

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

[Introduction](#)

[Présentation du matériel](#)

[Utilisation de Dell™ OpenManage™ Switch Administrator](#)

[Informations sur les ports et les câbles](#)

[Configuration du système Dell™ PowerConnect™](#)

[Configuration des informations sur le système](#)

[Configuration des fonctions de support pour le téléphone IP et les points d'accès](#)

[Configuration des paramètres de commutation](#)

[Affichage de statistiques/RMON](#)

[Configuration du routage](#)

[Configuration d'IPv6](#)

[Configuration de la qualité de service](#)

[Configuration de la multidiffusion IP](#)

[Obtention d'aide](#)

Remarques, avis et précautions



REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre ordinateur.



AVIS : Un AVIS vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.



PRÉCAUTION : Une PRÉCAUTION indique un risque potentiel d'endommagement du matériel, de blessure corporelle ou de mort.

Modèles PC6224, PC6248, PC6224P, PC6248P et PC6224F

Les informations contenues dans ce document peuvent être modifiées sans préavis.
© 2007 Dell Inc. Tous droits réservés.

La reproduction de ce document de quelque manière que ce soit sans l'autorisation écrite de Dell Inc. est strictement interdite.

Marques utilisées dans ce document : Dell, Dell OpenManage, le logo DELL, Inspiron, Dell Precision, Dimension, OptiPlex, PowerConnect, PowerApp, PowerVault, Axim, DellNet et Latitude sont des marques de Dell Inc. ; Microsoft, Windows et Windows Vista sont des marques ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays ; Procomm Plus est une marque de Symantec Corporation ou de ses filiales aux États-Unis et dans d'autres pays.

Tous les autres noms de marques et marques commerciales utilisés dans ce document se rapportent aux sociétés propriétaires de ces marques et de ces noms ou à leurs produits. Dell Inc. décline tout intérêt dans l'utilisation des marques déposées et des noms de marques ne lui appartenant pas.

Modèles PC6224, PC6248, PC6224P, PC6248P et PC6224F

Septembre 2007 Rév. A00

[Retour au sommaire](#)

Informations sur les ports et les câbles

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Interface Ethernet 10/100/1000](#)
- [Interfaces SFP](#)
- [Interfaces avec logements 10 Gbps double port](#)
- [Connexion du câble série](#)
- [Connexion des câbles d'alimentation en CA et en CC](#)

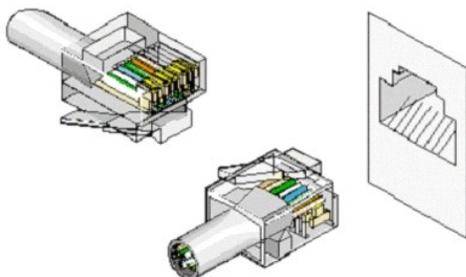
Cette section décrit les interfaces physiques du commutateur et contient des informations sur les connexions des câbles.

Les stations sont connectées aux ports du commutateur via les ports d'interface physiques situés sur le panneau avant. Le mode approprié (Half Duplex, Full Duplex et Auto) est défini sur chaque station.

Interface Ethernet 10/100/1000

Le port de commutation peut être relié à des stations équipées de ports Ethernet RJ-45 standard via des câbles directs. Pour connecter entre eux les périphériques de transmission, utilisez des câbles croisés. La [Figure 4-1](#) représente un connecteur RJ-45.

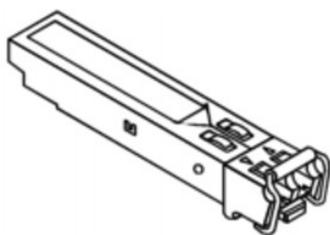
Figure 4-1. Connecteur RJ-45



Interfaces SFP

Les interfaces SFP se trouvent sur l'avant de la console. La [Figure 4-2](#) représente un connecteur SFP.

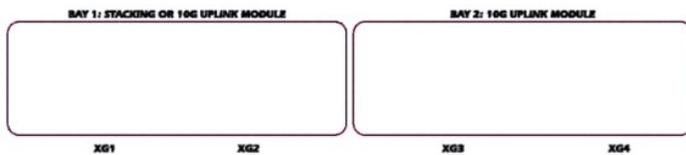
Figure 4-2. Connecteur SFP



Interfaces avec logements 10 Gbps double port

Les ports situés à l'arrière des commutateurs PowerConnect série 6200 prennent en charge les interfaces doubles XAUI. Ces dernières peuvent fonctionner à 10 Gbps (avec un module XFP) ou à 12 Gbps (logement de gauche uniquement, vu depuis l'arrière de l'appareil) avec un module d'empilage. La [Figure 4-3](#) représente les logements XAUI.

Figure 4-3. Logements XAUI



Connexion du câble série

Vous pouvez utiliser un câble série (simulateur de modem) pour relier le commutateur à un terminal afin de procéder à son installation et à sa configuration initiales. Il est également possible d'utiliser un ordinateur exécutant un logiciel d'émulation de terminal. Le câble série du commutateur est un câble croisé DB-9 femelle-femelle (voir la [Figure 4-4](#)).

Figure 4-4. Connecteur série



Connexion du commutateur à un terminal

1. Connectez le câble série sur le terminal (console) ASCII DTE RS-232.
2. Connectez le câble d'interface sur le port série du commutateur (voir la [Figure 4-5](#)).
3. Si vous configurez une pile de commutateurs, branchez le câble d'interface sur le port série du commutateur principal (maître).

Figure 4-5. Connexion série vers le commutateur



Connexion des câbles d'alimentation en CA et en CC

1. Branchez un câble d'alimentation standard de 1,5 m (5 pieds) avec mise à la terre sur la prise correspondante. Celle-ci est située à l'arrière de l'appareil (voir la [Figure 4-6](#)).
2. Branchez le câble d'alimentation sur une prise électrique avec mise à la terre.
3. Si vous utilisez un bloc d'alimentation en CC redondant (modèle RPS600 ou EPS470, par exemple), branchez le câble d'alimentation en CC sur la prise correspondante, à l'arrière de l'appareil (voir la [Figure 4-6](#)).
4. Vérifiez que le périphérique est alimenté et fonctionne correctement en observant les voyants du panneau avant.

Pour obtenir une description complète des voyants, voir [Comportement des voyants](#).

Figure 4-6. Connecteurs d'alimentation (CA et CC) du commutateur



Vers une source d'alimentation en CC

Vers une source d'alimentation en CA

[Retour au sommaire](#)

[Retour au sommaire](#)

Configuration des informations sur le système

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Ouverture de la page System \(Système\)](#)
- [Définition des informations générales sur le périphérique](#)
- [Configuration des paramètres SNTP](#)
- [Gestion des journaux](#)
- [Définition de l'adressage IP](#)
- [Exécution des diagnostics relatifs aux câbles](#)
- [Gestion de la sécurité du périphérique](#)
- [Définition des paramètres SNMP](#)
- [Gestion des fichiers](#)
- [Définition des paramètres avancés](#)
- [Définition de l'empilage](#)

Ouverture de la page System (Système)

Les menus de la page **System** (Système) permettent de configurer les paramètres définissant l'interaction du commutateur avec son environnement d'installation. Pour afficher cette page, cliquez sur **System** (Système) dans l'arborescence. Cette page contient des liens vers les fonctionnalités suivantes :

- | [Définition des informations générales sur le périphérique](#)
- | [Configuration des paramètres SNTP](#)
- | [Gestion des journaux](#)
- | [Définition de l'adressage IP](#)
- | [Exécution des diagnostics relatifs aux câbles](#)
- | [Gestion de la sécurité du périphérique](#)
- | [Définition des paramètres SNMP](#)
- | [Gestion des fichiers](#)
- | [Définition des paramètres avancés](#)
- | [Définition de l'empilage](#)

Définition des informations générales sur le périphérique

La page **General** (Général) contient des liens vers des pages permettant de configurer les paramètres du périphérique. Elle permet d'accéder aux fonctions suivantes :

- | [Inventaire](#)
- | [Santé du système](#)
- | [Versions](#)
- | [Ressources du système](#)
- | [Configuration du fuseau horaire](#)
- | [Configuration de l'heure d'été](#)
- | [Informations détaillées sur l'horloge](#)
- | [Réinitialisation](#)

Inventaire

La page **Asset** (Inventaire) contient des champs qui permettent de définir et d'afficher des informations générales sur le périphérique.

Pour afficher cette page, cliquez sur **System** (Système) → **General** (Général) → **Asset** (Inventaire) dans l'arborescence.

Figure 6-1. Page Asset (Inventaire)

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled 'Asset' and contains several input fields for system information. Below the fields is a 'Telnet' button and a table for Asset Tag configuration.

Unit No.	Service Tag	Asset Tag (0-16 characters)	Serial No.
1	23	none	23

Cette page contient les champs suivants :

System Name (0-255 characters) (Nom du système, 0-255 caractères) : permet d'attribuer un nom de système au périphérique.

System Contact (0-255 characters) (Nom du contact, 0-255 caractères) : permet d'indiquer le nom de la personne à contacter pour les questions concernant ce périphérique.

System Location (0-255 characters) (Emplacement du système, 0-255 caractères) : permet de définir l'emplacement du système.

Sys Object ID (ID d'objet du système) : ID d'objet affecté au système.

MAC Address (Adresse MAC) : indique l'adresse MAC du commutateur.

Sys Uptime (Durée de fonctionnement) : indique le délai écoulé (jours, heures et minutes) depuis le dernier redémarrage.

Date : affiche la date du système (au format MM/JJ/AAAA). Exemple : 11/01/05 correspond au 1er novembre 2005.

Time (Heure) : affiche l'heure du système (au format HH:MM:SS). Exemple : 20:12:03.

Unit No. (Numéro d'unité) : indique la position du commutateur dans la pile.

Service Tag (Numéro de service) : indique le numéro de référence à communiquer pour la maintenance du périphérique.

Asset Tag (0-16 characters) (Numéro d'inventaire, 0-16 caractères) : affiche la référence attribuée au périphérique par l'utilisateur.

Serial No. (Numéro de série) : indique le numéro de série du périphérique.

Définition des informations sur le système

1. Affichez la page **Asset** (Inventaire).
2. Complétez les champs suivants : **System Name** (Nom du système), **System Contact** (Nom du contact), **System Location** (Emplacement du système) et **Asset Tag** (Numéro d'inventaire).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont modifiés et le périphérique est mis à jour.

Ouverture d'une session Telnet

1. Affichez la page **Asset** (Inventaire).

REMARQUE : Les paramètres appropriés sont définis avant l'ouverture de la session Telnet. Voir [Configuration d'un mot de passe Telnet initial](#) pour plus d'informations. Si le client utilise un environnement Microsoft® Windows®, le programme doit être configuré pour l'utilisation de Telnet. Dans un environnement Unix, le programme Telnet doit se trouver directement dans le chemin d'accès.

2. Cliquez sur **Telnet**.

Une invite s'affiche pour indiquer que le système est prêt à recevoir des commandes.

Configuration des informations sur le périphérique à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous aux chapitres suivants du document *CLI Reference Guide* (Guide de référence CLI) :

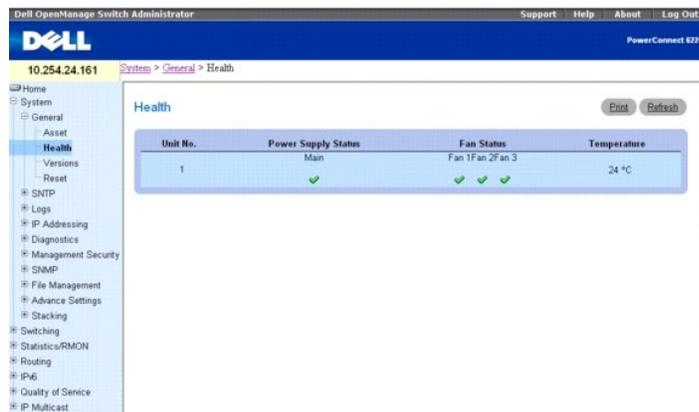
- 1 System Management Commands (Commandes de gestion du système)
- 1 SNMP Commands (Commandes SNMP)
- 1 Clock Commands (Commandes de synchronisation)

Santé du système

La page **Health** (Santé) permet d'afficher des informations concernant la configuration physique du périphérique, y compris les sources d'alimentation et de ventilation.

Pour afficher cette page, cliquez sur **System** (Système) → **General** (Général) → **Health** (Santé) dans l'arborescence.

Figure 6-2. Page Health (Santé)



Cette page contient les champs suivants :

Unit No. (Numéro d'unité) : indique la position de l'unité dans la pile.

Power Supply Status (État du bloc d'alimentation) : affiche l'état du bloc d'alimentation.

✓ - Le bloc d'alimentation fonctionne normalement.

✗ - Le bloc d'alimentation présente un dysfonctionnement.

Not Present (Absent) : le bloc d'alimentation n'est pas installé.

Fan Status (État du ventilateur) : indique l'état du ventilateur. Le PowerConnect 6224 comprend trois ventilateurs et le PowerConnect 6248 en contient quatre.

✓ - Le ventilateur fonctionne normalement.

✗ - Le ventilateur présente un dysfonctionnement.

Not Present (Absent) : le ventilateur n'est pas installé.

Temperature (Température) : température actuelle de fonctionnement du périphérique.

Affichage des informations concernant la santé du système à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

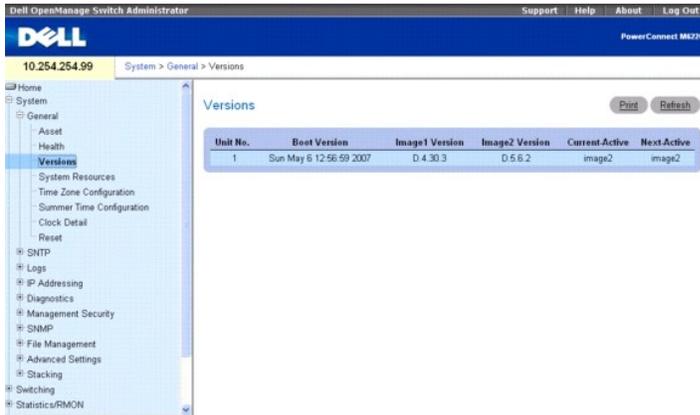
- 1 System Management Commands (Commandes de gestion du système)

Versions

La page **Versions** permet d'afficher des informations sur les versions de logiciels actuellement utilisées.

Pour afficher cette page, cliquez sur **System** (Système) → **General** (Général) → **Health** (Santé) dans l'arborescence.

Figure 6-3. Page Versions



Cette page contient les champs suivants :

Unit No. (Numéro d'unité) : indique la position de l'unité dans la pile.

Boot Version (Version d'amorçage) : affiche la version de l'image d'amorçage active.

Image1 Version : affiche le numéro de version de l'une des deux images logicielles disponibles.

Image2 Version : affiche le numéro de version de l'autre image logicielle disponible.

Current-Active (Active/En cours) : affiche la version de logiciel actuellement exécutée sur le périphérique.

Next-Active (Active/Suivante) : Affiche la version de logiciel qui doit être chargée en cas de non-fonctionnement de la version en cours.

Affichage des versions utilisées sur le périphérique à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

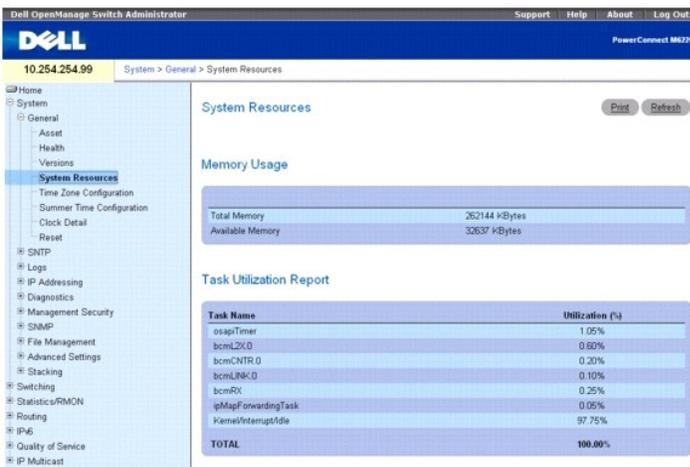
- 1 System Management Commands (Commandes de gestion du système)

Ressources du système

La page **System Resources** (Ressources du système) permet d'afficher des informations sur l'utilisation de la mémoire et des tâches.

Pour afficher cette page, cliquez sur **System** (Système) → **General** (Général) → **System Resources** (Ressources du système) dans l'arborescence.

Figure 6-4. Page System Resources (Ressources du système)



Cette page contient les champs suivants :

Total Memory (Mémoire totale) : affiche la quantité totale de mémoire présente sur le commutateur.

Available Memory (Mémoire disponible) : affiche la quantité de mémoire disponible (non affectée) présente sur le commutateur.

Task Name (Nom de la tâche) : nom de la tâche active exécutée sur le commutateur.

Utilization (%) (% d'utilisation) : affiche le pourcentage correspondant au temps processeur utilisé par la tâche correspondante. La valeur résultante est calculée sur une durée de 2 secondes.

Affichage des ressources du système à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

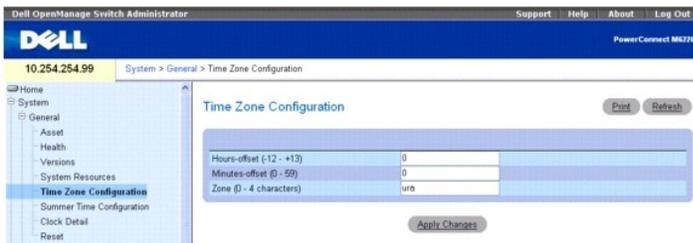
- 1 System Management Commands (Commandes de gestion du système)

Configuration du fuseau horaire

La page **Time Zone Configuration** (Configuration du fuseau horaire) permet de définir le décalage horaire par rapport au temps universel coordonné (UTC).

Pour afficher cette page, cliquez sur **System** (Système) → **General** (Général) → **Time Zone Configuration** (Configuration du fuseau horaire) dans l'arborescence.

Figure 6-5. Page Time Zone Configuration (Configuration du fuseau horaire)



Cette page contient les champs suivants :

Hours-offset (Heures de décalage) : permet de définir le décalage (en nombre d'heures) par rapport au temps universel coordonné (UTC). (Plage de valeurs admise : de -12 à +13)

Minutes-offset (Minutes de décalage) : permet de définir le décalage (en minutes) par rapport au temps universel coordonné (UTC). (Plage de valeurs admise : de 0 à 59)

Zone : permet de définir l'acronyme correspondant au fuseau horaire. (Plage de valeurs admise : de 0 à 4 caractères)

Définition des paramètres du fuseau horaire

1. Affichez la page **Time Zone Configuration** (Configuration du fuseau horaire).
2. Complétez les champs avec les valeurs appropriées.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres du fuseau horaire sont modifiés et le périphérique est mis à jour.

Configuration des paramètres du fuseau horaire à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

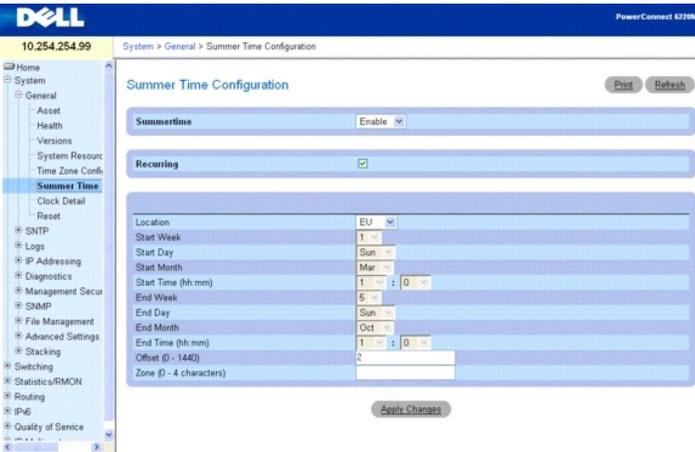
- 1 Clock Commands (Commandes de synchronisation)

Configuration de l'heure d'été

Utilisez la page **Summer Time Configuration** (Configuration de l'heure d'été) pour définir la durée de la période d'utilisation de l'heure d'été et le décalage correspondant.

Pour afficher cette page, cliquez sur **System** (Système) → **General** (Général) → **Summer Time Configuration** (Configuration de l'heure d'été) dans l'arborescence.

Figure 6-6. Page Summer Time Configuration (Configuration de l'heure d'été)



Les champs affichés dans cette page changent selon l'état (sélectionnée ou non) de la case à cocher Recurring (Récurrence). Cette page contient les champs suivants :

Recurring (Récurrence) : sélectionnez cette case à cocher pour indiquer que cette modification horaire doit être répétée tous les ans.

Location (Emplacement) : ce champ s'affiche uniquement lorsque la case Recurring (Récurrence) est cochée. La configuration de l'heure d'été est prédéfinie pour les États-Unis et l'Union européenne. Pour configurer l'heure d'été pour une autre région, sélectionnez None (Aucun).

Start Week (Semaine de début) : sélectionnez le numéro correspondant à la semaine de début. Ce champ s'affiche uniquement lorsque la case Recurring (Récurrence) est cochée.

Start Day (Jour de début) : sélectionnez le numéro du jour de début. Ce champ s'affiche uniquement lorsque la case Recurring (Récurrence) est cochée.

Start Month (Mois de début) : sélectionnez le mois de début.

Start Time (Heure de début) : sélectionnez l'heure de début au format hh:mm.

Start Date (Date de début) : sélectionnez la date de début. Ce champ s'affiche uniquement lorsque la case Recurring (Récurrence) n'est pas cochée.

Start Year (Année de début) : sélectionnez l'année de début. Ce champ s'affiche uniquement lorsque la case Recurring (Récurrence) n'est pas cochée.

End Week (Semaine de fin) : sélectionnez le numéro correspondant à la semaine de fin. Ce champ s'affiche uniquement lorsque la case Recurring (Récurrence) est cochée.

End Day (Jour de fin) : sélectionnez le numéro correspondant au jour de fin. Ce champ s'affiche uniquement lorsque la case Recurring (Récurrence) est cochée.

End Month (Mois de fin) : sélectionnez le mois de fin.

End Time (Heure de fin) : sélectionnez l'heure de fin au format hh:mm.

End Date (Date de fin) : sélectionnez la date de fin. Ce champ s'affiche uniquement lorsque la case Recurring (Récurrence) n'est pas cochée.

End Year (Année de fin) : sélectionnez l'année de fin. Ce champ s'affiche uniquement lorsque la case Recurring (Récurrence) n'est pas cochée.

Offset (Décalage) : définissez le nombre de minutes à ajouter pendant l'heure d'été. Les valeurs admises sont comprises entre 0 et 1440.

Zone : permet de définir l'acronyme du fuseau horaire qui doit être affiché lorsque l'heure d'été est en vigueur.

Définition des paramètres de l'heure d'été

1. Affichez la page **Summer Time Configuration** (Configuration de l'heure d'été).
2. Complétez les champs avec les valeurs appropriées.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de l'heure d'été sont modifiés et le périphérique est mis à jour.

Configuration des paramètres de l'heure d'été à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Clock Commands (Commandes de synchronisation)

Informations détaillées sur l'horloge

La page **Clock Detail** (Informations détaillées sur l'horloge) permet d'afficher l'heure en cours, le fuseau horaire et les paramètres de l'heure d'été.

Pour afficher cette page, cliquez sur **System** (Système) → **General** (Général) → **Clock Detail** (Informations détaillées sur l'horloge) dans l'arborescence.

Figure 6-7. Page Clock Detail (Informations détaillées sur l'horloge)

The screenshot shows the Dell OpenManage Switch Administrator interface. The top navigation bar includes 'Support', 'Help', 'About', and 'Log Out'. The main content area is titled 'Clock Detail' and contains three sections:

- Current Time**

Time (hh:mm)	11:01:19
Zone	ura (UTC + 0:00)
Date	1 Jan 1970
Time Source	No time source
- Time Zone**

Zone	ura
Offset	UTC + 0:00
- Summertime**

Recurring	No
Start Date	1 Jan 2000
Start Time (hh:mm)	00:00
End Date	2 Jan 2000
End Time (hh:mm)	00:00
Offset	0
Zone	Acronym not configured

Cette page contient des informations sur les fonctions suivantes de l'horloge :

Current Time (Heure en cours) : cette section affiche l'heure en cours.

Time Zone (Fuseau horaire) : cette section affiche les paramètres du fuseau horaire.

Summertime (Heure d'été) : cette section affiche les paramètres de l'heure d'été.

Affichage des informations détaillées sur l'horloge à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

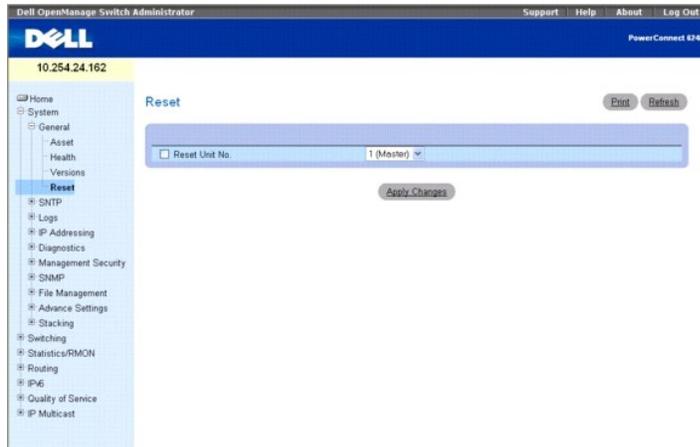
- 1 Clock Commands (Commandes de synchronisation)

Réinitialisation

La page **Reset** (Réinitialisation) permet de réinitialiser le périphérique.

Pour afficher cette page, cliquez sur **System** (Système) → **General** (Général) → **Reset** (Réinitialisation) dans l'arborescence.

Figure 6-8. Page Reset (Réinitialisation)



Cette page contient les champs suivants :

Reset Unit No. (Numéro de l'unité à réinitialiser) : permet de sélectionner le périphérique à réinitialiser dans la pile.

Réinitialisation du périphérique

1. Affichez la page **Reset** (Réinitialiser).
2. Cliquez sur **Reset Unit No.** (Numéro de l'unité à réinitialiser).
3. Sélectionnez **Individual Unit** (Une seule unité) ou **All** (Toutes).
4. Cliquez sur le bouton **Apply Changes** (Appliquer les modifications).
5. Lorsque le message de confirmation s'affiche, cliquez sur **OK**.

Le périphérique sélectionné est réinitialisé. Une fois l'opération terminée, entrez un nom d'utilisateur et un mot de passe.

Configuration des paramètres SNTP

Le périphérique prend en charge le protocole SNTP (Simple Network Time Protocol). Ce dernier synchronise l'horloge du périphérique réseau avec une précision d'un millième de seconde. Cette synchronisation est effectuée par un serveur réseau SNTP. Le périphérique fonctionnant uniquement comme client SNTP, il ne peut pas fournir des services de synchronisation à d'autres systèmes.

Les sources d'heure sont définies par des stratum. Ces derniers définissent la précision de l'horloge de référence. Plus le stratum est élevé (zéro représente la valeur la plus haute), plus l'horloge est précise. Le périphérique étant un stratum de niveau 2, il reçoit l'heure d'un serveur de stratum 1 et supérieur.

Exemple de stratum :

- 1 **Stratum 0** : une horloge temps réel (par exemple un système GPS) est utilisée comme source.
- 1 **Stratum 1** : un serveur directement relié à une source d'heure Stratum 0 est utilisé. Les serveurs d'heure Stratum 1 définissent les normes d'heure du réseau principal.
- 1 **Stratum 2** : la source d'heure est acheminée via le réseau à partir du serveur Stratum 1. Par exemple, un serveur Stratum 2 reçoit l'heure obtenue à partir d'un serveur Stratum 1 via une liaison réseau utilisant le protocole NTP.

Les informations reçues à partir des serveurs SNTP sont évaluées selon le niveau d'heure et le type de serveur.

Les définitions d'heure SNTP sont évaluées et définies selon les niveaux d'heure suivants :

- 1 **T1** : heure à laquelle la requête d'origine a été envoyée par le client.
- 1 **T2** : heure à laquelle la requête d'origine a été reçue par le serveur.
- 1 **T3** : heure à laquelle le serveur a envoyé une réponse.
- 1 **T4** : heure à laquelle le client a reçu la réponse du serveur.

Le périphérique peut interroger les serveurs de type monodiffusion et diffusion pour obtenir l'heure du serveur.

L'interrogation d'informations monodiffusion sert à interroger un serveur dont l'adresse IP est connue. Les serveurs SNTP configurés sur le périphérique sont les seuls serveurs interrogés pour obtenir des informations de synchronisation. Les niveaux T1 à T4 servent à déterminer l'heure du serveur. Ce mécanisme est à privilégier car il s'agit de la méthode la plus sûre pour synchroniser l'heure du périphérique. Si vous la sélectionnez, les informations SNTP seront acceptées uniquement si elles proviennent des serveurs SNTP définis sur le périphérique à l'aide de la page **SNTP Server** (Serveur SNTP).

Les informations de diffusion sont utilisées lorsque l'adresse IP du serveur est inconnue. Lorsqu'un message de diffusion est envoyé à partir d'un serveur SNMP, le client correspondant écoute ce message. Si l'interrogation de diffusion est activée, toutes les informations de synchronisation seront acceptées, même si elles n'ont pas été demandées par le périphérique. Cette méthode est la moins sécurisée.

Le périphérique récupère les informations de synchronisation en les demandant de façon active ou à chaque intervalle d'interrogation. Si les méthodes d'interrogation de monodiffusion et de diffusion sont activées, les informations seront récupérées dans cet ordre :

- 1 Les informations provenant des serveurs définis sur le périphérique sont extraites en priorité. Si la méthode d'interrogation monodiffusion est désactivée ou si aucun serveur n'est défini sur le périphérique, ce dernier accepte les informations de synchronisation provenant de n'importe quel serveur SNMP envoyant une réponse.
- 1 Si plusieurs périphériques monodiffusion répondent, les informations de synchronisation prioritaires sont celles qui proviennent du périphérique correspondant au stratum le plus bas.
- 1 Si les serveurs ont le même stratum, le périphérique accepte les informations de synchronisation provenant du serveur SNMP qui a répondu le premier.

L'authentification MD5 (Message Digest 5) protège les chemins de synchronisation entre le périphérique et les serveurs SNMP. MD5 est un algorithme qui crée un hachage 128 bits. Il s'agit d'une variante de MD4 offrant davantage de sécurité. MD5 vérifie l'intégrité de la communication et en authentifie l'origine.

La page du menu **SNTP** contient des liens vers des pages permettant de configurer les paramètres SNMP.

Pour afficher cette page, cliquez sur **System (Système) → SNTP** dans l'arborescence.

Cette page permet d'accéder aux fonctions suivantes :

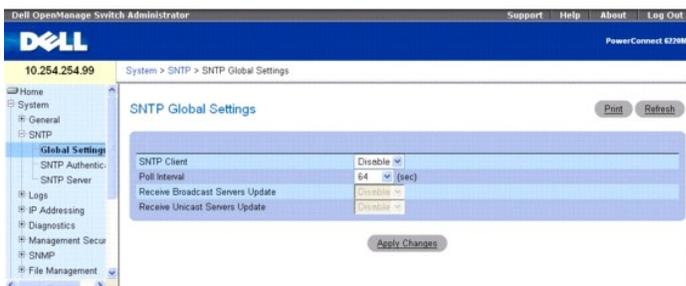
- 1 [Paramètres globaux SNTP](#)
- 1 [Authentification SNTP](#)
- 1 [Serveur SNTP](#)

Paramètres globaux SNTP

La page **SNTP Global Settings** (Paramètres globaux SNTP) permet d'afficher et de régler les paramètres SNTP.

Pour afficher cette page, cliquez sur **System (Système) → SNTP → Global Settings (Paramètres globaux SNTP)** dans l'arborescence.

Figure 6-9. Page **SNTP Global Settings (Paramètres globaux SNTP)**



Cette page contient les champs suivants :

SNTP Client (Client SNMP) : utilisez la liste déroulante pour activer ou désactiver le client. Lorsque le client est désactivé, certains des champs répertoriés ci-dessous le sont également.

Poll Interval (Intervalle d'interrogation) : définit l'intervalle d'interrogation selon lequel les informations de monodiffusion sont demandées au serveur SNMP. Les valeurs admises sont comprises entre 60 et 1024 secondes.

Receive Broadcast Servers Update (Recevoir les mises à jour des serveurs de diffusion) : si cette option est activée, le système écoute les serveurs SNMP sur les interfaces sélectionnées pour obtenir des informations sur l'heure des serveurs de diffusion. Le périphérique est synchronisé à chaque réception d'un paquet SNMP, même si aucune synchronisation n'a été demandée.

Receive Unicast Servers Update (Recevoir les mises à jour des serveurs monodiffusion) : si cette option est activée, les serveurs SNMP définis sur le périphérique sont interrogés pour obtenir l'heure à partir du serveur monodiffusion.

Définition des paramètres globaux SNTP

- 1 Affichez la page **SNTP Global Settings** (Paramètres globaux SNTP).
- 2 Complétez les champs avec les valeurs appropriées.
- 3 Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres globaux SNTP sont modifiés et le périphérique est mis à jour.

Définition des paramètres globaux SNMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

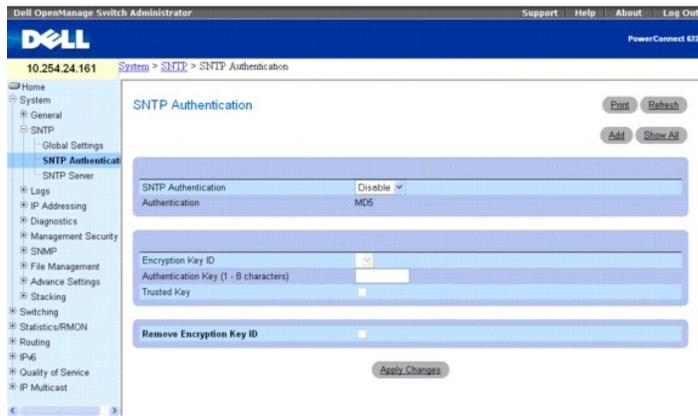
- 1 Clock Commands (Commandes de synchronisation)

Authentification SNMP

La page **SNMP Authentication** (Authentification SNMP) permet d'activer l'authentification SNMP entre le périphérique et un serveur SNMP. Elle permet également de sélectionner le serveur SNMP voulu. Utilisez-la pour activer ou désactiver l'authentification SNMP, modifier la clé d'authentification correspondant à un ID de clé de cryptage afin de définir cette clé d'authentification comme clé de confiance et supprimer l'ID de clé de cryptage sélectionné.

Pour afficher cette page, cliquez sur **System** (Système) → **SNMP** → **Authentication** (Authentification) dans l'arborescence.

Figure 6-10. Page SNMP Authentication (Authentification SNMP)



Cette page contient les champs suivants :

SNMP Authentication (Authentification SNMP) : si cette option est activée, les sessions SNMP ouvertes entre le périphérique et un serveur SNMP doivent être authentifiées.

Authentication (Authentification) : type d'authentification. Le système prend uniquement en charge l'algorithme MD5.

Encryption Key ID (ID de clé de cryptage) : contient la liste des ID de clés définis par l'utilisateur pour l'authentification du serveur SNMP et du périphérique. Les valeurs admises sont comprises entre 1 et 4294767295.

Authentication Key (1-8 Characters) (Clé d'authentification, 1-8 caractères) : affiche la clé utilisée pour l'authentification.

Trusted Key (Clé de confiance) : cochez cette option pour indiquer la clé de cryptage utilisée (monodiffusion) ou désélectionnez-la pour authentifier le serveur SNMP (diffusion).

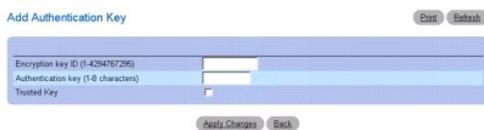
Remove Encryption Key ID (Supprimer un ID de clé de cryptage) : cochez cette option pour supprimer la clé d'authentification sélectionnée.

Ajout d'une clé d'authentification SNMP

1. Affichez la page **SNMP Authentication** (Authentification SNMP).
2. Cliquez sur **Add** (Ajouter).

La page **Add Authentication Key** (Ajouter une clé d'authentification) s'affiche.

Figure 6-11. Page Add Authentication Key (Ajouter une clé d'authentification)



3. Complétez les champs avec les valeurs appropriées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La clé d'authentification SNMP est ajoutée et le périphérique est mis à jour.

Affichage de la table des clés d'authentification

1. Affichez la page **SNTP Authentication** (Authentification SNMP).
2. Cliquez sur **Show All** (Afficher tout).

La page **Authentication Key Table** (Table des clés d'authentification) s'affiche.

Figure 6-12. Page **Authentication Key Table** (Table des clés d'authentification)

Encryption Key ID	Authentication Key	Trusted Key	Remove
4546	1038e	Yes	<input type="checkbox"/>

Suppression d'une clé d'authentification

1. Affichez la page **SNTP Authentication** (Authentification SNMP).
2. Cliquez sur **Show All** (Afficher tout).

La page **Authentication Key Table** (Table des clés d'authentification) s'affiche.

3. Sélectionnez une entrée de la **table des clés d'authentification** en cochant la case **Remove** (Supprimer) appropriée.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est supprimée et le périphérique est mis à jour.

Définition des paramètres d'authentification SNMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

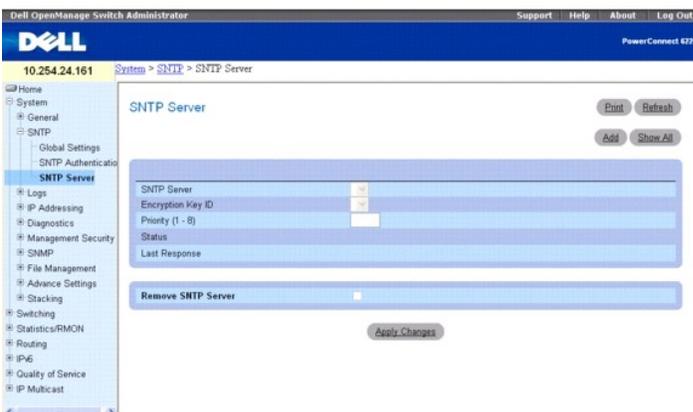
1. Clock Commands (Commandes de synchronisation)

Serveur SNTP

Utilisez la page **SNTP Server** (Serveur SNTP) pour afficher et modifier les informations permettant d'activer les serveurs SNTP, ou encore pour ajouter de nouveaux serveurs de ce type.

Pour afficher cette page, cliquez sur **System** (Système) → **SNTP** → **SNTP Server** (Serveur SNTP) dans l'arborescence.

Figure 6-13. Page **SNTP Servers** (Serveurs SNTP)



Cette page contient les champs suivants :

SNTP Server (Serveur SNTP) : contient un menu déroulant permettant de sélectionner l'adresse IP d'un serveur SNTP défini par l'utilisateur. Le bouton **Add** (Ajouter) permet de définir jusqu'à 8 serveurs SNTP.

Encryption Key ID (ID de clé de cryptage) : indique l'ID de clé défini par l'utilisateur pour la communication entre le serveur SNTP et le périphérique. Cet ID est défini dans la page **SNTP Authentication** (Authentification SNTP).

Priority (1-8) (Priorité, 1-8) : indique la priorité du serveur en ce qui concerne l'ordre d'envoi des requêtes SNTP. Les valeurs admises sont comprises entre 1 et 8, 1 étant la valeur par défaut. Les serveurs associés aux numéros les moins élevés sont prioritaires.

Status (État) : affiche l'état de fonctionnement du serveur SNTP. Les valeurs possibles sont les suivantes :

Up (En fonctionnement) : le serveur SNTP fonctionne normalement.

Down (Non disponible) : indique qu'un serveur SNTP n'est pas disponible, parce qu'il n'est pas connecté ou en panne, par exemple.

In progress (En cours) : le serveur SNTP est en train d'envoyer ou de recevoir des informations SNTP.

Unknown (Inconnu) : l'état d'avancement de l'envoi d'informations SNTP est inconnu. Par exemple, le périphérique recherche une interface.

Last Response (Dernière réponse) : affiche l'heure de réception de la dernière réponse envoyée par le serveur SNTP.

Remove SNTP Server (Supprimer un serveur SNTP) : lorsqu'elle est cochée, cette option supprime le serveur SNTP sélectionné dans la liste **SNTP Servers** (Serveurs SNTP).

Ajout d'un serveur SNTP

1. Affichez la page **SNTP Servers** (Serveurs SNTP).
2. Cliquez sur **Add** (Ajouter).

La page **Add SNTP Server** (Ajouter un serveur SNTP) s'affiche.

Figure 6-14. Page Add SNTP Server (Ajouter un serveur SNTP)



3. Complétez les champs avec les valeurs appropriées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le serveur SNTP est ajouté et le périphérique est mis à jour.

Affichage de la table des serveurs SNTP

1. Affichez la page **SNTP Servers** (Serveurs SNTP).
2. Cliquez sur **Show All** (Afficher tout).

La page **SNTP Servers Table** (Table des serveurs SNTP) s'affiche.

Figure 6-15. Page SNTP Servers Table (Table des serveurs SNTP)



SNTP Server	Encryption Key ID	Priority	Status	Last Response	Remove
10.240.1.10	None	1	Up	Thu 1 Jan 1970 00:00:00	<input type="checkbox"/> Edit

Modification d'un serveur SNTP

1. Affichez la page **SNTP Servers** (Serveurs SNTP).
2. Cliquez sur **Show All** (Afficher tout).

La page **SNTP Servers Table** (Table des serveurs SNTP) s'affiche.

3. Cliquez sur **Edit** (Modifier) en regard du nom du **serveur SNTP** à modifier.
4. Modifiez les champs appropriés.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les informations du serveur SNTP sont mises à jour.

Suppression du serveur SNTP

1. Affichez la page **SNTP Servers** (Serveurs SNTP).
2. Cliquez sur **Show All** (Afficher tout).

La page **SNTP Servers Table** (Table des serveurs SNTP) s'affiche.

3. Sélectionnez un **serveur SNTP**.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est supprimée et le périphérique est mis à jour.

Définition des serveurs SNTP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Clock Commands (Commandes de synchronisation)

Gestion des journaux

Le commutateur peut générer des messages suite à des événements, erreurs ou pannes se produisant sur la plate-forme, ou encore en cas de modifications affectant la configuration ou d'autres éléments. Ces messages sont enregistrés en local mais également transmis à un ou plusieurs points de collecte dans lesquels ils sont centralisés à des fins de surveillance et d'archivage à long terme. Lorsque vous configurez les paramètres locaux et distants de la fonction de consignation, vous pouvez filtrer les messages consignés ou transmis en fonction de leur sévérité et du composant par lequel ils ont été générés.

