- **Versions et flux de travail SNMP**
- **ID d'objet du modèle**
- **ID de moteur SNMP**
- **Configuration de vues SNMP**
- **Création de groupes SNMP**
- **Création d'utilisateurs SNMP**
- **Définition de communautés SNMP**
- **Définition de paramètres d'interceptions**
- **Destinataires de notifications**
- **Filtres de notification SNMP**

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 Sécurité > 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 SNMP -> Communautés, puis cliquez sur **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).
- **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 droits d'accès d'un groupe sont Lecture, Écriture et Notifier.

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 interceptions via la page Paramètres de filtre.

ÉTAPE 5 (Facultatif) Définissez un ou plusieurs filtres de notification via la page Filtre de notification.

ÉTAPE 6 Configurez les destinataires de notifications sur la page Destinataires de notifications SNMPv1,2.

Si vous décidez d'utiliser SNMPv3 :

ÉTAPE 1 Définissez le moteur SNMP sur la page ID du moteur. Vous pouvez soit créer un ID de moteur unique, soit utiliser l'ID de moteur par défaut. L'application d'une configuration ID du moteur efface le contenu de la base de données SNMP.

ÉTAPE 2 Vous pouvez également définir une ou plusieurs vues SNMP à l'aide de la page Vues (facultatif). 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 SNMP. Vous pouvez ainsi les associer 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 Activez ou désactivez les interceptions (filtre) via la page Paramètres de filtre (facultatif).

ÉTAPE 6 (Facultatif) Définissez un ou plusieurs filtres de notification via la page Filtre de notification.

ÉTAPE 7 Définissez un ou plusieurs destinataires de notifications 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

Ci-dessous figurent les *ID d'objet* (OID) du modèle de périphérique :

Nom du modèle	Description	ID d'objet
SG300-10	8 ports GE et 2 ports combinés spécifiques (GE/SFP)	9.6.1.83.10.1
SG300-10MP	8 ports GE et 2 ports combinés spécifiques (GE/SFP)	9.6.1.83.10.3
SG300-10P	8 ports GE et 2 ports combinés spécifiques (GE/SFP)	9.6.1.83.10.2
SG300-20	16 ports GE et 4 ports spécifiques - 2 liaisons montantes et 2 ports combo	9.6.1.83.20.1
SG300-28	24 ports GE et 4 ports spécifiques - 2 liaisons montantes et 2 ports combinés	9.6.1.83.28.1
SG300-28P	24 ports GE et 4 ports spécifiques - 2 liaisons montantes et 2 ports combinés	9.6.1.83.28.2
SG300-52	48 ports GE et 4 ports spécifiques - 2 liaisons montantes et 2 ports combinés	9.6.1.83.52.1
SF300-08	8 ports FE	9.6.1.82.08.4
SF302-08	8 ports FE plus 2 ports GE	9.6.1.82.08.1
SF302-08MP	8 ports FE plus 2 ports GE	9.6.1.82.08.3
SF302-08P	8 ports FE plus 2 ports GE	9.6.1.82.08.2
SF300-24	24 ports FE plus 4 ports GE spécifiques - 2 liaisons montantes et 2 ports combo	9.6.1.82.24.1
SF300-24P	24 ports FE plus 4 ports GE spécifiques - 2 liaisons montantes et 2 ports combo	9.6.1.82.24.2
SF300-48	48 ports FE plus 4 ports GE spécifiques - 2 liaisons montantes et 2 ports combo	9.6.1.82.48.1
SF300-48P	48 ports FE plus 4 ports GE spécifiques - 2 liaisons montantes et 2 ports combo	9.6.1.82.48.2
SG300-52P	Commutateur administrable PoE Gigabit à 52 ports	9.6.1.83.52.2