Le journal *résidant en mémoire* enregistre les messages dans la mémoire en fonction du composant source et de la sévérité. Sur les systèmes empilables, seule la plate-forme principale contient ce journal. Les autres plates-formes transmettent leurs messages à cette dernière. Il n'est pas possible d'accéder aux journaux résidant en mémoire sur les plates-formes autres que la plate-forme principale.

Le journal *persistant* réside dans la mémoire persistante. Il est possible de définir deux types de journal persistant.

- 1 Le premier type est le **journal de démarrage du système**. Ce dernier enregistre les n premiers messages reçus après le redémarrage du système. Lorsqu'il est saturé, les messages ne sont plus consignés (le nombre maximal de messages pouvant être consignés est de 32).
- 1 Le second type est le **journal de fonctionnement du système**. Ce dernier enregistre les n derniers messages reçus lors du fonctionnement du système. En cas de saturation de ce journal, les nouveaux messages écrasent les messages existants. Ce journal peut contenir jusqu'à 1000 messages.

Les messages correspondant aux critères de consignation définis sont enregistrés dans l'un ou l'autre de ces journaux, mais pas les deux. En d'autres termes, si le journal de démarrage est activé, il enregistre tous les messages générés au démarrage du système jusqu'à saturation. Ensuite, les messages sont ajoutés au journal de fonctionnement, s'il est activé.

Le système conserve jusqu'à trois versions des journaux persistants, nommés <FICHIER>0.txt, <FICHIER>1.txt et <FICHIER>2.txt. Au démarrage du système, <FICHIER>2.txt est supprimé, <FICHIER>1.txt est renommé <FICHIER>2.txt, <FICHIER>0.txt est renommé <FICHIER>1.txt, <FICHIER>0.txt est créé et la consignation commence dans ce fichier. (Le terme <FICHIER> ci-dessus est à remplacer par olog dans le cas du journal de fonctionnement et par slog dans le cas du journal de démarrage.)

Les journaux persistants locaux peuvent être obtenus via l'interface CLI, via xmodem (par l'intermédiaire du câble série local) et via TFTP.

Pour afficher la page **Logs** (Journaux), cliquez sur **System** (Système) → **Logs** (Journaux) dans l'arborescence. Cette page permet d'accéder aux fonctions suivantes :

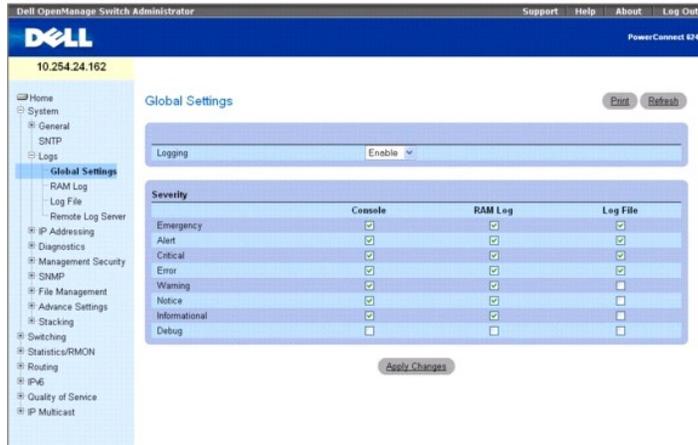
- 1 [Paramètres globaux](#)
- 1 [Journal stocké dans la RAM](#)
- 1 [Fichier journal](#)
- 1 [Paramètres des serveurs de journalisation distants](#)

Paramètres globaux

La page **Global Settings** (Paramètres globaux) permet d'activer les journaux globalement et de définir leurs paramètres. Les messages sont classés par ordre de **sévérité** décroissant.

Pour afficher cette page, cliquez sur **System** (Système) → **Logs** (Journaux) → **Global Settings** (Paramètres globaux) dans l'arborescence.

Figure 6-16. Page **Global Settings** (Paramètres globaux)



Cette page contient les champs suivants :

Logging (Journalisation) : active une journalisation globale du périphérique pour la mémoire cache, les fichiers et le serveur. Tous les journaux affichés sur la console sont enregistrés dans les fichiers journaux. Les valeurs admises sont les suivantes :

Enable (Activer) : active l'enregistrement des journaux pour la mémoire cache (RAM), les fichiers (FLASH) et un serveur externe.

Disable (Désactiver) : désactive l'enregistrement des journaux. L'enregistrement des journaux affichés sur la console ne peut pas être désactivé.

Section Severity (Sévérité)

Utilisez les cases à cocher de cette section pour régler la sensibilité de la console, de la mémoire persistante et des fichiers journaux.

Lorsque vous sélectionnez un niveau spécifique, tous les niveaux supérieurs sont automatiquement sélectionnés. Par exemple, si vous sélectionnez le niveau **Error**, le système sélectionne automatiquement **Error**, **Critical**, **Alert** et **Emergency** (Erreur, Critique, Alerte et Urgence). De même, si vous désélectionnez le niveau **Error**, tous les niveaux inférieurs (par exemple **Error**, **Warning**, **Notice**, **Informational**, **Debug**) sont également désélectionnés.

Emergency (Urgence) : niveau d'avertissement le plus élevé. Si le périphérique est en panne ou ne fonctionne pas correctement, un journal des urgences est enregistré sur celui-ci.

Alert (Alerte) : niveau d'avertissement élevé, au second rang sur l'échelle de sévérité. Un journal des alertes est enregistré en cas de dysfonctionnement grave du périphérique (toutes les fonctions sont arrêtées, etc.).

Critical (Critique) : niveau d'avertissement élevé, au troisième rang sur l'échelle de sévérité. Un journal des événements critiques est enregistré en cas de dysfonctionnement critique du périphérique (par exemple lorsque deux ports ne fonctionnent plus alors que tous les autres sont opérationnels).

Error (Erreur) : une erreur s'est produite sur le périphérique (port déconnecté, par exemple).

Warning (Avertissement) : niveau d'avertissement le plus faible.

Notice (Remarque) : fournit des informations sur le périphérique aux administrateurs réseau.

Informational (Information) : fournit des informations sur le périphérique.

Debug (Débogage) : fournit des informations détaillées sur le journal. Doit être utilisé uniquement par un technicien de support qualifié.

Les cases à cocher apparaissent sous les trois colonnes suivantes :

Console : entrées envoyées à la console.

RAM Logs (Journaux stockés dans la RAM) : entrées envoyées à la mémoire cache (RAM).

Log File (Fichier journal) : entrées envoyées à la mémoire FLASH.

Activation de la journalisation

1. Affichez la page **Global Settings** (Paramètres globaux).
2. Dans le menu déroulant **Logging** (Journalisation), sélectionnez **Enable** (Activer).
3. Utilisez les cases à cocher pour sélectionner le type de consignation et la sévérité.

REMARQUE : Lorsque vous sélectionnez un niveau spécifique, tous les niveaux supérieurs sont automatiquement sélectionnés.

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de journalisation sont enregistrés et le périphérique est mis à jour.

Activation de la journalisation globale à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Syslog Commands (Commandes syslog)

Journal stocké dans la RAM

La page **RAM Log Table** (Journal stocké dans la RAM) fournit des informations sur des entrées spécifiques du journal stocké en mémoire cache (RAM). Elle indique notamment l'heure de création de l'entrée, sa sévérité et inclut une description.

Pour afficher cette page, cliquez sur **System** (Système) → **Logs** (Journaux) → **RAM Log** (Journal stocké dans la RAM) dans l'arborescence.

Figure 6-17. Page **RAM Log Table** (Journal stocké dans la RAM)

Log Index	Severity	Log Time	Component	Description
1	Alert	JAN 01 00:00:02:UN-N	%	Error 0 (DxD)
2	Critical	JAN 01 00:00:05:UN-N	%	Event(Draaaaaaa)
3	Informational	JAN 01 00:00:05:UN-N	%	Starting code...
4	Informational	JAN 01 00:00:29:UN-N	%	EDE Callback: Unit Join: 1
5	Informational	JAN 01 00:00:29:UN-N	%	File simCgData.cfg: same version (4) but the sizes (300->684) differ
6	Informational	JAN 01 00:00:29:UN-N	%	Migrating config file simCgData.cfg from version 4 to 4
7	Informational	JAN 01 00:00:29:UN-N	%	sysapiCgFileGet failed size = 684 version = 4
8	Informational	JAN 01 00:00:29:UN-N	%	Building Defaults
9	Informational	JAN 01 00:00:30:UN-N	%	fdbDelete: received delete for unexpected FDB entry.
10	Informational	JAN 01 00:00:30:UN-N	%	fdbStatsUpdate called with unknown netNum 1
11	Informational	JAN 01 00:00:37:UN-N	%	not able to open the file specified
12	Informational	JAN 01 00:00:37:UN-N	%	Migrating config file trapCgData.cfg from version 5 to 6
13	Informational	JAN 01 00:00:37:UN-N	%	File dot1x.cfg: same version (4) but the sizes (30104->37604) differ
14	Informational	JAN 01 00:00:37:UN-N	%	Migrating config file dot1x.cfg from version 4 to 4
15	Informational	JAN 01 00:00:37:UN-N	%	sysapiCgFileGet failed size = 37604 version = 4
16	Informational	JAN 01 00:00:37:UN-N	%	Building Defaults
17	Informational	JAN 01 00:00:37:UN-N	%	SSH: mode 0 unchanged
18	Informational	JAN 01 00:00:38:UN-N	%	Migrating config file ipStaticRoutesCg.cfg from version 4 to 5
19	Informational	JAN 01 00:00:39:UN-N	%	macalSysnetRegisterDeregister(): Failed to deregister with sysnet

Cette page contient les champs suivants :

Log Index (Index du journal) : numéro de l'entrée dans la table du journal stocké dans la RAM.

Severity (Sévérité) : sévérité de l'entrée.

Log Time (Heure de journalisation) : indique l'heure à laquelle l'entrée a été ajoutée à la table du journal stocké dans la RAM.

Component (Composant) : composant auquel l'entrée se rapporte.

Description : description de l'entrée.

Suppression d'entrées de journal

1. Affichez la page **RAM Log** (Journal stocké dans la RAM).
2. Cliquez sur **Clear Log** (Effacer le journal).

Les informations consignées sont supprimées de la table du fichier journal et le périphérique est mis à jour.

Suppression d'entrées de journal à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

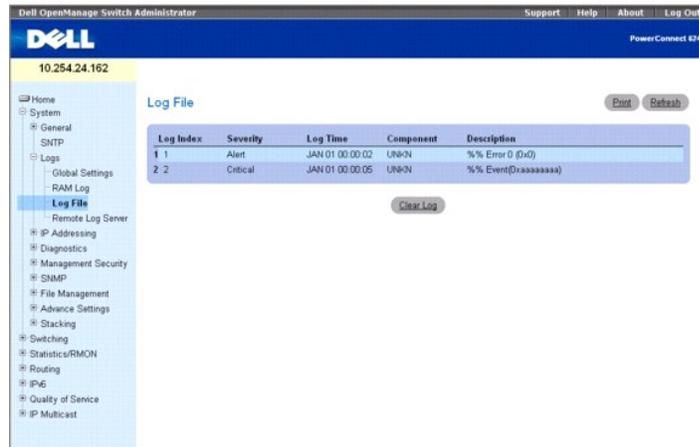
- 1 Syslog Commands (Commandes syslog)

Fichier journal

La page **Log File** (Fichier journal) contient des informations sur des entrées spécifiques du journal : heure de création, sévérité et description.

Pour afficher cette page, cliquez sur **System** (Système) → **Logs** (Journaux) → **Log File** (Fichier journal) dans l'arborescence.

Figure 6-18. Page Log File (Fichier journal)



Cette page contient les champs suivants :

- 1 **Log Index** (Index de journalisation) : numéro de l'entrée dans la table du fichier journal.
- 1 **Severity** (Sévérité) : sévérité de l'entrée.
- 1 **Log Time** (Heure de journalisation) : indique l'heure à laquelle l'entrée a été créée dans la table du fichier journal.
- 1 **Component** (Composant) : composant auquel l'entrée se rapporte.
- 1 **Description** : description de l'entrée.

Suppression d'entrées de journal

1. Affichez la page **Log File Table** (Table du fichier journal).
2. Cliquez sur **Clear Log** (Effacer le journal).

Les informations consignées sont supprimées de la table du fichier journal et le périphérique est mis à jour.

Suppression d'entrées de journal à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

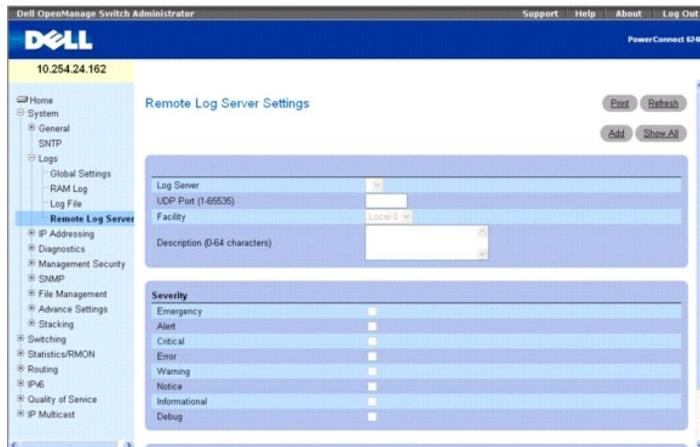
- 1 Syslog Commands (Commandes syslog)

Paramètres des serveurs de journalisation distants

La page **Remote Log Server Settings** (Paramètres des serveurs de journalisation distants) permet d'afficher les serveurs de journalisation disponibles, de configurer de nouveaux serveurs de journalisation et de définir la sévérité des entrées envoyées au serveur.

Pour afficher cette page, cliquez sur **System** (Système) → **Logs** (Journaux) → **Remote Log Server** (Serveur de journalisation distant).

Figure 6-19. Page Remote Log Server Settings (Paramètres des serveurs de journalisation distants)



Cette page contient les champs suivants :

Log Server (Serveur de journalisation) : serveur auxquels les entrées peuvent être envoyées.

UDP Port (1-65535) (Port UDP, 1-65535) : port UDP à partir duquel les entrées sont envoyées. La valeur par défaut est de 514.

Facility (Voie de transmission) : application définie par l'utilisateur, à partir de laquelle les journaux système sont envoyés au serveur distant. Une seule voie de transmission peut être affectée à chaque serveur. Si vous en définissez une seconde, celle-ci remplace la première. Toutes les applications définies pour un périphérique utilisent la même voie de transmission sur un serveur. Les valeurs admises vont de **Local 0** à **Local 7**.

Description : définit la description du serveur. La longueur maximale est de 64 caractères.

Severity (Sévérité) : sévérité des entrées. Lorsque vous sélectionnez un niveau spécifique, tous les niveaux supérieurs sont automatiquement sélectionnés.

Remove Log Server (Supprimer un serveur de journalisation) : supprime un serveur de la liste **Log Server** (Serveur de journalisation). Cochez la case pour supprimer le serveur de la liste.

La page **Remote Log Server Settings** (Paramètres des serveurs de journalisation distants) affiche également une liste des niveaux de sévérité. Ces niveaux sont identiques à ceux indiqués dans la page **RAM Log Table** (Table du journal stocké dans la RAM).

Envoi de journaux à un serveur

1. Affichez la page **Remote Log Server Settings** (Paramètres des serveurs de journalisation distants).
2. Définissez les champs **UDP Port** (Port UDP), **Facility** (Voie de transmission) et **Description**.
3. Sélectionnez le type d'entrée et la sévérité à l'aide des cases à cocher **Log Parameters** (Paramètres de journalisation).

REMARQUE : Lorsque vous sélectionnez un niveau spécifique, tous les niveaux supérieurs sont automatiquement sélectionnés.

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de journalisation sont enregistrés et le périphérique est mis à jour.

Ajout d'un nouveau serveur

1. Affichez la page **Remote Log Server Settings** (Paramètres des serveurs de journalisation distants).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add Remote Log Server** (Ajouter un serveur de journalisation distant).

REMARQUE : Avant d'ajouter un nouveau serveur, identifiez l'adresse IP du serveur de journalisation distant.

Figure 6-20. Page **Add Remote Log Server** (Ajouter un serveur de journalisation distant) - Paramètres

Add Remote Log Server Print Refresh

Log Server	<input type="text"/>
UDP Port (1-65535)	514
Facility	Local 7
Description (64 characters)	<input type="text"/>

Severity	
Emergency	<input checked="" type="checkbox"/>
Alert	<input checked="" type="checkbox"/>
Critical	<input checked="" type="checkbox"/>
Error	<input checked="" type="checkbox"/>
Warning	<input checked="" type="checkbox"/>
Notice	<input checked="" type="checkbox"/>
Informational	<input checked="" type="checkbox"/>
Debug	<input type="checkbox"/>

Apply Changes Back

3. Complétez les champs de la boîte de dialogue et cliquez sur **Apply Changes** (Appliquer les modifications).

La liste **Log Server** (Serveur de journalisation) n'affiche le nom du serveur que lorsque vous revenez à la page **Remote Log Server Settings** (Paramètres des serveurs de journalisation distants).

Affichage/Suppression d'un serveur de journalisation

1. Affichez la page **Remote Log Server Settings** (Paramètres des serveurs de journalisation distants).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Remote Log Servers Table** (Table des serveurs de journalisation distants).

Figure 6-21. Page Remote Log Servers Table (Table des serveurs de journalisation distants)

Remote Log Servers Table Print Refresh

Log Server	UDP Port	Facility	Description	Minimum Severity	Remove
1 10.240.10.1	23	Local 7		Informational	<input type="checkbox"/> Edit

Apply Changes Back

3. Pour supprimer un serveur, cochez la case **Remove** (Supprimer) appropriée.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le serveur est supprimé et le périphérique est mis à jour.

Utilisation des serveurs de journalisation distants à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Syslog Commands (Commandes syslog)

Définition de l'adressage IP

La page **IP Addressing** (Adressage IP) permet d'effectuer plusieurs opérations : affectation des adresses IP à l'interface de gestion et à la passerelle par défaut, définition des paramètres pour la négociation avec le système de noms de domaines (DNS), définition d'un nom de domaine par défaut, mappage des noms d'hôtes, définition des paramètres ARP et DHCP pour les interfaces.

Pour afficher cette page, cliquez sur **System** (Système) → **IP Addressing** (Adressage IP) dans l'arborescence. Cette page permet d'accéder aux fonctions suivantes :

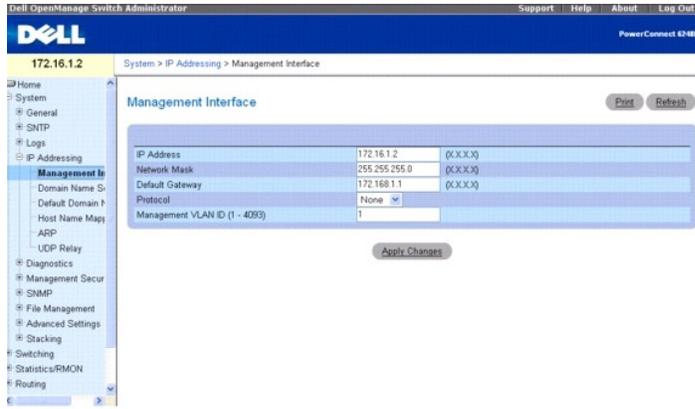
- 1 [Interface de gestion](#)
- 1 [Serveur DNS](#)
- 1 [Nom de domaine par défaut](#)
- 1 [Mappage des noms d'hôtes](#)
- 1 [Table ARP](#)
- 1 Relais UDP

Interface de gestion

La page **Management Interface** (Interface de gestion) permet de définir l'adresse IP de l'interface de gestion, le masque de sous-réseau et l'adresse IP de la passerelle par défaut. Elle permet également d'activer et de désactiver le protocole d'amorçage.

Pour afficher cette page, cliquez sur **System** (Système) → **IP Addressing** (Adressage IP) → **Management Interface** (Interface de gestion) dans l'arborescence.

Figure 6-22. Page Management Interface (Interface de gestion)



Page Management Interface (Interface de gestion)

Cette page contient les champs suivants :

IP Address (Adresse IP) : affiche l'adresse IP de l'interface de gestion.

Network Mask (Masque de réseau) : indique le masque de sous-réseau de l'adresse IP source.

REMARQUE : Chaque partie de l'adresse IP doit commencer par un chiffre différent de zéro. Par exemple, les adresses IP 001.100.192.6 et 192.001.10.3 ne sont pas valides.

Default Gateway (Passerelle par défaut) : définit l'adresse IP de la passerelle par défaut.

Protocol (Protocole) : utilisez le menu déroulant pour sélectionner Bootp, DHCP ou l'option None (Aucun).

Management VLAN ID (1-4093) (ID du VLAN de gestion, 1-4093) : définit l'ID du VLAN de gestion. Les valeurs admises sont comprises entre 1 et 4093.

AVIS : Le fait de changer de VLAN de gestion ferme votre session Web.

Modification des paramètres d'adresse IP de l'interface de gestion

1. Affichez la page **Management Interface** (Interface de gestion).
2. Modifiez l'adresse IP indiquée dans le champ **IP Address** (Adresse IP).
3. Modifiez les autres champs avec les valeurs appropriées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont modifiés et le périphérique est mis à jour.

Définition des paramètres d'interface IP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 IP Routing Commands (Commandes de routage IP)

Serveur DNS

Le serveur DNS convertit les noms de domaines définis par l'utilisateur en adresses IP. Chaque nom de domaine défini est converti en adresse IP numérique. Par exemple, www.exempleip.com devient 192.87.56.2. Les serveurs DNS gèrent les bases de données de noms de domaines et les adresses IP correspondantes.

La page **Domain Name Server** (Serveur DNS) permet d'activer des serveurs DNS spécifiques.

Pour afficher cette page, cliquez sur **System (Système)** → **IP Addressing (Adressage IP)** → **Domain Name Server (Serveur DNS)** dans l'arborescence.

Figure 6-23. Page Domain Name Server (Serveur DNS)



Cette page contient les champs suivants :

DNS Status (État du DNS) : active ou désactive la conversion des noms en adresses IP par le serveur DNS.

DNS Server (Serveur DNS) : contient la liste des serveurs DNS. Pour ajouter de tels serveurs, utilisez la page **Add DNS Server (Ajouter un serveur DNS)**.

Remove (Supprimer) : lorsqu'elle est cochée, cette option supprime le serveur DNS sélectionné.

Ajout d'un serveur DNS

1. Affichez la page **Domain Name Server (Serveur DNS)**.
2. Cliquez sur **Add (Ajouter)**.

La page **Add DNS Server (Ajouter un serveur DNS)** s'affiche.

Figure 6-24. Page Add DNS Server (Ajouter un serveur DNS)



3. Complétez les champs appropriés.
4. Cliquez sur **Apply Changes (Appliquer les modifications)**.

Le nouveau serveur DNS est défini et le périphérique est mis à jour.

Configuration des serveurs DNS à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

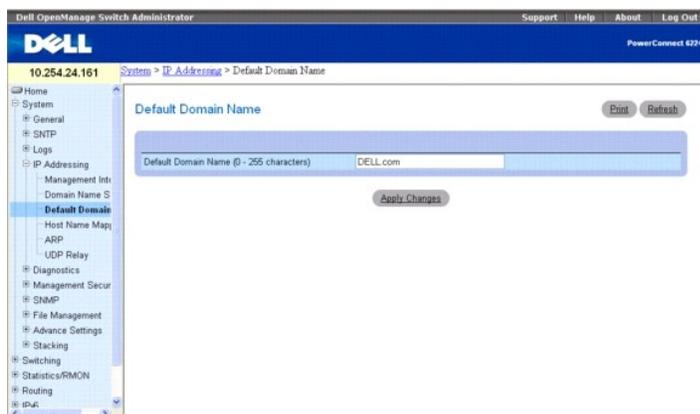
- 1 IP Addressing Commands (Commandes d'adressage IP)

Nom de domaine par défaut

La page **Default Domain Name (Nom de domaine par défaut)** permet d'afficher et de définir des noms de domaines DNS par défaut.

Pour afficher cette page, cliquez sur **System (Système)** → **IP Addressing (Adressage IP)** → **Default Domain Name (Nom de domaine par défaut)**.

Figure 6-25. Page Default Domain Name (Nom de domaine par défaut)



Cette page contient le champ suivant :

Default Domain Name (0-255 characters) (Nom de domaine par défaut, 0-255 caractères) : contient le nom de domaine par défaut défini par l'utilisateur. Une fois défini, le nom de domaine par défaut est appliqué à tous les noms d'hôtes non qualifiés.

Définition des noms de domaines DNS à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

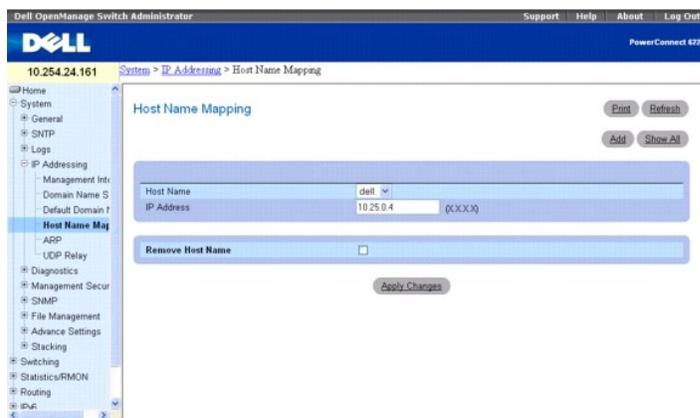
- 1 IP Addressing Commands (Commandes d'adressage IP)

Mappage des noms d'hôtes

La page **Host Name Mapping** (Mappage des noms d'hôtes) permet d'affecter une adresse IP à un nom d'hôte statique. Elle fournit une adresse IP par système hôte.

Pour afficher cette page, cliquez sur **System** (Système) → **IP Addressing** (Adressage IP) → **Host Name Mapping** (Mappage des noms d'hôtes).

Figure 6-26. Page Host Name Mapping (Mappage des noms d'hôtes)



Cette page contient les champs suivants :

Host Name (Nom d'hôte) : répertorie les noms d'hôtes. Ces derniers sont définis dans la page **Add Static Host Name Mapping** (Ajouter un mappage de nom d'hôte statique). Chaque hôte fournit une adresse IP.

IP Address (Adresse IP) : indique l'adresse IP affectée au nom d'hôte spécifié.

Remove Host Name (Supprimer un nom d'hôte) : lorsqu'elle est cochée, cette option supprime le mappage IP pour le nom d'hôte sélectionné.

Ajout de noms de domaines hôtes

1. Affichez la page **Host Name Mapping** (Mappage des noms d'hôtes).
2. Cliquez sur **Add** (Ajouter).

La page **Add Static Host Name Mapping** (Ajouter un mappage de nom d'hôte statique) s'affiche.

Figure 6-27. Page Add Static Host Name Mapping (Ajouter un mappage de nom d'hôte statique)

Host Name (0 - 255 characters) DELL
IP Address 10.25.0.4 (XXXX)

Apply Changes Back

3. Complétez les champs appropriés.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse IP est mappée avec le nom d'hôte et le périphérique est mis à jour.

Affichage de la table de mappage des noms d'hôte statiques

1. Affichez la page **Host Name Mapping** (Mappage des noms d'hôtes).
2. Cliquez sur **Show All** (Afficher tout).

La page **Static Hosts Name Mapping Table** (Table de mappage des noms d'hôtes statiques) s'affiche.

Figure 6-28. Page Static Host Name Mapping Table (Table de mappage des noms d'hôtes statiques)

Host Name	IP Address	Remove
DELL	10.25.0.4	<input type="checkbox"/>

Previous Next
Apply Changes Back

Suppression du mappage entre un nom d'hôte et une adresse IP

1. Affichez la page **Host Name Mapping** (Mappage des noms d'hôtes).
2. Cliquez sur **Show All** (Afficher tout).

La page **Host Name Mapping Table** (Table de mappage des noms d'hôtes) s'affiche.

3. Sélectionnez une entrée dans cette table.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est supprimée de la table de mappage des noms d'hôtes et le périphérique est mis à jour.

Mappage d'une adresse IP avec un nom de domaine hôte à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 IP Addressing Commands (Commandes d'adressage IP)

Table ARP

La page **ARP Table** (Table ARP) permet d'afficher les paramètres ARP pour les interfaces IP. Elle affiche la corrélation entre chaque adresse MAC et l'adresse IP

correspondante.

Pour afficher cette page, cliquez sur **System (Système)** → **IP Addressing (Adressage IP)** → **ARP** dans l'arborescence.

Figure 6-29. Page ARP Table (Table ARP)



Cette page contient les champs suivants :

IP Address (Adresse IP) : adresse IP de la station associée à l'adresse MAC spécifiée ci-dessous.

MAC Address (Adresse MAC) : adresse MAC de la station associée à l'adresse IP dans la table ARP.

Affichage de la table ARP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 IP Addressing Commands (Commandes d'adressage IP)

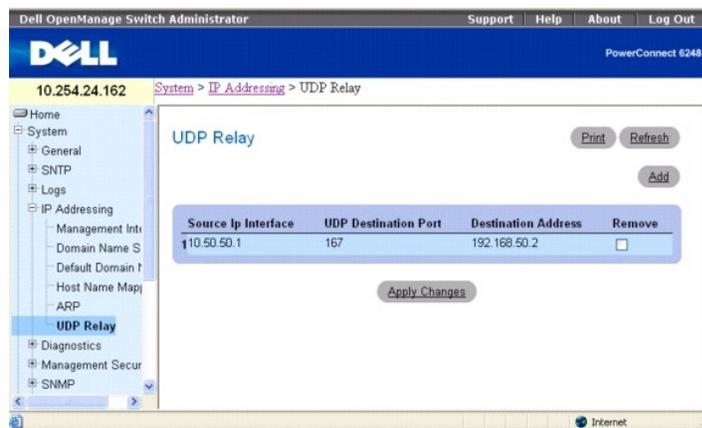
Relais UDP

La fonction de relais UDP permet au périphérique de transmettre des diffusions UDP spécifiques d'une interface à l'autre. En général, les paquets de diffusion IP ne font pas l'objet d'un tel transfert, mais certaines applications utilisent la diffusion UDP pour détecter la disponibilité d'un service. D'autres services requièrent le routage de paquets de diffusion UDP pour fournir des services aux clients d'un autre sous-réseau. Cette fonction permet également la navigation lorsque les stations de travail et les serveurs sont sur des réseaux différents.

La page UDP Relay (Relais UDP) permet d'ajouter, d'afficher ou de supprimer la configuration d'un relais UDP.

Pour afficher cette page, cliquez sur **System (Système)** → **IP Addressing (Adressage IP)** → **UDP Relay (Relais UDP)**.

Figure 6-30. Page Relais UDP (Relais UDP)



Cette page contient les champs suivants :

Source IP Interface (Interface IP source) : interface IP d'entrée qui relaie les paquets UDP. Si le contenu de ce champ est 255.255.255.255, les paquets UDP de toutes les interfaces sont relayés. Les plages d'adresses suivantes ne sont pas valides :

0.0.0.0 à 0.255.255.255

127.0.0.0 à 127.255.255.255

UDP Destination Port (1-65535) (Port de destination UDP, 1-65535) : numéro du port UDP de destination des paquets UDP à relayer. Le tableau suivant répertorie les affectations des ports UDP.

Numéro du port UDP	Nom	Application
7	Echo	Echo
11	SysStat	Utilisateur actif
15	NetStat	NetStat
17	Quote	Citation du jour
19	CHARGEN	Générateur de caractères
20	FTP-data	Données FTP
21	FTP	FTP
37	Heure	Heure
42	NAMESERVER	Serveur de nom d'hôte
43	NICNAME	Qui est-ce
53	DOMAIN	Serveur DNS
69	TFTP	Transfert de fichiers simple
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Heure réseau
137	NetBiosNameService	Connexions du serveur NT vers les stations
138	NetBiosDatagramService	Connexions du serveur NT vers les stations
139	NetBios	Connexions du serveur SessionServiceNT vers les stations
161	SNMP	Protocole SNMP
162	SNMP-trap	Interruptions SNMP
513	who	Démon Unix Rwho
514	syslog	Journal système
525	timed	Démon heure

Destination Address (Adresse de destination) : interface IP qui reçoit les relais de paquets UDP. Si le contenu de ce champ est 0.0.0.0, les paquets UDP sont rejetés. Si le contenu de ce champ est 255.255.255.255, les paquets UDP sont acheminés en masse vers toutes les interfaces IP.

Remove (Supprimer) : cochez cette case pour supprimer le relais UDP sélectionné.

Ajout d'une entrée de relais UDP

1. Affichez la page **UDP Relay** (Relais UDP).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add UDP Relay** (Ajouter un relais UDP).

Figure 6-31. Page Add UDP Relay (Ajouter un relais UDP)



3. Complétez les champs **Source IP Interface** (Interface IP source), **UDP Destination Port** (Port de destination UDP) et **Destination Address** (Adresse de destination).

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le relais UDP est ajouté et le périphérique est mis à jour.

5. Cliquez sur **Back** (Précédent) pour revenir à la page **UDP Relay** (Relais UDP).

 **REMARQUE :** Si le relais UDP est activé alors qu'aucun numéro de port UDP n'a été défini, le périphérique transmet par défaut les paquets de diffusion UDP pour les services suivants : service de noms IEN-116 (port 42), DNS (port 53), serveur de noms NetBIOS (port 137), serveur de datagrammes NetBIOS (port 138), serveur TACACS (port 49) et service d'heure (port 37).

Suppression d'un relais UDP

1. Affichez la page **UDP Relay** (Relais UDP).

2. Cochez la case **Remove** (Supprimer) correspondant à l'élément à supprimer.

3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est supprimée et le périphérique est mis à jour.

Configuration des informations sur le relais UDP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- IP Addressing Commands (Commandes d'adressage IP)

Exécution des diagnostics relatifs aux câbles

La page **Diagnostics** permet d'effectuer des tests virtuels pour câbles en cuivre et à fibre optique.

Pour afficher cette page, cliquez sur **System** (Système) → **Diagnostics** dans l'arborescence.

Cette page permet d'accéder aux fonctions suivantes :

- [Test intégré pour les câbles de cuivre](#)
- [Diagnostics des émetteurs-récepteurs optiques](#)

Test intégré pour les câbles de cuivre

La page **Integrated Cable Test for Copper Cables** (Test intégré pour les câbles de cuivre) permet de tester les câbles de cuivre, afin de savoir où les erreurs sont survenues sur le câble, quand un test de câble a été effectué pour la dernière fois et d'identifier le type d'erreur survenue. Les tests utilisent la technologie TDR (Time Domain Reflectometry - Réflectométrie en domaine temporel) pour tester la qualité et les caractéristiques d'un câble en cuivre raccordé à un port. Il est possible de tester des câbles mesurant jusqu'à 120 mètres. Ces tests sont effectués lorsque les ports sont inactifs, à l'exception du test de longueur approximative de câble.

Pour afficher cette page, cliquez sur **System** (Système) → **Diagnostics** → **Integrated Cable Test** (Test intégré pour les câbles) dans l'arborescence.

Figure 6-32. Page Integrated Cable Test for Copper Cables (Test intégré pour les câbles de cuivre)



Cette page contient les champs suivants :

Interface : interface à laquelle le câble est connecté.

Test Result (Résultat du test) : résultats du test du câble. Ce champ peut prendre les valeurs suivantes :

No Cable (Aucun câble) : aucun câble n'est connecté au port.

Open Cable (Câble ouvert) : le câble est ouvert.

Short Cable (Câble en court-circuit) : un court-circuit est survenu sur le câble.

OK : le test du câble a abouti.

Fiber Cable (Câble à fibre optique) : un câble à fibre optique est raccordé au port.

Cable Fault Distance (Emplacement du défaut du câble) : distance entre le port et l'endroit où l'erreur est survenue sur le câble.

Last Update (Dernière mise à jour) : dernier test effectué sur ce port.

Cable Length (Longueur du câble) : longueur approximative du câble. Ce test peut être effectué uniquement lorsque les ports sont activés et fonctionnent à 1 Gbps.

Réalisation d'un test de câble

1. Vérifiez que les deux extrémités du câble de cuivre sont raccordées à un périphérique.
2. Affichez la page **Integrated Cable Test for Copper Cables** (Test intégré pour les câbles de cuivre).
3. Cliquez sur **Run Test** (Lancer le test).

Le test du câble en cuivre est réalisé et les résultats s'affichent dans la page **Integrated Cable Test for Copper Cables** (Test intégré pour les câbles de cuivre).

Affichage de la table de résultats du test intégré pour les câbles

1. Affichez la page **Integrated Cable Test for Copper Cables** (Test intégré pour les câbles de cuivre).
2. Cliquez sur **Show All** (Afficher tout).
3. Sélectionnez l'unité voulue dans le menu déroulant.

La page Web **Integrated Cable Test Results Table** (Table de résultats du test intégré pour les câbles) affiche les résultats des tests précédents pour chaque port de l'unité sélectionnée.

Figure 6-33. **Integrated Cable Test Results Table** (Table de résultats du test intégré pour les câbles)

Integrated Cable Test Results Table Print Refresh

Unit: 1

Interface	Test Result	Cable Fault Distance (m)	Last Update	Cable Length (m)
1/g1	Test has not been performed			
1/g2	Test has not been performed			
1/g3	Test has not been performed			
1/g4	Test has not been performed			
1/g5	Test has not been performed			
1/g6	Test has not been performed			
1/g7	Test has not been performed			
1/g8	Test has not been performed			
1/g9	Test has not been performed			
1/g10	Test has not been performed			
1/g11	Test has not been performed			

Tests des câbles de cuivre à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 PHY Diagnostics Commands (Commandes de diagnostic PHY)

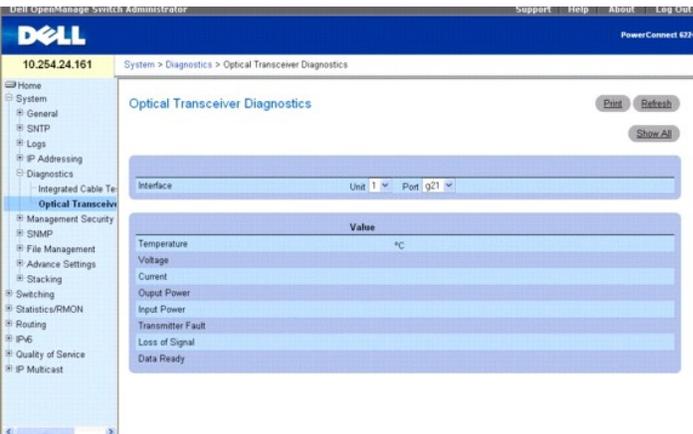
Diagnostics des émetteurs-récepteurs optiques

La page **Optical Transceiver Diagnostics** (Diagnostics des émetteurs-récepteurs optiques) permet de tester les câbles à fibre optique.

Pour afficher cette page, cliquez sur **System** (Système) → **Diagnostics** → **Optical Transceiver Diagnostics** (Diagnostics des émetteurs-récepteurs optiques) dans l'arborescence.

REMARQUE : Les diagnostics des émetteurs-récepteurs optiques ne peuvent être lancés que si la liaison est établie.

Figure 6-34. Page **Optical Transceiver Diagnostics** (Diagnostics des émetteurs-récepteurs optiques)



Cette page contient les champs suivants :

Interface : adresse IP du port sur lequel le câble est testé.

Temperature (Température) : température (en °C) de fonctionnement du câble.

Voltage (Tension) : tension de fonctionnement du câble.

Current (Courant) : courant de fonctionnement du câble.

Output Power (Puissance de sortie) : niveau auquel la puissance de sortie est transmise.

Input Power (Puissance d'entrée) : niveau auquel la puissance d'entrée est transmise.

Transmitter Fault (Défaillance de l'émetteur-transmetteur) : indique si une défaillance est survenue lors de la transmission.

Loss of Signal (Perte de signal) : indique si une perte de signal s'est produite sur le câble.

Data Ready (Données prêtes) : indique que l'émetteur-récepteur est sous tension et que les données sont prêtes.

REMARQUE : Les émetteurs-récepteurs Finisar ne prennent pas en charge le diagnostic des pannes des émetteurs-transmetteurs. La fonction d'analyse de fibre optique fonctionne uniquement sur les SFP prenant en charge la norme de diagnostic numérique SFF-4872.

Affichage de la table de résultats des diagnostics pour les émetteurs-récepteurs optiques

1. Affichez la page **Optical Transceiver Diagnostics** (Diagnostics des émetteurs-récepteurs optiques).
2. Cliquez sur **Show All** (Afficher tout).
3. Sélectionnez l'unité voulue dans le menu déroulant.

Figure 6-35. Page **Optical Transceiver Diagnostics Table** (Table des diagnostics des émetteurs-récepteurs optiques)

Interface	Temperature (°C)	Voltage (V)	Current (mA)	Output Power (mW)	Input Power (mW)	Transmitter Fault	Loss of Signal (dB)
1/g45							
1/g46							
1/g47							
1/g48							

Le test est effectué et la page **Optical Transceiver Diagnostics Table** (Table des diagnostics des émetteurs-récepteurs optiques) s'affiche.

Test des câbles à fibre optique à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 PHY Diagnostics Commands (Commandes de diagnostic PHY)

Gestion de la sécurité du périphérique

Utilisez la page **Management Security** (Gestion de la sécurité) pour définir les paramètres permettant de sécuriser les ports, les utilisateurs et les serveurs.

Pour afficher cette page, cliquez sur **System** (Système) → **Management Security** (Gestion de la sécurité) dans l'arborescence. Cette page permet d'accéder aux fonctions suivantes :

- 1 [Profil d'accès](#)
- 1 [Profils d'authentification](#)
- 1 [Sélection d'une authentification](#)
- 1 [Gestion des mots de passe](#)
- 1 [Base de données utilisateurs locale](#)
- 1 [Mots de passe de ligne](#)
- 1 [Mot de passe d'activation](#)
- 1 [Paramètres TACACS+](#)
- 1 [Paramètres RADIUS](#)
- 1 [Serveur Telnet](#)
- 1 [Refus de service](#)

Profil d'accès

La page **Access Profile** (Profil d'accès) permet de définir des profils et des règles d'accès au périphérique. Vous pouvez limiter l'accès à certaines fonctions de gestion spécifiques, à des interfaces d'entrée et/ou à des adresses IP source ou des sous-réseaux IP source.

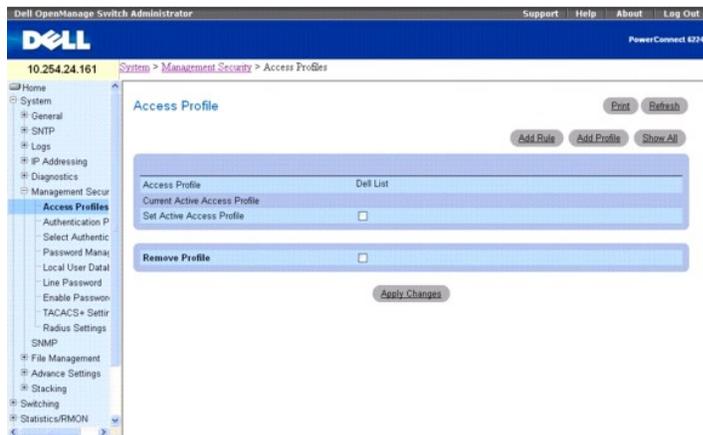
Un accès de gestion peut être défini pour chaque type de méthode d'accès de gestion : Web (HTTP), Web sécurisé (HTTPS), Telnet, SSH et SNMP.

Les listes d'accès de gestion contiennent les règles qui déterminent les modalités de gestion du périphérique et les utilisateurs auxquels cette gestion incombe. Il est également possible d'interdire l'accès au périphérique à certains utilisateurs.

La page **Access Profile** (Profil d'accès) permet de configurer des listes de gestion et de les appliquer à des interfaces spécifiques.

Pour afficher cette page, cliquez sur **System** (Système) → **Management Security** (Gestion de la sécurité) → **Access Profiles** (Profils d'accès) dans l'arborescence.

Figure 6-36. Page **Access Profile** (Profil d'accès)



Access Profile (Profil d'accès) : affiche le profil d'accès.

Current Active Access Profile (Profil d'accès actif) : affiche le profil actuellement activé.

Set Active Access Profile (Définir le profil d'accès actif) : active le profil d'accès.

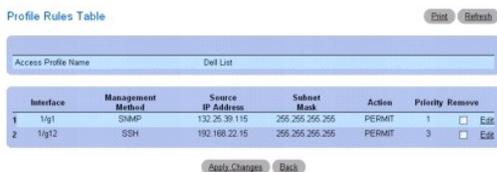
Remove Profile (Supprimer un profil) : lorsqu'elle est cochée, cette option supprime un profil d'accès de la liste **Access Profile** (Profil d'accès).

REMARQUE : L'attribution d'un profil d'accès à une interface implique que l'accès via les autres interfaces est refusé. Si aucun profil d'accès n'est activé, le périphérique est accessible via toutes les interfaces.

Affichage du profil d'accès

1. Affichez la page **Access Profile** (Profil d'accès).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Profile Rules Table** (Table des règles de profil).

Figure 6-37. Page **Profile Rules Table** (Table des règles de profil)



Ajout d'un profil d'accès

1. Affichez la page **Access Profile** (Profil d'accès).
2. Cliquez sur **Add Profile** (Ajouter un profil).

La page **Add An Access Profile** (Ajouter un profil d'accès) s'affiche.

Figure 6-38. Page **Add an Access Profile** (Ajouter un profil d'accès)



3. Entrez le nom du profil dans la zone de texte **Access Profile Name** (Nom du profil d'accès).

4. Complétez les champs suivants :

Management Method (Méthode de gestion) : effectuez une sélection dans la liste déroulante. La stratégie appliquée est limitée par la méthode de gestion choisie.

Interface : si la stratégie doit utiliser une règle basée sur l'interface, cochez la case correspondant à cette dernière. Il peut s'agir d'une interface physique, d'un LAG ou d'un VLAN.

Source IP Address (Adresse IP source) : cochez cette case si la stratégie doit utiliser une règle basée sur l'adresse IP du client à l'origine du trafic de gestion. Indiquez le masque et l'adresse IP source dans les champs prévus à cet effet. Le masque peut être indiqué dans les deux formats suivants : notation IP à points (exemple : 255.255.255.0) ou longueur du préfixe (exemple : 32).

Action : choisissez l'action à exécuter lorsque les conditions définies dans les règles ci-dessus sont réunies. Utilisez la liste déroulante pour autoriser (Permit) ou refuser (Deny) l'accès.

Rule Priority (Priorité des règles) : définit la priorité des règles. Ces dernières sont vérifiées par rapport à la demande entrante, dans l'ordre de priorité croissant. Lorsqu'une correspondance est identifiée, l'action est effectuée et les règles de priorité inférieure ne sont pas exécutées. Par exemple, si vous configurez l'adresse IP source 10.10.10.10 sur Permit (Autoriser) en priorité 1 et sur Deny (Refuser) en priorité 2, l'accès est autorisé si le profil est actif, et la seconde règle est ignorée.

5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau profil d'accès est ajouté et le périphérique est mis à jour.

Activation d'un profil d'accès

1. Affichez la page **Access Profile** (Profil d'accès).
2. Cochez la case **Set Access Profile Active** (Définir le profil d'accès comme actif).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le profil d'accès est activé pour le périphérique.

Ajout de règles à un profil d'accès

1. Affichez la page **Access Profile** (Profil d'accès).

Le champ **Access Profile** (Profil d'accès) affiche le profil auquel les règles sont ajoutées lorsque la page **Add An Access Profile Rule** (Ajouter une règle à un profil d'accès) est ouverte.

2. Cliquez sur **Add Rule** (Ajouter une règle).

La page **Add An Access Profile Rule** (Ajouter une règle à un profil d'accès) s'affiche.

Figure 6-39. Page **Add An Access Profile Rule** (Ajouter une règle à un profil d'accès)

3. Complétez les champs de la boîte de dialogue.

Management Method (Méthode de gestion) : effectuez une sélection dans la liste déroulante. La stratégie appliquée est limitée par la méthode de gestion choisie.

Interface : si la stratégie doit utiliser une règle basée sur l'interface, cochez la case correspondant à cette dernière. Il peut s'agir d'une interface physique, d'un LAG ou d'un VLAN.

Source IP (Adresse IP source) : cochez cette case si la stratégie doit utiliser une règle basée sur l'adresse IP du client à l'origine du trafic de gestion. Indiquez le masque et l'adresse IP source dans les zones de texte prévues à cet effet. Le masque peut être indiqué de deux façons : notation IP à points (exemple : 255.255.255.0) ou longueur du préfixe (exemple : 32).

Action : choisissez l'action à exécuter lorsque les conditions définies dans les règles ci-dessus sont réunies. Utilisez la liste déroulante pour autoriser (Permit) ou refuser (Deny) l'accès.

Rule Priority (Priorité des règles) : définit la priorité des règles. Ces dernières sont vérifiées par rapport à la demande entrante, dans l'ordre de priorité

croissant. Lorsqu'une correspondance est identifiée, l'action est effectuée et les règles de priorité inférieure ne sont pas exécutées. Par exemple, si vous configurez l'adresse IP source 10.10.10.10 sur Permit (Autoriser) en priorité 1 et sur Deny (Refuser) en priorité 2, l'accès est autorisé si le profil est actif, et la seconde règle est ignorée.

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La règle est ajoutée au profil d'accès et le périphérique est mis à jour.

Suppression d'une règle

1. Affichez la page **Access Profile** (Profil d'accès).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Profile Rules Table** (Table des règles de profil).
3. Sélectionnez une règle.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La règle est supprimée et le périphérique est mis à jour.

Définition des profils d'accès à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

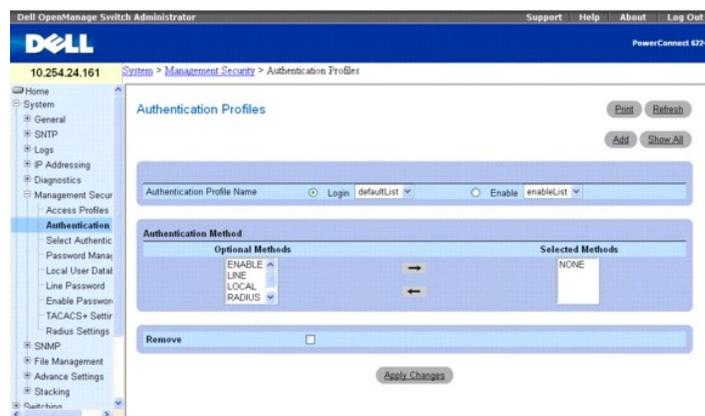
- 1 Management ACL Commands (Commandes de gestion ACL)

Profils d'authentification

L'authentification des utilisateurs est effectuée localement et sur un serveur externe. La page **Authentication Profiles** (Profils d'authentification) permet de sélectionner la méthode d'authentification des utilisateurs sur le périphérique.

Pour afficher cette page, cliquez sur **System** (Système) → **Management Security** (Gestion de la sécurité) → **Authentication Profiles** (Profils d'authentification) dans l'arborescence.

Figure 6-40. Page Authentication Profiles (Profils d'authentification)



Cette page contient les champs suivants :

Authentication Profile Name (Nom du profil d'authentification)

Affiche les listes auxquelles les profils d'authentification définis par l'utilisateur seront ajoutés. Utilisez les boutons radio pour appliquer le profil d'authentification à utiliser pour contrôler les paramètres de connexion ou d'activation relatifs au fonctionnement du commutateur. Vous pouvez sélectionner l'une des deux listes suivantes :

Login (Connexion) : permet de vous connecter au commutateur. Les options disponibles sont **defaultList**, **networkList** et tout profil d'authentification de connexion défini par l'utilisateur.

Enable (Activer) : active le mode privilège.

Authentication Method (Méthode d'authentification)

Optional Methods (Méthodes facultatives) : méthodes d'authentification des utilisateurs. Les options disponibles sont les suivantes :

None (Aucune) : aucune authentification des utilisateurs n'est effectuée.

Local (Locale) : l'authentification des utilisateurs est effectuée au niveau du périphérique, qui vérifie le nom d'utilisateur et le mot de passe.

RADIUS : l'authentification des utilisateurs est effectuée au niveau du serveur RADIUS. Pour plus d'informations sur les serveurs RADIUS, voir [Paramètres RADIUS](#).

TACACS+ : l'authentification des utilisateurs est effectuée au niveau du serveur TACACS+. Pour plus d'informations sur les serveurs TACACS+, voir [Paramètres TACACS+](#).

Line (Ligne) : le mot de passe de ligne est utilisé pour l'authentification des utilisateurs.

Enable (Activation) : le mot de passe d'activation est utilisé pour l'authentification.

REMARQUE : L'authentification des utilisateurs est effectuée selon l'ordre des méthodes sélectionnées. Si une erreur survient au cours de l'authentification, la méthode sélectionnée suivante est utilisée. Par exemple, si les options sélectionnées sont **Local**, puis **RADIUS**, l'utilisateur est d'abord authentifié localement puis via un serveur **RADIUS** externe.

Selected Methods (Méthodes sélectionnées) : méthode d'authentification sélectionnée.

Remove (Supprimer) : supprime le profil sélectionné.

Ajout d'un profil d'authentification

1. Affichez la page **Authentication Profiles** (Profils d'authentification).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add Authentication Profile** (Ajouter un profil d'authentification).

Figure 6-41. Page Add Authentication Profile (Ajouter un profil d'authentification)

3. Entrez le nom du profil (1 à 12 caractères) dans le champ **Profile Name** (Nom du profil).

REMARQUE : Le nom du profil ne doit contenir aucun espace.

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Un profil est créé. Vous pouvez activer un profil d'authentification à l'aide de la page **Web System** (Système) → **Management Security** (Gestion de la sécurité) → **Select Authentication** (Sélectionner une authentification).

Modification de profils d'authentification

1. Affichez la page **Authentication Profiles** (Profils d'authentification).
2. Sélectionnez un élément dans la liste **Authentication Profile Name** (Nom du profil d'authentification).
3. Utilisez les flèches pour effectuer une ou plusieurs sélections dans le champ **Optional Methods** (Méthodes facultatives).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le profil d'authentification utilisateur est mis à jour sur le périphérique.

Suppression d'une entrée de profil d'authentification

1. Affichez la page **Authentication Profiles** (Profils d'authentification).
2. Cliquez sur **Show All** (Afficher tout).

La page **Authentication Profiles** (Profils d'authentification) s'affiche.

Figure 6-42. Page Authentication Profiles Table (Table des profils d'authentification)

Authentication Profiles Table Print Refresh

Login Authentication Profiles		Methods	Remove
1	defaultList	NONE,LINE	<input type="checkbox"/> Edit

Enable Authentication Profiles		Methods	Remove
1	enableList	NONE	<input type="checkbox"/> Edit
2	R&D	LINE,NONE	<input type="checkbox"/> Edit

Apply Changes Back

3. Cochez la case **Remove** (Supprimer) en regard du profil à supprimer.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est supprimée.

Configuration d'un profil d'authentification à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 AAA Commands (Commandes AAA)

Sélection d'une authentification

Une fois définis, les profils d'authentification peuvent être appliqués à des méthodes d'accès de gestion. Par exemple, les utilisateurs de la console peuvent être authentifiés par la liste de profils d'authentification 1 alors que les utilisateurs Telnet sont authentifiés par la liste de profils d'authentification 2.

Pour afficher la page **Select Authentication** (Sélectionner une authentification), cliquez sur **System** (Système) → **Management Security** (Gestion de la sécurité) → **Select Authentication** (Sélectionner une authentification) dans l'arborescence.

Figure 6-43. Page Select Authentication (Sélectionner une authentification)

The screenshot shows the 'Select Authentication' page in the Dell OpenManage Switch Administrator. The page has a navigation tree on the left and a main content area. The main content area is titled 'Select Authentication' and contains several sections:

- Console:** Login: defaultList, Enable: enableList
- Telnet:** Login: networkList, Enable: enableList
- Secure Telnet (SSH):** Login: networkList, Enable: enableList
- Secure HTTP:** Optional Methods: ENABLE, LINE, NONE, RADIUS; Selected Methods: LOCAL
- HTTP:** Optional Methods: ENABLE, LINE, NONE, RADIUS; Selected Methods: LOCAL

Cette page contient les champs suivants :

Console : profils utilisés pour authentifier les utilisateurs de la console.

Telnet : profils utilisés pour authentifier les utilisateurs Telnet.

Secure Telnet (SSH) (Telnet sécurisé [SSH]) : profils utilisés pour authentifier les utilisateurs du shell sécurisé (SSH). Le protocole SSH permet aux clients d'établir une connexion distante sécurisée et cryptée avec un périphérique.

Secure HTTP/HTTP (HTTP sécurisé et HTTP) : méthode d'authentification utilisée pour les accès HTTP et HTTP sécurisés. Ce champ peut prendre les valeurs suivantes :

None (Aucune) : aucune méthode d'authentification n'est utilisée pour l'accès.

Local : l'authentification est effectuée en local.

RADIUS : l'authentification est effectuée au niveau du serveur RADIUS.

TACACS+ : l'authentification est effectuée au niveau du serveur TACACS+.

Local, None (Locale, aucune) : l'authentification est d'abord effectuée en local.

RADIUS, None (RADIUS, aucune) : l'authentification est d'abord effectuée au niveau du serveur RADIUS. Si celle-ci ne peut pas être vérifiée, aucune autre méthode d'authentification n'est utilisée. Une authentification n'est possible que si le serveur distant permettant d'identifier l'utilisateur peut être contacté. S'il peut l'être, la réponse qu'il envoie est toujours prise en compte.

TACACS+, None (TACACS+, aucune) : l'authentification est d'abord effectuée au niveau du serveur TACACS+. Si celle-ci ne peut pas être vérifiée, aucune autre méthode d'authentification n'est utilisée. Une authentification n'est possible que si le serveur distant permettant d'identifier l'utilisateur peut être contacté. S'il peut l'être, la réponse qu'il envoie est toujours prise en compte.

Local, RADIUS (Locale, RADIUS) : l'authentification est d'abord effectuée en local. Si cette opération n'aboutit pas, le serveur RADIUS tente d'authentifier la méthode de gestion. Si cette deuxième opération n'aboutit pas, la session est bloquée.

Local, TACACS+ (Locale, TACACS+) : l'authentification est d'abord effectuée en local. Si cette opération n'aboutit pas, le serveur TACACS+ tente d'authentifier la méthode de gestion. Si cette deuxième opération n'aboutit pas, la session est bloquée.

RADIUS, Local (RADIUS, locale) : l'authentification est d'abord effectuée au niveau du serveur RADIUS. Si cette opération n'aboutit pas, la session est authentifiée en local. Si cette deuxième opération n'aboutit pas, la session est bloquée.

TACACS+, Local (TACACS+, locale) : l'authentification est d'abord effectuée au niveau du serveur TACACS+. Si cette opération n'aboutit pas, la session est authentifiée en local. Si cette deuxième opération n'aboutit pas, la session est bloquée.

Local, RADIUS, None (Locale, RADIUS, aucune) : l'authentification est d'abord effectuée en local. Si cette opération n'aboutit pas, le serveur RADIUS tente d'authentifier la méthode de gestion. Si cette deuxième opération n'aboutit pas, la session est autorisée.

RADIUS, Local, None (RADIUS, locale, aucune) : l'authentification est d'abord effectuée au niveau du serveur RADIUS. Si cette opération n'aboutit pas, la session est authentifiée en local. Si cette deuxième opération n'aboutit pas, la session est autorisée.

Local, TACACS+, None (Locale, TACACS+, aucune) : l'authentification est d'abord effectuée en local. Si cette opération n'aboutit pas, le serveur TACACS+ tente d'authentifier la méthode de gestion. Si cette deuxième opération n'aboutit pas, la session est autorisée.

TACACS+, Local, None (TACACS+, locale, aucune) : l'authentification est d'abord effectuée au niveau du serveur TACACS+. Si cette opération n'aboutit pas, la session est authentifiée en local. Si cette deuxième opération n'aboutit pas, la session est autorisée.

Application d'une liste de méthodes d'authentification à des sessions de console

1. Affichez la page **Select Authentication** (Sélectionner une authentification).
2. Sélectionnez un profil d'authentification dans le champ **Console**.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les sessions de la console sont associées à une liste de méthodes d'authentification.

Application d'un profil d'authentification à des sessions Telnet

1. Affichez la page **Select Authentication** (Sélectionner une authentification).
2. Sélectionnez un profil d'authentification dans le champ **Telnet**.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les sessions de la console sont associées à des profils d'authentification.

Application d'un profil d'authentification à des sessions Telnet sécurisées (SSH)

1. Affichez la page **Select Authentication** (Sélectionner une authentification).
2. Sélectionnez un profil d'authentification dans le champ **Secure Telnet (SSH)** (Telnet sécurisé [SSH]).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les sessions Telnet sécurisées (SSH) sont associées à des profils d'authentification.

Attribution d'une séquence d'authentification à des sessions HTTP

1. Affichez la page **Select Authentication** (Sélectionner une authentification).
2. Sous **HTTP**, sélectionnez une méthode d'authentification dans le champ **Optional Methods** (Méthodes facultatives) et cliquez sur le bouton représentant une flèche vers la droite.

La méthode d'authentification sélectionnée passe dans le champ **Selected Methods** (Méthodes sélectionnées).
3. Répétez l'opération jusqu'à ce que la séquence d'authentification souhaitée s'affiche dans le champ **Selected Methods** (Méthodes sélectionnées).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les sessions HTTP sont associées à la séquence d'authentification.

Affectation de méthodes d'accès, de profils ou de séquences d'authentification à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 AAA Commands (Commandes AAA)

Affectation d'une séquence d'authentification à des sessions HTTP sécurisées

1. Affichez la page **Select Authentication** (Sélectionner une authentification).
2. Sous **Secure HTTP** (HTTP sécurisé), sélectionnez une méthode d'authentification dans le champ **Optional Methods** (Méthodes facultatives) et cliquez sur le bouton représentant une flèche vers la droite.

La méthode d'authentification sélectionnée passe dans le champ **Selected Methods** (Méthodes sélectionnées).
3. Répétez l'opération jusqu'à ce que la séquence d'authentification souhaitée s'affiche dans le champ **Selected Methods** (Méthodes sélectionnées).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les sessions HTTP sécurisées sont associées à la séquence d'authentification.

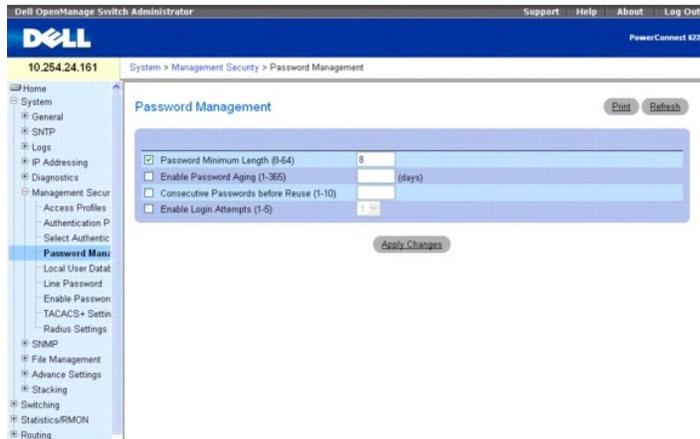
Gestion des mots de passe

La gestion des mots de passe permet d'améliorer la sécurité du réseau et de bénéficier d'un contrôle amélioré des mots de passe. Les mots de passe d'accès SSH, Telnet, HTTP, HTTPS et SNMP sont associés aux fonctions de sécurité suivantes :

- 1 Définition de la longueur minimum d'un mot de passe
- 1 Expiration d'un mot de passe
- 1 Prévention d'une réutilisation trop fréquente des mêmes mots de passe
- 1 Blocage des utilisateurs après plusieurs tentatives de connexion infructueuses

Pour afficher la page appropriée, cliquez sur **System** (Système) → **Management Security** (Gestion de la sécurité) → **Password Management** (Gestion des mots de passe) dans l'arborescence.

Figure 6-44. Page Password Management (Gestion des mots de passe)



Cette page contient les champs suivants :

Password Minimum Length (8-64) (Longueur minimale du mot de passe, 8-64) : lorsqu'elle est cochée, cette option indique le nombre minimum de caractères que le mot de passe doit contenir. Par exemple, l'administrateur peut indiquer que tous les mots de passe de ligne doivent contenir au moins 10 caractères.

Enable Password Aging (1-365) (Activer l'expiration du mot de passe, 1-365) : lorsqu'elle est cochée, cette option indique le délai qui s'écoule avant l'expiration du mot de passe. Les valeurs possibles sont comprises entre 1 et 365 jours. Cette fonction n'est opérationnelle que si l'horloge du commutateur est synchronisée avec un serveur SNTP. Pour plus d'informations, reportez-vous à la section "Clock Commands" (Commandes de synchronisation) du document "CLI Reference Guide" (Guide de référence CLI).

Consecutive Passwords Before Reuse (1-10) (Mots de passe consécutifs avant réutilisation, 1-10) : indique le nombre de modifications du mot de passe au terme duquel il est possible de réutiliser un ancien mot de passe. Les valeurs possibles sont comprises entre 1 et 10.

REMARQUE : L'utilisateur reçoit une notification lui demandant de changer le mot de passe avant son expiration. Les utilisateurs Web ne visualisent pas cette notification.

Enable Login Attempts(1-5) (Nombre de tentatives de connexion autorisées, 1-5) : lorsqu'elle est sélectionnée, cette option permet de bloquer un utilisateur après un certain nombre de tentatives de connexion infructueuses (mot de passe incorrect). Par exemple, si le nombre maximum de tentatives de connexion a été défini sur cinq et si l'utilisateur tente de se connecter cinq fois en utilisant un mot de passe non valide, le périphérique bloque cet utilisateur à la sixième tentative. Le compte de l'utilisateur doit alors être réactivé par un superutilisateur. Les valeurs admises sont comprises entre 1 et 5.

Définition des contraintes liées aux mots de passe

1. Affichez la page **Password Management** (Gestion des mots de passe).
2. Complétez les champs appropriés.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les contraintes liées au mot de passe sont définies et le périphérique est mis à jour.

Définition des contraintes liées aux mots de passe à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

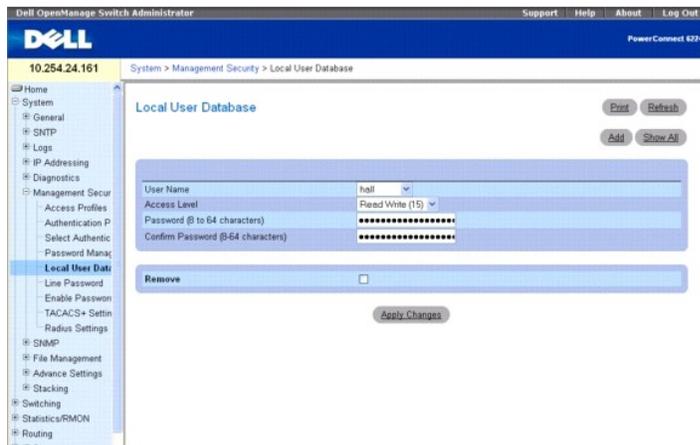
- 1 Password Management Commands (Commandes de gestion des mots de passe)

Base de données utilisateurs locale

La page **Local User Database** (Base de données utilisateurs locale) permet de définir les mots de passe et les droits d'accès des utilisateurs, ainsi que de réactiver les comptes des utilisateurs ayant été suspendus.

Pour afficher cette page, cliquez sur **System** (Système) → **Management Security** (Gestion de la sécurité) → **Local User Database** (Base de données utilisateurs locale) dans l'arborescence.

Figure 6-45. Page Local User Database (Base de données utilisateurs locale)



Cette page contient les champs suivants :

User Name (Nom d'utilisateur) : liste des utilisateurs.

Access Level (Niveau d'accès) : niveau d'accès des utilisateurs. Le niveau d'accès le plus bas est **1 (lecture seule)** et le plus élevé est **15 (lecture/écriture)**. Pour suspendre l'accès d'un utilisateur, définissez le niveau 0. Cette opération ne peut être effectuée que par un utilisateur possédant le niveau d'accès 15.

Password (8-64 Characters) (Mot de passe, 8-64 caractères) : mot de passe défini par l'utilisateur.

Confirm Password (Confirmer le mot de passe) : permet de confirmer le mot de passe défini par l'utilisateur.

Remove (Supprimer) : lorsque cette option est sélectionnée, elle permet de supprimer des utilisateurs de la base de données utilisateurs locale.

Attribution de droits d'accès à un utilisateur

1. Affichez la page **Local User Database** (Base de données utilisateurs locale).
2. Sélectionnez un utilisateur dans le champ **User Name** (Nom d'utilisateur).
3. Complétez les champs avec les valeurs appropriées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les droits d'accès et les mots de passe de l'utilisateur sont définis et le périphérique est mis à jour.

Ajout d'un utilisateur à la base de données utilisateurs locale

1. Affichez la page **Local User Database** (Base de données utilisateurs locale).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add User** (Ajouter un utilisateur).

La page correspondante s'affiche.

Figure 6-46. Page Add a New User (Ajouter un nouvel utilisateur)



3. Complétez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouvel utilisateur est défini et le périphérique est mis à jour.

REMARQUE : Vous pouvez définir jusqu'à 8 utilisateurs locaux sur le périphérique

Affichage des utilisateurs de la base de données locale

1. Affichez la page **Local User Database** (Base de données utilisateurs locale).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Local User Table** (Table des utilisateurs locaux).

Tous les membres de la base de données utilisateurs locale sont affichés.

Figure 6-47. Page Local User Table (Table des utilisateurs locaux)



	User Name	Access Level	Remove
1	anyviewer	Read Write	<input type="checkbox"/> Edit
2	helpviewer	Read Write	<input type="checkbox"/> Edit
3	tail	Read Write	<input type="checkbox"/> Edit

Suppression d'utilisateurs de la base de données utilisateurs locale

1. Affichez la page **Local User Database** (Base de données utilisateurs locale).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Local User Table** (Table des utilisateurs locaux).
3. Sélectionnez un nom d'utilisateur.
4. Cliquez sur **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'utilisateur est supprimé et le périphérique est mis à jour.

Affectation d'utilisateurs à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

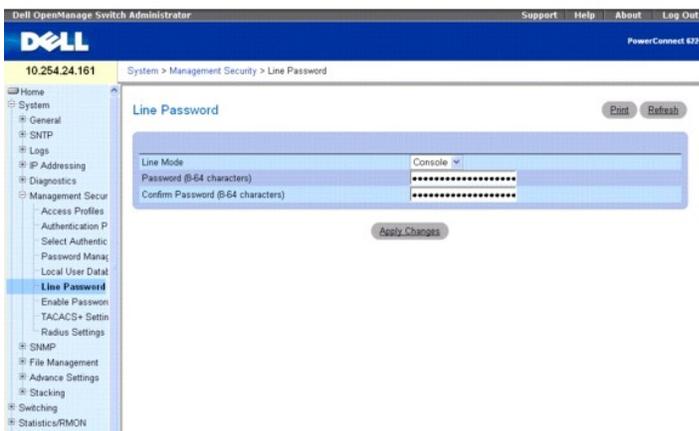
- 1 AAA Commands (Commandes AAA)

Mots de passe de ligne

La page **Line Password** (Mot de passe de ligne) permet de définir les mots de passe de ligne associés aux méthodes de gestion.

Pour afficher cette page, cliquez sur **System** (Système) → **Management Security** (Gestion de la sécurité) → **Line Password** (Mot de passe de ligne) dans l'arborescence.

Figure 6-48. Page Line Password (Mot de passe de ligne)



Dell OpenManage Switch Administrator | Support | Help | About | Log Out | PowerConnect 6224

10.254.24.161 | System > Management Security > Line Password

Line Password

Line Mode: Console

Password (8-64 characters): [masked]

Confirm Password (8-64 characters): [masked]

Apply Changes

Cette page contient les champs suivants :

Line Mode (Mode de la ligne) : le menu déroulant indique si l'accès au périphérique est effectué au moyen d'une console, d'une session Telnet standard ou d'une session Telnet sécurisée (SSH).

Line Password (8-64 characters) (Mot de passe de ligne, 8-64 caractères) : mot de passe de ligne permettant d'accéder au périphérique au moyen d'une console, d'une session Telnet standard ou d'une session Telnet sécurisée. Le mot de passe s'affiche sous la forme d'une chaîne d'astérisques (*****).

Confirm Password (8-64 characters) (Confirmer le mot de passe, 8-64 caractères) : confirme le nouveau mot de passe de ligne. Le mot de passe s'affiche sous la forme d'une chaîne d'astérisques (*****).

Définition de mots de passe de ligne

1. Affichez la page **Line Password** (Mot de passe de ligne).
2. Indiquez si l'accès au périphérique est effectué au moyen d'une console, d'une session Telnet standard ou d'une session Telnet sécurisée (SSH).
3. Renseignez le champ **Line Password** (Mot de passe de ligne) correspondant au type de session que vous utilisez pour vous connecter au périphérique.
4. Confirmez le mot de passe de ligne.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mot de passe de ligne correspondant au type de session utilisé est défini et le périphérique est mis à jour.

Attribution de mots de passe de ligne à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

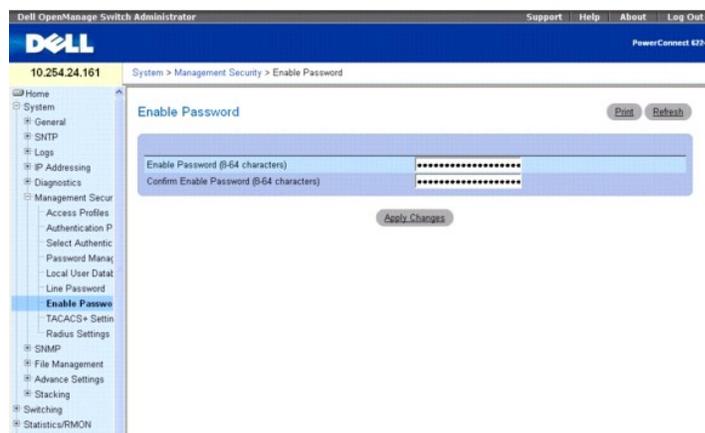
- 1 AAA Commands (Commandes AAA)

Mot de passe d'activation

La page **Enable Password** (Mot de passe d'activation) permet de définir un mot de passe local et de contrôler l'accès des utilisateurs disposant de droits normaux ou privilégiés.

Pour afficher cette page, cliquez sur **System** (Système) → **Management Security** (Gestion de la sécurité) → **Enable Password** (Mot de passe d'activation) dans l'arborescence.

Figure 6-49. Page Enable Password (Mot de passe d'activation)



Cette page contient les champs suivants :

Enable Password (8-64 characters) (Mot de passe d'activation, 8-64 caractères) : mot de passe utilisé pour contrôler l'accès des utilisateurs disposant de droits normaux ou privilégiés. Le mot de passe s'affiche sous la forme d'une chaîne d'astérisques (*****).

Confirm Enable Password (Confirmer le mot de passe d'activation) : permet de confirmer le nouveau mot de passe d'activation. Le mot de passe s'affiche sous la forme d'une chaîne d'astérisques (*****).

Définition de mots de passe d'activation

1. Affichez la page **Enable Password** (Mot de passe d'activation).
2. Indiquez le mot de passe d'activation.
3. Confirmez le mot de passe d'activation.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mot de passe d'activation est défini.

Attribution de mots de passe d'activation à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 AAA Commands (Commandes AAA)

Paramètres TACACS+

Le périphérique prend en charge le client TACACS+ (Terminal Access Controller Access Control System). Ce dernier permet de centraliser et de sécuriser la vérification des utilisateurs qui accèdent au périphérique.

TACACS+ permet de disposer d'un système de gestion centralisée des utilisateurs tout en continuant à utiliser le mécanisme RADIUS et les autres processus d'authentification. TACACS+ fournit les services suivants :

- 1 **Authentication** (Authentification) : permet une authentification pendant la connexion et par le biais des noms d'utilisateur et des mots de passe définis par les utilisateurs.
- 1 **Authorization** (Autorisation) : effectuée lors de la connexion. Une fois l'authentification terminée, une session d'autorisation est ouverte pour le nom d'utilisateur authentifié. Le serveur TACACS+ vérifie les droits d'accès de l'utilisateur.

Le protocole TACACS+ sécurise le réseau grâce à des échanges de protocole cryptés entre le périphérique et le serveur TACACS+.

La page **TACACS+ Settings** (Paramètres TACACS+) contient les paramètres définis par l'utilisateur, ainsi que les paramètres TACACS+ par défaut correspondant au port de gestion intrabande.

Pour afficher cette page, cliquez sur **System** (Système) → **Management Security** (Gestion de la sécurité) → **TACACS+** dans l'arborescence.

Figure 6-50. Page TACACS+ Settings (Paramètres TACACS+)

The screenshot shows the Dell OpenManage Switch Administrator interface. The top navigation bar includes 'Support', 'Help', 'About', and 'Log Out'. The main content area is titled 'TACACS+ Settings' and features a navigation menu on the left. The 'TACACS+ Server' section includes fields for Host Name/IP Address, Priority (0-65535), Authentication Port (0-65535), Key String (0-128 characters), and Timeout for Reply (1-30). The 'Default Parameters' section includes fields for Key String (0-128 characters) and Timeout for Reply (1-30). There are 'Print', 'Refresh', 'Add', and 'Show All' buttons at the top right, and an 'Apply Changes' button at the bottom center.

Cette page contient les champs suivants :

Host Name / IP Address (Nom d'hôte/Adresse IP) : identifie le serveur TACACS+.

Priority (0-65535) (Priorité, 0-65535) : indique l'ordre d'utilisation des serveurs TACACS+. La valeur par défaut est de 0.

Authentication Port (0-65535) (Port d'authentification, 0-65535) : numéro du port utilisé par la session TACACS+. Le numéro de port par défaut est 49.

Key String (0-128 Characters) (Clé de cryptage, 0-128 caractères) : définit la clé utilisée pour l'authentification et le cryptage des communications TACACS+ entre le périphérique et le serveur TACACS+. Cette clé doit correspondre à la clé de cryptage utilisée sur le serveur TACACS+. Cochez **Use Default** (Utiliser la valeur par défaut) pour sélectionner la valeur par défaut.

Timeout for Reply (1-30) (Délai de réponse, 1-30 secondes) : délai qui s'écoule avant l'expiration de la connexion entre le périphérique et le serveur TACACS+. Les valeurs admises sont comprises entre 1 et 30 secondes. Cochez **Use Default** (Utiliser la valeur par défaut) pour sélectionner la valeur définie en

usine.

Status (État) : état de la connexion entre le périphérique et le serveur TACACS+. Les valeurs possibles sont les suivantes :

Connected (Connecté) : le périphérique est actuellement connecté au serveur TACACS+.

Not Connected (Non connecté) : le périphérique n'est pas connecté au serveur TACACS+ actuellement.

Les champs de la section Default Parameters (Paramètres par défaut) contiennent des valeurs qui sont automatiquement appliquées aux nouveaux serveurs TACACS+.

Key String (0-128 Characters) (Clé de cryptage, 0-128 caractères) : entrez la clé par défaut à utiliser pour l'authentification et le cryptage des communications TACACS+ entre le périphérique et le serveur TACACS+.

Timeout for Reply (1-30) (Délai de réponse, 1-30 secondes) : indiquez le délai qui doit s'écouler avant l'expiration de la connexion entre le périphérique et le serveur TACACS+.

Définition des paramètres TACACS+

1. Affichez la page **TACACS+ Settings** (Paramètres TACACS+).
 2. Complétez les champs avec les valeurs appropriées.
 3. Cliquez sur **Apply Changes** (Appliquer les modifications).
- Les paramètres TACACS+ sont mis à jour sur le périphérique.

Ajout d'un serveur TACACS+

1. Affichez la page **TACACS+ Settings** (Paramètres TACACS+).
2. Cliquez sur **Add** (Ajouter).

La page **Add TACACS+ Host** (Ajouter un hôte TACACS+) s'affiche.

Figure 6-51. Page **Add TACACS+ Host** (Ajouter un hôte TACACS+)

Add TACACS+ Host Print Refresh

Host Name/IP Address	10.240.13.45	(XXXX)
Priority (0-65535)	258	
Authentication Port (0-65535)	43	
Key String (0-128 characters)	*****	<input type="checkbox"/> Use Default
Timeout for Reply (1-30)	5	(sec) <input type="checkbox"/> Use Default

Apply Changes Back

3. Complétez les champs avec les valeurs appropriées.
 4. Cliquez sur **Apply Changes** (Appliquer les modifications).
- Le serveur TACACS+ est ajouté et le périphérique est mis à jour.

Affichage de la liste des serveurs TACACS+

1. Affichez la page **TACACS+ Settings** (Paramètres TACACS+).
2. Cliquez sur **Show All** (Afficher tout).

La page **TACACS+ Servers Table** (Table des serveurs TACACS+) s'affiche.

Figure 6-52. Page **TACACS+ Servers Table** (Table des serveurs TACACS+)

TACACS+ Servers Table Print Refresh

Host IP Address	Priority	Authentication Port	Timeout for Reply (sec)	Status	Remove
10.240.13.45	258	43	5	Not Connected	<input type="checkbox"/> Edit

Apply Changes Back

Suppression d'un serveur de la liste des serveurs TACACS+

1. Affichez la page **TACACS+ Settings** (Paramètres TACACS+).

2. Cliquez sur **Show All** (Afficher tout).

La page **TACACS+ Servers Table** (Table des serveurs TACACS+) s'affiche.

3. Sélectionnez une entrée dans la table.

4. Cochez la case **Remove** (Supprimer).

5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le serveur TACACS+ est supprimé et le périphérique est mis à jour.

Définition de serveurs TACACS+ à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 TACACS+ Commands (Commandes TACACS+)

Paramètres RADIUS

Un serveur RADIUS (Remote Authorization Dial-In User Service) fournit un niveau de sécurité réseau supplémentaire. Il gère une base de données utilisateurs contenant des données d'authentification pour chaque utilisateur. Il fournit en outre une méthode d'authentification centralisée pour :

- 1 les accès Telnet,
- 1 les accès Web,
- 1 les accès au commutateur effectués à partir de la console,
- 1 le port de contrôle d'accès (802.1x).

La page **RADIUS Settings** (Paramètres RADIUS) contient les paramètres RADIUS par défaut et ceux définis par l'utilisateur.

Pour afficher cette page, cliquez sur **System Management** (Gestion du système) → **Security** (Sécurité) → **RADIUS Settings** (Paramètres RADIUS) dans l'arborescence.

Figure 6-53. Page **RADIUS Settings** (Paramètres RADIUS)

RADIUS Server	
IP Address	10.24.100.18
Priority (0-65535)	256
Authentication Port (0-65535)	1043
Number of Retries (1-10)	4 <input type="checkbox"/> Use Default
Timeout for Reply (1-30)	20 (sec) <input type="checkbox"/> Use Default
Deadtime (0-2000)	500 (min) <input type="checkbox"/> Use Default
Key String (0-128 characters)	drowyek <input type="checkbox"/> Use Default
Source IP Address	10.240.1.0? (XXXX) <input type="checkbox"/> Use Default
Usage Type	Login

Default Parameters	
Default Retries (1-10)	3
Default Timeout for Reply (1-30)	20 (sec)
Default Deadtime (0-2000)	1000 (min)
Default Key String (0-128 characters)	key
Source IP Address	202.241.43 (XXXX)

Cette page contient les champs suivants :

IP Address (Adresse IP) : adresse IP du serveur RADIUS.

Priority (0-65535) (Priorité, 0-65535) : indique la priorité du port. Les valeurs admises sont comprises entre 0 et 65535.

Authentication Port (0-65535) (Port d'authentification, 0-65535) : identifie le port utilisé pour vérifier l'authentification du serveur RADIUS.

Number of Retries (1-10) (Nombre de tentatives, 1-10) : indique le nombre de demandes de transmission envoyées au serveur RADIUS avant échec. Les

valeurs possibles vont de 1 à 10. La valeur par défaut est de 3. Si aucune valeur spécifique n'est définie pour l'hôte, la valeur globale s'applique à tous les hôtes. Cochez **Use Default** (Utiliser la valeur par défaut) pour sélectionner la valeur par défaut définie par l'utilisateur.

Timeout for Reply (1-30) (Délai de réponse, 1-30) : délai (en secondes) pendant lequel le périphérique attend une réponse du serveur RADIUS avant expiration. Les valeurs possibles vont de 1 à 30. La valeur par défaut est de 3. Si aucune valeur spécifique n'est définie pour l'hôte, la valeur globale s'applique à tous les hôtes. Cochez **Use Default** (Utiliser la valeur par défaut) pour sélectionner la valeur par défaut définie par l'utilisateur.

Deadtime (0-2000) (Délai d'inactivité, 0-2000) : délai pendant lequel un serveur RADIUS est ignoré lors des demandes de service. Les valeurs possibles vont de 0 à 2000. Si aucune valeur spécifique n'est définie pour l'hôte, la valeur globale s'applique à tous les hôtes. Cochez **Use Default** (Utiliser la valeur par défaut) pour sélectionner la valeur par défaut définie par l'utilisateur.