Nom du modèle	Description	ID d'objet
SG300-52MP	Commutateur administrable PoE Gigabit à 52 ports	9.6.1.83.52.3
SG300-10SFP	Commutateur SFP administrable Gigabit à 10 ports	9.6.1.83.10.5
ESW2-350G-52	Commutateur administrable Gigabit à 52 ports	9.6.1.86.52.1
ESW2-350G-52DC	Commutateur administrable Gigabit à 52 ports	9.6.1.86.52.6
SF300-24MP	Commutateur administrable PoE 10/100 à 24 ports	9.6.1.82.24.3
SG300-28MP	Commutateur administrable PoE Gigabit à 28 ports	9.6.1.83.28.3
SF302-08P	8 ports FE plus 2 ports GE	9.6.1.82.08.2
SF302-08PP	Commutateur administrable PoE 10/100 à 8 ports	9.6.1.82.08.2
SF302-08MPP	Commutateur administrable PoE 10/100 à 8 ports	9.6.1.82.08.3
SG300-10PP	Commutateur administrable PoE 10/100 à 8 ports	9.6.1.83.10.2
SF300-24PP	Commutateur administrable PoE 10/100 à 8 ports	9.6.1.82.24.1
SG300-28PP	Commutateur administrable PoE Gigabit à 10 ports	9.6.1.83.28.2
SF300-24PP	Commutateur administrable PoE 10/100 à 24 ports	9.6.1.82.24.1
SG300-28PP	Commutateur administrable PoE Gigabit à 28 ports	9.6.1.83.28.2
SF300-48PP	Commutateur administrable PoE 10/100 à 48 ports	9.6.1.82.48.2

Les ID d'objet privés se trouvent dans : enterprises(1).cisco(9).otherEnterprises(6).ciscosb(1).switch001(101).

ID de moteur SNMP

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).

AVERTISSEMENT 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 du moteur généré par le périphérique. L'ID du moteur par défaut est basé sur l'adresse MAC du périphérique. Il est défini de manière standard par :
  - *4 premiers octets* : premier bit = 1, le reste correspond au numéro d'entreprise IANA.
  - *Cinquième octet* : défini à l'aide de la valeur 3 pour indiquer l'adresse MAC qui suit.
  - *6 derniers octets* : adresse MAC du périphérique.
- **Aucun** : aucun ID de moteur n'est utilisé.

- **Défini par l'utilisateur** : saisissez l'ID de moteur de l'unité locale. La valeur du champ est une chaîne hexadécimale **(plage : 10 - 64)**. Chaque octet dans les chaînes de caractères hexadécimales est représenté par deux chiffres hexadécimaux.

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 :

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

Configuration de vues SNMP

Une vue est une étiquette définie par l'utilisateur pour une collecte de sous-arborescences MIB. Chaque ID de sous-arborescence est défini par l'*ID d'objet* (OID) de la racine des sous-arborescences concernées. 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**.

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.

D'autres vues peuvent être ajoutées.

- **Sous-arborescence d'ID d'objet** : affiche la sous-arborescence à inclure dans la vue SNMP ou à exclure de cette dernière.
- **Type de vue de sous-arborescence d'ID d'objet** : indique si la sous-arborescence définie est incluse dans la vue SNMP sélectionnée ou exclue de cette dernière.

Création de groupes SNMP

Dans SNMPv1 et SNMPv2, une chaîne de communauté est envoyée accompagnée des trames SNMP. La chaîne de communauté agit en tant que mot de passe pour accéder à un agent SNMP. Cependant, ni les trames, ni la chaîne de communauté ne sont cryptées. Par conséquent, SNMPv1 et SNMPv2 ne sont pas sécurisés.

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 qui n'est pas une vue 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** : l'association d'une vue avec les privilèges d'accès Lecture, Écriture et Notifier du groupe limite l'étendue de l'arborescence MIB à laquelle le groupe a un accès Lecture, Écriture et Notifier.
  - *Vue* : sélectionnez une vue précédemment définie pour Lecture, Écriture et Notifier.
  - *Lecture* : l'accès à la gestion est en lecture seule pour la vue sélectionnée. Sinon, un utilisateur ou une communauté associé(e) à ce groupe peut lire toutes les bases MIB, à l'exception de celles qui contrôlent le SNMP lui-même.
  - *Écriture* : l'accès à la gestion est en écriture pour la vue sélectionnée. Sinon, un utilisateur ou une communauté associé(e) à ce groupe peut écrire 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 interceptions. Cette option peut être sélectionnée pour SNMPv3.

ÉTAPE 4 Cliquez sur **Appliquer**. Le groupe SNMP est enregistré dans le fichier Configuration d'exécution.

Création d'utilisateurs SNMP

Un utilisateur SNMP est défini par les informations de connexion (nom d'utilisateur, mots de passe et méthode d'authentification), ainsi que par le contexte et l'étendue de son fonctionnement en association avec un groupe et un ID de moteur.

L'utilisateur configuré a les attributs de son groupe et dispose des privilèges d'accès définis dans la vue associée.

Les groupes permettent aux gestionnaires de réseaux d'affecter des droits d'accès à un groupe d'utilisateurs plutôt qu'à un utilisateur unique.

Un utilisateur 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. Cette opération s'effectue sur la page ID du 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 contient les utilisateurs existants.

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.