Key String (0-128 Characters) (Clé de cryptage, 0-128 caractères) : clé utilisée pour l'authentification et le cryptage des communications RADIUS entre le périphérique et le serveur RADIUS. Cette clé doit correspondre au cryptage RADIUS. Si aucune valeur spécifique n'est définie pour l'hôte, la valeur globale s'applique. Cochez **Use Default** (Utiliser la valeur par défaut) pour sélectionner la valeur par défaut définie par l'utilisateur.

Source IP Address (Adresse IP source) : adresse IP du périphérique qui accède au serveur RADIUS. Cochez **Use Default** (Utiliser la valeur par défaut) pour sélectionner la valeur par défaut définie par l'utilisateur.

Usage Type (Type d'utilisation) : liste déroulante permettant de sélectionner le type d'utilisation du serveur RADIUS.

 **REMARQUE** : Les paramètres par défaut de cette page sont définis par l'utilisateur.

Default Retries (1-10) (Tentatives par défaut, 1-10) : indique le nombre par défaut de requêtes transmises au serveur RADIUS avant échec.

Default Timeout for Reply (1-30) (Délai de réponse par défaut, 1-30) : délai par défaut (en secondes) pendant lequel le périphérique attend une réponse du serveur RADIUS avant échec. Les valeurs admises vont de 1 à 30.

Default Deadtime (0-2000) (Délai d'inactivité par défaut, 0-2000) : délai par défaut (en minutes) pendant lequel un serveur RADIUS est ignoré lors des demandes de service. Les valeurs admises vont de 0 à 2000.

Default Key String (0-128 Characters) (Clé de cryptage par défaut, 0-128 caractères) : clé par défaut utilisée pour l'authentification et le cryptage des communications RADIUS entre le périphérique et le serveur RADIUS. Cette clé doit correspondre au cryptage RADIUS.

Source IP Address (Adresse IP source) : adresse IP par défaut du périphérique qui accède au serveur RADIUS.

Ajout d'un serveur RADIUS

1. Affichez la page **RADIUS Settings** (Paramètres RADIUS).
2. Cliquez sur **Add** (Ajouter).

La page **Add RADIUS Server** (Ajouter un serveur RADIUS) s'affiche.

Figure 6-54. Page Add RADIUS Server (Ajouter un serveur RADIUS)



3. Complétez les champs de la boîte de dialogue.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau serveur RADIUS est ajouté et le périphérique est mis à jour.

Définition des paramètres RADIUS

1. Affichez la page **RADIUS Settings** (Paramètres RADIUS).
2. Complétez les champs de la boîte de dialogue.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres RADIUS sont mis à jour sur le périphérique.

Modification des paramètres des serveurs RADIUS

1. Affichez la page **RADIUS Settings** (Paramètres RADIUS).
2. Cliquez sur **Show All** (Afficher tout).

La page **RADIUS Servers Table** (Table des serveurs RADIUS) s'affiche.

Figure 6-55. Page RADIUS Servers Table (Table des serveurs RADIUS)

#	IP Address	Priority	Authentication Port	Number of Retries	Timeout For Reply (sec)	Deadtime (min)	Source IP Address	Usage Type	Remove
1	10.240.10.13	2	23	45	56	3	10.240.13.45	Login	<input type="checkbox"/> Edit
2	10.240.10.40	4	26	34	63	2	10.240.13.56	Login	<input type="checkbox"/> Edit
3	10.240.10.14	2	23	43	57	1	10.240.13.45	Login	<input type="checkbox"/> Edit

3. Cliquez sur le lien **Edit** (Modifier) correspondant à l'entrée sélectionnée.
4. À partir de la page **RADIUS Settings** (Paramètres RADIUS), modifiez les paramètres correspondant au serveur RADIUS.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des serveurs RADIUS sont modifiés et le périphérique est mis à jour.

Suppression d'un serveur de la liste des serveurs RADIUS

1. Affichez la page **RADIUS Settings** (Paramètres RADIUS).
2. Cliquez sur **Show All** (Afficher tout).
3. Sélectionnez un serveur RADIUS et cochez **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le serveur RADIUS est supprimé de la liste.

Définition des serveurs RADIUS à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

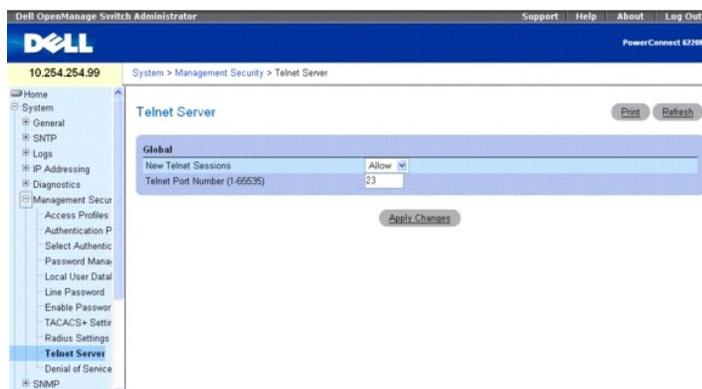
- 1 RADIUS Commands (Commandes RADIUS)

Serveur Telnet

La page **Telnet Server** (Serveur Telnet) permet d'activer et de désactiver le service Telnet sur le commutateur, ou bien de modifier le port Telnet.

Pour afficher cette page, cliquez sur **System** (Système) → **Management Security** (Gestion de la sécurité) → **Telnet Server** (Serveur Telnet).

Figure 6-56. Page Telnet Server (Serveur Telnet)



Cette page contient les champs suivants :

New Telnet Sessions (Nouvelles sessions Telnet) : contrôle le mode d'administration des sessions Telnet entrantes. Si vous définissez ce mode sur Block (Bloquer), les nouvelles sessions Telnet ne sont pas autorisées, mais les sessions existantes ne sont pas interrompues. La valeur par défaut est Allow (Autoriser).

Telnet Port Number (Numéro de port Telnet) : numéro de port à utiliser pour le lancement de la session Telnet. Ce port sera utilisé pour la nouvelle session Telnet entrante. Si vous avez modifié le port du serveur Telnet, seules les nouvelles sessions Telnet entrantes utiliseront ce nouveau port. Les sessions Telnet existantes ne sont pas affectées.

Modification des paramètres du serveur Telnet

1. Affichez la page **Telnet Server Configuration** (Configuration du serveur Telnet).
2. Complétez les champs appropriés.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont enregistrés et le périphérique est mis à jour.

Configuration du serveur Telnet à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

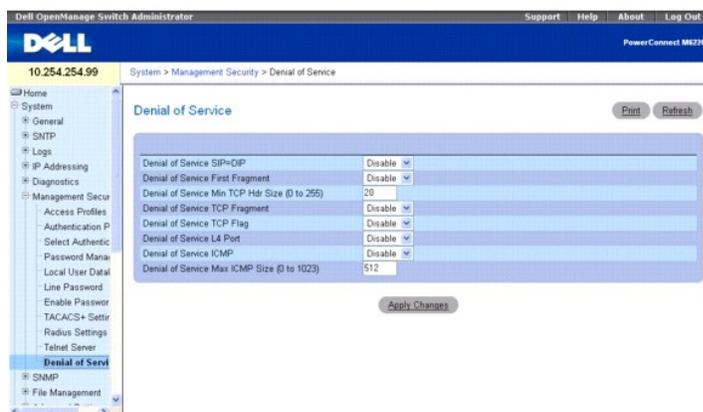
- 1 Telnet Server Commands (Commandes relatives au serveur Telnet)

Refus de service

Le terme "refus de service" désigne des attaques consistant à exploiter différentes failles afin d'interrompre les services fournis par un système hôte ou de provoquer une instabilité du réseau. La page **Denial of Service** (Refus de service) permet de configurer les paramètres de manière à prévenir ce type d'attaques.

Pour afficher cette page, cliquez sur **System** (Système) → **Management Security** (Gestion de la sécurité) → **Denial of Service** (Refus de service) dans l'arborescence.

Figure 6-57. Page Denial of Service (Refus de service)



Cette page contient les champs suivants :

Denial of Service SIP=DIP (Refus de service - IP source égale à IP cible) : lorsque cette fonction de prévention est activée, le commutateur rejette les paquets dont les adresses IP source et cible sont identiques.

Denial of Service First Fragment (Refus de service - Premier fragment) : lorsque cette fonction de prévention est activée, le commutateur rejette les paquets dont l'en-tête TCP est d'une taille inférieure à la limite minimale définie.

Denial of Service Min TCP Hdr Size (Refus de service - Taille minimale de l'en-tête TCP) : définit la taille minimale autorisée pour l'en-tête TCP. Si l'option de prévention Denial of Service First Fragment (Refus de service - Premier fragment) est activée, le commutateur rejette les paquets possédant un en-tête TCP dont la taille est inférieure à cette taille minimale.

Denial of Service TCP Fragment (Refus de service - Fragment TCP) : lorsque cette fonction de prévention est activée, le commutateur rejette les paquets pour lesquels le décalage de fragments IP est égal à 1.

Denial of Service TCP Flag (Refus de service - Indicateur TCP) : lorsque cette fonction de prévention est activée, le commutateur rejette les paquets répondant à l'une des conditions suivantes :

- 1 Indicateur TCP SYN défini et port TCP source inférieur à 1024
- 1 Indicateurs de contrôle TCP et numéro de séquence TCP définis sur 0
- 1 Indicateurs TCP FIN, URG et PSH définis et numéro de séquence TCP défini sur 0
- 1 Indicateurs TCP SYN et FIN tous deux définis

Denial of Service L4 Port (Refus de service - Port L4) : lorsque cette fonction de prévention est activée, le commutateur rejette les paquets dont les ports TCP/UDP source et cible sont identiques.

Denial of Service ICMP (Refus de service - ICMP) : lorsque cette fonction de prévention est activée, le commutateur rejette les paquets ICMP dont le type est défini sur ECHO_REQ (ping) et dont la taille est supérieure à la limite maximale autorisée.

Denial of Service Max ICMP Pkt Size (Refus de service - Taille maximale des paquets ICMP) : définit la taille maximale pouvant être utilisée pour les paquets ICMP. Si l'option de prévention Denial of Service ICMP (Refus de service - ICMP) est activée, le commutateur rejette les paquets ping ICMP dont la taille est supérieure à cette taille maximale.

Configuration des paramètres de protection contre les refus de service

1. Affichez la page **Denial of Service** (Refus de service).
2. Définissez les paramètres voulus.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le périphérique est mis à jour en fonction des nouveaux paramètres.

Configuration des paramètres de protection contre les refus de service à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Denial of Service Commands (Commandes de protection contre les refus de service)

Définition des paramètres SNMP

Le protocole SNMP (*Simple Network Management Protocol*) fournit une méthode pour la gestion des périphériques réseau. Le périphérique prend en charge les

versions 1, 2 et 3 de ce protocole.

REMARQUE : Par défaut, SNMPv2 est automatiquement activé sur le périphérique. Pour activer SNMPv3, un identifiant de moteur local doit être défini pour le périphérique. Par défaut, cet identifiant correspond à l'adresse MAC du commutateur. Cependant, lorsque ce dernier fonctionne en mode empilage, il est important de configurer l'ID du moteur local approprié pour la pile. En outre, l'ID défini doit être unique au sein du réseau. Cette opération est indispensable car l'ID du moteur par défaut d'une pile correspond à l'adresse MAC de l'unité principale, qui peut changer si cette dernière tombe en panne et est remplacée par une autre unité de la pile. Pour plus d'informations sur la configuration de l'ID de moteur local, voir [Paramètres globaux SNMP](#).

SNMP v1 et v2

L'agent SNMP gère une liste de variables qui sont utilisées pour gérer le commutateur. Ces variables sont définies dans la *base MIB* (Management Information Base, base d'informations de gestion). Celle-ci contient les variables gérées par l'agent SNMP, lequel définit le format de spécifications MIB et celui qui est utilisé pour accéder aux informations sur le réseau. Les droits d'accès à l'agent SNMP sont contrôlés par des chaînes d'accès.

SNMP v3

SNMP v3 applique également un contrôle d'accès et un nouveau mécanisme d'interruption aux PDU SNMPv1 et SNMPv2. Par ailleurs, le modèle de sécurité utilisateur (User Security Model ou USM) est défini pour SNMPv3. Il comprend les éléments suivants :

- 1 **Authentication** (Authentification) : garantit l'intégrité des données et authentifie leur origine.
- 1 **Privacy** (Confidentialité) : garantit la confidentialité des informations contenues dans les messages. Le mode CBC (Cipher-Block-Chaining, cryptage par chaînage de blocs) est utilisé pour le cryptage. Un message SNMP peut être protégé par la fonction d'authentification uniquement, ou bien à la fois par l'authentification et la confidentialité. Toutefois, la confidentialité ne peut pas être activée sans authentification.
- 1 **Timeliness** (Ponctualité) : offre une protection contre le retard dans la transmission de messages ou contre la transmission de messages redondants. L'agent SNMP compare le message entrant et les informations d'horodatage des messages.
- 1 **Key Management** (Gestion des clés) : définit la création, les mises à jour et l'utilisation des clés.

Le périphérique prend en charge les filtres de notification SNMP basés sur les ID d'objet (OID). Les OID sont utilisés par le système pour gérer les fonctions du périphérique. SNMP v3 prend en charge les fonctions suivantes :

- 1 Sécurité
- 1 Contrôle des accès aux fonctions
- 1 Interruptions

Les clés d'authentification ou de confidentialité sont modifiées dans le modèle de sécurité utilisateur (USM) SNMPv3.

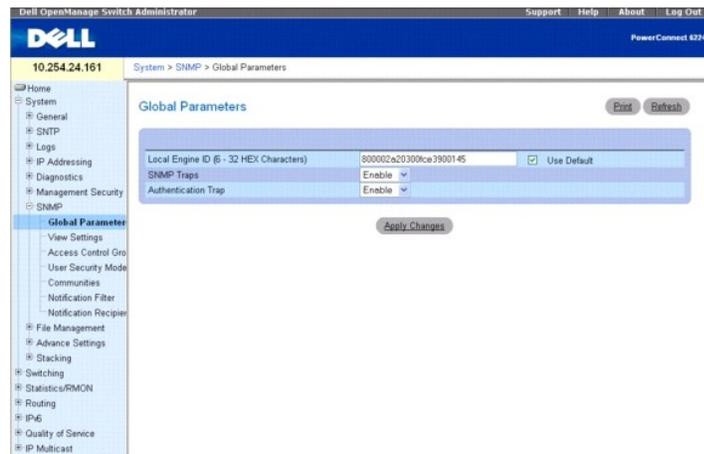
La page **SNMP** permet de définir les paramètres SNMP. Pour afficher cette page, cliquez sur **System** (Système) → **SNMP** dans l'arborescence.

Paramètres globaux SNMP

La page **Global Parameters** (Paramètres globaux) permet d'activer les notifications SNMP et d'authentification.

Pour afficher cette page, cliquez sur **System** (Système) → **SNMP** → **Global Parameters** (Paramètres globaux) dans l'arborescence.

Figure 6-58. Page **Global Parameters** (Paramètres globaux)



Cette page contient les champs suivants :

Local Engine ID (6-32 hexadecimal characters) (ID du moteur local, 6-32 caractères hexadécimaux) : définit l'ID du moteur SNMP local.

Use Default (Utiliser la valeur par défaut) : configure le périphérique pour qu'il utilise l'ID de moteur SNMP par défaut.

SNMP Traps (Interruptions SNMP) : active ou désactive le périphérique qui envoie les notifications SNMP.

Authentication Trap (Interruption liée à l'authentification) : active ou désactive le périphérique qui envoie les interruptions SNMP en cas d'échec de l'authentification.

Définition de l'ID du moteur SNMP local

1. Affichez la page **Global Parameters** (Paramètres globaux).
2. Entrez l'ID hexadécimal voulu dans le champ **Local Engine ID** (ID du moteur local).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouvel ID du moteur local est défini et le périphérique est mis à jour.

Utilisation de l'ID de moteur SNMP par défaut

1. Affichez la page **Global Parameters** (Paramètres globaux).
2. Cochez la case **Use Default** (Utiliser la valeur par défaut).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'ID du moteur SNMP par défaut (basé sur l'adresse MAC) est créé et le périphérique est mis à jour.

Activation des interruptions SNMP

1. Affichez la page **Global Parameters** (Paramètres globaux).
2. Sélectionnez **Enable** (Activer) dans le champ **SNMP Traps** (Interruptions SNMP).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les notifications SNMP sont activées et le périphérique est mis à jour.

Activation des interruptions liées à l'authentification

1. Affichez la page **Global Parameters** (Paramètres globaux).
2. Sélectionnez **Enable** (Activer) dans le champ **Authentication trap** (Interruption liée à l'authentification).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les notifications liées à l'authentification sont activées et le périphérique est mis à jour.

Activation des notifications SNMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 | SNMP Commands (Commandes SNMP)

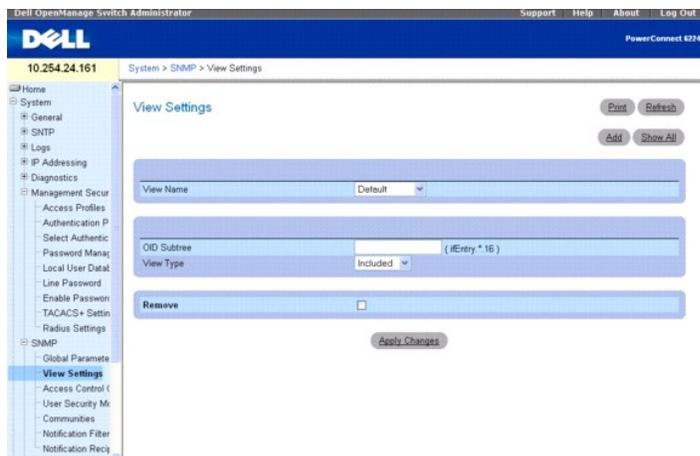
Paramètres des vues SNMP

Les vues SNMP permettent de définir les fonctions du périphérique qui sont accessibles et celles qui ne le sont pas. Vous pouvez créer une vue incluant ou excluant les ID d'objet correspondant aux interfaces.

La page **SNMP View Settings** (Paramètres des vues SNMP) permet de définir les vues SNMP.

Pour afficher cette page, cliquez sur **System** (Système) → **SNMP** → **View Settings** (Paramètres des vues) dans l'arborescence.

Figure 6-59. Page SNMP View Settings ((Paramètres des vues SNMP)



Cette page contient les champs suivants :

View Name (Nom des vues) : répertorie les vues définies par l'utilisateur. Un nom de vue peut contenir jusqu'à 30 caractères alphanumériques.

OID Subtree (Sous-arborescence des OID) : définit une chaîne d'ID d'objet SNMP valide pouvant contenir des métacaractères (tels qu'un astérisque, par exemple).

View Type (Type de vue) : indique si les OID de la vue sont inclus ou exclus.

Remove (Supprimer) : cochez cette option pour supprimer le type de vue affiché.

Ajout d'une vue

1. Affichez la page **SNMP View Settings** (Paramètres des vues SNMP).
2. Cliquez sur **Add** (Ajouter).

La page **Add View** (Ajouter une vue) s'affiche.

Figure 6-60. Page Add View (Ajouter une vue)



3. Complétez les champs appropriés.
 4. Cliquez sur **Apply Changes** (Appliquer les modifications).
- La vue SNMP est ajoutée et le périphérique est mis à jour.

Affichage de la table des vues

1. Affichez la page **SNMP View Settings** (Paramètres des vues SNMP).
2. Cliquez sur **Show All** (Afficher tout).

La page **View Table** (Table des vues) s'affiche.

Figure 6-61. Page View Table (Table des vues)



Suppression de vues SNMP

1. Affichez la page **SNMP View Settings** (Paramètres des vues SNMP).

2. Cliquez sur **Show All** (Afficher tout).

La page **View Table** (Table des vues) s'affiche.

3. Sélectionnez une vue SNMP.

4. Cochez la case **Remove** (Supprimer).

5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La vue SNMP est supprimée et le périphérique est mis à jour.

Définition de vues SNMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. SNMP Commands (Commandes SNMP)

Groupe de contrôle d'accès

Utilisez la page **Access Control Group** (Groupe de contrôle d'accès) pour afficher les informations permettant de créer des groupes SNMP et d'attribuer des droits d'accès SNMP. Les groupes permettent aux administrateurs réseau de définir les droits d'accès relatifs à certaines fonctions ou aspects fonctionnels du périphérique.

Pour afficher cette page, cliquez sur **System** (Système) → **SNMP** → **Access Control (Contrôle d'accès)** dans l'arborescence.

Figure 6-62. Page Access Control Group (Groupe de contrôle d'accès)



Cette page contient les champs suivants :

Group Name (Nom de groupe) : répertorie les groupes définis par l'utilisateur auxquels les règles de contrôle d'accès s'appliquent. Un nom de groupe peut contenir jusqu'à 30 caractères alphanumériques.

Security Model (Modèle de sécurité) : définit la version SNMP associée au groupe. Les valeurs possibles sont les suivantes :

SNMPv1 : le groupe est associé à la version SNMPv1.

SNMPv2 : le groupe est associé à la version SNMPv2.

SNMPv3 : le groupe est associé au modèle de sécurité utilisateur (USM) SNMPv3.

Security Level (Niveau de sécurité) : niveau de sécurité associé au groupe. Les niveaux de sécurité ne s'appliquent qu'aux groupes SNMPv3. Les valeurs possibles sont les suivantes :

noauth nopriv (Pas d'authentification ni de confidentialité) : aucun niveau de sécurité, qu'il s'agisse de l'authentification ou de la confidentialité, n'est associé au groupe.

auth nopriv (Authentification sans confidentialité) : authentifie les messages SNMP sans les crypter.

auth priv (Authentification avec confidentialité) : authentifie et crypte les messages SNMP.

Context Prefix (1-30) (Préfixe de contexte, 1-30) : ce champ permet à l'utilisateur d'entrer les 30 premiers caractères du nom du contexte.

Operation (Actions) : définit les droits d'accès du groupe. Les valeurs possibles sont les suivantes :

Read (Lecture) : sélectionnez une vue autorisant uniquement l'affichage du contenu de l'agent. Si aucune vue n'est sélectionnée, tous les objets peuvent être visualisés, à l'exception des tables correspondant à la communauté, aux utilisateurs SNMPv3 et aux accès.

Write (Écriture) : sélectionnez une vue autorisant l'accès en lecture-écriture au contenu de l'agent.

Notify (Notification) : sélectionnez une vue autorisant l'envoi d'informations ou d'interruptions SNMP.

Ajout de groupes SNMP

1. Affichez la page **Access Control Configuration** (Configuration du contrôle d'accès).
2. Cliquez sur **Add** (Ajouter).

La page **Add an Access Control Configuration** (Ajouter une définition de contrôle d'accès) s'affiche.

Figure 6-63. Page **Add an Access Control Configuration** (Ajouter une définition de contrôle d'accès)

Group Name (1-30)

Security Model

Security Level

Context Prefix (0-30)

Operation Read Write Notify

3. Complétez les champs avec les valeurs appropriées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le groupe est ajouté et le périphérique est mis à jour.

Affichage de la table des accès

1. Affichez la page **Access Control Configuration** (Configuration du contrôle d'accès).
2. Cliquez sur **Show All** (Afficher tout).

La page **Access Table** (Table des accès) s'affiche.

Figure 6-64. **Access Table** (Table des accès)

Access Table

Group Name	Context Prefix	SNMP Version	Security Level	Read	Write	Notify	Remove
1 DefaultRead		SNMPv1	NoAuth NoPriv	Default		Default	<input type="checkbox"/>
2 DefaultRead		SNMPv2	NoAuth NoPriv	Default		Default	<input type="checkbox"/>
3 DefaultSuper		SNMPv1	NoAuth NoPriv	DefaultSuper	DefaultSuper	DefaultSuper	<input type="checkbox"/>
4 DefaultSuper		SNMPv2	NoAuth NoPriv	DefaultSuper	DefaultSuper	DefaultSuper	<input type="checkbox"/>
5 DefaultWrite		SNMPv1	NoAuth NoPriv	Default	Default	Default	<input type="checkbox"/>
6 DefaultWrite		SNMPv2	NoAuth NoPriv	Default	Default	Default	<input type="checkbox"/>

Suppression d'un groupe

1. Affichez la page **Access Control Configuration** (Configuration du contrôle d'accès).
 2. Cliquez sur **Show All** (Afficher tout).
- La **table des accès** s'affiche.
3. Sélectionnez un groupe.
 4. Cliquez sur **Remove** (Supprimer).
 5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le groupe est supprimé et le périphérique est mis à jour.

Définition du contrôle d'accès SNMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. SNMP Commands (Commandes SNMP)

Modèle de sécurité utilisateur SNMPv3

La page **SNMPv3 User Security Model (USM)** (Modèle de sécurité utilisateur SNMPv3) permet d'affecter les utilisateurs du système à des groupes SNMP et de définir la méthode d'authentification correspondante.

Pour afficher cette page, cliquez sur **System** (Système) → **SNMP** → **User Security Model** (Modèle de sécurité utilisateur) dans l'arborescence.

Figure 6-65. **SNMPv3 User Security Model (Modèle de sécurité utilisateur SNMPv3)**

The screenshot shows the 'SNMPv3 User Security Model' configuration page. The left sidebar contains a navigation tree with 'User Security' selected. The main content area has the following fields and controls:

- User Name:** dropdown menu with 'admin' selected.
- Group Name:** dropdown menu with 'WRITE' selected.
- Engine ID:** radio buttons for 'Local' and 'Remote'.
- Authentication Method:** dropdown menu with 'None' selected.
- Password:** text input field with masked characters (*****).
- Privacy:** dropdown menu with 'None' selected.
- Authentication Key (MD5-16, SHA-20 HEX character pairs):** text input field.
- Remove:** checkbox.
- Buttons:** 'Add Local User', 'Add Remote User', 'Show All', 'Print', 'Refresh', and 'Apply Changes'.

Cette page contient les champs suivants :

User Name (Nom d'utilisateur) : répertorie les noms d'utilisateur.

Group Name (Nom de groupe) : répertorie les groupes SNMP définis par l'utilisateur. Les groupes SNMP sont définis dans la page **Access Control Group** (Groupe de contrôle d'accès).

Engine ID (ID du moteur) : indique si l'utilisateur sélectionné est associé à un périphérique local ou distant utilisant SNMPv3.

Remote Engine ID (ID de moteur distant) : indique que l'utilisateur est configuré sur un périphérique distant utilisant SNMPv3.

Authentication Method (Méthode d'authentification) : indique la méthode utilisée pour authentifier les utilisateurs. Les valeurs possibles sont les suivantes :

None (Aucune) : pas d'authentification des utilisateurs.

MD5 : les utilisateurs sont authentifiés via le niveau d'authentification HMAC-MD5-96. L'utilisateur doit saisir un mot de passe.

SHA : les utilisateurs sont authentifiés via le niveau d'authentification HMAC-SHA-96. L'utilisateur doit saisir un mot de passe.

Password (Mot de passe) : permet de modifier le mot de passe défini par l'utilisateur pour le groupe. Les mots de passe peuvent contenir jusqu'à 32 caractères. Un mot de passe n'est défini que si la méthode d'authentification est MD5 Password (Mot de passe MD5) ou SHA Password (Mot de passe SHA). La définition du mot de passe est effectuée à partir de la page **Add Local User** (Ajouter un utilisateur local).

Privacy (Confidentialité) : indique si la clé d'authentification doit être utilisée ou non. Choisissez l'une des valeurs suivantes :

None (Aucune) : aucune clé d'authentification n'est utilisée.

des : un mot de passe à cryptage symétrique CBC-DES est utilisé pour la clé d'authentification.

des-key (Clé DES) : une clé d'authentification HMAC-MD5-96 pré-générée est utilisée.

Authentication Key (MD5-16; SHA-20 HEX character pairs) (Clé d'authentification, paires de caractères hexadécimaux MD5-16/SHA-20) : définit la clé d'authentification. Une clé d'authentification n'est définie que si la méthode d'authentification est MD5 ou SHA.

Remove (Supprimer) : lorsqu'elle est cochée, cette option supprime un utilisateur d'un groupe donné.

Ajout d'utilisateurs SNMPv3 locaux à un groupe

1. Affichez la page **SNMPv3 User Security Model** (Modèle de sécurité utilisateur SNMPv3).
2. Cliquez sur **Add Local User** (Ajouter un utilisateur local).

La page correspondante s'affiche.

Figure 6-66. Page Add Local User (Ajouter un utilisateur local)



3. Complétez les champs appropriés.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).
5. L'utilisateur est ajouté au groupe et le périphérique est mis à jour.

Ajout d'utilisateurs SNMPv3 distants à un groupe

1. Affichez la page **SNMPv3 User Security Model** (Modèle de sécurité utilisateur SNMPv3).
2. Cliquez sur **Add Remote User** (Ajouter un utilisateur distant).

La page correspondante s'affiche.

Figure 6-67. Page Add Remote User (Ajouter un utilisateur distant)



3. Complétez les champs appropriés.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).
5. L'utilisateur est ajouté au groupe et le périphérique est mis à jour.

Affichage de la table du modèle de sécurité utilisateur

1. Affichez la page **SNMPv3 User Security Model (USM)** (Modèle de sécurité utilisateur SNMPv3).
2. Cliquez sur **Show All** (Afficher tout).

La page **User Security Model Table** (Table du modèle de sécurité utilisateur) s'affiche :

Figure 6-68. Page User Security Model Table (Table du modèle de sécurité utilisateur)



User Name	Group Name	Remote Engine ID	Authentication	Remove
1 Admin	DefaultRead	800002403000643900145	NONE	<input type="checkbox"/>
2 pippin	DefaultRead	800002403000643900145	NONE	<input type="checkbox"/>
3 gandalf	DefaultRead	800002403000643900145	NONE	<input type="checkbox"/>

Suppression d'une entrée de la table du modèle de sécurité utilisateur

1. Affichez la page **User Security Model** (Modèle de sécurité utilisateur).
2. Cliquez sur **Show All** (Afficher tout).

La page **User Security Model Table** (Table du modèle de sécurité utilisateur) s'affiche.

3. Sélectionnez une entrée.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est supprimée et le périphérique est mis à jour.

Définition d'utilisateurs SNMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

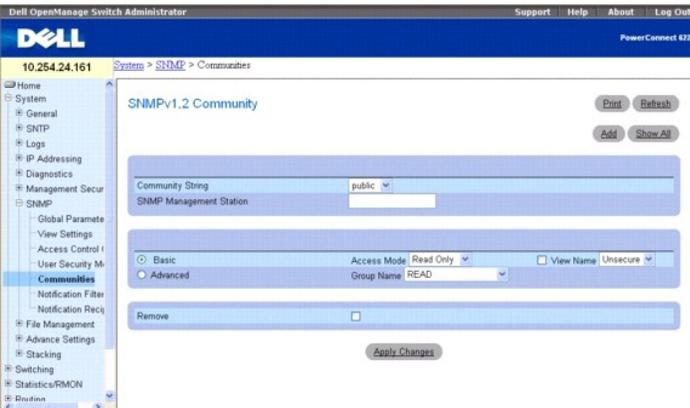
1. SNMP Commands (Commandes SNMP)

Communautés

Les droits d'accès sont gérés via la définition de communautés, qui est effectuée dans la page **SNMPv1, 2 Community** (Communauté SNMPv1, 2). Lorsqu'un nom de communauté est modifié, les droits d'accès associés le sont également. Les communautés SNMP sont définies uniquement pour SNMP v1 et v2.

Pour afficher la page **SNMPv1, 2 Community** (Communauté SNMPv1, 2), cliquez sur **System** (Système) → **SNMP** → **Communities** (Communautés) dans l'arborescence.

Figure 6-69. SNMPv1, 2 Community (Communauté SNMPv1, 2)



Cette page contient les champs suivants :

Community String (Chaîne de communauté) : contient la liste des chaînes de communauté définies par l'utilisateur. Ces chaînes font office de mot de passe et permettent au périphérique d'authentifier la station de gestion SNMP. Une chaîne de communauté peut contenir jusqu'à 20 caractères.

SNMP Management Station (Station de gestion SNMP) : répertorie les adresses IP des stations de gestion pour lesquelles des chaînes communautaires ont été définies.

Basic (De base) : active le mode SNMP de base pour la communauté sélectionnée. Les valeurs possibles sont les suivantes :

Access Mode (Mode d'accès) : définit les droits d'accès de la communauté. Les valeurs possibles sont les suivantes :

Read-Only (Lecture seule) : la communauté dispose uniquement d'un accès en lecture pour les objets de la base MIB qui sont inclus dans la vue.

Read-Write (Lecture-écriture) : la communauté dispose d'un accès en lecture-écriture aux objets de la base MIB qui sont inclus dans la vue.

Super User (Superutilisateur) : la communauté peut lire et modifier tous les objets de la base MIB.

View Name (Nom de vue) : répertorie les vues SNMP définies par l'utilisateur.

Advanced (Avancé) : répertorie les groupes définis par l'utilisateur. Lorsque le mode SNMP avancé est sélectionné, les règles de contrôle d'accès SNMP correspondant au groupe sont activées pour la communauté sélectionnée. Ce mode active également des groupes SNMP pour des communautés SNMP spécifiques (il est défini uniquement avec SNMPv3).

Remove (Supprimer) : lorsqu'elle est cochée, cette option supprime une communauté.

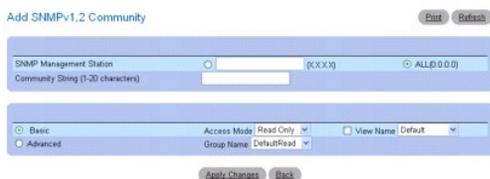
Ajout d'une nouvelle communauté

1. Affichez la page **SNMPv1, 2 Community** (Communauté SNMPv1, 2).

2. Cliquez sur **Add** (Ajouter).

La page **Add SNMPv1,2 Community** (Ajouter une communauté SNMPv1, 2) s'affiche.

Figure 6-70. Page Add SNMPv1,2 Community (Ajouter une communauté SNMPv1, 2)



3. Complétez les champs appropriés.

Outre les champs de la page **SNMPv1, 2 Community** (Communauté SNMPv1, 2), la page **Add SNMPv1, 2 Community** (Ajouter une communauté SNMPv1, 2) contient le champ **All (0.0.0.0)** (Tout, 0.0.0.0.), qui indique que la communauté peut être utilisée à partir de n'importe quelle station de gestion.

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle communauté est enregistrée et le périphérique est mis à jour.

Affichage des communautés

1. Affichez la page **SNMPv1, 2 Community** (Communauté SNMPv1, 2).

2. Cliquez sur **Show All** (Afficher tout).

La page **Basic Table** (Table de base) s'affiche.

Figure 6-71. Page Basic Table (Table de base)



Management Station	Community String	Access Mode	View Mode	Remove
1 All	private	Read Only	Default	<input type="checkbox"/>
2 All	public	Read Write	Default	<input type="checkbox"/>

Community String	Management Station	Group Name
1 private	All	DefaultRead
2 public	All	DefaultWrite

Suppression de communautés

1. Affichez la page **SNMPv1, 2 Community** (Communauté SNMPv1, 2).

2. Cliquez sur **Show All** (Afficher tout).

La page **Basic Table** (Table de base) s'affiche.

3. Sélectionnez une communauté et cochez la case **Remove** (Supprimer).

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée correspondant à la communauté est supprimée et le périphérique est mis à jour.

Configuration des communautés à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

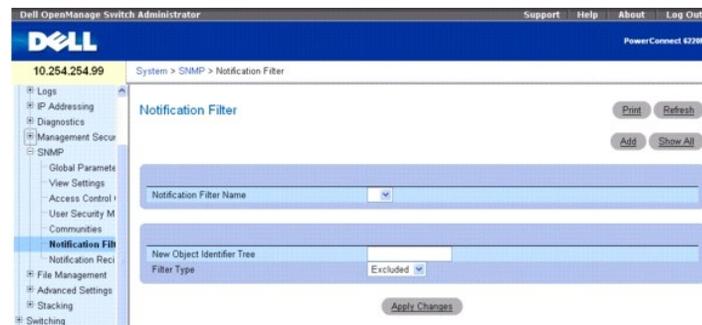
n SNMP Commands (Commandes SNMP)

Filtre de notification

La page **Notification Filter** (Filtre de notification) permet de filtrer les interruptions en fonction des OID (chaque OID est lié à une fonction du périphérique ou un aspect fonctionnel). Elle permet également aux administrateurs réseau de filtrer les notifications.

Pour afficher cette page, cliquez sur **System** (Système) → **SNMP** → **Notification Filters** (Filtres de notification) dans l'arborescence.

Figure 6-72. Page Notification Filter (Filtre de notification)



Cette page contient les champs suivants :

Notification Filter Name (Nom de filtre de notification) : répertorie les filtres de notification définis par l'utilisateur. Un nom de filtre de notification peut contenir jusqu'à 30 caractères.

New Object Identifier Tree (Arborescence du nouvel OID) : affiche les OID configurés pour le filtre sélectionné. Ce champ peut être modifié.

Filter Type (Type de filtre) : indique si des informations ou des interruptions liées à l'OID sont envoyées aux destinataires des interruptions.

Excluded (Exclusion) : désactive l'envoi d'interruptions ou d'informations concernant les OID.

Included (Inclusion) : les interruptions et informations concernant les OID sont envoyées.

Ajout de filtres SNMP

1. Affichez la page **Notification Filter** (Filtre de notification).

2. Cliquez sur **Add** (Ajouter).

La page **Add Filter** (Ajouter un filtre) s'affiche.

Figure 6-73. Page Add Filter (Ajouter un filtre)

Add Filter End Refresh

Filter Name (1 - 30 characters)	UserFilter1
New Object Identifier Tree	1.3.6.1.2.1.1.7
Filter Type	Included

Apply Changes Back

3. Complétez les champs appropriés.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).
Le nouveau filtre est ajouté et le périphérique est mis à jour.

Affichage de la table des filtres

1. Affichez la page **Notification Filter** (Filtre de notification).
2. Cliquez sur **Show All** (Afficher tout).

La page **Filter Table** (Table des filtres) affiche tous les filtres correspondant au nom sélectionné.

Figure 6-74. Page Show Notification (Afficher une notification)

Show Notification End Refresh

Filter Name

Object ID Subtree	Filter Type	Remove

Apply Changes Back

Suppression d'un filtre

1. Affichez la page **Notification Filter** (Filtre de notification).
2. Cliquez sur **Show All** (Afficher tout).
La page **Show Notification** (Afficher une notification) s'affiche.
3. Sélectionnez l'entrée **Filter Table** (Table des filtres).
4. Cliquez sur **Remove** (Supprimer).
L'entrée correspondant au filtre est supprimée et le périphérique est mis à jour.

Configuration des filtres de notification à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 SNMP Commands (Commandes SNMP)

Destinataires des notifications

La page **Notification Recipients** (Destinataires des notifications) contient des informations permettant de définir des filtres qui déterminent si des interruptions sont envoyées à des utilisateurs spécifiques et quel est le type d'interruption envoyé. Les filtres de notification SNMP fournissent les services suivants :

- 1 Identification des cibles des interruptions de gestion
- 1 Filtrage des interruptions
- 1 Sélection des paramètres de création des interruptions
- 1 Mise en place de vérifications du contrôle d'accès

Pour afficher cette page, cliquez sur **System** (Système) → **SNMP** → **Notification Recipients** (Destinataires des notifications) dans l'arborescence.

Figure 6-75. Page Notification Recipients (Destinataires des notifications)

Cette page contient les champs suivants :

Recipient IP (IP destinataire) : contient la liste des adresses IP correspondant aux destinataires des notifications. Cette liste est définie par l'utilisateur.

Notification Type (Type de notification) : type de la notification envoyée. Les valeurs possibles sont les suivantes :

Trap (Interruption) : des interruptions sont envoyées.

Inform (Informations) : des informations sont envoyées.

SNMPv1, 2 : les versions SNMP 1 ou 2 sont activées pour le destinataire sélectionné. Les valeurs possibles sont les suivantes :

Community String (Chaîne de communauté) : affiche la chaîne de communauté à envoyer avec la notification.

Notification Version (Version de la notification) : détermine la version de la notification. Les valeurs possibles sont les suivantes :

SNMP V1 : des interruptions de type SNMP version 1 sont envoyées. Si le type de notification sélectionné est Inform (Informations), vous ne pouvez pas sélectionner SNMPv1.

SNMP V2 : des interruptions ou des informations de type SNMP version 2 sont envoyées.

SNMPv3 : SNMP version 3 est activé pour le destinataire sélectionné. Les valeurs possibles sont les suivantes :

User Name (Nom d'utilisateur) : sélectionnez l'utilisateur approprié pour la création des notifications.

Security Level (Niveau de sécurité) : niveau de sécurité associé aux notifications. Les valeurs possibles sont les suivantes :

NoAu NoPriv (Pas d'authentification ni de confidentialité) : le paquet n'est ni authentifié, ni crypté.

Auth NoPriv (Authentification sans confidentialité) : le paquet est authentifié.

Auth Priv (Authentification et confidentialité) : le paquet est à la fois authentifié et crypté.

UDP Port (1-65535) (Port UDP, 1-65535) : port UDP utilisé pour l'envoi des notifications. La valeur par défaut est de 162.

Filter Name (Nom du filtre) : cochez cette case pour appliquer un filtre SNMP défini par l'utilisateur (sélectionné dans le menu déroulant) aux notifications.

Timeout (1-300) (Délai, 1-300 secondes) : durée pendant laquelle le périphérique attend avant de renvoyer des informations. La valeur par défaut est de 15 secondes.

Retries (1-255) (Nombre de tentatives, 1-255) : nombre maximal de fois où le périphérique renvoie une demande d'informations. La valeur par défaut est de 3.

Ajout d'un nouveau destinataire de notifications

1. Affichez la page **Notification Recipients** (Destinataires des notifications).
2. Cliquez sur **Add** (Ajouter).

La page **Add Notification Recipients** (Ajouter des destinataires de notifications) s'affiche.

Figure 6-76. Page Add Notification Recipient (Ajouter des destinataires de notifications)

Add Notification Recipients Print Refresh

Recipient IP/Host Name
 Notification Type

SNMPV1.2
 Community String
 Notification Version

SNMPV3
 User Name
 Security Level

UDP Port (1 - 65535)
 Filter Name
 Timeout (1 - 300) (sec)
 Retries (1 - 255)

3. Complétez les champs appropriés.
 4. Cliquez sur **Apply Changes** (Appliquer les modifications).
- Le destinataire des notifications est ajouté et le périphérique est mis à jour.

Affichage des tables des destinataires de notifications

1. Affichez la page **Notification Recipients** (Destinataires des notifications).
 2. Cliquez sur **Show All** (Afficher tout).
- La page **Notification Recipients Tables** (Tables des destinataires de notifications) s'affiche.

Figure 6-77. Page Notification Recipient Tables (Tables des destinataires de notifications)

Notification Recipients Tables Print Refresh

SNMPV1.2 Notification Recipients

Recipients IP/Host Name	Notification Type	Community String	Notification Version	UDP Port	Filter Name	Timeout	Retries	Remove

SNMPV3 Notification Recipients

Recipients IP/Host Name	Notification Type	User Name	Security Level	UDP Port	Filter Name	Timeout	Retries	Remove

Apply Changes Back

Suppression de destinataires de notifications

1. Affichez la page **Notification Recipients** (Destinataires des notifications).
 2. Cliquez sur **Show All** (Afficher tout).
- La page **Notification Recipients Tables** (Tables des destinataires de notifications) s'affiche.
3. Cochez la case **Remove** (Supprimer) correspondant à un ou plusieurs destinataires de notifications dans les tables **SNMPV1,2 Notification Recipients** et/ou **SNMPV3 Notification Recipients**.
 4. Cliquez sur **Apply Changes** (Appliquer les modifications).
- Les destinataires sont supprimés et le périphérique est mis à jour.

Définition de destinataires de notifications SNMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 SNMP Commands (Commandes SNMP)

Gestion des fichiers

La page **File Management** (Gestion des fichiers) permet de gérer les logiciels du périphérique, le fichier image et les fichiers de configuration. Les fichiers peuvent être téléchargés ou chargés via un serveur TFTP. Le système peut gérer deux versions des logiciels. Ainsi, un système exécutant une ancienne version ne chargera pas un fichier de configuration créé par la nouvelle (s'il détecte une version de ce type, un avertissement s'affiche).

Présentation des fichiers de gestion

La structure des fichiers de gestion s'établit comme suit :

- 1 **Startup configuration file** (Fichier de configuration de démarrage) : conserve la configuration exacte du périphérique lors de sa mise sous tension ou de son redémarrage. Le fichier de démarrage gère les commandes de configuration ; il peut également contenir celles du fichier de configuration d'exécution.
- 1 **Running configuration file** (Fichier de configuration d'exécution) : contient toutes les commandes du fichier de démarrage, ainsi que celles entrées pendant la session en cours. À la mise hors tension ou au redémarrage du périphérique, toutes les commandes stockées dans le fichier de configuration d'exécution sont perdues. Pendant le processus de démarrage, toutes les commandes du fichier de démarrage sont copiées dans le fichier de configuration d'exécution et appliquées au périphérique. Pendant la session, toutes les nouvelles commandes saisies sont ajoutées aux commandes existantes du fichier de configuration d'exécution. Les commandes ne sont pas remplacées. Pour mettre à jour le fichier de démarrage, le fichier de configuration d'exécution doit être copié dans le fichier de configuration de démarrage avant la mise hors tension du périphérique. Au prochain redémarrage du périphérique, les commandes sont recopiées dans le fichier de configuration d'exécution à partir du fichier de configuration de démarrage.
- 1 **Backup Configuration File** (Fichier de configuration de sauvegarde) : contient une copie de sauvegarde de la configuration du périphérique. Le fichier de sauvegarde est mis à jour lorsqu'il reçoit le contenu du fichier de configuration d'exécution ou du fichier de démarrage. Les commandes copiées dans le fichier de sauvegarde remplacent celles qui y sont déjà enregistrées. Le contenu de ce fichier peut aussi bien être copié dans le fichier de configuration d'exécution que dans le fichier de configuration de démarrage. Vous pouvez aussi effectuer une copie vers le fichier de sauvegarde et le fichier de démarrage à partir d'un serveur TFTP distant (ou effectuer l'opération inverse).
- 1 **Image Files** (Fichiers image) : des images du système sont enregistrées dans deux secteurs Flash appelés "images" (Image 1 et Image 2). L'image active contient la copie active tandis que l'autre image contient une deuxième copie. Le périphérique démarre et s'exécute à partir de l'image active. Si cette dernière est endommagée, le système démarre automatiquement à partir de l'image non active. Ce mécanisme de sécurité permet de remédier aux dysfonctionnements qui peuvent se produire lors du processus de mise à niveau de l'amorçage.

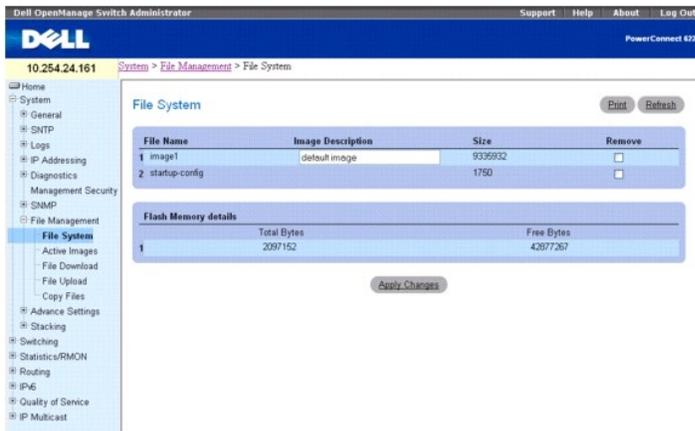
Pour afficher la page **File Management** (Gestion des fichiers), cliquez sur **System** (Système) → **File Management** (Gestion des fichiers) dans l'arborescence.

Système de fichiers

La page **File System** (Système de fichiers) permet d'afficher la liste des fichiers se trouvant sur le périphérique.

Pour afficher cette page, cliquez sur **System** (Système) → **File Management** (Gestion des fichiers) → **File System** (Système de fichiers) dans l'arborescence.

Figure 6-78. Page **File System** (Système de fichiers)



The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "File System" and contains a table with the following data:

File Name	Image Description	Size	Remove
1 image1	default image	9335932	<input type="checkbox"/>
2 startup-config		1790	<input type="checkbox"/>

Below the table is a section for "Flash Memory details" with the following data:

	Total Bytes	Free Bytes
1	2097152	4207267

The interface also includes a navigation menu on the left, a top navigation bar with "Support", "Help", "About", and "Log Out", and a "PowerConnect 6224" label in the top right corner.

Cette page contient les champs suivants :

File Name (Nom de fichier) : cette zone de texte répertorie les fichiers figurant dans les systèmes de fichiers.

Image Description (0-128) (Description de l'image, 0-128) : ce champ permet de définir et d'afficher une description de l'image. La description peut comprendre jusqu'à 128 caractères.

Size (Taille) : affiche la taille du fichier spécifié.

Remove (Supprimer) : sélectionnez cette option pour supprimer le fichier sélectionné.

Flash Memory Details (Informations sur la mémoire flash) : indique l'état de la mémoire flash.

Total Bytes (Nombre total d'octets) : affiche la quantité de mémoire flash utilisée.

Free Bytes (Octets disponibles) : affiche la quantité de mémoire flash disponible.

Suppression de fichiers

1. Affichez la page **File System** (Système de fichiers).
2. Utilisez le champ **File Name** (Nom de fichier) pour sélectionner le fichier à supprimer.
3. Cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le fichier est supprimé.

Affichage des fichiers à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

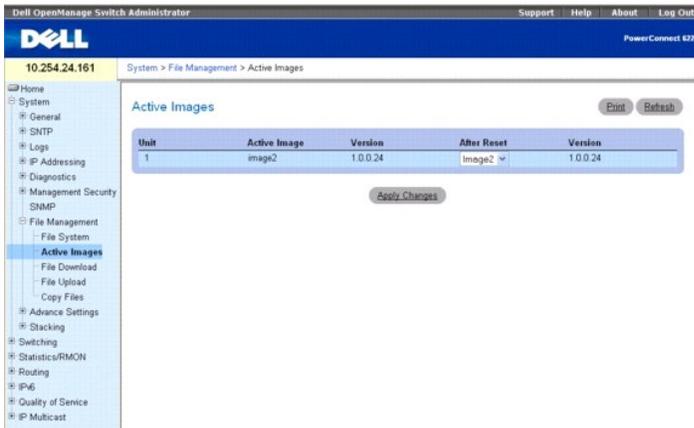
- 1 Configuration and Image Files Commands (Commandes portant sur les fichiers Image et les fichiers de configuration)

Images actives

La page **Active Image** (Image active) permet de définir l'image d'amorçage.

Pour afficher cette page, cliquez sur **System** (Système) → **File Management** (Gestion des fichiers) → **Active Images** (Images actives) dans l'arborescence.

Figure 6-79. Page Active Images (Images actives)



Cette page contient les champs suivants :

Unit (Unité) : identifie le numéro d'unité du système installé dans la pile.

Active Image (Image active) : indique le nom de l'image actuellement active.

Version : affiche le numéro de version de l'image actuellement active.

After Reset (Après réinitialisation) : menu déroulant permettant de sélectionner l'image à activer après la prochaine réinitialisation.

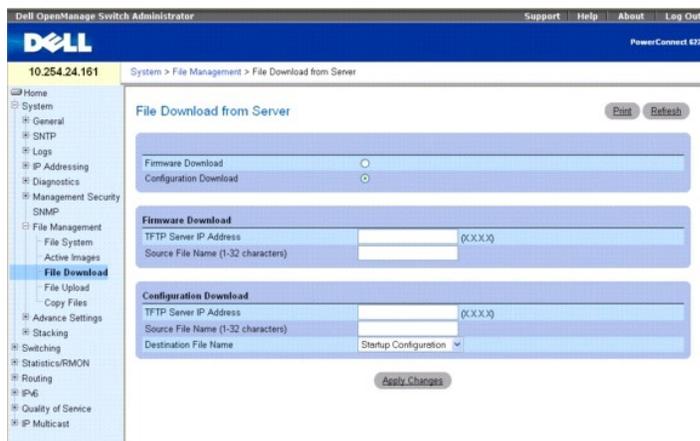
Version : affiche le numéro de version de l'image qui sera active après la prochaine réinitialisation.

Téléchargement de fichiers à partir du serveur

La page **File Download From Server** (Téléchargement de fichiers à partir du serveur) permet de télécharger des fichiers de configuration (ASCII) et des fichiers image (binaires) à partir du serveur TFTP.

Pour afficher cette page, cliquez sur **System** (Système) → **File Management** (Gestion des fichiers) → **File Download** (Téléchargement de fichiers) dans l'arborescence.

Figure 6-80. Page File Download From Server (Téléchargement de fichiers à partir du serveur)



Cette page contient les champs suivants :

Firmware Download (Téléchargement de micrologiciel) : lorsqu'elle est sélectionnée, cette option indique que le fichier de micrologiciel doit être téléchargé. Dans ce cas, les champs de la section **Configuration Download** (Téléchargement de la configuration) sont grisés.

Configuration Download (Téléchargement de la configuration) : lorsqu'elle est sélectionnée, cette option indique que le fichier de configuration doit être téléchargé. Dans ce cas, les champs de la section **Firmware Download** (Téléchargement de micrologiciel) sont grisés.

Firmware Download (Téléchargement de micrologiciel)

TFTP Server IP Address (Adresse IP du serveur TFTP) : adresse IP du serveur TFTP à partir duquel les fichiers de micrologiciel sont téléchargés.

Source File Name (1-32 characters) (Nom du fichier source, 1-32 caractères) : nom du fichier sur le serveur TFTP, avec chemin relatif par rapport au répertoire tftpboot. Par exemple, si TFTP est configuré sur un serveur distant sur lequel le répertoire tftpboot est *e:\tftp* et si le fichier *test.scr* se trouve à l'emplacement *e:\tftp\latest\test.scr*, vous devez entrer *\latest\test.scr*.

Configuration Download (Téléchargement de la configuration)

TFTP Server IP Address (Adresse IP du serveur TFTP) : adresse IP du serveur TFTP via lequel les fichiers de configuration sont téléchargés.

Source File Name (1-32 Characters) (Nom du fichier source, 1-32 caractères) : nom du fichier sur le serveur TFTP.

Destination File Name (Nom du fichier de destination) : fichier cible dans lequel le fichier de configuration est téléchargé. Ce champ peut prendre les valeurs suivantes :

Startup Configuration (Configuration de démarrage) : télécharge les fichiers de configuration de démarrage.

Backup Configuration (Configuration de sauvegarde) : télécharge les fichiers de configuration de sauvegarde.

Téléchargement de fichiers

1. Affichez la page **File Download From Server** (Téléchargement de fichiers à partir du serveur).
2. Vérifiez l'adresse IP du serveur TFTP et assurez-vous que l'image de logiciel ou le fichier d'amorçage à télécharger est disponible sur le serveur TFTP.
3. Renseignez les champs **TFTP Server IP Address** (Adresse IP du serveur TFTP) et **Source File Name** (Nom du fichier source), en indiquant le chemin complet sans l'adresse IP du serveur TFTP.

 **REMARQUE** : Il est conseillé de ne pas écraser l'image active.

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

 **REMARQUE** : Lorsque vous lancez le téléchargement d'un fichier, la page est actualisée et un champ d'état s'affiche pour indiquer le nombre d'octets transférés. L'interface Web est bloquée jusqu'à ce que le téléchargement du fichier soit terminé.

Figure 6-81. Progression du téléchargement

0% — 50% — 100%	
Percent Complete	Upload Completed
TFTP Server IP Address	172.16.1.1
TFTP Path	/
TFTP Filename	07-06-04 dell_gos.stk
Data Type	Code
Local Filename	image

Le logiciel est téléchargé sur le périphérique.

Téléchargement de fichiers à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Configuration and Image Files Commands (Commandes portant sur les fichiers image et les fichiers de configuration)

Chargement de fichiers

La page **File Upload To Server** (Chargement de fichiers sur le serveur) permet de charger des fichiers de configuration (ASCII) et des fichiers image (binaires) à partir du périphérique pour les placer sur le serveur TFTP.

Pour afficher cette page, cliquez sur **System** (Système) → **File Management** (Gestion des fichiers) → **File Upload** (Chargement de fichiers) dans l'arborescence.

Figure 6-82. Page File Upload to Server (Chargement de fichiers sur le serveur)

Cette page contient les champs suivants :

Firmware Upload (Chargement de micrologiciel) : indique que le fichier de micrologiciel doit être chargé sur le serveur. Si cette option est sélectionnée, les champs de la section **Configuration Upload** (Chargement de la configuration) sont grisés.

Configuration Upload (Chargement de la configuration) : indique que le fichier de configuration est chargé. Si cette option est sélectionnée, les champs de la section **Firmware Upload** (Chargement de micrologiciel) sont grisés.

Software Image Upload (Chargement d'une image de logiciel)

TFTP Server IP Address (Adresse IP du serveur TFTP) : adresse IP du serveur TFTP sur lequel l'image de logiciel est chargée.

Destination File Name (1-32 characters) (Nom du fichier de destination, 1-32 caractères) : nom du fichier après son chargement sur le serveur.

Transfer File Name (Nom du fichier de transfert) : permet de sélectionner le fichier source à charger sur le serveur.

Configuration Upload (Chargement de la configuration)

TFTP Server IP Address (Adresse IP du serveur TFTP) : adresse IP du serveur TFTP sur lequel le fichier de configuration est chargé.

Destination File Name (1-32 characters) (Nom du fichier de destination, 1-32 caractères) : nom du fichier après son chargement sur le serveur.

Transfer File Name (Nom du fichier de transfert) : permet de sélectionner le fichier source à charger sur le serveur. Les valeurs admises sont les suivantes :

Running Configuration (Configuration d'exécution) : charge les fichiers de configuration d'exécution sur le serveur.

Startup Configuration (Configuration de démarrage) : charge les fichiers de configuration de démarrage sur le serveur.

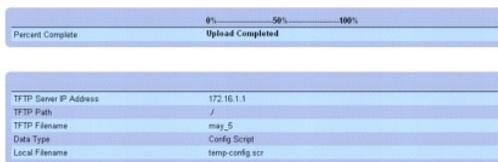
Backup Configuration (Configuration de sauvegarde) : charge les fichiers de configuration de sauvegarde sur le serveur.

Chargement de fichiers sur le serveur

1. Affichez la page **File Upload to Server** (Chargement de fichiers sur le serveur).
2. Complétez les champs appropriés.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

 **REMARQUE :** Lorsque vous lancez le chargement d'un fichier, la page est actualisée et un champ d'état s'affiche pour indiquer le nombre d'octets transférés. L'interface Web est bloquée jusqu'à ce que le chargement du fichier soit terminé.

Figure 6-83. Progression du chargement



Le logiciel est chargé sur le serveur.

Chargement de fichiers sur le serveur à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Configuration and Image Files Commands (Commandes portant sur les fichiers image et les fichiers de configuration)

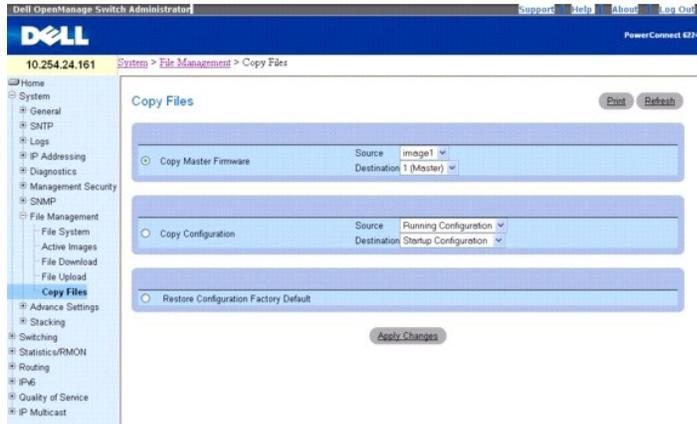
Copie de fichiers

La page Web Copy Files (Copie de fichiers) permet d'effectuer les opérations suivantes :

- 1 Copie d'images dans le système de fichiers
- 1 Copie d'images vers et depuis des serveurs distants
- 1 Sauvegarde d'images sur des systèmes locaux ou distants
- 1 Restauration d'images à partir de systèmes locaux ou distants
- 1 Sauvegarde des fichiers de configuration dans le système de fichiers

Pour afficher cette page, cliquez sur **System** (Système) → **File Management** (Gestion des fichiers) → **Copy** (Copie) dans l'arborescence.

Figure 6-84. Page Copy Files (Copie de fichiers)



Cette page contient les champs suivants :

Copy Master Firmware (Copier le micrologiciel principal) : indique qu'un fichier contenant une image de logiciel doit être copié.

Source : fichier source de l'image de logiciel à partir duquel le fichier est copié.

Destination : unité cible sur laquelle le fichier est copié.

Copy Configuration (Copier la configuration) : indique qu'un fichier de configuration doit être copié.

Source : fichier de configuration source (exécution, démarrage, sauvegarde) à partir duquel le fichier est copié.

Destination : fichier de configuration cible (exécution, démarrage, sauvegarde) dans lequel le fichier est copié.

Restore Configuration Factory Default (Restaurer les paramètres de configuration définis en usine) : lorsqu'elle est sélectionnée, cette option indique que les fichiers de configuration par défaut définis en usine doivent être restaurés. Si elle n'est pas cochée, les paramètres de configuration actuels sont conservés.

Copie de fichiers

1. Affichez la page **Copy Files** (Copie de fichiers).
2. Sélectionnez **Copy** (Copier) ou **Restore** (Restaurer) et complétez les champs appropriés.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le fichier est copié.

Copie de fichiers à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Configuration and Image Files Commands (Commandes portant sur les fichiers image et les fichiers de configuration)

Définition des paramètres avancés

Les paramètres avancés permettent de définir divers attributs globaux du périphérique. Les modifications apportées à ces attributs n'entrent en vigueur qu'après la réinitialisation du périphérique. Pour afficher la page **Advanced Settings** (Paramètres avancés), cliquez sur **System** (Système) → **Advanced Settings** (Paramètres avancés) dans l'arborescence.

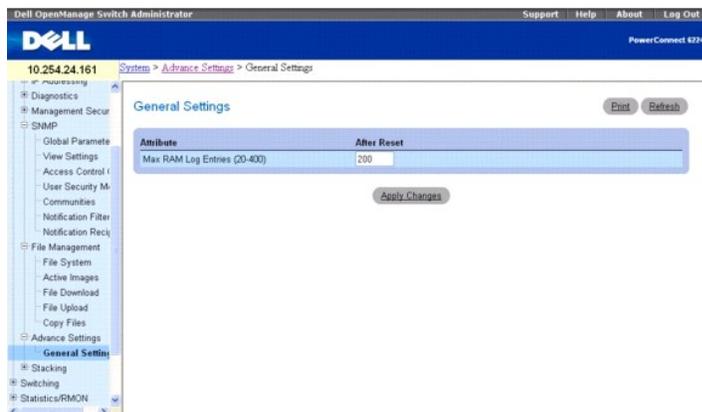
Cette page contient un lien qui permet de configurer des paramètres généraux.

Paramètres généraux

La page **General Settings** (Paramètres généraux) permet de définir les paramètres généraux du périphérique.

Pour afficher cette page, cliquez sur **System** (Système) → **Advanced Settings** (Paramètres avancés) → **General** (Général) dans l'arborescence.

Figure 6-85. Page **General Settings** (Paramètres généraux)



Cette page contient les champs suivants :

Attribute (Attribut) : nombre maximal d'entrées dans la table des journaux stockés dans la RAM. La valeur par défaut est de 200 entrées.

After Reset (Après réinitialisation) : nombre maximum d'entrées après la réinitialisation du périphérique. Lorsqu'une valeur est saisie dans cette colonne, la mémoire est allouée à la table de champs.

Modification du nombre d'entrées pour les journaux stockés dans la RAM

1. Affichez la page **General Settings** (Paramètres généraux).
2. Entrez la valeur souhaitée dans le champ **After Reset** (Après réinitialisation).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'espace alloué aux entrées des journaux stockés dans la RAM prend effet à la prochaine réinitialisation du périphérique.

Affichage des statistiques générales à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Syslog Commands (Commandes syslog)

Définition de l'empilage

Les menus Stacking (Empilage) permettent de définir les caractéristiques d'empilage du périphérique. Les modifications apportées à ces attributs n'entrent en vigueur qu'après la réinitialisation du périphérique. Pour afficher la page **Stacking** (Empilage), cliquez sur **System** (Système) → **Stacking** (Empilage) dans l'arborescence. Cette page permet d'accéder aux fonctions suivantes :

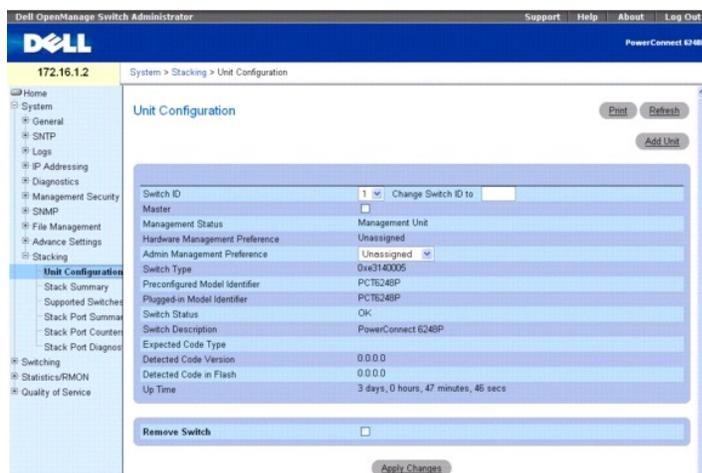
- 1 [Configuration de l'unité](#)
- 1 [Récapitulatif de la pile](#)
- 1 [Commutateurs pris en charge](#)
- 1 [Récapitulatif des ports de la pile](#)
- 1 [Compteurs des ports de la pile](#)
- 1 [Diagnostics des ports de la pile](#)

Configuration de l'unité

La page **Unit Configuration** (Configuration de l'unité) permet de définir les paramètres généraux du périphérique.

Pour afficher cette page, cliquez sur **System** (Système) → **Stacking** (Empilage) → **Unit Configuration** (Configuration de l'unité) dans l'arborescence.

Figure 6-86. Page Unit Configuration (Configuration de l'unité)



Cette page contient les champs suivants :

Switch ID (ID du commutateur) : identifie l'unité à configurer.

Change Switch ID to (Remplacer l'ID du commutateur par) : change le numéro de l'unité sélectionnée.

Master (Maître) : sélectionnez cette option pour désigner cette unité comme maître (unité utilisée pour la gestion de la pile). La valeur par défaut est Unassigned (Non affecté).

Management Status (État de gestion) : indique si l'unité sélectionnée est une unité de gestion ou un simple membre de la pile.

Hardware Management Preference (Préférence de gestion au niveau du matériel) : caractéristiques matérielles prioritaires à prendre en compte pour la sélection d'une unité de gestion.

Admin Management Preference (Préférence de gestion pour l'administration) : indique si l'unité possède les caractéristiques requises pour devenir le commutateur maître d'une pile. Les valeurs possibles vont de **Disable** (Désactivé - l'unité ne prend pas en charge la fonction de commutateur maître) à **Preference 15**. Une valeur élevée signifie que l'unité est plus adaptée au rôle de commutateur maître que les commutateurs associés à des valeurs inférieures. La valeur **Unassigned** (Non affecté) signifie qu'aucune préférence n'est définie ; la désignation de l'unité principale est effectuée par les membres de la pile.

Switch Type (Type de commutateur) : ID de matériel attribué au système pour déterminer le type du commutateur.

Preconfigured Model Identifier (Identificateur du modèle préconfiguré) : chaîne de caractères (16 octets) identifiant le modèle préconfiguré de l'unité sélectionnée.

Plugged-in Model Identifier (Identificateur du modèle ajouté) : chaîne de caractères (16 octets) identifiant le modèle ajouté pour l'unité sélectionnée.

Switch Status (État du commutateur) : affiche l'état de l'unité sélectionnée. Les valeurs possibles sont les suivantes :

OK : l'unité est installée et opérationnelle.

Unsupported (Non prise en charge) : l'unité est installée mais ne peut pas fonctionner en tant que membre de la pile.

Code Mismatch (Code non conforme) : les éléments logiciels du commutateur ne correspondent pas à ceux de l'unité maître.

Config Mismatch (Configuration non conforme) : la configuration du commutateur ne correspond pas à celle de l'unité maître.

Not Present (Absente) : l'unité sélectionnée est introuvable.

Switch Description (Description du commutateur) : champ de données (80 octets) utilisé pour identifier le périphérique.

Expected Code Type (Type de code attendu) : indique l'identificateur de code attendu.

Detected Code Version (Version de code détectée) : numéro de version et d'édition du code en cours d'exécution.

Detected Code in Flash (Code détecté dans la mémoire flash) : numéro de version et d'édition du code détecté dans la mémoire flash.

Up Time (Durée de fonctionnement) : indique la durée qui s'est écoulée depuis la dernière réinitialisation de l'unité.

Remove Switch (Supprimer un commutateur) : sélectionnez cette option pour retirer un commutateur de la pile.

Définition de la configuration de l'unité

1. Affichez la page **Unit Configuration** (Configuration de l'unité).
2. Complétez les champs en indiquant les valeurs appropriées.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications prendront effet à la prochaine réinitialisation du périphérique.

Suppression d'un commutateur

1. Affichez la page **Unit Configuration** (Configuration de l'unité).
2. Cochez l'option **Remove Switch** (Supprimer un commutateur).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications prendront effet à la prochaine réinitialisation du périphérique.

Ajout d'une unité

La page **Add Unit** (Ajouter une unité) permet de définir les paramètres généraux du périphérique.

Pour afficher cette page, cliquez sur **System** (Système) → **Stacking** (Empilage) → **Unit Configuration** (Configuration de l'unité) dans l'arborescence, puis cliquez sur **Add Unit** (Ajouter une unité).

Figure 6-87. Page Add Unit (Ajouter une unité)



Cette page contient les champs suivants :

Switch ID (ID du commutateur) : affiche l'ID du commutateur sélectionné dans la pile. Les administrateurs peuvent modifier cet ID afin de renuméroter un commutateur. Seuls les utilisateurs possédant le niveau d'accès 15 peuvent modifier ce champ à l'aide de l'interface Web.

Switch Type (Type de commutateur) : identifie l'ID de matériel attribué au commutateur.

Ajout d'une unité

1. Affichez la page **Unit Configuration** (Configuration de l'unité).
2. Cliquez sur **Add Unit** (Ajouter une unité).
La page **Add Unit** (Ajouter une unité) s'affiche.
3. Entrez la valeur souhaitée dans le champ **Switch ID** (ID du commutateur).
4. Sélectionnez la valeur souhaitée dans la liste déroulante **Switch Type** (Type de commutateur).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications prendront effet à la prochaine réinitialisation du périphérique.

Affichage de la configuration d'une unité à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

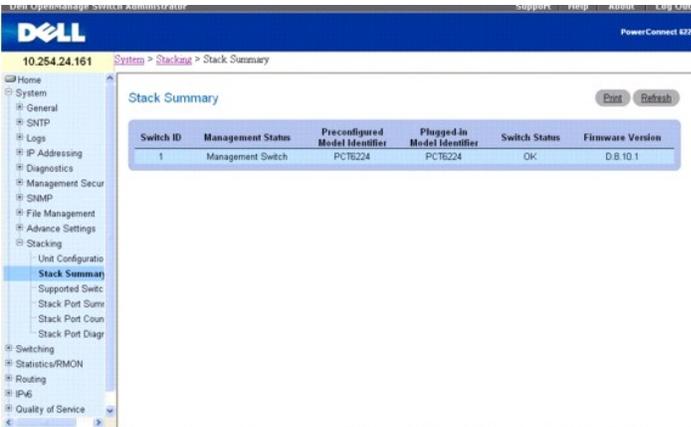
- 1 System Management Commands (Commandes de gestion du système)

Récapitulatif de la pile

La page **Stack Summary** (Récapitulatif de la pile) permet d'afficher un récapitulatif décrivant les commutateurs inclus dans la pile.

Pour afficher cette page, cliquez sur **System** (Système) → **Stacking** (Empilage) → **Stack Summary** (Récapitulatif de la pile) dans l'arborescence.

Figure 6-88. Page Stack Summary (Récapitulatif de la pile)



Cette page contient les champs suivants :

Switch ID (ID du commutateur) : ID de l'unité. Le nombre maximal de commutateurs pouvant être inclus dans une pile est de 8.

Management Status (État de gestion) : ce champ indique si le commutateur est utilisé pour la gestion, s'il s'agit d'un simple membre de la pile ou si l'état n'est pas déterminé.

Pre-configured Model Identifier (Identificateur du modèle préconfiguré) : ce champ contient la chaîne de caractères (16 octets) définie par le fabricant pour identifier le périphérique préconfiguré.

Plugged-in Model Identifier (Identificateur du modèle ajouté) : ce champ contient la chaîne de caractères (16 octets) définie par le fabricant pour identifier le périphérique ajouté.

Switch Status (État du commutateur) : indique l'état de l'unité. Ce champ peut contenir les 5 valeurs suivantes :

OK : l'unité est installée et opérationnelle.

Unsupported (Non prise en charge) : l'unité ne peut pas être utilisée dans la pile.

Code Mismatch (Code non conforme) : l'image logicielle de l'unité ne correspond pas à celle du commutateur maître de la pile.

Config Mismatch (Configuration non conforme) : le fichier de configuration de l'unité ne correspond pas à celui du commutateur maître de la pile.

Not Present (Absente) : l'unité est introuvable.

Firmware Version (Version du micrologiciel) : indique la version de code détectée sur l'unité.

Affichage du récapitulatif de la pile à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 System Management Commands (Commandes de gestion du système)

Commutateurs pris en charge

La page **Supported Switches** (Commutateurs pris en charge) permet d'afficher des informations sur chaque type de commutateur pris en charge pour l'empilage, ainsi que des informations sur les commutateurs supportés.

Pour afficher cette page, cliquez sur **System** (Système) → **Stacking** (Empilage) → **Supported Switches** (Commutateurs pris en charge) dans l'arborescence.

Figure 6-89. Page Supported Switches (Commutateurs pris en charge)



Cette page contient les champs suivants :

Supported Switches (Commutateurs pris en charge) : liste déroulante permettant de sélectionner les commutateurs pris en charge.

Switch Index (Index du commutateur) : indique l'index du commutateur dans la base de données répertoriant les types de commutateurs pris en charge.

Switch Type (Type de commutateur) : ID de matériel attribué au commutateur.

Switch Model ID (ID du modèle de commutateur) : affiche une chaîne de caractères (16 octets) identifiant le modèle du commutateur pris en charge.

Description : affiche un champ de données (256 octets) utilisé pour identifier le périphérique.

Management Preference (Préférence de gestion) : indique si l'unité possède les caractéristiques requises pour devenir le commutateur maître d'une pile. Si la valeur définie est 0, l'unité ne prend pas en charge la fonction de commutateur maître. Une valeur élevée signifie que l'unité est plus adaptée au rôle de commutateur maître que les commutateurs associés à des valeurs inférieures. La valeur initiale de ce champ est définie par le fabricant du périphérique.

Expected Code Type (Type de code attendu) : affiche les numéros de version et d'édition attendus pour le code.

Affichage des caractéristiques d'un commutateur pris en charge

1. Affichez la page **Supported Switches** (Commutateurs pris en charge).
2. Sélectionnez le commutateur souhaité dans la liste déroulante **Supported Switches** (Commutateurs pris en charge).

Affichage de la configuration des commutateurs pris en charge à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- System Management Commands (Commandes de gestion du système)

Récapitulatif des ports de la pile

La page **Stack Port Summary** (Récapitulatif des ports de la pile) permet d'afficher les ports d'empilage. Cet écran affiche l'unité, l'interface d'empilage, le mode configuré pour l'interface, le mode d'exécution, l'état du lien et la vitesse de transmission du port d'empilage.

Pour afficher cette page, cliquez sur **System** (Système) → **Stacking** (Empilage) → **Stack Port Summary** (Récapitulatif des ports de la pile) dans l'arborescence.

Figure 6-90. Page **Stack Port Summary** (Récapitulatif des ports de la pile)

Unit	Interface	Configured Stack-mode	Running Stack-mode	Link Status	Link Speed (Gb/s)
1	1/xg1	Ethernet	Ethernet	Link Down	12
1	1/xg2	Ethernet	Ethernet	Link Down	12
1	1/xg3	Ethernet	Ethernet	Link Down	12
1	1/xg4	Ethernet	Ethernet	Link Down	12

Cette page contient les champs suivants :

Unit (Unité) : numéro d'ID de l'unité.

Interface : identifie l'interface d'empilage affectée à l'unité.

Configured Stack Mode (Mode configuré sur la pile) : indique si chaque unité est ou non en mesure de participer au fonctionnement de la pile.

Running Stack Mode (Mode exécuté sur la pile) : indique si chaque unité participe ou non au fonctionnement de la pile.

Link Status (État du lien) : indique si l'interface d'empilage de chaque unité est opérationnelle.

Link Speed (Gb/s) (Vitesse de la liaison [Gbps]) : indique la vitesse nominale de transfert pour chaque unité.

Affichage du récapitulatif des ports de la pile à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 System Management Commands (Commandes de gestion du système)

Compteurs des ports de la pile

La page **Stack Port Counters** (Compteurs des ports de la pile) permet d'afficher les statistiques d'envoi et de réception, ainsi que le débit de données et le pourcentage d'erreurs.

Pour afficher cette page, cliquez sur **System** (Système) → **Stacking** (Empilage) → **Stack Point Counters** (Compteurs des ports de la pile) dans l'arborescence.

Figure 6-91. Page Stack Port Counters (Compteurs des ports de la pile)

Unit	Interface	Data Rate (Mb/s)	Transmit Error Rate (Errors/sec)	Total Errors	Data Rate (Mb/s)	Receive Error Rate (Errors/sec)	Total Errors
1	1/xg1	0	0	0	0	0	0
1	1/xg2	0	0	0	0	0	0
1	1/xg3	0	0	0	0	0	0
1	1/xg4	0	0	0	0	0	0

Cette page contient les champs suivants :

Unit (Unité) : indique le commutateur subordonné en cours d'affichage.

Interface : indique le nom de l'interface.

Data Rate (Mb/s) (Débit de données [Mbps]) : indique la vitesse de transfert des données.

Transmit Error Rate (Errors/sec) (Taux d'erreurs de transmission [Erreurs/sec]) : indique le nombre d'erreurs de transmission par seconde.

Total Errors (Total d'erreurs) : nombre total d'erreurs de transmission.

Data Rate (Mb/s) (Débit de données [Mbps]) : indique la vitesse de réception des données.

Receive Error Rate (Errors/sec) (Taux d'erreurs de réception [Erreurs/sec]) : indique le nombre d'erreurs de réception par seconde.

Total Errors (Total d'erreurs) : nombre total d'erreurs de réception.

Affichage des compteurs relatifs aux ports de la pile

1. Affichez la page **Stack Port Counters** (Compteurs des ports de la pile).

Affichage des compteurs pour les ports de la pile à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. System Management Commands (Commandes de gestion du système)

Diagnostics des ports de la pile

La page **Stack Port Diagnostics** (Diagnostics des ports de la pile) est réservée aux ingénieurs d'applications (FAE) et aux développeurs.

[Retour au sommaire](#)

[Retour au sommaire](#)

Configuration des fonctions de support pour le téléphone IP et les points d'accès

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Configuration de la fonction Power Over Ethernet](#)
- [Configuration de LLDP-MED](#)
- [Configuration des ports d'un VLAN voix](#)

Cette section décrit différentes fonctions de support disponibles sur le système pour le téléphone IP et les points d'accès :

- 1 [Configuration de la fonction Power Over Ethernet](#)
- 1 [Configuration de LLDP-MED](#)
- 1 [Configuration des ports d'un VLAN voix](#)

Configuration de la fonction Power Over Ethernet

La fonction Power over Ethernet (PoE) permet d'alimenter les périphériques par l'intermédiaire du câblage existant sur le réseau local, sans avoir à modifier ni mettre à jour l'infrastructure du réseau. Son utilisation évite d'avoir à installer les périphériques réseau à proximité des sources d'alimentation. De nombreux périphériques peuvent être alimentés à l'aide de la fonction PoE : téléphones IP, points d'accès sans fil, passerelles IP, PDA, périphériques de contrôle audio et vidéo à distance, etc.

Cette section présente les options PoE accessibles à partir de la page **System** (Système) → **General** (Général) → **Power Over Ethernet**. Ces options permettent notamment de configurer et d'afficher les informations PoE relatives au système ou à chaque interface. La page **Power Over Ethernet** permet d'effectuer les opérations suivantes :

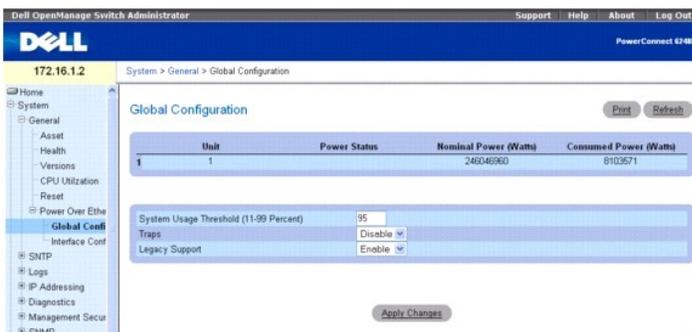
- 1 [Configuration de la fonction Power Over Ethernet](#)
- 1 [Configuration des interfaces](#)

Configuration globale

La page **Global Configuration** (Configuration globale) permet de configurer et d'afficher les paramètres PoE appliqués à l'ensemble du système, notamment les informations concernant l'utilisation du système, les interruptions et le support disponible pour les périphériques PoE de génération antérieure.

Pour afficher cette page, cliquez sur **System** (Système) → **General** (Général) → **Power Over Ethernet** → **Global Configuration** (Configuration globale) dans l'arborescence.

Figure 7-1. Page Global Configuration (Configuration globale)



Cette page contient les champs suivants :

Unit (Unité) : identifie l'unité installée dans la pile.

Power Status (État de l'alimentation) : indique l'état de l'équipement fournissant l'alimentation électrique en ligne.

Nominal Power (Puissance nominale) : puissance nominale (en watts) de l'équipement fournissant l'alimentation électrique en ligne.

Consumed Power (Consommation) : mesure de la consommation en watts.

System Usage Threshold (Seuil d'utilisation du système) : seuil d'utilisation à partir duquel une alarme doit être générée en cas de dépassement. Cette valeur est exprimée en pourcentage par rapport à la puissance consommée.

Traps (Interruptions) : indique si les interruptions liées à l'alimentation en ligne sont activées ou désactivées.

Legacy Support (Prise en charge des périphériques de génération antérieure) : permet d'activer et de désactiver la prise en charge des périphériques PoE de génération antérieure.

Configuration des paramètres PoE globaux

1. Affichez la page **Global Configuration** (Configuration globale).
2. Définissez le seuil d'utilisation du système, les interruptions ou les modalités de prise en charge des périphériques PoE de génération antérieure.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont modifiés et le périphérique est mis à jour.

Configuration de PoE à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

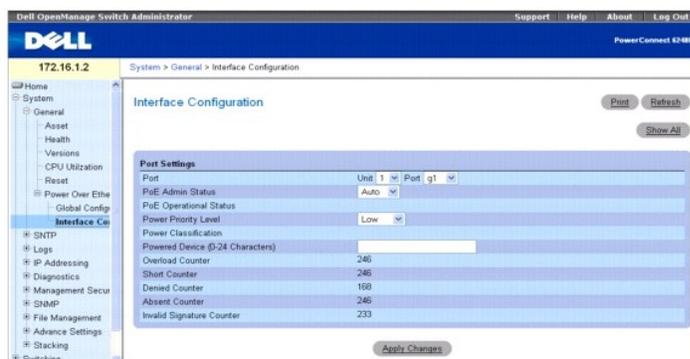
- 1 Power Over Ethernet Commands (Commandes portant sur la fonction Power Over Ethernet)

Configuration des interfaces

La page **Interface Configuration** (Configuration des interfaces) permet de configurer et d'afficher les paramètres PoE de chaque port.

Pour afficher cette page, cliquez sur **System** (Système) → **General** (Général) → **Power Over Ethernet** → **Interface Configuration** (Configuration des interfaces) dans l'arborescence.

Figure 7-2. Page Interface Configuration (Configuration des interfaces)



Cette page contient les champs suivants :

Port : indique l'unité et le port pour lesquels les paramètres sont définis.

PoE Admin Status (État de gestion PoE) : indique si le port peut fournir une alimentation électrique.

Auto (Automatique) : le port alimente automatiquement un périphérique PoE connecté.

Never (Jamais) : le port n'alimente aucun périphérique connecté.

PoE Operational Status (État de fonctionnement PoE) : décrit l'état de fonctionnement du port par rapport à l'alimentation en ligne. Ce champ peut prendre l'une des valeurs suivantes :

Off (Désactivé) : aucune alimentation n'est fournie.

On (Activé) : le périphérique consomme de l'électricité.

Test-Fail (Échec du test) : indique qu'un incident lié au port s'est produit.