- **Nom d'utilisateur** : 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 de 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 :
  - *Aucune* : aucune authentification d'utilisateur n'est utilisée.
  - *Mot de passe MD5* : mot de passe utilisé pour la génération d'une clé par la méthode d'authentification MD5.
  - *Mot de passe 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.

Définition de communautés SNMP

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 SNMP).
- **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 droits d'accès d'un groupe sont Lecture, Écriture et Notifier.

Pour définir des communautés SNMP :

ÉTAPE 1 Cliquez sur **SNMP** > **Communautés**.

Cette page contient une table des communautés SNMP configurées et de leurs propriétés.

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 uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, spécifiez si la réception s'effectue via 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.
- **De base** : sélectionnez ce mode pour une communauté spécifique. Avec ce mode, aucune connexion n'est établie avec quelque groupe que ce soit. Vous pouvez uniquement choisir le niveau d'accès de la communauté (Lecture seule, Lecture/écriture ou 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).
- **Avancé** : sélectionnez ce mode pour une communauté spécifique.
  - *Nom du groupe* : sélectionnez un groupe SNMP qui détermine les droits d'accès.

ÉTAPE 4 Cliquez sur **Appliquer**. La communauté SNMP est définie et le fichier de Configuration d'exécution est mis à jour.

Définition de paramètres d'interceptions

La page Paramètres de filtre permet de spécifier si les notifications SNMP doivent être envoyées à partir du périphérique, et à quelles conditions. Vous pouvez configurer les destinataires des notifications SNMP sur la page Destinataires de notifications SNMPv1,2 ou sur la page Destinataires de notifications SNMPv3.

Pour définir des paramètres d'interception :

ÉTAPE 1 Cliquez sur **SNMP** > **Paramètres d'interception**.

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 interceptions sont générées pour signaler des événements système, tels que défini dans la RFC 1215. Le système peut générer des interceptions définies dans la base MIB qu'il prend en charge.

Les récepteurs d'interruption (connus sous le nom de destinataires de notifications) sont des nœuds réseau où des interceptions sont envoyées par le périphérique. Plusieurs destinataires de notification sont répertoriés comme cibles des interceptions.

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'une interception, cette dernière est envoyée 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 de configurer la destination d'envoi des notifications SNMP, ainsi que les types de notifications SNMP envoyées vers chaque destination (interceptions 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.

Définition de 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 IPv4 sera utilisée comme adresse IPv4 source dans les interceptions utilisés dans les communications avec les serveurs SNMP IPv4.
- **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 utilisées 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*.
  - *Liaison locale* : l'adresse IPv6 identifie uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : si le type d'adresse IPv6 est Liaison locale, spécifiez si la réception s'effectue via VLAN ou ISATAP.
- **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 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 d'interceptions. Les noms de chaîne de communauté sont générés à partir de ceux répertoriés sur la page Communauté.

- **Version de notification** : sélectionnez la version SNMP de l'interception. Vous pouvez utiliser SNMPv1 ou SNMPv2 comme version des interceptions, 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 sur la page Filtre de notification.
- **Nom du filtre** : sélectionnez le filtre SNMP qui spécifie les informations contenues dans les interceptions (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.

Définition de destinataires de notification 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 IPv4 sera utilisée comme adresse IPv4 source dans les interceptions utilisés dans les communications avec les serveurs SNMP IPv4.
- **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 uniquement des hôtes sur une liaison de réseau unique. Une adresse locale de liaison possède le préfixe **FE80**, ne peut routée et ne peut servir à la communication que sur le réseau local. Une seule adresse locale de liaison est possible. S'il existe une adresse locale de liaison sur l'interface, cette saisie remplacera l'adresse dans la configuration.
  - *Global* : l'adresse IPv6 est de type global IPv6 monodiffusion, visible et joignable à partir d'autres réseaux.
- **Interface de liaison locale** : 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/interceptions. 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 Utilisateur SNMP, 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 Authentification et confidentialité a été défini pour ce nom d'utilisateur sur la page Utilisateur, le niveau de sécurité sur cet écran peut être Aucune authentification, Authentification ou 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 sur la page Filtre de notification.
- **Nom du filtre** : sélectionnez le filtre SNMP qui spécifie les informations contenues dans les interceptions (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.

Filtres de notification SNMP

La page Filtre de notification permet de configurer des filtres de notification SNMP et des ID d'objet (OID) soumis à vérification. Après avoir créé un filtre de notification, vous pouvez le joindre à un destinataire de notification via la page Destinataires de notifications SNMPv1,2 et 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.

78-21341-01