Testing (Test en cours) : indique que le port est en mode test.

Fault (Panne) : indique que le port est inactif suite à une erreur.

Searching (Recherche en cours) : indique que le port ne se trouve dans aucun des états répertoriés ci-dessus.

Power Priority Level (Niveau de priorité de l'alimentation) : priorité du port par rapport à la gestion de l'alimentation en ligne. Ce champ peut prendre l'une des valeurs suivantes :

- 1 Critical (Critique)

- 1 High (Haute)

- 1 Low (Basse)

Power Classification (Classification électrique) : niveau de consommation du périphérique alimenté. Les classes existantes sont les suivantes :

- 1 Classe 0 (0,44 à 12,95)
- 1 Classe 1 (0,44 à 3,84)
- 1 Classe 2 (3,84 à 6,49)
- 1 Classe 3 (6,49 à 12,95)

Powered Device (Périphérique alimenté) : description du type correspondant au périphérique alimenté (24 caractères maximum).

Overload Counter (Nombre de surcharges) : indique le nombre de conditions de surcharge ayant été détectées.

Short Counter (Nombre de courts-circuits) : indique le nombre de courts-circuits ayant été détectés.

Denied Counter (Nombre de refus) : indique le nombre de fois où l'alimentation en électricité a été refusée.

Absent Counter (Nombre d'absences) : indique le nombre de fois où l'alimentation électrique a été coupée en raison de la perte d'un périphérique alimenté.

Invalid Signature Counter (Nombre de signatures non valides) : indique le nombre de fois où un périphérique alimenté possédant une signature non valide a été détecté.

Définition des paramètres PoE d'une interface

1. Affichez la page **Interface Configuration** (Configuration des interfaces).
2. Sélectionnez l'unité et le port à configurer.
3. Définissez l'état de gestion, le niveau de priorité de l'alimentation ou le nom du périphérique alimenté par le port.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

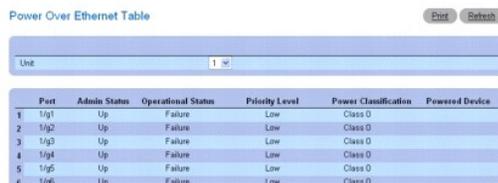
Les paramètres sont modifiés et le périphérique est mis à jour.

Affichage de la table Power Over Ethernet

1. Affichez la page **Interface Configuration** (Configuration des interfaces).
2. Cliquez sur **Show All** (Afficher tout).

La page **Power Over Ethernet Table** (Table Power Over Ethernet) affiche un récapitulatif des informations relatives à toutes les interfaces par rapport à la fonction PoE.

Figure 7-3. Table Power Over Ethernet



Port	Admin Status	Operational Status	Priority Level	Power Classification	Powered Device
1 1/1/1	Up	Failure	Low	Class 0	
2 1/1/2	Up	Failure	Low	Class 0	
3 1/1/3	Up	Failure	Low	Class 0	
4 1/1/4	Up	Failure	Low	Class 0	
5 1/1/5	Up	Failure	Low	Class 0	
6 1/1/6	Up	Failure	Low	Class 0	

Configuration de PoE à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Power Over Ethernet Commands (Commandes portant sur la fonction Power Over Ethernet)

Configuration de LLDP-MED

La norme IEEE 802.1AB décrit le protocole LLDP (Link Layer Discovery Protocol). Elle formalise la détection des éléments composant un réseau de données dans un environnement LAN/MAN, ainsi que l'identification de leurs capacités. Les informations échangées sont stockées dans des bases MIB et accessibles via un système de gestion réseau tel que SNMP. Cette architecture extensible permet l'utilisation de fonctions avancées dans divers domaines (réseaux VoIP, etc.).

La fonction LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) est une extension de la norme LLDP appliquée à différentes fonctionnalités : configuration des réseaux, implémentation de stratégies, détection de périphériques, gestion de la fonction PoE et gestion de l'inventaire.

Le protocole LLDP-MED utilise les extensions TLV (ensembles Type, Longueur, Valeur) spécifiques de chaque organisation, mais il définit également de nouveaux TLV facilitant le déploiement des fonctions VoIP (voix sur IP) dans les environnements LAN/MAN câblés ou sans fil. Il détermine quels sont les TLV obligatoires et quels sont ceux qui au contraire ne devraient pas être transmis.

LLDP-MED utilisant l'architecture du protocole LLDP, il présente les mêmes exigences que les spécifications d'origine (format des trames, restrictions, etc.).

Les TLV ne font que communiquer des informations ; ils ne se traduisent pas automatiquement en une configuration spécifique. Une application externe peut interroger la base MIB contenant les informations sur les périphériques réseau et configurer les fonctions requises en lançant les opérations de gestion appropriées.

La page de menu **LLDP-MED** contient des liens vers les fonctionnalités suivantes :

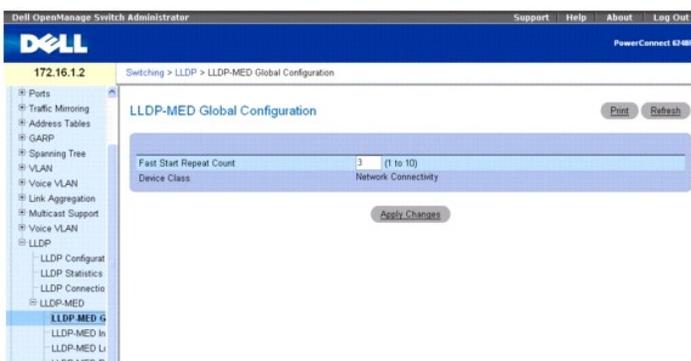
- 1 [Configuration LLDP-MED globale](#)
- 1 [Configuration des interfaces LLDP-MED](#)
- 1 [Informations LLDP-MED sur les périphériques locaux](#)
- 1 [Informations LLDP-MED sur les périphériques distants](#)

Configuration LLDP-MED globale

La page **LLDP-MED Global Configuration** (Configuration LLDP-MED globale) permet d'afficher et de modifier les paramètres LLDP-MED qui affectent l'intégralité du système.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **LLDP** → **LLDP-MED** → **LLDP-MED Global Configuration** (Configuration LLDP-MED globale) dans l'arborescence.

Figure 7-4. Page LLDP-MED Global Configuration (Configuration LLDP-MED globale)



Cette page contient les champs suivants :

Fast Start Repeat Count (Nombre de répétitions pour le démarrage rapide) : indique le nombre de PDU (Protocol Data Unit, unités de données de protocole) qui seront envoyées à l'activation du protocole. Les valeurs possibles vont de 1 à 10. La valeur par défaut est de 4.

Device Class (Classe du périphérique) : indique la classification MED du périphérique local. Il existe quatre types de périphériques dont trois représentent les points de terminaison. La classe I représente une catégorie générique (contrôleurs de communications IP, etc.), la classe II représente les dispositifs tels que les ponts de conférences, etc., et la classe III les périphériques de communication (téléphones IP, etc.). Le quatrième type désigne les périphériques de connexion réseau : commutateurs ou routeurs de réseau local, ponts IEEE 802.1, points d'accès sans fil IEEE 802.11, etc.

Modification de la configuration LLDP-MED globale

1. Affichez la page **LLDP Configuration** (Configuration LLDP).
2. Entrez une nouvelle valeur dans le champ **Fast Start Repeat Count** (Nombre de répétitions pour le démarrage rapide).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres LLDP-MED sont sauvegardés sur le commutateur.

Configuration des paramètres LLDP-MED globaux à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 LLDP Commands (Commandes LLDP)

Configuration des interfaces LLDP-MED

La page **LLDP-MED Interface Configuration** (Configuration des interfaces LLDP-MED) permet de définir les paramètres LLDP-MED affectant une interface spécifique.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **LLDP** → **LLDP-MED** → **LLDP-MED Interface Configuration** (Configuration des interfaces LLDP-MED) dans l'arborescence.

Figure 7-5. Page LLDP-MED Interface Configuration (Configuration des interfaces LLDP-MED)



Cette page contient les champs suivants :

Interface : définit la liste des ports pouvant être configurés en LLDP-MED - 802.1AB. Pour appliquer les mêmes paramètres LLDP-MED à toutes les interfaces du système, sélectionnez **All** (Tous) dans le menu déroulant **Port**.

REMARQUE : Lorsque vous sélectionnez **All** (Tous) dans le champ **Port**, la page affiche le mode LLDP-MED et le mode de modification comme étant désactivés (Disabled). Toutes les cases à cocher **Transmit TLVs** (TLV à transmettre) sont désélectionnées. Ce comportement se produit même si vous configurez tous les ports avec les mêmes paramètres. Sélectionnez une interface spécifique ou cliquez sur **Show All** (Afficher tout) pour afficher les paramètres LLDP-MED de toutes les interfaces.

LLDP-MED Mode (Mode LLDP-MED) : définit le mode LLDP-MED correspondant à l'interface sélectionnée. L'activation de la fonction MED active la fonction de transmission et de réception LLDP.

Config Notification Mode (Mode de notification de la configuration) : définit le mode de notification de la topologie LLDP-MED correspondant à l'interface sélectionnée.

Transmit TLVs (TLV à transmettre) : indique quels TLV LLDP-MED facultatifs doivent être transmis dans les trames des PDU LLDP pour l'interface sélectionnée.

MED Capabilities (Capacités des périphériques réseau) : les TLV contenant des informations sur les capacités sont transmis dans les trames LLDP.

Network Policy (Stratégie réseau) : les TLV contenant des informations sur la stratégie réseau sont transmis dans les trames LLDP.

Location Identification (Identification de l'emplacement) : les TLV contenant des informations d'emplacement sont transmis dans les trames LLDP.

Extended Power via MDI - PSE (Fonctions d'alimentation étendues via l'interface MDI - PSE) : les TLV contenant des informations sur les PSE (Power Supply Equipment, équipements de source d'alimentation) étendus sont transmis dans les trames LLDP.

Extended Power via MDI - PD (Fonctions d'alimentation étendues via l'interface MDI - PD) : les TLV contenant des informations sur les PD (Powered Devices, équipements alimentés) étendus sont transmis dans les trames LLDP.

Inventory (Inventaire) : les TLV contenant des informations d'inventaire sont transmis dans les trames LLDP.

Modification de la configuration des interfaces LLDP-MED

1. Affichez la page **LLDP Configuration** (Configuration LLDP).
2. Sélectionnez l'unité et le port à configurer, ou bien sélectionnez **All** (Tout) pour appliquer les mêmes paramètres à tous les ports.
3. Configurez les paramètres LLDP-MED de l'interface ou des interfaces.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres LLDP-MED sont sauvegardés sur le commutateur.

REMARQUE : Si vous avez sélectionné **All** pour configurer tous les ports, les paramètres appliqués ne sont pas affichés une fois la page mise à jour. Sélectionnez une interface spécifique ou cliquez sur **Show All** (Afficher tout) pour afficher les paramètres LLDP-MED de toutes les interfaces.

Affichage du récapitulatif des interfaces

1. Affichez la page **LLDP-MED Interface Configuration** (Configuration des interfaces LLDP-MED).
2. Cliquez sur **Show All** (Afficher tout).

La page **LLDP-MED Interface Summary** (Récapitulatif des interfaces LLDP-MED) affiche un résumé des informations LLDP-MED relatives à toutes les interfaces.

Figure 7-6. Page **LLDP-MED Interface Summary** (Récapitulatif des interfaces LLDP-MED)

LLDP-MED Interface Summary [Print] [Refresh]

Unit: 1

Interface	Link Status	MED Status	Operational Status	Notification Status	Transmit TLV(s)
1/1	Up	Disable	Disable	Disable	Capabilities Network Policy
1/2	Down	Disable	Disable	Disable	Capabilities Network Policy
1/3	Down	Disable	Disable	Disable	Capabilities Network Policy
1/4	Down	Disable	Disable	Disable	Capabilities Network Policy
1/5	Down	Disable	Disable	Disable	Capabilities Network Policy

1/68	Down	Disable	Disable	Disable	Capabilities Network Policy
1/69	Down	Disable	Disable	Disable	Capabilities Network Policy
1/70	Down	Disable	Disable	Disable	Capabilities Network Policy
1/71	Down	Disable	Disable	Disable	Capabilities Network Policy
1/72	Down	Disable	Disable	Disable	Capabilities Network Policy
1/73	Down	Disable	Disable	Disable	Capabilities Network Policy
1/74	Down	Disable	Disable	Disable	Capabilities Network Policy

[Apply Changes] [Back]

Configuration des paramètres des interfaces LLDP-MED à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 LLDP Commands (Commandes LLDP)

Informations LLDP-MED sur les périphériques locaux

Utilisez la page **LLDP-MED Local Device Information** (Informations LLDP-MED sur les périphériques locaux) pour afficher les données LLDP locales annoncées pour chaque port.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **LLDP** → **LLDP-MED** → **LLDP-MED Local Device Information** (Informations LLDP-MED sur les périphériques locaux) dans l'arborescence.

Figure 7-7. Page **LLDP-MED Local Device Information** (Informations LLDP-MED sur les périphériques locaux)

Dell OpenManage Switch Administrator | 10.240.3.147 | Switching > LLDP > LLDP-MED Local Device Information | PowerConnect G800

LLDP-MED Local Device Information [Print] [Refresh]

Unit: 1 | Port: 43

Network Policies Information:

Network Application	VLAN ID	Priority	DSCP	Unknown Bit Status	Tagged Bit Status
Voice	4	0	6	False	True

Extended PoE:

Device Type: PSE

Extended PoE PSE:

Available	10.00 Watts
Source	Primary
Priority	Critical

Cette page contient les champs suivants :

Port : sélectionnez l'unité et le port à utiliser pour afficher les données LLDP locales annoncées par le port. Cette liste déroulante contient uniquement les ports sur lesquels LLDP-MED est activé.

Network Policies Information (Informations sur les stratégies réseau) : si un TLV décrivant une stratégie réseau est présent dans les trames LLDP, les

informations suivantes s'affichent :

Network Application (Application réseau) : indique le type d'application qui est annoncé par le périphérique local dans la stratégie. Un port peut recevoir un ou plusieurs types, notamment les suivants :

- 1 unknown (inconnu)
- 1 voicesignaling
- 1 guestvoice
- 1 guestvoicesignaling
- 1 softphonevoice
- 1 videoconferencing
- 1 streamingvideo
- 1 videesignaling

Vlan Id (ID du VLAN) : indique l'ID de VLAN associé à un type spécifique de stratégie.

Priority (Priorité) : indique la priorité associée à un type spécifique de stratégie.

DSCP : indique le DSCP (Differentiated Services Code Point) associé à un type spécifique de stratégie.

Unknown Bit Status (État du bit inconnu) : indique l'état du bit inconnu associé à un type spécifique de stratégie.

Tagged Bit Status (État du bit balisé) : indique l'état du bit balisé associé à un type spécifique de stratégie.

Inventory (Inventaire) : si un TLV contenant des informations d'inventaire est présent dans les trames LLDP, les informations suivantes s'affichent :

Hardware Revisions (Niveau de révision du matériel) : indique la version du matériel.

Firmware Revisions (Niveau de révision du micrologiciel) : indique la version du micrologiciel.

Software Revisions (Niveau de révision du logiciel) : indique la version du logiciel.

Serial Number (Numéro de série) : indique le numéro de série.

Manufacturer Name (Nom du constructeur) : indique le nom du constructeur.

Model Name (Nom du modèle) : indique le nom du modèle.

Asset ID (ID d'inventaire) : indique l'ID d'inventaire.

Location Information (Informations d'emplacement) : si un TLV contenant des informations d'emplacement est présent dans les trames LLDP, les informations suivantes s'affichent :

Sub Type (Sous-type) : contient des informations sur le type d'emplacement.

Location Information (Informations d'emplacement) : contient une chaîne correspondant à l'ID d'un type d'emplacement donné.

Extended PoE (PoE étendu) : si le périphérique local est un périphérique PoE, les informations suivantes s'affichent :

Device Type (Type de périphérique) : indique le type du périphérique.

Extended PoE PSE (Périphérique PSE PoE étendu) : si un TLV contenant des informations sur un périphérique PSE étendu est présent dans la trame LLDP, les informations suivantes s'affichent :

Available (Disponible) : indique la puissance du périphérique PSE (en dixièmes de watts) qui est disponible sur le port du périphérique local.

Source : indique la source d'alimentation de ce port.

Priority (Priorité) : indique la priorité d'alimentation du port de l'équipement PSE.

Extended PoE PD (Périphérique alimenté PoE étendu) : si un TLV contenant des informations sur un périphérique alimenté étendu est présent dans la trame LLDP, les informations suivantes s'affichent :

Required (Requise) : indique la puissance requise (en dixièmes de watts) pour le périphérique sur le port du périphérique local.

Source : indique la source d'alimentation de ce port.

Priority (Priorité) : indique la priorité d'alimentation du port du périphérique d'alimentation.

Affichage d'informations LLDP-MED sur les périphériques locaux à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 LLDP Commands (Commandes LLDP)

Informations LLDP-MED sur les périphériques distants

La page **LLDP-MED Remote Device Information** (Informations LLDP-MED sur les périphériques distants) permet d'afficher les données LLDP annoncées par les périphériques distants.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **LLDP** → **LLDP-MED** → **LLDP-MED Remote Device Information** (Informations LLDP-MED sur les périphériques distants) dans l'arborescence.

Figure 7-8. Page LLDP-MED Remote Device Information (Informations LLDP-MED sur les périphériques distants)

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "LLDP-MED Remote Device Information". It includes a "Local Interface" dropdown menu set to "1/g3". Below this, there are sections for "Capability Information", "Display Network Policies", "Inventory Information", "Location Information", "Extended PoE", and "Extended PoE PD".

Capability Information

Supported Capabilities	Capabilities, Network Policy, Location, Extended PD, Inventory
Enabled Capabilities	Capabilities, Network Policy, Location, Extended PD, Inventory
Device Class	Endpoint Class III

Display Network Policies

Network Application	VLAN ID	Priority	DSCP	Unknown Bit Status	Tagged Bit Status
Voice	777	7	6	False	True

Inventory Information:

Hardware Revision	7.7.7.7
Firmware Revision	rrr rrr
Software Revision	software revision 4.5
Serial Number	serial number 777
Manufacturer Name	Broadcom Corp.
Model Name	Model XGS3
Asset ID	asset 1717

Location Information:

Sub Type	Location Information
ELIN	100777100777

Extended PoE:

Device Type	PD
-------------	----

Extended PoE PD:

Required	7.00 Watts
Source	Local
Priority	High

Cette page contient les champs suivants :

Local Interface (Interface locale) : indique la liste des ports sur lesquels LLDP-MED est activé.

Capability Information (Informations sur les capacités) : indique les capacités prises en charge et activées ayant été reçues dans un TLV MED sur ce port.

Supported Capabilities (Capacités prises en charge) : indique les capacités prises en charge ayant été reçues dans un TLV MED sur ce port.

Enabled Capabilities (Capacités activées) : indique les capacités activées ayant été reçues dans un TLV MED sur ce port.

Device Class (Classe de périphérique) : indique la classe de périphérique telle qu'elle est annoncée par le périphérique distant connecté au port.

Network Policy Information (Informations sur la stratégie réseau) : si un TLV contenant des informations sur une stratégie réseau est reçu dans les trames LLDP sur ce port, les informations suivantes s'affichent :

Network Application (Application réseau) : indique le type d'application qui est annoncé par le périphérique local dans la stratégie. Un port peut recevoir un ou plusieurs types d'application, notamment les suivants :

- 1 unknown (inconnu)
- 1 voicesignaling
- 1 guestvoice
- 1 guestvoicesignalling
- 1 softphonevoice
- 1 videoconferencing
- 1 streamingvideo
- 1 videesignalling

Vlan Id (ID du VLAN) : indique l'ID de VLAN associé à un type spécifique de stratégie.

Priority (Priorité) : indique la priorité associée à un type spécifique de stratégie.

DSCP : indique le DSCP (Differentiated Services Code Point) associé à un type spécifique de stratégie.

Unknown Bit Status (État du bit inconnu) : indique l'état du bit inconnu associé à un type spécifique de stratégie.

Tagged Bit Status (État du bit balisé) : indique l'état du bit balisé associé à un type spécifique de stratégie.

Inventory (Inventaire) : si un TLV contenant des informations d'inventaire est présent dans les trames LLDP, les informations suivantes s'affichent :

Hardware Revisions (Niveau de révision du matériel) : indique la version du matériel utilisé par le périphérique distant.

Firmware Revisions (Niveau de révision du micrologiciel) : indique la version du micrologiciel utilisé par le périphérique distant.

Software Revisions (Niveau de révision du logiciel) : indique la version du logiciel utilisé par le périphérique distant.

Serial Number (Numéro de série) : indique le numéro de série du périphérique distant.

Manufacturer Name (Nom du constructeur) : indique le nom du constructeur du périphérique distant.

Model Name (Nom du modèle) : indique le nom de modèle du périphérique distant.

Asset ID (ID d'inventaire) : indique l'ID d'inventaire du périphérique distant.

Location Information (Informations d'emplacement) : si un TLV contenant des informations d'emplacement est présent dans les trames LLDP, les informations suivantes s'affichent :

Sub Type (Sous-type) : contient des informations sur le type d'emplacement.

Location Information (Informations d'emplacement) : contient une chaîne correspondant à l'ID d'un type d'emplacement donné.

Extended PoE (Périphérique PoE étendu) : indique si le périphérique distant est un périphérique PoE.

Device Type (Type de périphérique) : indique le type PoE du périphérique distant connecté à ce port.

Extended PoE PSE (Périphérique PSE PoE étendu) : si un TLV contenant des informations sur un périphérique PSE étendu est présent dans la trame LLDP reçue sur ce port, les informations suivantes s'affichent :

Available (Disponible) : indique la puissance du périphérique PSE (en dixièmes de watts) associé au port distant.

Source : indique la source d'alimentation du périphérique PSE associé au port distant.

Priority (Priorité) : indique la priorité d'alimentation du périphérique PSE associé au port distant.

Extended PoE PD (Périphérique alimenté PoE étendu) : si un TLV contenant des informations sur un périphérique alimenté étendu est présent dans la trame LLDP reçue sur ce port, les informations suivantes s'affichent :

Required (Requise) : indique la puissance requise par le périphérique alimenté associé au port distant.

Source : indique la source d'alimentation du port distant.

Priority (Priorité) : indique la priorité d'alimentation du périphérique alimenté associé au port distant.

Affichage d'informations LLDP-MED sur un périphérique distant à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 LLDP Commands (Commandes LLDP)

Configuration des ports d'un VLAN voix

La fonction de VLAN voix permet aux ports de commutation de transmettre le trafic correspondant aux données vocales en fonction d'une priorité prédéfinie. Le niveau de priorité permet de séparer le trafic lié aux données entrant sur le port de celui lié à la voix. L'utilisation d'un VLAN voix permet notamment d'éviter la dégradation pouvant affecter la qualité des communications des téléphones IP lorsque le trafic de données entrant sur un port est très important. Le système utilise l'adresse MAC source du trafic qui transite sur le port pour identifier le flux de données lié au téléphone IP.

La page **Voice VLAN** (VLAN voix) contient un lien qui permet de configurer les paramètres du VLAN, tant au niveau global qu'en ce qui concerne les ports utilisés pour les données vocales.

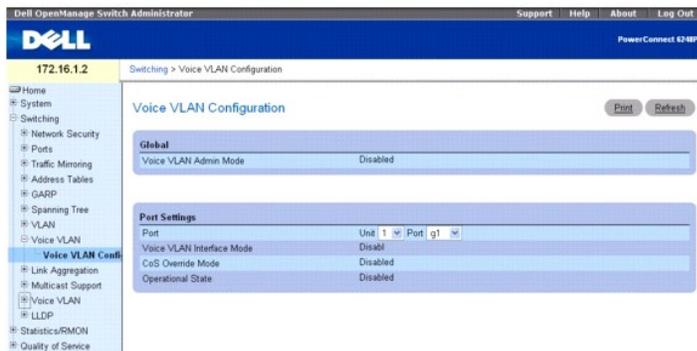
Configuration d'un VLAN voix

La page **Voice VLAN Configuration** (Configuration d'un VLAN voix) permet de configurer et d'afficher les paramètres du VLAN voix qui s'appliquent à l'intégralité du système et à des interfaces spécifiques.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Voice VLAN** (VLAN voix) → **Voice VLAN Configuration** (Configuration d'un VLAN voix) dans

l'arborescence.

Figure 7-9. Page Voice VLAN Configuration (Configuration d'un VLAN voix)



Cette page contient les champs suivants :

Voice VLAN Admin Mode (Mode d'administration du VLAN voix) : utilisez le menu déroulant pour sélectionner le mode d'administration du commutateur pour le VLAN voix. La valeur par défaut est Disable (Désactiver).

Port : sélectionnez l'interface à afficher ou à configurer.

Voice VLAN Interface Mode (Mode d'interface du VLAN voix) : sélectionnez le mode du VLAN voix pour l'interface sélectionnée. La valeur par défaut est Disable (Désactiver). Le mode peut être l'un des suivants :

Disable (Désactiver) : le VLAN voix est désactivé sur le port.

None (Aucun) : autorise le téléphone IP à utiliser sa propre configuration pour l'envoi d'un trafic vocal non balisé.

VLAN ID (ID du VLAN) : permet de configurer la définition des balises VLAN pour le trafic vocal. Les ID de VLAN pouvant être utilisés vont de 1 à 4093.

dot1p : permet de définir la priorité du trafic vocal au moyen de balises VLAN 802.1p. Les balises de priorité pouvant être utilisées vont de 0 à 7.

Untagged (Non balisé) : le téléphone est configuré pour envoyer un trafic vocal non balisé.

CoS Override Mode (Mode d'écrasement CoS) : permet de sélectionner le mode d'écrasement CoS pour l'interface sélectionnée. La valeur par défaut est Disable (Désactiver).

Operational State (État de fonctionnement) : état de fonctionnement du VLAN voix sur une interface donnée.

Configuration des paramètres d'un VLAN voix

1. Affichez la page **Voice VLAN Configuration** (Configuration d'un VLAN voix).
2. Configurez les paramètres pour l'ensemble du système ou pour chaque port.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont modifiés et le périphérique est mis à jour.

Configuration d'un VLAN voix à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Voice VLAN Commands (Commandes portant sur les VLAN voix)

[Retour au sommaire](#)

[Retour au sommaire](#)

Configuration des paramètres de commutation

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Configuration de la sécurité du réseau](#)
- [Configuration des ports](#)
- [Configuration de la mise en miroir du trafic](#)
- [Configuration des tables d'adresses](#)
- [Configuration du protocole GARP](#)
- [Configuration du protocole Spanning Tree](#)
- [Configuration des VLAN](#)
- [Agrégation de ports](#)
- [Prise en charge de la transmission multidiffusion](#)
- [Configuration du protocole LLDP](#)

Cette section contient des informations concernant le fonctionnement du système, la sécurité du réseau, les ports, les tables d'adresses, les protocoles GARP et STP (Spanning Tree), l'agrégation des ports et la prise en charge de la transmission multidiffusion.

La page de menu **Switching** (Commutation) contient des liens vers les fonctionnalités suivantes :

- 1 [Configuration de la sécurité du réseau](#)
- 1 [Configuration des ports](#)
- 1 [Configuration de la mise en miroir du trafic](#)
- 1 [Configuration des tables d'adresses](#)
- 1 [Configuration du protocole GARP](#)
- 1 [Configuration du protocole Spanning Tree](#)
- 1 [Configuration des VLAN](#)
- 1 [Agrégation de ports](#)
- 1 [Prise en charge de la transmission multidiffusion](#)
- 1 [Configuration du protocole LLDP](#)

Configuration de la sécurité du réseau

La page **Network Security** (Sécurité réseau) permet de définir la sécurité réseau grâce à l'authentification basée sur les ports, le verrouillage des ports, la configuration du filtrage DHCP et les listes de contrôle d'accès.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Network Security** (Sécurité réseau) dans l'arborescence.

Cette page contient des liens vers les fonctionnalités suivantes :

- 1 [Authentification basée sur les ports](#)
- 1 [Hôtes multiples](#)
- 1 [Utilisateurs authentifiés](#)
- 1 [Verrouillage des ports](#)
- 1 [Filtrage DHCP](#)
- 1 Listes de contrôle d'accès
- 1 [Configuration de liaisons pour les ACL](#)

Authentification basée sur les ports

En mode d'authentification basée sur les ports, lorsque le protocole 802.1x est activé de façon globale et sur le port, l'authentification réussie d'un demandeur relié au port donne à tous les autres utilisateurs la possibilité d'utiliser le port sans restriction. Un seul demandeur est autorisé à tenter de s'authentifier sur un port donné à tout moment. Les ports fonctionnant dans ce mode sont sous contrôle bidirectionnel. Il s'agit du mode d'authentification par défaut.

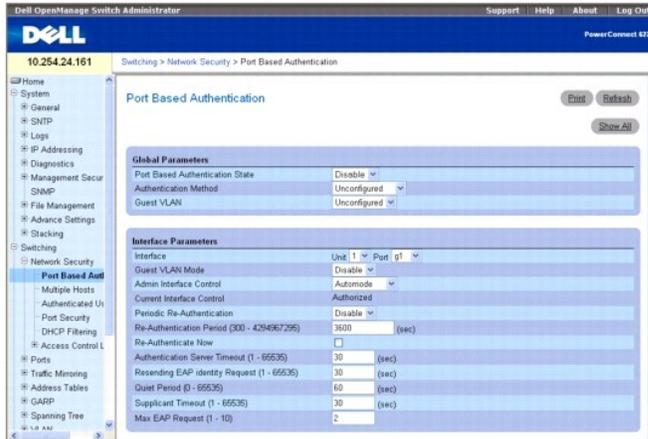
Le réseau 802.1x se compose de trois éléments :

- 1 **Authenticators** (Authentificateurs) : indique le port authentifié avant d'autoriser l'accès au système.
- 1 **Supplicants** (Demandeurs) : indique l'hôte connecté au port authentifié demandant l'accès aux services du système.
- 1 **Authentication Server** (Serveur d'authentification) : indique le serveur externe, par exemple, le serveur RADIUS qui effectue l'authentification pour le compte de l'authentificateur, et indique si l'utilisateur est autorisé à accéder aux services du système.

La page **Port Based Authentication** (Authentification basée sur les ports) permet de configurer les paramètres 802.1x généraux d'un port.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Network Security** (Sécurité réseau) → **Port Based Authentication** (Authentification basée sur les ports) dans l'arborescence.

Figure 8-1. Page Port Based Authentication (Authentification basée sur les ports)



Cette page contient les champs suivants :

Paramètres globaux

Port Based Authentication State (État de l'authentification basée sur les ports) : active l'authentification basée sur les ports au niveau du commutateur. Les valeurs possibles sont les suivantes :

Enable (Activer) : active l'authentification basée sur les ports au niveau du commutateur.

Disable (Désactiver) : désactive l'authentification basée sur les ports au niveau du commutateur.

Authentication Method (Méthode d'authentification) : sélectionne la méthode d'authentification utilisée. Les valeurs possibles sont les suivantes :

Unconfigured (Non configuré) : indique qu'aucune méthode d'authentification n'a été sélectionnée.

None (Aucune) : indique qu'aucune méthode d'authentification n'est utilisée.

RADIUS : indique que l'authentification est effectuée au niveau du serveur RADIUS.

RADIUS, None (RADIUS, aucune) : indique que l'authentification est effectuée au niveau du serveur RADIUS. Si le serveur RADIUS n'est pas disponible, aucune méthode d'authentification n'est utilisée.

None, RADIUS (Aucune, RADIUS) : indique qu'aucune méthode d'authentification n'est utilisée. Si une authentification est requise, elle est effectuée au niveau du serveur RADIUS.

Guest VLAN (VLAN invité) : définit un VLAN invité pour l'ensemble des ports. Les valeurs possibles sont les suivantes :

Unconfigured (Non configuré) : le VLAN invité n'est pas configuré pour l'ensemble des ports.

VLAN ID (ID des VLAN) : indique l'identificateur des VLAN configurés sur le système. Sélectionnez le VLAN à utiliser en tant que VLAN invité pour l'ensemble des ports.

Paramètres de l'interface

Interface : sélectionne l'unité et le port à affecter.

Guest VLAN Mode (Mode VLAN invité) : active ou désactive le mode VLAN invité sur cette interface.

Admin Interface Control (Contrôle de l'interface d'administration) : définit l'état d'autorisation des ports. Les valeurs possibles sont les suivantes :

Automode (Mode automatique) : détecte automatiquement le mode de l'interface.

Authorized (Autorisé) : place l'interface à l'état autorisé sans l'authentifier. L'interface envoie et reçoit normalement le trafic ; aucune authentification basée sur les ports n'est effectuée sur le client.

Unauthorized (Non autorisé) : refuse l'accès au système d'interface sélectionné, en passant cette interface sur l'état "non autorisé". Le commutateur ne peut pas fournir de services d'authentification au client via cette interface.

Current Interface Control (Contrôle actuel de l'interface) : affiche l'état actuel de l'autorisation pour le port.

Periodic Re-Authentication (Ré-authentification périodique) : lorsque cette option est activée, le port sélectionné est ré-authentifié régulièrement.

Re-Authentication Period (300-4294967295) (Période de ré-authentification, 300-4294967295) : indique le délai au terme duquel le port sélectionné est ré-authentifié. La valeur de ce champ est exprimée en secondes. La valeur par défaut est de 3600 secondes.

Re-Authenticate Now (Ré-authentifier maintenant) : lorsque cette option est sélectionnée, le port est immédiatement ré-authentifié.

Authentication Server Timeout (1-65535) (Délai d'authentification du serveur, 1-65535) : définit le délai qui s'écoule avant que le commutateur renvoie une requête au serveur d'authentification. La valeur de ce champ est exprimée en secondes. La valeur par défaut est de 30 secondes.

Resending EAP Identity Request (1-65535) (Renvoi d'une requête d'identité EAP, 1-65535) : définit le délai qui s'écoule avant le renvoi de requêtes EAP. La valeur de ce champ est exprimée en secondes. La valeur par défaut est de 30 secondes.

Quiet Period (1-65535) (Période de latence, 1-65535 secondes) : définit le délai de latence du commutateur après l'échec d'une authentification. Les valeurs possibles vont de 1 à 65535. La valeur de ce champ est exprimée en secondes. La valeur par défaut est de 60 secondes.

Supplicant Timeout (0-65535) (Délai pour le demandeur, 0-65535 secondes) : définit le délai qui s'écoule avant que les requêtes EAP soient renvoyées à l'utilisateur. La valeur de ce champ est exprimée en secondes. La valeur par défaut est de 30 secondes.

Max EAP Requests (1-10) (Nombre maximal de requêtes EAP, 1-10) : définit le nombre maximal d'envoi d'une requête EAP que le commutateur peut effectuer avant de relancer le processus d'authentification, s'il ne reçoit pas de réponse. Les valeurs possibles vont de 1 à 10. La valeur par défaut est de 2 tentatives.

Affichage de la table d'authentification basée sur les ports

1. Affichez la page **Port Based Authentication** (Authentification basée sur les ports).
2. Cliquez sur **Show All** (Afficher tout).

La page **Port Based Authentication Table** (Table d'authentification basée sur les ports) s'affiche.

Figure 8-2. Page Port Based Authentication Table (Table d'authentification basée sur les ports)

Ports	Admin Port Control	Current Port Control	Periodic Re-Authentication	Re-Authentication Period	Re-Authenticate Now	On
1 1/ig1	Authenticate	Authorized	Disable	3000	<input type="checkbox"/>	OK
2 1/ig2	Authenticate	Authorized	Disable	3000	<input type="checkbox"/>	OK
3 1/ig3	Authenticate	Authorized	Disable	3000	<input type="checkbox"/>	OK
4 1/ig4	Authenticate	Authorized	Disable	3000	<input type="checkbox"/>	OK
5 1/ig5	Authenticate	Authorized	Disable	3000	<input type="checkbox"/>	OK

3. Utilisez la barre de défilement horizontale ou cliquez sur la flèche vers la droite située au bas de l'écran pour afficher la partie droite de la table.
4. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **Port Based Authentication Table** (Table d'authentification basée sur les ports) pour les autres unités de la pile, le cas échéant.

Ré-authentification d'un port

1. Affichez la page **Port Based Authentication** (Authentification basée sur les ports).
2. Sélectionnez **Edit** (Modifier) pour choisir l'unité/le port à ré-authentifier.
3. Cochez **Reauthenticate Now** (Ré-authentification immédiate).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port spécifié est ré-authentifié et le périphérique est mis à jour.

Ré-authentification de plusieurs ports inclus dans la table d'authentification basée sur les ports

1. Affichez la page **Port Based Authentication** (Authentification basée sur les ports).
 2. Cliquez sur **Show All** (Afficher tout).
- La page **Port Based Authentication Table** (Table d'authentification basée sur les ports) s'affiche.
3. Sélectionnez **Edit** (Modifier) pour choisir les unités/les ports à ré-authentifier.
 4. Pour définir une ré-authentification périodique, réglez le paramètre **Periodic Re-Authentication** (Ré-authentification périodique) sur **Enable** (Activer). Renseignez ensuite le champ **Re-Authentication Period** (Délai de ré-authentification) pour tous les ports souhaités.

5. Pour activer une ré-authentification immédiate, cochez l'option **Reauthenticate Now** (Ré-authentification immédiate) correspondant à chaque port à ré-authentifier.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les ports spécifiés sont ré-authentifiés (soit immédiatement, soit périodiquement) et le périphérique est mis à jour.

Modification du contrôle administratif des ports

1. Affichez la page **Port Based Authentication** (Authentification basée sur les ports).
2. Cliquez sur **Show All** (Afficher tout).

La page **Port Based Authentication Table** (Table d'authentification basée sur les ports) s'affiche.

3. Accédez à la partie droite de la table et cochez la case **Edit** (Modifier) pour chaque port à configurer. Modifiez le champ **Admin Port Control** (Contrôle administratif des ports) en sélectionnant **Authorized** (Autorisé), **Unauthorized** (Non autorisé) ou **Automode** (Mode automatique) selon le cas, pour les ports sélectionnés. Seul le mode automatique utilise dot1x pour l'authentification. Les paramètres **Authorized** (Autorisé) et **Unauthorized** (Non autorisé) requièrent un remplacement manuel.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le contrôle administratif est actualisé pour les ports sélectionnés et le périphérique est mis à jour.

Activation de l'authentification basée sur les ports à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 802.1X Commands (Commandes 802.1x)

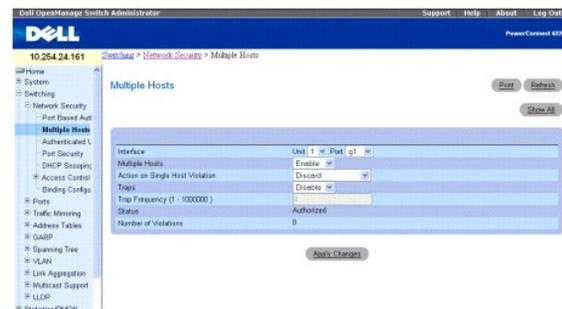
Hôtes multiples

Lorsqu'un port est en mode Hôtes multiples, l'authentification d'un seul commutateur suffit. Une fois l'authentification réussie, tout commutateur connecté à ce port peut accéder au réseau. Si pour une raison quelconque, le port devient non autorisé, tous les commutateurs perdent l'accès au réseau. Le processus d'authentification doit alors recommencer.

La page **Multiple Hosts** (Hôtes multiples) fournit des informations permettant de définir des paramètres d'authentification avancés pour des ports spécifiques.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Network Security** (Sécurité réseau) → **Multiple Host** (Hôtes multiples) dans l'arborescence.

Figure 8-3. Page **Multiple Hosts** (Hôtes multiples)



Cette page contient les champs suivants :

Interface : indique l'unité et les numéros des ports sur lesquels les paramètres d'authentification avancés basés sur les ports doivent être définis.

Multiple Hosts (Hôtes multiples) : active ou désactive un hôte unique afin d'autoriser plusieurs hôtes à accéder au système. Ce paramètre doit être activé pour que vous puissiez désactiver le filtre en entrée ou utiliser la fonction de verrouillage sur le port sélectionné.

Action on Single Host Violation (Action si violation en mode hôte unique) : définit l'action à appliquer aux paquets reçus en mode hôte unique à partir d'un hôte dont l'adresse MAC n'est pas celle du client (demandeur). Les valeurs possibles sont les suivantes :

Forward (Transmettre) : transmet les paquets provenant d'une source inconnue. Toutefois, l'adresse MAC n'est pas apprise.

Discard (Rejeter) : rejette les paquets provenant d'une source inconnue. Il s'agit de la valeur par défaut.

Discard Shutdown (Rejeter, Fermer) : rejette le paquet provenant d'une source inconnue et ferme le port. Le port reste désactivé jusqu'à sa réactivation ou jusqu'à la prochaine réinitialisation du commutateur.

Traps (Interruptions) : active ou désactive l'envoi d'interruptions vers l'hôte en cas de violation.

Trap Frequency (1-1000000) (Fréquence des interruptions, 1-1000000) : définit la fréquence d'envoi des interruptions à l'hôte. La valeur par défaut est de 10 secondes. L'interruption de sécurité est envoyée toutes les 10 secondes, avec un décompte du nombre de violations.

Status (État) : affiche l'état de l'hôte. Les valeurs possibles sont les suivantes :

Authorized (Autorisé) : indique que le contrôle du port est défini sur le mode automatique et que les clients peuvent accéder au port sans restriction.

Unauthorized (Non autorisé) : Indique que le contrôle du port est défini sur *Force Unauthorized* (Forcé sur non autorisé) ou sur *Auto*, ou bien que la liaison associée à ce port est désactivée, et qu'un client n'a pas été authentifié via ce port.

Not in auto mode (Pas en mode automatique) : indique que le contrôle du port est défini sur *Forced Authorized* (Forcé sur autorisé) et que les clients peuvent accéder au port sans restriction.

Single-host Lock (Verrouillage hôte unique) : indique que le contrôle du port est défini sur *Auto* et qu'un client unique a été authentifié via le port.

No Single Host (Hôte unique désactivé) : indique que le mode *Multiple Host* (Hôtes multiples) est activé.

Number of Violations (Nombre de violations) : affiche le nombre de paquets reçus sur l'interface en mode hôte unique et provenant d'un hôte dont l'adresse MAC n'est pas celle du client (demandeur).

Affichage de la table **Multiple Hosts** (Hôtes multiples)

1. Affichez la page **Multiple Hosts** (Hôtes multiples).
2. Cliquez sur **Show All** (Afficher tout).

La table **Multiple Host** (Hôtes multiples) s'affiche.

Figure 8-4. Page Multiple Host Table (Table des hôtes multiples)

Port	Enable Multiple Hosts	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations	Edit
1 1/ig1	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
2 1/ig2	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
3 1/ig3	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
4 1/ig4	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>

10 1/ig0	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
11 1/ig1	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
12 1/ig2	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
13 1/ig3	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>
14 1/ig4	Enable	Discard	Disable	0	Authorized	0	<input type="checkbox"/>

3. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **Multiple Host Table** (Table des hôtes multiples) pour les autres unités de la pile, le cas échéant.

Activation/Désactivation du mode **Hôtes multiples** pour un port

1. Affichez la page **Multiple Hosts** (Hôtes multiples).
2. Sélectionnez l'unité et le port à affecter dans le champ **Interface**.
3. Définissez les variables voulues.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mode **Hôtes multiples** est activé pour le port spécifié et le périphérique est mis à jour.

Activation/Désactivation du mode **Hôtes multiples** pour plusieurs ports

1. Affichez la page **Multiple Hosts** (Hôtes multiples).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Multiple Host Table** (Table des hôtes multiples).

- Sélectionnez la case Edit (Modifier) située en regard des ports que vous souhaitez configurer.
- Modifiez les variables correspondant aux ports voulus.
- Cliquez sur **Apply Changes** (Appliquer les modifications).

Les ports modifiés sont actualisés et le périphérique est mis à jour.

Configuration de l'authentification avancée d'un port à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

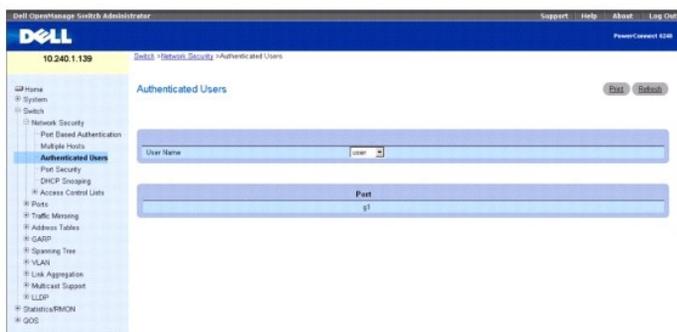
- 802.1X Commands (Commandes 802.1X)

Utilisateurs authentifiés

La page **Authenticated Users** (Utilisateurs authentifiés) affiche des listes d'utilisateurs autorisés à accéder au port.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Network Security** (Sécurité réseau) → **Authenticated Users** (Utilisateurs authentifiés) dans l'arborescence.

Figure 8-5. Page Authenticated Users (Utilisateurs authentifiés)



La page **Authenticated Users** (Utilisateurs authentifiés) contient les champs suivants :

User Name (Nom d'utilisateur) : identifie un utilisateur inclus dans la liste des personnes autorisées via le serveur RADIUS.

Port : indique le port utilisé pour l'authentification.

Affichage des utilisateurs authentifiés à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 802.1X Commands (Commandes 802.1X)

Verrouillage des ports

Le verrouillage des ports peut être activé pour chaque port individuel. Lorsqu'un port est verrouillé, seuls les paquets dont les adresses MAC source sont autorisées peuvent être transmis. Tous les autres paquets sont rejetés. Une adresse MAC peut être définie comme autorisée grâce à deux méthodes : dynamiquement ou statiquement. Lorsqu'un port est verrouillé, ces deux méthodes sont utilisées simultanément.

Le verrouillage dynamique active un mécanisme de type "premier arrivé". Vous spécifiez le nombre d'adresses pouvant être apprises sur le port verrouillé. Si la limite n'a pas été atteinte, un paquet associé à une adresse MAC source inconnue est appris et transmis normalement. Une fois la limite atteinte, le port n'apprend plus aucune adresse. Tout paquet dont l'adresse MAC source n'a pas été apprise est alors rejeté. Vous pouvez désactiver le verrouillage dynamique en définissant le nombre d'entrées dynamiques autorisées sur zéro.

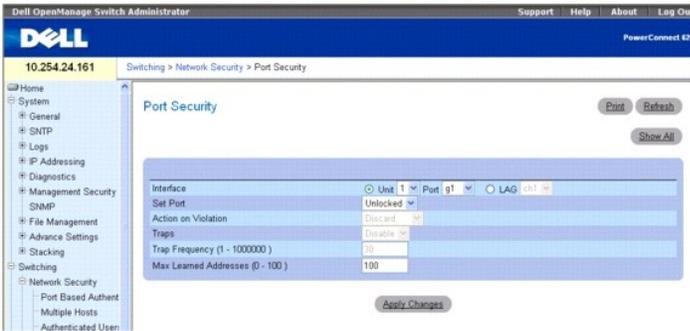
Le verrouillage statique permet de définir la liste des adresses MAC autorisées sur un port. Le comportement des paquets est identique à celui du verrouillage dynamique : seuls les paquets dont l'adresse MAC source est autorisée peuvent être transmis.

Pour visualiser les adresses MAC apprises sur un port spécifique, ajouter une adresse MAC statique à un port ou supprimer des adresses MAC statiques, voir [Configuration des tables d'adresses](#).

Les ports désactivés ne peuvent être réactivés qu'à partir de la page **Configuring Ports** (Configuration des ports).

Pour afficher la page **Port Security** (Verrouillage des ports), cliquez sur **Switching** (Commutation) → **Network Security** (Sécurité réseau) → **Port Security** (Verrouillage des ports) dans l'arborescence.

Figure 8-6. Page Port Security (Verrouillage des ports)



Interface : sélectionne l'unité et le port ou le LAG sur lesquels les paramètres de verrouillage des ports doivent être configurés.

Set Port (Définir le port) : active le verrouillage du port ou LAG. Lorsqu'un port est verrouillé, toutes les adresses en cours qui ont été apprises de façon dynamique par le commutateur sur ce port sont supprimées de la base de données.

Action on Violation (Action si violation) : définit l'action à appliquer aux paquets qui arrivent sur le port/LAG. Le champ est grisé si le port/LAG est déverrouillé. Ce champ peut prendre les valeurs suivantes :

Discard (Rejeter) : rejette les paquets provenant d'une source inconnue. Il s'agit de la valeur par défaut.

Forward (Transmettre) : transmet les paquets provenant d'une source inconnue. L'adresse MAC n'est pas apprise.

Shutdown (Fermer) : rejette le paquet provenant d'une source inconnue et envoie une interruption. En outre, le port d'entrée est désactivé.

Traps (Interruptions) : active ou désactive l'envoi d'une interruption lorsqu'un paquet est reçu sur un port/LAG verrouillé.

Trap Frequency (1-1000000) (Fréquence des interruptions, 1-1000000) : définit le délai (en secondes) entre deux interruptions.

Max Learned Addresses (1-100) (Nombre maximal d'adresses apprises, 1-100) : définit le nombre maximal d'adresses MAC sécurisées pouvant être apprises sur un port.

Définition d'un port verrouillé

1. Affichez la page **Port Security** (Verrouillage des ports).
2. Sélectionnez un type et un numéro d'interface.
3. Sélectionnez **Locked** (Verrouillé) dans le menu déroulant **Set Port** (Définir le port).
4. Complétez les autres champs.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port/LAG verrouillé est ajouté à la table Port Security (Verrouillage des ports) et le périphérique est mis à jour.

Affichage de la table Port Security (Verrouillage des ports)

1. Affichez la page **Port Security** (Verrouillage des ports).
2. Cliquez sur **Show All** (Afficher tout).

La table **Port Security** (Verrouillage des ports) s'affiche.

Figure 8-7. Page Port Security Table (Table de verrouillage des ports)

Port Security Table Print Refresh

Unit 1

Ports	Current Port Control	Set Port	Set Port Action	Trap	Trap Frequency	Edit
1 1/g1	Link Up	Unlock	Discard	Disable	30	
2 1/g2	Link Down	Unlock	Discard	Disable	30	
3 1/g3	Link Up	Unlock	Discard	Disable	30	

26 1/rq2	Link Down	Unlock	Discard	Disable	30	
27 1/rq3	Link Down	Unlock	Discard	Discard	30	
28 1/rq4	Link Down	Unlock	Discard	Discard	30	

Apply Changes Back

- Utilisez le menu déroulant Unit (Unité) pour afficher la page Port Security Table (Table de verrouillage des ports) pour les autres unités de la pile, le cas échéant.

Définition de plusieurs ports verrouillés

- Affichez la page **Port Security** (Verrouillage des ports).
 - Cliquez sur **Show All** (Afficher tout).
- La table **Port Security** (Verrouillage des ports) s'affiche.
- Cliquez sur **Edit** (Modifier) pour chaque port dont les paramètres doivent être modifiés.
 - Les champs peuvent maintenant être modifiés selon vos besoins.
 - Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications sont apportées à la table et le périphérique est mis à jour.

Configuration du verrouillage des ports à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

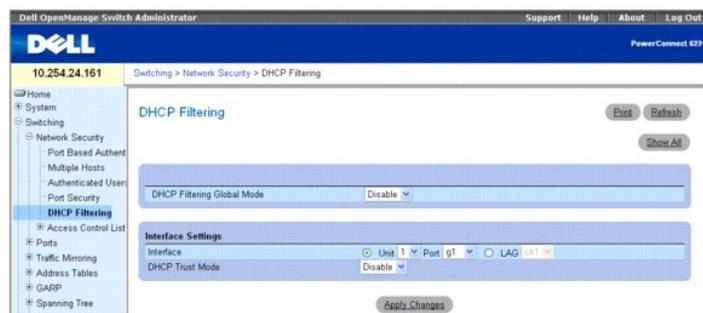
- Address Table Commands (Commandes portant sur les tables d'adresses)

Filtrage DHCP

Le filtrage DHCP peut être employé comme mesure de protection contre les serveurs DHCP non autorisés. Un serveur DHCP non autorisé répondant à un client qui demande une adresse IP constitue un type d'attaque connue. Le serveur configure la passerelle du client de sorte que celle-ci soit identique à l'adresse IP du serveur. Le client envoie alors tout le trafic IP destiné à d'autres réseaux à la machine non autorisée. Cela permet à l'attaquant d'intercepter le trafic pour se procurer des mots de passe ou de procéder à une attaque de type "homme au milieu" (MITM, "man in the middle"). Le filtrage DHCP permet à l'administrateur de définir chaque port en tant que port de confiance ou port non fiable. Le port relié au serveur DHCP autorisé doit être configuré comme port de confiance. Toute réponse DHCP reçue sur un port de confiance sera donc transmise. Tous les autres ports devront être configurés comme des ports non fiables. Toute réponse DHCP (ou BootP) reçue sera alors rejetée.

Pour afficher la page **DHCP Filtering** (Filtrage DHCP), cliquez sur **Switching** (Commutation) → **Network Security** (Sécurité réseau) → **DHCP Filtering** (Filtrage DHCP) dans l'arborescence.

Figure 8-8. Page DHCP Filtering (Filtrage DHCP)



Cette page contient les champs suivants :

DHCP Filtering Global Mode (Mode global de filtrage DHCP) : active et désactive le filtrage DHCP. Le paramètre par défaut est Disabled (Désactivé).

Interface : indique l'unité et le port ou le LAG affectés. Choisissez l'unité et le port/LAG voulus dans les menus déroulants.

DHCP Trust Mode (Mode de confiance DHCP) : active ou désactive le mode de confiance. La valeur par défaut est Disabled (Désactivé).

Ajout du filtrage DHCP

1. Affichez la page **DHCP Filtering** (Filtrage DHCP).
2. Indiquez l'**interface** ou le **LAG** à affecter.
3. Définissez les paramètres voulus dans les champs **DHCP Filtering Global Mode** (Mode global de filtrage DHCP) et **DHCP Filtering Trust Mode** (Mode de confiance du filtrage DHCP).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le périphérique est mis à jour.

Affichage de la table de configuration des interfaces de filtrage DHCP

1. Affichez la page **DHCP Filtering** (Filtrage DHCP).
2. Cliquez sur **Show All** (Afficher tout).

La page **DHCP Filtering Table** (Table de filtrage DHCP) affiche tous les ports, les unités sur lesquelles ils se trouvent et le **mode de confiance DHCP** correspondant.

Figure 8-9. DHCP Filtering Interface Configuration Table (Table de configuration de l'interface du filtrage DHCP)

DHCP Filtering - Interface Configuration Table

Unit: 1

	Port	DHCP Trust Mode	Edit
1	1/sg1	<input type="checkbox"/>	<input type="checkbox"/>
2	1/sg2	<input type="checkbox"/>	<input type="checkbox"/>
3	1/sg3	<input type="checkbox"/>	<input type="checkbox"/>

26	1/sg2	<input type="checkbox"/>	<input type="checkbox"/>
27	1/sg3	<input type="checkbox"/>	<input type="checkbox"/>
28	1/sg4	<input type="checkbox"/>	<input type="checkbox"/>

Apply Changes Back

3. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **DHCP Filtering Table** (Table de filtrage DHCP) pour les autres unités de la pile, le cas échéant.

Configuration du filtrage DHCP sur plusieurs ports

1. Affichez la page **DHCP Filtering** (Filtrage DHCP).
2. Cliquez sur **Show All** (Afficher tout).

La page **DHCP Filtering Interface Configuration Table** (Table de configuration de l'interface du filtrage DHCP) s'affiche.

3. Cliquez sur **Edit** (Modifier) pour chaque port à configurer.
4. Activez ou désactivez le champ **DHCP Trust Mode** (Mode de confiance DHCP) pour chaque port selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications sont apportées à la table et le périphérique est mis à jour.

Configuration du filtrage DHCP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

Configuration des ACL IP

Les listes de contrôle d'accès (ACL) permettent aux administrateurs réseau de définir des actions et des règles de classification pour des ports d'entrée spécifiques. Votre commutateur prend en charge jusqu'à 100 ACL. Toutefois, les ressources matérielles étant limitées, il est possible que le système ne puisse pas prendre en charge 100 listes complètes.

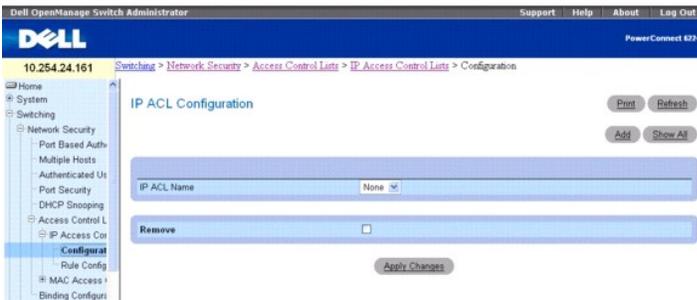
Les paquets peuvent être filtrés en entrée. Le filtrage détermine les actions devant être lancées : rejet du paquet ou désactivation du port, par exemple. Par exemple, un administrateur réseau peut définir une règle d'ACL indiquant que le port numéro 20 peut recevoir des paquets TCP. Cependant, si un paquet UDP est reçu, il est rejeté.

Les ACL se composent d'ACE (access control entries), c'est-à-dire de règles définissant les filtres utilisés pour la classification du trafic. Le nombre total de règles pouvant être définies pour chaque ACL est de 10.

La page **IP ACL Configuration** (Configuration des ACL IP) permet d'ajouter ou de supprimer des listes de contrôle d'accès basées sur les paramètres IP.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Network Security** (Sécurité réseau) → **Access Control Lists** (Listes de contrôle d'accès) → **IP Access Control Lists** (Listes de contrôle d'accès IP) → **Configuration** dans l'arborescence.

Figure 8-10. Page IP ACL Configuration (Configuration des ACL IP)



Cette page contient les champs suivants :

IP ACL Name (Nom de l'ACL IP) : indique le nom défini par l'utilisateur pour la liste de contrôle d'accès.

Remove (Supprimer) : retire les ACL IP sélectionnées dans le champ IP ACL.

Ajout d'une ACL basée sur les adresses IP

1. Affichez la page **IP ACL Configuration** (Configuration des ACL IP).
2. Cliquez sur **Add** (Ajouter).

La page **Add IP ACL** (Ajouter une ACL IP) s'affiche.

Figure 8-11. Page Add IP ACL (Ajouter une ACL basée sur les adresses IP)



3. Entrez le nom voulu pour la liste dans le champ **ACL Name** (Nom de l'ACL).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La liste ACL basée sur les adresses IP est ajoutée et le périphérique est mis à jour.

Suppression d'une ACL basée sur les paramètres IP

1. Affichez la page **IP ACL Configuration** (Configuration des ACL IP) et sélectionnez les ACL à supprimer dans le menu déroulant **IP ACL** (ACL IP).
2. Cochez la case **Remove ACL** (Supprimer une ACL).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La liste ACL basée sur les adresses IP est supprimée et le périphérique est mis à jour.

Affichage des ACL IP

1. Affichez la page **IP ACL Configuration** (Configuration des ACL IP).
2. Cliquez sur **Show All** (Afficher tout).

Toutes les listes de contrôle d'accès basées sur les paramètres IP et les données correspondantes s'affichent dans la table.

Figure 8-12. Table IP ACL (ACL IP)

IP ACL Name	Rules	Direction	Interface	VLAN
1 ACL1	1	NONE	NONE	
2 ACL2	1	NONE	NONE	

Ajout d'une ACL IP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. ACL Commands (Commandes ACL)

Configuration de règles pour les ACL IP

La page **IP ACL Rule Configuration** (Configuration de règles pour les ACL IP) permet de définir des règles pour les listes de contrôle d'accès basées sur les paramètres IP. La définition des listes d'accès inclut des règles indiquant si les paquets répondant aux critères définis doivent être rejetés ou transmis. Vous pouvez également choisir d'affecter le trafic à une file d'attente particulière, définir des filtres pour certains types de trafic, modifier la balise de VLAN, fermer un port et/ou rediriger le trafic vers un port spécifique.

➡ **AVIS :** Une règle implicite "deny all" figure à la fin de chaque ACL. Cela signifie que si aucune des règles explicites n'est vérifiée lorsqu'une ACL est appliquée à un paquet, la dernière règle implicite "deny all" est utilisée et le paquet est rejeté.

Pour afficher la page **IP ACL Rule Configuration** (Configuration de règles pour les ACL IP), cliquez sur **Switching** (Commutation) → **Network Security** (Sécurité réseau) → **Access Control Lists** (Listes de contrôle d'accès) → **IP Access Control Lists** (Listes de contrôle d'accès IP) → **Rule Configuration** (Configuration des règles) dans l'arborescence.

Figure 8-13. Page IP ACL - Rule Configuration (Configuration de règles pour les ACL IP) - Version standard

The screenshot shows the 'IP ACL - Rule Configuration' page in the Dell OpenManage Switch Administrator. The interface includes a navigation sidebar on the left and a main configuration area. The configuration area contains several sections: 'IP ACL Name' (ALC1), 'Rule ID' (1), 'Action' (Permit), 'Assign Queue ID' (0-6), 'Redirect Interface' (Limit 1, Port 1), 'Mirror Interface' (Limit 1, Port 1), 'Match Every' (checked), 'Protocol' (Select From List), 'Match to Value' (1-255), 'Source IP Address' (0.0.0.0, Wild Card Mask 255.255.255.255), 'Source L4 Port' (Select From List, Match to Port 1, 0-65535), 'Destination IP Address' (0.0.0.0, Wild Card Mask 0.0.0.0), 'Destination L4 Port' (Select From List, Match to Port 1, 0-65535), 'Service Type' (Select From List, Match to Port 1, 0-63), 'IP DSCP' (Select From List, Match to Port 1, 0-7), 'IP Precedence' (0-7), 'IP TOS Bits' (00-FF), 'IP TOS Mask' (00-FF), and a 'Remove' checkbox.

Cette page contient les champs suivants :

IP ACL Name (Nom de l'ACL IP) : identifie une ACL IP existante. Pour définir une nouvelle ACL IP, utilisez la page [IP ACL Configuration](#) (Configuration des ACL IP).

Rule ID (ID de la règle) : sélectionne ou crée des ACL définies par l'utilisateur. Entrez l'ID d'une règle existante ou créez une nouvelle règle en sélectionnant **Create** (Créer) dans le menu déroulant et en entrant l'ID de la nouvelle règle. Le nouvel ID est créé lorsque vous cliquez sur **Apply Changes** (Appliquer les modifications). Jusqu'à 10 règles peuvent être créées pour chaque ACL.

Action : sélectionne l'action de transfert appliquée par l'ACL. Choisissez l'action de transfert à appliquer dans le menu déroulant. Ce champ peut prendre les valeurs suivantes :

Permit (Autoriser) : transmet les paquets répondant aux critères de la liste de contrôle d'accès.

Deny (Refuser) : rejette les paquets ne répondant pas aux critères de la liste de contrôle d'accès.

Assign Queue ID (Affecter un ID de file d'attente) : cochez cette case pour appliquer ce critère, puis entrez un numéro d'identification compris entre 0 et 6.

Redirect Interface (Interface de redirection) : utilisez la liste déroulante pour sélectionner une interface vers laquelle les paquets correspondant aux critères de la règle peuvent être redirigés.

Mirror Interface (Interface de mise en miroir) : utilisez la liste déroulante pour sélectionner une interface vers laquelle les paquets correspondant aux critères de la règle peuvent être mis en miroir.

Logging (Consignation) : lorsque la case à cocher est sélectionnée, la consignation est activée pour une ACL donnée. La consignation est prise en charge uniquement pour l'action "Deny" (Refuser).

Match Every (Comparer tous les critères) : exige du paquet qu'il réponde aux critères de la liste de contrôle d'accès. Cochez la case pour appliquer ces critères. Le paramètre Match Every (Comparer tous les critères) prévaut sur toutes les autres règles de filtrage ; si cette option est cochée, les autres règles affichées à l'écran ne sont pas accessibles.

Protocol (Protocole) : le protocole d'un paquet doit correspondre au protocole indiqué. Cochez la case pour appliquer ce critère, puis sélectionnez l'un des éléments suivants :

Select from List (Sélectionner dans la liste) : sélectionnez dans la liste déroulante le protocole sur lequel la liste doit être basée.

Match to Value (Comparer avec la valeur) : cliquez pour ajouter un ID de protocole défini par l'utilisateur et devant servir pour vérification de la règle.

Source IP Address (Adresse IP source) : l'adresse IP du port source associé à un paquet doit correspondre à l'adresse indiquée ici. Cochez la case et saisissez une adresse pour appliquer ce critère.

Wild Card Mask (Masque à caractères génériques) : définit le masque à caractères génériques correspondant à l'adresse IP source. Les masques à caractères génériques déterminent les bits qui sont utilisés et ceux qui sont ignorés. Un masque à caractères génériques de 255.255.255.255 signifie qu'aucun bit n'est important. Un masque à caractères génériques de 0.0.0.0 indique que tous les bits sont importants. Ce champ doit être renseigné lorsque la case **Source IP Address (Adresse IP source)** est cochée.

Source L4 Port (Port L4 source) : le port source TCP/UDP d'un paquet doit correspondre au port indiqué ici. Cochez la case pour appliquer ce critère, puis sélectionnez l'un des éléments suivants dans le menu déroulant :

Select From List (Sélectionner dans la liste) : cliquez ici pour effectuer une sélection dans une liste de ports source sur lesquels la règle peut être basée.

Match to Port (Comparer avec le port) : cliquez pour ajouter un ID de port défini par l'utilisateur et devant servir pour vérification de la règle.

Destination IP Address (Adresse IP de destination) : l'adresse IP du port de destination associé à un paquet doit correspondre à l'adresse indiquée ici. Cochez la case et saisissez une adresse pour appliquer ce critère.

Wild Card Mask (Masque à caractères génériques) : définit le masque à caractères génériques correspondant à l'adresse IP de destination. Ce champ doit être renseigné lorsque la case **Destination IP Address (Adresse IP de destination)** est cochée.

Destination L4 Port (Port L4 de destination) : le port TCP/UDP de destination d'un paquet doit correspondre au port indiqué ici. Cochez la case pour appliquer ce critère, puis sélectionnez l'un des éléments suivants :

Select From List (Sélectionner dans la liste) : cliquez ici pour effectuer une sélection dans une liste de ports de destination sur lesquels la règle peut être basée.

Match to Port (Comparer avec le port) : cliquez pour ajouter un ID de port défini par l'utilisateur et devant servir pour vérification de la règle.

Champs de la zone Service Type (Type de service)

Sélectionnez l'un des trois champs suivants. La sélection sera utilisée pour la comparaison des paquets et des ACL.

IP DSCP (DSCP IP) : compare la valeur DSCP du paquet avec la règle. La valeur DSCP ou la valeur IP Precedence (Priorité IP) est utilisée pour comparer les paquets aux ACL.

Select From List (Sélectionner dans la liste) : permet d'effectuer une sélection dans une liste de valeurs de mots clés DSCP.

Match to Port (Comparer avec le port) : cliquez ici pour ajouter un ID de port défini par l'utilisateur.

IP Precedence (Priorité IP) : lorsque cette case est cochée, la valeur de priorité IP du paquet est comparée à la règle. Entrez la priorité IP à respecter. La valeur DSCP ou la valeur IP Precedence (Priorité IP) est utilisée pour comparer les paquets aux ACL.

IP TOS Bits (Bits du type de service IP) : lorsque cette case est cochée, la comparaison porte sur les bits du type de service figurant dans l'en-tête IP.

TOS Bits (Bits du type de service) : les bits du champ définissant le type de service (TOS) d'un paquet doivent correspondre au numéro hexadécimal à deux chiffres indiqué ici.

TOS Mask (Masque du type de service) : définit la position des bits utilisés pour la comparaison avec le champ définissant le type de service IP d'un paquet.

Remove (Supprimer) : si vous cochez cette option, l'ID de règle correspondant est supprimé lorsque vous cliquez sur **Apply Changes** (Appliquer les modifications).

Modification d'une règle basée sur les adresses IP

REMARQUE : Les règles ne peuvent être modifiées que lorsque la liste de contrôle d'accès dont elles font partie n'est pas liée à une interface.

1. Affichez la page **IP ACL Rule Configuration** (Configuration de règles pour les ACL IP).
2. Sélectionnez la liste de contrôle d'accès voulue dans le menu déroulant **IP ACL** (ACL IP).
3. Sélectionnez la règle voulue dans le menu déroulant **Rule ID** (ID de la règle).
4. Modifiez les autres champs selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La règle est modifiée et le périphérique est mis à jour.

Ajout d'une nouvelle règle à une ACL basée sur les paramètres IP

1. Affichez la page **IP ACL Rule Configuration** (Configuration de règles pour les ACL IP).
2. Sélectionnez la liste de contrôle d'accès voulue dans le menu déroulant **IP ACL** (ACL IP).
3. Sélectionnez **Create Rule** (Créer une règle) dans le menu déroulant **Rule ID** (ID de la règle) et entrez un nouvel ID.
4. Complétez les autres champs, le cas échéant.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle règle est affectée à la liste de contrôle d'accès basée sur les adresses IP.

Définition d'une règle pour une ACL basée sur les adresses IP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. ACL Commands (Commandes ACL)

Configuration des ACL MAC

La page **MAC ACL Configuration** (Configuration des ACL MAC) permet aux administrateurs réseau de définir une liste de contrôle d'accès basée sur les adresses MAC. Pour plus d'informations sur les listes ACL, voir [Configuration des ACL IP](#).

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Network Security** (Sécurité réseau) → **Access Control Lists** (Listes de contrôle d'accès) → **MAC Access Control Lists** (Listes de contrôle d'accès MAC) → **Configuration** dans l'arborescence.

Figure 8-14. Page MAC ACL Configuration (Configuration des ACL MAC)



Cette page contient les champs suivants :

MAC ACL Name (Nom de l'ACL MAC) : nom défini par l'utilisateur pour la liste de contrôle d'accès.

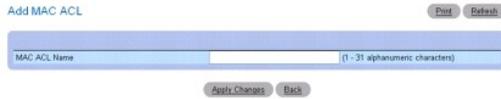
Rename MAC ACL (Renommer l'ACL MAC) : pour renommer l'ACL basée sur les adresses MAC, cochez la case et saisissez un nouveau nom dans ce champ.

Remove (Supprimer) : cliquez sur ce champ puis sur le bouton **Apply Changes** (Appliquer les modifications) pour supprimer l'ACL indiquée dans le champ **MAC ACL** (ACL MAC).

Ajout d'une ACL basée sur les adresses MAC

1. Affichez la page **MAC ACL Configuration** (Configuration des ACL MAC).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add MAC ACL** (Ajouter une ACL MAC).

Figure 8-15. Page Add MAC ACL (Ajouter une ACL MAC)



3. Entrez le nom voulu pour la liste dans le champ **ACL Name** (Nom de l'ACL).
 4. Cliquez sur **Apply Changes** (Appliquer les modifications).
- L'ACL basée sur les adresses MAC est ajoutée et le périphérique est mis à jour.

Suppression d'une ACL basée sur les adresses MAC

1. Affichez la page **MAC ACL Configuration** (Configuration des ACL MAC) et sélectionnez l'ACL à supprimer dans le menu déroulant **MAC ACL** (ACL MAC).
2. Cochez la case **Remove** (Supprimer).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

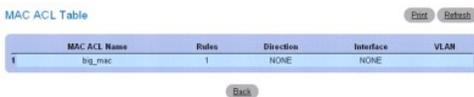
La liste ACL basée sur les paramètres MAC est supprimée et le périphérique est mis à jour.

Affichage des ACL MAC

1. Affichez la page **MAC ACL Configuration** (Configuration des ACL MAC).
2. Cliquez sur **Show All** (Afficher tout).

Toutes les listes de contrôle d'accès basées sur les paramètres MAC et les données correspondantes s'affichent à l'écran.

Figure 8-16. Page MAC ACL Table (Table des ACL MAC)



MAC ACL Name	Rules	Direction	Interface	VLAN
1	big_mac	1	NONE	NONE

Configuration d'ACL MAC à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

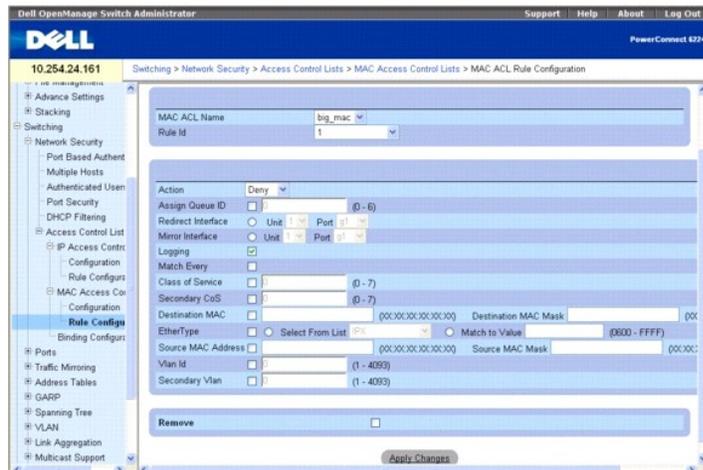
1. ACL Commands (Commandes ACL)

Configuration de règles pour les ACL MAC

La page **MAC ACL Configuration** (Configuration des ACL MAC) permet de définir des règles pour les listes de contrôle d'accès basées sur les paramètres MAC. La définition des listes d'accès inclut des règles indiquant si les paquets répondant aux critères définis doivent être rejetés ou transmis. Une règle par défaut "deny all" figure à la fin de chaque ACL.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Network Security** (Sécurité réseau) → **Access Control Lists** (Listes de contrôle d'accès) → **MAC Access Control Lists** (Listes de contrôle d'accès MAC) → **Rule Configuration** (Configuration des règles) dans l'arborescence.

Figure 8-17. Page MAC ACL - Rule Configuration (Configuration de règles pour les ACL MAC)



Cette page contient les champs suivants :

MAC ACL Name (Nom de l'ACL MAC) : identifie une ACL MAC existante. Pour définir une nouvelle ACL MAC, utilisez la page [MAC ACL Configuration](#) (Configuration des ACL MAC).

Rule Id (ID de la règle) : sélectionne ou crée une liste de contrôle d'accès définie par l'utilisateur. Entrez l'ID d'une règle existante ou créez une nouvelle règle en sélectionnant Create (Créer) dans le menu déroulant et en entrant l'ID de la nouvelle règle. Le nouvel ID est créé lorsque vous cliquez sur Apply Changes (Appliquer les modifications).

Action : sélectionne l'action de transfert de l'ACL. Les valeurs admises sont les suivantes :

Permit (Autoriser) : transmet les paquets répondant aux critères de la liste de contrôle d'accès.

Deny (Refuser) : rejette les paquets ne répondant pas aux critères de la liste de contrôle d'accès.

Assign Queue ID (Affecter un ID de file d'attente) : cochez cette case pour appliquer ce critère, puis entrez un numéro d'identification compris entre 0 et 6.

Redirect Interface (Interface de redirection) : utilisez la liste déroulante pour sélectionner une interface vers laquelle les paquets correspondant aux critères de la règle peuvent être redirigés.

Mirror Interface (Interface de mise en miroir) : utilisez la liste déroulante pour sélectionner une interface vers laquelle les paquets correspondant aux critères de la règle peuvent être mis en miroir.

Logging (Consigner) : cochez la case pour activer la consignation pour cette ACL. Cette fonction est prise en charge uniquement pour l'action "Deny" (Refuser).

Match Every (Comparer tous les critères) : exige du paquet qu'il réponde aux critères de la liste de contrôle d'accès. Cochez la case pour appliquer ces critères.

Class of Service (Classe de service) : la classe de service d'un paquet doit correspondre à la valeur indiquée ici. Cochez la case et entrez une valeur de classe de service comprise entre 0 et 7 pour appliquer ce critère.

Secondary CoS (Classe de service secondaire) : la classe de service secondaire d'un paquet doit correspondre à la valeur indiquée ici. Cochez la case et entrez une valeur de classe de service comprise entre 0 et 7 pour appliquer ce critère.

Destination MAC Address (Adresse MAC de destination) : l'adresse MAC du port de destination associé à un paquet doit correspondre à l'adresse indiquée ici. Cochez la case et saisissez une adresse pour appliquer ce critère.

Destination MAC Mask (Masque de l'adresse MAC de destination) : si vous souhaitez utiliser cette option, entrez le masque correspondant à l'adresse MAC de destination voulue.

EtherType (Type Ethernet) : le type Ethernet d'un paquet doit correspondre à la valeur indiquée ici. Cochez cette case et sélectionnez le type Ethernet dans la liste ou saisissez-le.

Select from List (Sélectionner dans la liste) : sélectionnez le type Ethernet voulu dans le menu déroulant.

Match to Value (Comparer avec la valeur) : entrez le numéro de port voulu.

Source MAC Address (Adresse MAC source) : l'adresse MAC du port source associé à un paquet doit correspondre à l'adresse indiquée ici. Cochez la case et saisissez une adresse pour appliquer ce critère.

Source MAC Mask (Masque de l'adresse MAC source) : si vous souhaitez utiliser cette option, entrez le masque correspondant à l'adresse MAC source voulue.

Vlan Id (ID de VLAN) : l'ID de VLAN d'un paquet doit correspondre à celui indiqué ici. Cochez la case et saisissez l'ID du VLAN pour appliquer ce critère. Les valeurs possibles vont de 1 à 4093.

Secondary Vlan (VLAN secondaire) : l'ID de VLAN secondaire d'un paquet doit correspondre à celui indiqué ici. Cochez la case et saisissez l'ID du VLAN secondaire pour appliquer ce critère. Les valeurs possibles vont de 1 à 4093.

Remove (Supprimer) : si vous cochez cette option, la règle pour ACL MAC correspondante est supprimée lorsque vous cliquez sur **Apply Changes** (Appliquer les modifications).

Modification d'une règle basée sur les paramètres MAC

 **REMARQUE :** Les règles ne peuvent être modifiées que lorsque la liste de contrôle d'accès dont elles font partie n'est pas liée à une interface.

1. Affichez la page **MAC ACL Rule Configuration** (Configuration de règles pour les ACL MAC).
2. Sélectionnez la liste de contrôle d'accès voulue dans le menu déroulant **MAC ACL** (ACL MAC).
3. Sélectionnez la règle voulue dans le menu déroulant **Rule ID** (ID de la règle).
4. Modifiez les autres champs selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La règle est modifiée et le périphérique est mis à jour.

Ajout d'une nouvelle règle à une ACL basée sur les paramètres MAC

1. Affichez la page **MAC ACL Rule Configuration** (Configuration de règles pour les ACL MAC).
2. Sélectionnez la liste de contrôle d'accès voulue dans le menu déroulant **MAC ACL** (ACL MAC).
3. Pour **Rule ID** (ID de la règle), sélectionnez **Create New Rule** (Créer une nouvelle règle).
4. Entrez un nouvel ID.
5. Complétez les autres champs, le cas échéant.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle règle est affectée à la liste de contrôle d'accès basée sur les paramètres MAC.

Suppression d'une règle d'ACL basée sur les paramètres MAC

1. Sélectionnez une ACL.
2. Sélectionnez une règle dans le menu déroulant **Rule ID** (ID de la règle).
3. Cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La liste ACL basée sur les paramètres MAC est supprimée et le périphérique est mis à jour.

Définition d'une règle pour une ACL basée sur les paramètres MAC à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1 ACL Commands (Commandes ACL)

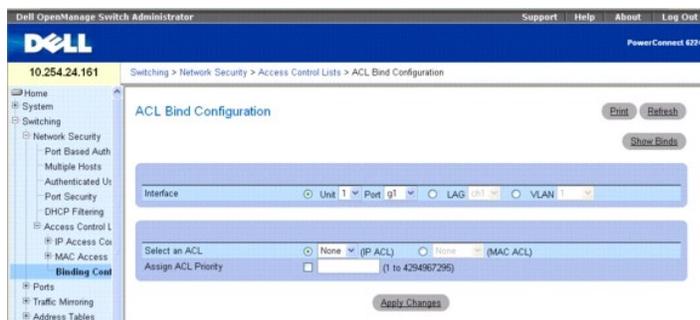
Configuration de liaisons pour les ACL

Lorsqu'une ACL est liée à une interface, toutes les règles définies sont appliquées à cette dernière. La page **ACL Bind Configuration** (Configuration de liaisons pour les ACL) permet d'affecter des ACL à des interfaces et de définir des priorités.

À partir de l'interface Web, vous pouvez configurer la règle d'ACL pour le trafic entrant afin que la règle s'applique aux paquets qui arrivent sur le port. À partir de l'interface CLI, vous pouvez configurer la règle d'ACL pour le trafic entrant ou sortant. Les ACL appliquées au trafic sortant implémentent des règles de sécurité sur le trafic sortant du port. Les ACL peuvent être appliquées à toute interface physique (10G comprise), ainsi qu'à tout LAG ou port de routage.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Network Security** (Sécurité réseau) → **Access Control Lists** (Listes de contrôle d'accès) → **Binding Configuration** (Configuration des liaisons) dans l'arborescence.

Figure 8-18. Page ACL Bind Configuration (Configuration de liaisons pour les ACL)



Cette page contient les champs suivants :

Interface : les boutons radio permettent de sélectionner l'interface en fonction de l'unité/du port, du LAG ou du VLAN.

Select an ACL (Sélectionner une ACL) : sélectionne le type d'ACL auquel les paquets entrants sont comparés. Les paquets peuvent être comparés à des ACL basées sur les paramètres IP ou MAC.

Assign ACL Priority (Définir la priorité de l'ACL) : permet d'affecter une priorité à l'ACL. Si plusieurs ACL sont appliquées à une interface, les critères de comparaison des listes possédant la priorité la plus élevée sont évalués en premier.

Affectation d'une ACL à une interface

1. Affichez la page **ACL Bind Configuration** (Configuration de liaisons pour les ACL).
2. Dans le champ **Interface**, indiquez l'unité et le port, le LAG ou le VLAN à configurer.
3. Sélectionnez le type d'ACL (IP ou MAC) dans le champ **Select an ACL** (Sélectionner une ACL).

 **REMARQUE** : Lorsqu'une ACL est affectée à un port, LAG ou VLAN, les flux provenant de cette interface d'entrée et qui ne correspondent pas à l'ACL sont soumis à la règle par défaut, "Drop unmatched packets" (Rejeter les paquets non conformes).

4. Définissez la priorité dans le champ **Assign ACL Priority** (Définir la priorité de l'ACL).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'ACL est associée aux interfaces spécifiées.

Suppression d'une interface associée à une ACL

1. Affichez la page **ACL Bind Configuration** (Configuration de liaisons pour les ACL).
2. Cliquez sur **Show All** (Afficher tout).
3. Dans le champ **Interface**, indiquez l'unité et le port, le LAG ou le VLAN pour lequel vous souhaitez afficher les liaisons d'ACL.
4. Cochez la case **Remove** (Supprimer) en regard d'une ou plusieurs ACL à supprimer.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les ACL indiquées sont supprimées de l'interface.

Affectation de l'appartenance à une ACL à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1 ACL Commands (Commandes ACL)

Configuration des ports

La page **Ports** contient des liens permettant de configurer la fonctionnalité des ports, y compris des fonctions avancées telles que Storm Control et la mise en miroir des ports, et d'effectuer des tests virtuels sur les ports.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Ports** dans l'arborescence. Cette page contient des liens vers les fonctionnalités suivantes :

- 1 [Paramètres globaux](#)
- 1 [Configuration des ports](#)
- 1 [Configuration des ports protégés](#)
- 1 [Configuration des LAG](#)
- 1 [Storm Control](#)

Paramètres globaux

La page Global Parameters (Paramètres globaux) permet de configurer le contrôle de flux. Le contrôle de flux permet de réduire momentanément le trafic provenant d'un commutateur. Il ne peut être défini que sur les commutateurs directement connectés, et uniquement pour les ports configurés pour fonctionner en duplex intégral. Étant donné que les ports configurés pour la négociation automatique ne peuvent pas être ajoutés en tant que membres d'un LAG, le contrôle de flux ne peut pas être configuré sur automatique pour les ports faisant partie d'un LAG.

REMARQUE : Le contrôle de flux est incompatible avec le mode de prévention utilisant le blocage HOL (tête de ligne). Le commutateur peut fonctionner dans l'un ou l'autre de ces modes, mais pas simultanément.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Ports** → **Global Parameters** (Paramètres globaux) dans l'arborescence.

Figure 8-19. Page Global Parameters (Paramètres globaux)



Cette page contient le champ suivant :

Flow Control (Contrôle de flux) : sélectionnez Enabled (Activé) ou Disabled (Désactivé) dans le menu déroulant. Cette commande affecte tous les ports de la pile. La valeur par défaut est Enabled (Activé).

Enabled (Activé) : active le mécanisme de contre-pression en entrée du commutateur.

Disabled (Désactivé) : restaure le mode de prévention avec blocage HOL (tête de ligne).

Activation de la contre-pression en entrée

1. Affichez la page **Ports Global Parameters** (Paramètres globaux des ports).
2. Sélectionnez Enable (Activer) dans le menu déroulant du champ **Flow Control** (Contrôle de flux).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).
4. La contre-pression en entrée est maintenant activée.

Configuration du contrôle de flux à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

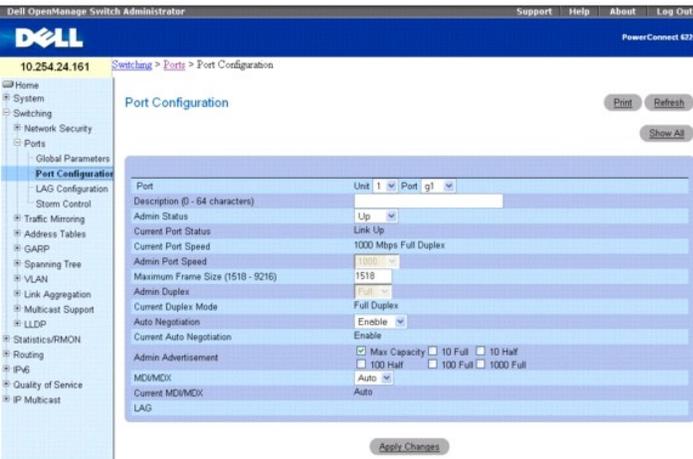
- 1 Ethernet Configuration Commands (Commandes de configuration Ethernet)

Configuration des ports

La page **Port Configuration** (Configuration des ports) permet de définir les paramètres des ports.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Ports** → **Port Configuration** (Configuration des ports) dans l'arborescence.

Figure 8-20. Page Port Configuration (Configuration des ports)



Cette page contient les champs suivants :

Port : indique l'unité et le port pour lesquels les paramètres sont définis.

Description (0-64 Characters) (Description, 0 à 64 caractères) : contient une brève description de l'interface (par exemple, Ethernet).

Admin Status (État admin) : active ou désactive le transfert du trafic via ce port.

Current Port Status (État actuel du port) : indique si le port est opérationnel ou non.

Current Port Speed (Vitesse actuelle du port) : affiche la vitesse actuelle du port synchronisé (en bps).

Admin Port Speed (Vitesse admin du port) : force la vitesse du port sur la valeur sélectionnée (10 M, 100 M, 1000 M ou 10000 M).

Maximum Frame Size (1518-9216) (Taille de trame maximale, 1518-9216) : indique la taille maximale acceptée pour les paquets. Les paquets de taille supérieure sont rejetés. La valeur par défaut est de 1518.

Admin Duplex (Duplex admin) : définit le mode duplex du port. Les options disponibles sont Full (Intégral) et Half (Semi).

Full (Intégral) : indique que l'interface prend en charge la transmission bidirectionnelle entre le commutateur et le client.

Half (Semi duplex) : indique que l'interface prend en charge la transmission entre le commutateur et le client, dans un seul sens à la fois.

Current Duplex Mode (Mode duplex actuel) : affiche le mode duplex du port synchronisé.

Auto Negotiation (Négociation automatique) : active la négociation automatique sur le port. La négociation automatique est un protocole entre deux partenaires de liaison. Elle permet à un port d'informer son partenaire de sa vitesse de transfert, de son mode duplex et de ses capacités de contrôle de flux.

Current Auto Negotiation (Négociation automatique en cours) : affiche la configuration actuelle de la négociation automatique.

Admin Advertisement (Annonce admin) : indique les capacités devant être annoncées par le port. Les valeurs possibles sont les suivantes :

Max Capability (Capacité maximale) : indique que toutes les vitesses et tous les modes duplex peuvent être acceptés.

10 Half (10 Mbps, semi duplex) : indique que le port annonce une vitesse de 10 Mbps en mode semi duplex.

10 Full (10 Mbps, duplex intégral) : indique que le port annonce une vitesse de 10 Mbps en mode duplex intégral.

100 Half (100 Mbps, semi duplex) : indique que le port annonce une vitesse de 100 Mbps en mode semi duplex.

100 Full (100 Mbps, duplex intégral) : indique que le port annonce une vitesse de 100 Mbps en mode duplex intégral.

1000 Full (1000 Mbps, duplex intégral) : indique que le port annonce une vitesse de 1000 Mbps en mode duplex intégral.

MDI/MDX : permet au commutateur de distinguer câbles croisés et câbles directs.

Les concentrateurs et les commutateurs sont délibérément câblés de façon opposée à celle des stations terminales. Ainsi, lorsqu'un concentrateur ou un commutateur est connecté à une station terminale, il est possible d'utiliser un câble Ethernet direct et les paires correspondent correctement. Lorsque deux concentrateurs/commutateurs sont connectés entre eux, ou deux stations terminales entre elles, un câble inverseur est utilisé afin de garantir la correspondance entre les paires connectées.

Ce champ peut prendre les valeurs suivantes :

On (Activé) : permet au commutateur de détecter le type de connexion.

Off (Désactivé) : nécessite le type de câble approprié pour la connexion du commutateur.

Auto : la valeur est définie automatiquement.

Current MDI/MDX (MDI/MDX en cours) : indique la configuration MDX actuelle du commutateur. Ce champ peut prendre les valeurs suivantes :

MDI : la configuration en cours est MDI.

MDX : la configuration en cours est MDX.

Auto : la valeur est définie automatiquement.

LAG : affiche le numéro de LAG, si ce port est membre d'un LAG.

Définition des paramètres des ports

1. Affichez la page **Port Configuration** (Configuration des ports).
2. Sélectionnez une unité et un port dans les champs **Unit** (Unité) et **Port**.
3. Complétez les champs affichés.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des ports sont sauvegardés sur le commutateur.

Affichage de la table des ports

1. Affichez la page **Port Configuration** (Configuration des ports).
2. Cliquez sur **Show All** (Afficher tout).

La page **Port Configuration Table** (Table de configuration des ports) s'affiche.

Figure 8-21. Page Port Configuration Table (Table de configuration des ports)

Port	Port Status	Port Speed	Max Frame Size	Duplex Mode	Auto Negotiation	Flow Control	MDI/MDX	Copy To	Edit
1 1/1g1	Up	1000	1518	Full	Disable	Disable	Auto		
2 1/1g2	Up	1000	1518	Full	Disable	Disable	Auto		
3 1/1g3	Up	1000	1518	Full	Disable	Disable	Auto		
2/1ag2	Up	1000	1518	Full	Disable	Disable	Auto		
2/1ag3	Up	1000	1518	Full	Disable	Disable	Auto		
2/1ag4	Up	1000	1518	Full	Disable	Disable	Auto		

3. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **Port Configuration Table** (Table de configuration des ports) pour les autres unités de la pile, le cas échéant.

Copie des paramètres de configuration des ports

1. Affichez la page **Port Configuration** (Configuration des ports).
2. Cliquez sur **Show All** (Afficher tout).

La page **Port Configuration Table** (Table de configuration des ports) s'affiche.

3. Indiquez l'unité et le port à partir desquels vous effectuez la copie dans **Copy Parameters From** (Copie les paramètres à partir de).
4. Cliquez sur **Copy To** (Copier vers) pour chacun des ports cible.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de configuration des ports sont copiés et le périphérique est mis à jour.

Modification des paramètres de configuration pour plusieurs ports

1. Affichez la page **Port Configuration** (Configuration des ports).
2. Cliquez sur **Show All** (Afficher tout).

La table **Port Configuration** (Configuration des ports) s'affiche.

3. Cliquez sur **Edit** (Modifier) pour chacun des ports à modifier.
4. Modifiez les champs de configuration selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de configuration des ports sont modifiés et le périphérique est mis à jour.

Configuration des ports à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

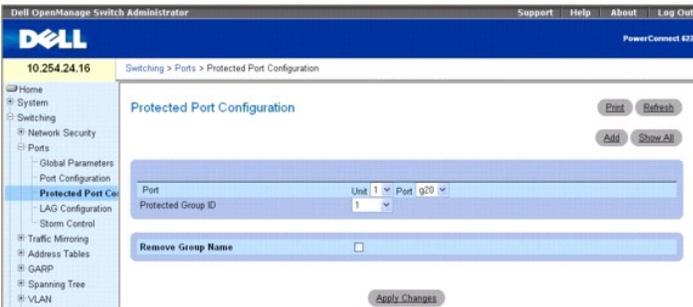
- 1 Ethernet Configuration Commands (Commandes de configuration Ethernet)

Configuration des ports protégés

La page **Protected Port Configuration** (Configuration des ports protégés) permet de configurer des ports PVE (Private VLAN Edge). Il s'agit d'une fonction de sécurité de couche 2 applicable aux ports faisant partie d'un même VLAN. Le trafic provenant des ports protégés par cette fonction est transmis uniquement aux ports situés en amont et ne peut pas être envoyé aux autres ports du VLAN.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Ports** → **Protected Port Configuration** (Configuration des ports protégés) dans l'arborescence.

Figure 8-22. Page Protected Port Configuration (Configuration des ports protégés)



Cette page contient les champs suivants :

Port : indique l'unité et le port pour lesquels les paramètres sont définis.

Protected Group ID (ID de groupe protégé) : menu déroulant utilisé pour affecter un port aux groupes 0, 1 ou 2.

Remove Group Name (Supprimer le nom du groupe) : cochez cette case pour désassocier le port sélectionné du groupe protégé.

Affichage de la table des ports protégés

1. Affichez la page **Protected Port Configuration** (Configuration des ports protégés).
2. Cliquez sur **Show All** (Afficher tout).

La page **Protected Ports Summary** (Récapitulatif des ports protégés) s'affiche.

Figure 8-23. Page Protected Port Summary Table (Récapitulatif des ports protégés)



3. Cochez la case **Remove** (Supprimer) puis cliquez sur **Apply Changes** (Appliquer les modifications) pour dissocier un port d'un groupe protégé.
4. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **Protected Port Summary** (Récapitulatif des ports protégés) pour les autres unités de la pile, le cas échéant.

Ajout de groupes de ports protégés

1. Affichez la page **Protected Port Configuration** (Configuration des ports protégés).
2. Cliquez sur **Add** (Ajouter).

La page **Add Protected Group** (Ajouter un groupe protégé) s'affiche.

Figure 8-24. Page Add Protected Group (Ajouter un groupe protégé)



3. Utilisez le menu déroulant pour affecter l'ID 0, 1 ou 2 dans le champ **Protected Group ID** (ID de groupe protégé).
4. Complétez le champ **Protected Group Name (1-32 characters)** (Nom du groupe protégé, 1 à 32 caractères).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres du groupe protégé sont copiés et le périphérique est mis à jour.

Configuration de ports protégés à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 switchport protected Commands (Commandes portant sur les ports protégés du commutateur)

Configuration des LAG

La fonction d'agrégation des liaisons permet de regrouper des liaisons Ethernet en mode duplex intégral, de façon à former un LAG (groupe de liaisons agrégées). Le commutateur peut traiter un LAG comme s'il s'agissait d'une seule liaison.

Pour afficher la page **LAG Configuration** (Configuration des LAG), cliquez sur **Switching** (Commutation) → **Ports** → **LAG Configuration** (Configuration des LAG) dans l'arborescence.

Figure 8-25. Page LAG Configuration (Configuration des LAG)



Cette page contient les champs suivants :

LAG : répertorie les numéros de LAG.

LAG Type (Type de LAG) : types de ports inclus dans le LAG.

Description (0-64 Characters) (Description, 0-64 caractères) : description du port.

Admin Status (État admin) : active ou désactive le transfert du trafic sur le LAG sélectionné.

Current LAG Status (État actuel du LAG) : indique si le LAG sélectionné est actuellement en cours de fonctionnement ou indisponible.

Définition des paramètres des LAG

1. Affichez la page **LAG Configuration** (Configuration des LAG).
2. Sélectionnez un LAG dans le champ **LAG**.
3. Complétez les champs affichés.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des LAG sont sauvegardés sur le commutateur.

Affichage de la table de configuration des LAG

1. Affichez la page **LAG Configuration** (Configuration des LAG).
2. Cliquez sur **Show All** (Afficher tout).
3. La page **LAG Configuration Table** (Table de configuration des LAG) s'affiche.

Figure 8-26. Page LAG Configuration Table (Table de configuration des LAG)

LAG	Description	LAG Type	Admin Status	Current Flow Control	Edit
1 lag1		Link Aggregation	Up	Disable	<input type="checkbox"/>
2 lag2		Link Aggregation	Up	Disable	<input type="checkbox"/>
3 lag3		Link Aggregation	Up	Disable	<input type="checkbox"/>
4 lag4		Link Aggregation	Up	Disable	<input type="checkbox"/>
5 lag5		Link Aggregation	Up	Disable	<input type="checkbox"/>
6 lag6		Link Aggregation	Up	Disable	<input type="checkbox"/>
7 lag7		Link Aggregation	Up	Disable	<input type="checkbox"/>
8 lag8		Link Aggregation	Up	Disable	<input type="checkbox"/>

Modification des paramètres des LAG

1. Affichez la page **LAG Configuration** (Configuration des LAG).
2. Cliquez sur **Show All** (Afficher tout).
3. La page **LAG Configuration Table** (Table de configuration des LAG) s'affiche.
4. Cochez l'option **Edit** (Modifier) pour tous les LAG à modifier.

5. Les champs **Admin Status** (État admin) et **Description** peuvent maintenant être modifiés.

6. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des LAG sont sauvegardés sur le commutateur.

Configuration des LAG à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Port Channel Commands (Commandes portant sur les canaux des ports)

Storm Control

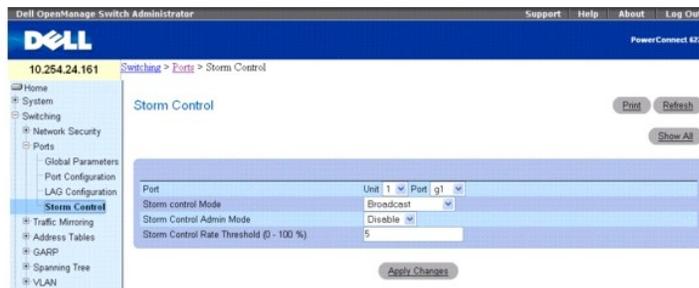
Le terme "Broadcast Storm" désigne une quantité excessive de messages de diffusion transmis simultanément sur un réseau à travers un seul port. Les réponses transmises peuvent surcharger les ressources du réseau et/ou entraîner des dépassements de délai.

Le commutateur mesure le taux de réception des paquets de diffusion, de multidiffusion et de monodiffusion inconnue pour chaque port et rejette les paquets excédentaires lorsque le taux dépasse le seuil défini. La fonction Storm Control est activée au niveau de chaque interface, en définissant le type de paquet et la vitesse à laquelle les paquets sont transmis.

La page **Storm Control** permet d'activer et de configurer la fonction Storm Control.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Ports** → **Storm Control** dans l'arborescence.

Figure 8-27. Page Storm Control



Cette page contient les champs suivants :

Port : indique l'**unité** et le **port** pour lesquels la fonction Storm Control est activée.

Storm Control Mode (Mode Storm Control) : indique le mode de diffusion affecté par Storm Control.

Broadcast (Diffusion) : si le taux du trafic de diffusion L2 entrant sur une interface augmente au-delà du seuil défini, le trafic sera rejeté.

Multicast (Multidiffusion) : si le taux du trafic de multidiffusion L2 entrant sur une interface augmente au-delà du seuil défini, le trafic sera rejeté.

Unknown Unicast (Monodiffusion inconnue) : si le taux du trafic de monodiffusion L2 inconnue (échec de la recherche de destination) entrant sur une interface augmente au-delà du seuil défini, le trafic sera rejeté.

Storm Control Admin Mode (Mode admin de Control Storm) : active ou désactive Storm Control.

Storm Control Rate Threshold (0-100%) (Vitesse de diffusion maximale pour Storm Control, 0-100%) : vitesse maximale de transfert des paquets inconnus. La plage représente un pourcentage du seuil total.

Définition des paramètres des ports pour la fonction Storm Control

1. Affichez la page **Storm Control**.
2. Modifiez les champs affichés.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des ports pour la fonction Storm Control sont sauvegardés sur le commutateur.

Affichage de la table des paramètres de la fonction Storm Control

1. Affichez la page **Storm Control**.
2. Cliquez sur **Show All** (Afficher tout).

La table **Storm Control Settings** (Paramètres de Storm Control) s'affiche.

Figure 8-28. Page Storm Control Settings Table (Table des paramètres de Storm Control)

Storm Control Settings Table Print Default

Unit 1 ▼

Unit	Broadcast Control Mode	Broadcast Rate Threshold	Multicast Control Mode	Multicast Rate Threshold	Unicast Control Mode	Unicast Rate Threshold	Edit
1 1/fg1	Disable ▼	5	Disable ▼	5	Disable ▼	5	<input checked="" type="checkbox"/>
2 1/fg2	Disable ▼	5	Disable ▼	5	Disable ▼	5	<input type="checkbox"/>
3 1/fg3	Disable ▼	5	Disable ▼	5	Disable ▼	5	<input type="checkbox"/>

26 1/fg2	Disable ▼	5	Disable ▼	5	Disable ▼	5	<input type="checkbox"/>
27 1/fg3	Disable ▼	5	Disable ▼	5	Disable ▼	5	<input type="checkbox"/>
28 1/fg4	Disable ▼	5	Disable ▼	5	Disable ▼	5	<input type="checkbox"/>

Apply Changes Back

3. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **Storm Control Settings Table** (Table des paramètres de Storm Control) pour les autres unités de la pile, le cas échéant.

Modification du contrôle de diffusion

1. Affichez la page **Storm Control**.
 2. Cliquez sur **Show All** (Afficher tout).
- La table **Storm Control Settings** (Paramètres de Storm Control) s'affiche.
3. Cochez **Edit** (Modifier) pour chaque port pour lequel le contrôle de diffusion (**Broadcast Control**) doit être modifié.
 4. Modifiez les paramètres de **Broadcast Control** (Contrôle de diffusion) selon vos besoins.
 5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des ports pour la fonction Storm Control sont sauvegardés sur le commutateur.

Configuration de Storm Control à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Ethernet Configuration Commands (Commandes de configuration Ethernet)

Configuration de la mise en miroir du trafic

La mise en miroir du trafic permet de configurer le commutateur pour qu'il envoie des copies des paquets vers un port utilisé comme miroir. La mise en miroir peut être basée sur les ports ou sur les flux.

La page **Traffic Mirroring** (Mise en miroir du trafic) permet de définir les sessions de mise en miroir basées sur les ports ou sur les flux.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Traffic Mirroring** (Mise en miroir du trafic) dans l'arborescence. Cette page contient des liens vers les fonctionnalités suivantes :

- 1 [Mise en miroir des ports](#)
- 1 [Mise en miroir basée sur les flux](#)

Mise en miroir des ports

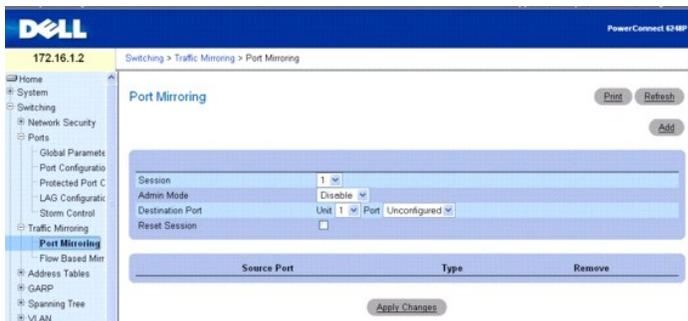
La mise en miroir des ports sélectionne le trafic réseau devant être examiné par un analyseur de réseau. Cette opération est appliquée à des ports spécifiques du commutateur. Plusieurs ports du commutateur sont configurés en tant que ports source tandis qu'un seul port du commutateur est défini comme cible. Vous pouvez définir la méthode utilisée pour la mise en miroir du trafic du port source. Les paquets reçus sur le port source, transmis, ou à la fois transmis et reçus peuvent être mis en miroir sur le port de destination.

Le paquet qui est copié vers le port de destination est au même format que le paquet d'origine. Si le paquet copié est un paquet reçu, il contient ou ne contient pas de balise VLAN, selon sa configuration lors de sa réception sur le port source. Si le paquet copié est un paquet transmis, il contient ou ne contient

pas de balise VLAN, selon sa configuration lors de sa transmission sur le port source.

Pour afficher la page **Port Mirroring** (Mise en miroir des ports), cliquez sur **Switching** (Commutation) → **Traffic Mirroring** (Mise en miroir du trafic) → **Port Mirroring** (Mise en miroir des ports) dans l'arborescence.

Figure 8-29. Page Port Mirroring (Mise en miroir des ports)



Cette page contient les champs suivants :

Session : identifie la session de surveillance.

Admin Mode (Mode admin) : active ou désactive la mise en miroir des ports.

Destination Port (Port de destination) : sélectionnez le port sur lequel le trafic peut être copié.

Reset Session (Réinitialiser la session) : permet de réinitialiser la session de surveillance du port.

Source Port (Port source) : répertorie les ports source ayant été ajoutés à partir de la page Add Source Port (Ajouter un port source).

Type : indique le type de trafic surveillé sur le port source.

Ajout d'une session de mise en miroir des ports

REMARQUE : Un port défini comme miroir est automatiquement supprimé d'un VLAN ou d'un LAG.

1. Affichez la page **Port Mirroring** (Mise en miroir des ports).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add Source Port** (Ajouter un port source).

Figure 8-30. Page Add Source Port (Ajouter un port source)



3. Complétez les champs suivants :

Session : sélectionnez la session à surveiller.

Source Port (Port source) : sélectionnez l'unité et le port source du trafic mis en miroir. Jusqu'à quatre ports source peuvent être mis en miroir sur un port de destination.

Type : définit le type de trafic surveillé. Ce champ peut prendre les valeurs suivantes :

TX (Transmission) : surveille uniquement les paquets transmis.

RX (Réception) : surveille uniquement les paquets reçus.

TX and RX (Transmission et réception) : surveille les paquets transmis et reçus.

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle session de mise en miroir des ports est activée et le périphérique est mis à jour. Le port source apparaît dans la table Source Port (Ports source) figurant dans la page Port Mirroring (Mise en miroir des ports).

Modification d'une session de mise en miroir des ports

1. Affichez la page **Port Mirroring** (Mise en miroir des ports).
2. Modifiez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les champs de la session de la mise en miroir de ports sont modifiés et le périphérique est mis à jour.

Suppression d'une session de mise en miroir des ports

1. Affichez la page **Port Mirroring** (Mise en miroir des ports).
2. Cochez la case **Reset Session** (Réinitialiser la session).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La session de mise en miroir des ports est supprimée et le périphérique est mis à jour.

Configuration d'une session de mise en miroir des ports à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Port Monitor Commands (Commandes de surveillance des ports)

Mise en miroir basée sur les flux

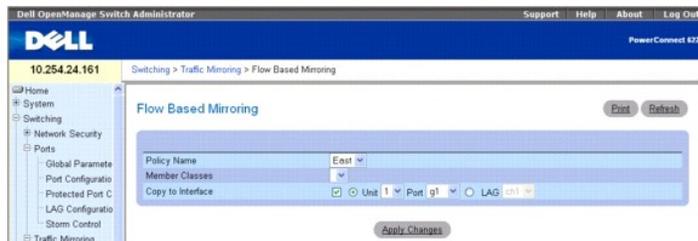
La fonction de mise en miroir basée sur les flux repose sur le composant DiffServ de QoS. Dans QoS, l'utilisateur définit les critères permettant de créer des classes de trafic, puis il crée les stratégies définissant l'action à appliquer à ces classes.

La mise en miroir basée sur les flux permet à l'utilisateur de copier certains types de trafic vers un port de destination unique. Cela confère une certaine flexibilité : au lieu de mettre en miroir l'ensemble du trafic entrant et sortant sur un port, le commutateur peut mettre en miroir un sous-ensemble de ce trafic. Vous pouvez configurer le commutateur pour qu'il mette les flux en miroir sur la base des informations des couches 2, 3 et 4.

La page **Flow Based Mirroring** (Mise en miroir basée sur les flux) permet de définir les ports utilisés.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Traffic Mirroring** (Mise en miroir du trafic) → **Flow Based Mirroring** (Mise en miroir basée sur les flux) dans l'arborescence.

Figure 8-31. Page Flow Based Mirroring (Mise en miroir basée sur les flux)



Cette page contient les champs suivants :

Policy Name (Nom de la stratégie) : sélectionne la stratégie à associer à une classe de trafic. Le nom de la stratégie est défini à l'aide de la page web DiffServ [Policy Configuration](#) (Configuration de la stratégie).

Member Classes (Classes membres) : sélectionne la classe de trafic associée à cette stratégie. La classe membre est définie à l'aide de la page web DiffServ [Class Configuration](#) (Configuration de la classe).

Copy to Interface (Copier vers une interface) : lorsque cette option est sélectionnée, elle permet de copier les paquets vers une unité/un port ou un LAG.

Copie de la mise en miroir vers un port de destination

1. Affichez la page **Flow Based Mirroring** (Mise en miroir basée sur les flux).
2. Indiquez un nom de stratégie (**Policy Name**) et une classe membre (**Member Class**), puis sélectionnez l'unité et le port de destination à affecter dans le champ **Copy to Interface** (Copier vers l'interface).

3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les informations sur la mise en miroir basée sur les flux sont copiées vers le port spécifié et le périphérique est mis à jour.

Configuration de la mise en miroir basée sur les flux à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. QOS Commands (Commandes QOS)

Configuration des tables d'adresses

Les adresses MAC sont sauvegardées dans la table des adresses statiques ou dynamiques. Les adresses statiques sont définies par l'utilisateur. Les adresses dynamiques sont apprises par le système et supprimées après un certain délai. Un paquet envoyé à une destination enregistrée dans l'une des tables est immédiatement transmis vers les ports. Les tables des adresses statiques et dynamiques peuvent être triées en fonction de l'interface, de l'ID de VLAN ou du nom de VLAN. En outre, des adresses peuvent y être ajoutées.

Pour afficher la page **Address Tables** (Tables d'adresses), cliquez sur **Switching** (Commutation) → **Address Tables** (Tables d'adresses) dans l'arborescence. Cette page contient des liens vers les fonctionnalités suivantes :

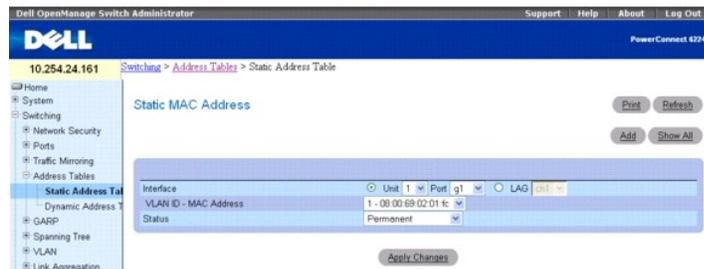
1. [Table des adresses statiques](#)
1. [Table des adresses dynamiques](#)

Table des adresses statiques

La page **Static MAC Address** (Adresses MAC statiques) contient une liste d'adresses MAC statiques. Cette liste permet d'ajouter et de supprimer des adresses MAC statiques.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Address Tables** (Tables d'adresses) → **Static Address Table** (Table des adresses statiques) dans l'arborescence.

Figure 8-32. Page Static MAC Address (Adresse MAC statique)



Cette page contient les champs suivants :

Interface : indique l'unité et le port ou LAG auxquels l'adresse MAC statique s'applique. Pour afficher les adresses associées à une autre unité ou port/LAG, modifiez l'interface mentionnée à cet endroit.

VLAN ID - MAC Address (ID de VLAN - Adresse MAC) : indique l'ID de VLAN associé à l'adresse MAC et les adresses MAC incluses dans la liste d'adresses statiques en cours.

REMARQUE : Seules les adresses MAC affectées à l'interface et au VLAN spécifiés sont affichées.

Status (État) : indique l'état de l'adresse MAC. Ce champ peut prendre les valeurs suivantes :

Permanent : l'adresse MAC est permanente.

Secure (Protégée) : permet de s'assurer que l'adresse MAC d'un port verrouillé ne sera pas supprimée.

Delete on Reset (Supprimer à la réinitialisation) : l'adresse MAC est supprimée lors de la réinitialisation du commutateur.

Delete on Timeout (Supprimer à l'expiration) : l'adresse MAC est supprimée à l'expiration d'un délai.

Ajout d'une adresse MAC statique

1. Affichez la page **Static MAC Address** (Adresse MAC statique).

2. Cliquez sur **Add** (Ajouter).

La page **Add Static MAC Address** (Ajouter une adresse MAC statique) s'affiche.

Figure 8-33. Page Add Static MAC Address (Ajouter une adresse MAC statique)

Print Refresh

New Entry

Interface: Untl 1 | Port: g5 | LAG: 00/0

MAC Address: 08:00:02:01:FC

VLAN ID: 2

VLAN Name: Default

Status: Permanent

Apply Changes Back

3. Complétez les champs selon vos besoins.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle adresse statique est ajoutée à la **table des adresses MAC statiques** et le périphérique est mis à jour.

Modification d'une adresse de la table des adresses MAC statiques

1. Affichez la page **Static MAC Address** (Adresse MAC statique).
2. Modifiez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse MAC statique est modifiée et le périphérique est mis à jour.

Affichage de la table des adresses MAC statiques

1. Affichez la page **Static MAC Address** (Adresse MAC statique).
2. Cliquez sur **Show All** (Afficher tout).

La page **Static MAC Address Table** (Table des adresses MAC statiques) affiche toutes les adresses MAC statiques existantes.

Figure 8-34. Page Static MAC Address Table (Table des adresses MAC statiques)

Print Refresh

	MAC	VLAN ID	Interface	Status	Remove
1	08:00:02:01:FC	1	1/g5	Permanent	<input type="checkbox"/>
2	08:00:02:01:2B	2	1/g5	Permanent	<input type="checkbox"/>

Apply Changes Back

Suppression d'une adresse de la table des adresses statiques

1. Affichez la page **Static MAC Address** (Adresse MAC statique).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **Static MAC Address** (Adresses MAC statiques).
3. Cochez la case **Remove** (Supprimer) en regard de l'adresse à supprimer.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse statique est supprimée et le périphérique est mis à jour.

Configuration des paramètres des adresses statiques à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. Address Table Commands (Commandes portant sur les tables d'adresses)

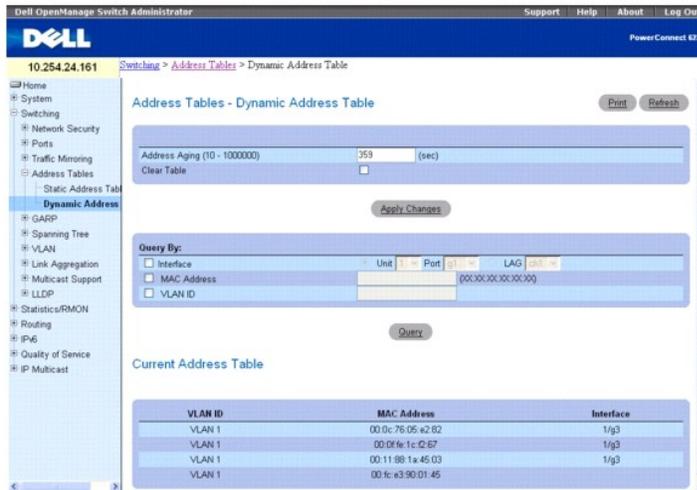
Table des adresses dynamiques

La page **Dynamic Address Table** (Table des adresses dynamiques) contient diverses informations : type d'interface, adresses MAC, VLAN. Elle permet également de sélectionner un critère de tri. Les paquets transmis à une adresse stockée dans la table des adresses sont transférés directement à ces ports.

Cette page contient également des informations sur le délai d'expiration qui s'écoule avant qu'une adresse MAC dynamique ne soit supprimée de la table.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Address Tables** (Tables d'adresses) → **Dynamic Address Table** (Table des adresses dynamiques) dans l'arborescence.

Figure 8-35. Page Dynamic Address Table (Table des adresses dynamiques)



Cette page contient les champs suivants :

Address Aging (10-1000000) (Expiration de l'adresse, 10-1000000) : indique le délai (en secondes) avant suppression d'une adresse MAC dynamique. La valeur par défaut est de 300 secondes.

Clear Table (Effacer la table) : si vous cochez cette option, toutes les données relatives aux adresses MAC dynamiques sont effacées de la table lorsque vous cliquez sur **Apply Changes** (Appliquer les modifications).

La table des adresses dynamiques peut être interrogée en fonction de plusieurs critères :

Interface : indique l'unité et le port interrogés pour une adresse.

LAG : indique le LAG interrogé pour une adresse.

MAC Address (Adresse MAC) : indique l'adresse MAC interrogée pour une adresse.

VLAN ID (ID de VLAN) : indique le numéro de VLAN (auquel l'adresse MAC est rattachée) qui est interrogé pour une adresse.

La section **Current Address Table** (Table des adresses en cours) contient les paramètres d'adresses dynamiques en fonction desquels les paquets sont directement transférés aux ports. Elle contient les champs suivants :

VLAN ID (ID de VLAN) : indique la valeur de la balise VLAN.

MAC Address (Adresse MAC) : affiche l'adresse MAC.

Interface : indique le numéro de port.

Définition du délai d'expiration

1. Affichez la page **Dynamic Address Table** (Table des adresses dynamiques).
2. Définissez le champ **Address Aging** (Expiration de l'adresse).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le délai d'expiration est modifié et le périphérique est mis à jour.

Interrogation de la table des adresses dynamiques

1. Affichez la page **Dynamic Address Table** (Table des adresses dynamiques).
2. Définissez le paramètre à utiliser pour interroger la table.
L'interrogation peut être basée sur l'**interface**, le **LAG**, l'**adresse MAC** ou l'**ID de VLAN**.
3. Cliquez sur **Query** (Interroger) pour interroger la table des adresses dynamiques.

Suppression de données de la table des adresses dynamiques

1. Affichez la page **Dynamic Address Table** (Table des adresses dynamiques).
2. Cochez la case **Clear Table** (Effacer la table).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les données de la table sont effacées.

Interrogation et tri des adresses dynamiques à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Address Table Commands (Commandes portant sur les tables d'adresses)

Configuration du protocole GARP

Le protocole GARP (Generic Attribute Registration Protocol) est un protocole universel qui enregistre toutes les informations relatives à la connectivité du réseau ou au style d'appartenance au réseau. Il définit un ensemble de commutateurs concernés par un attribut réseau donné, tel que le VLAN ou l'adresse de multidiffusion. La page **GARP Timers** (Temporisateurs GARP) est accessible à partir de la page de menu **GARP**.

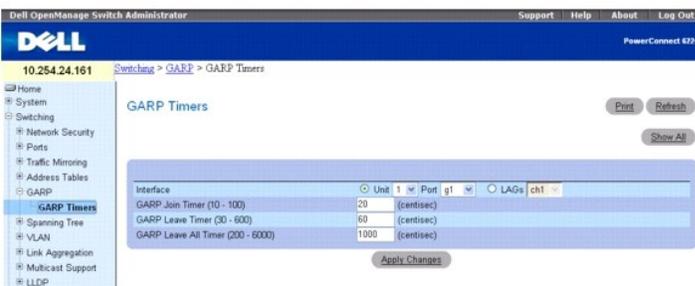
Pour afficher cette page, cliquez sur **Switching** (Commutation) → **GARP** dans l'arborescence.

Temporisateurs GARP

La page **GARP Timers** (Temporisateurs GARP) contient des champs qui permettent d'activer le protocole GARP sur le commutateur.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **GARP** → **GARP Timers** (Temporisateurs GARP) dans l'arborescence.

Figure 8-36. Page GARP Timers (Temporisateurs GARP)



Cette page contient les champs suivants :

Interface : indique l'unité et le port ou LAG sur lesquels le temporisateur GARP est activé.

GARP Join Timer (10-100) (Temporisateur "Join" GARP, 10-100) : affiche le délai (en centièmes de seconde) pendant lequel des PDU sont transmises. Les valeurs admises sont comprises entre 10 et 100. La valeur par défaut est de 100 centièmes de seconde.

GARP Leave Timer (30-600) (Temporisateur "Leave" GARP, 10-600) : affiche le délai (en centièmes de seconde) pendant lequel le commutateur attend avant de quitter son état GARP. Le délai de sortie "Leave Time" est activé par un message "Leave All Time" (Délai général de sortie) envoyé/reçu et annulé par le message "Join" reçu. Le délai de sortie (Leave) doit être supérieur ou égal à trois fois le délai de jonction (Join). Les valeurs admises sont comprises entre 30 et 600. La valeur par défaut est de 60 centièmes de seconde.

GARP Leave All Timer (200-6000) (Temporisateur "Leave All" GARP, 200-6000) : affiche le délai (en centièmes de seconde) pendant lequel tous les commutateurs attendent avant de quitter l'état GARP. Le délai général de sortie (Leave all) doit être supérieur au délai de sortie (Leave). Les valeurs admises sont comprises entre 200 et 6000. La valeur par défaut est de 1000 centièmes de seconde.

Définition des temporisateurs GARP

1. Affichez la page **GARP Timers** (Temporisateurs GARP).
2. Complétez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont copiés sur les ports ou LAG sélectionnés dans la table des temporisateurs GARP et le périphérique est mis à jour.

Affichage des paramètres de la table des temporisateurs GARP

1. Affichez la page **GARP Timers** (Temporisateurs GARP).
2. Cliquez sur **Show All** (Afficher tout).

La table **GARP Timers** (Temporisateurs GARP) s'affiche.

Figure 8-37. Page GARP Timers Table (Table des temporisateurs GARP)

Interface	GARP Join Timer	GARP Leave Timer	GARP Leave All Timer	Copy To	Edit	
1	1/g1	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
2	1/g2	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
3	1/g3	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
27	1/ig3	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
28	1/ig4	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
LAGs						
29	ch1	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
30	ch2	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
31	ch3	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
32	ch4	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
33	ch5	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
34	ch6	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
35	ch7	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>
36	ch8	20	60	1000	<input type="checkbox"/>	<input type="checkbox"/>

3. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **GARP Timers Table** (Table des temporisateurs GARP) pour les autres unités de la pile, le cas échéant.

Copie des paramètres des temporisateurs GARP

1. Affichez la page **GARP Timers** (Temporisateurs GARP).
2. Cliquez sur **Show All** (Afficher tout).

La page **GARP Timers Table** (Table des temporisateurs GARP) s'affiche.

3. Indiquez l'unité et le port à partir desquels vous effectuez la copie dans **Copy Parameters From** (Copie les paramètres à partir de).
4. Cliquez sur **Copy To** (Copier vers) pour chaque interface cible.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des temporisateurs GARP sont copiés et le périphérique est mis à jour.

Modification des paramètres des temporisateurs GARP pour plusieurs ports

1. Affichez la page **GARP Timers** (Temporisateurs GARP).
2. Cliquez sur **Show All** (Afficher tout).

La table **GARP Timers** (Temporisateurs GARP) s'affiche.

3. Cliquez sur **Edit** (Modifier) pour chacune des interfaces à modifier.
4. Modifiez les champs de configuration selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des temporisateurs GARP sont modifiés et le périphérique est mis à jour.

Définition de temporisateurs GARP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 GVRP Commands (Commandes GVRP)

Configuration du protocole Spanning Tree

Le protocole STP (Spanning Tree Protocol) fournit une topologie en arborescence, quelle que soit l'architecture des ponts. Il fournit également un chemin unique entre les stations terminales d'un réseau, éliminant ainsi la formation de boucles. Les versions prises en charge pour ce protocole sont les suivantes : Classic STP, Multiple STP et Rapid STP.

La version Classic STP fournit un chemin unique entre les stations terminales et élimine ainsi la formation de boucles. Pour plus d'informations sur la configuration de Classic STP, voir [Paramètres globaux STP](#).

Le protocole MSTP (Multiple Spanning Tree Protocol) prend en charge plusieurs instances de l'arborescence Spanning Tree afin de canaliser efficacement le trafic VLAN sur différentes interfaces. Le comportement de chacune de ces instances est conforme aux spécifications IEEE 802.1w (Rapid Spanning Tree [RSTP]), avec de légères modifications au niveau du fonctionnement, mais pas de l'effet final. L'un des effets principaux est la transition rapide du port vers l'état Forwarding (Transmission). La différence entre le RSTP et le STP traditionnel (IEEE 802.1d) est la capacité à configurer et à reconnaître la connectivité en duplex intégral et les ports connectés aux stations terminales, ce qui permet d'accélérer le passage du port à l'état "Forwarding" (Transmission) et de supprimer la notification de modification de la topologie. Ces fonctionnalités sont représentées par les paramètres "pointtopoint" et "edgeport". MSTP est compatible avec RSTP et STP. Il se comporte en adéquation avec les ponts STP et RSTP. Un pont MSTP peut en outre être configuré pour se comporter comme un pont RSTP ou STP.

Pour afficher la page **Spanning Tree**, cliquez sur **Switching** (Commutation) → **Spanning Tree** dans l'arborescence. Cette page contient des liens vers les procédures STP suivantes :

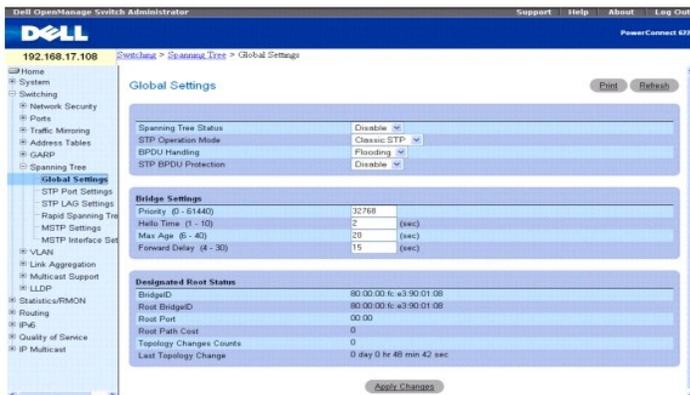
- 1 [Paramètres globaux STP](#)
- 1 [Paramètres des ports STP](#)
- 1 [Paramètres des LAG STP](#)
- 1 [Rapid Spanning Tree \(RSTP\)](#)
- 1 [Paramètres MSTP](#)
- 1 [Paramètres des interfaces MSTP](#)

Paramètres globaux STP

La page **STP Global Settings** (Paramètres globaux STP) contient des champs qui permettent d'activer le protocole STP sur le commutateur.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Spanning Tree** → **Global Settings** (Paramètres globaux) dans l'arborescence.

Figure 8-38. Page Global Settings (Paramètres globaux) de Spanning Tree



Cette page contient les champs suivants :

Spanning Tree Status (État de Spanning Tree) : active ou désactive le protocole STP, Rapid STP ou MSTP sur le commutateur.

STP Operation Mode (Mode de fonctionnement STP) : indique le mode de fonctionnement STP activé sur le commutateur. Ce champ peut prendre les valeurs suivantes : **Classic STP**, **Rapid STP**, **Multiple STP**.

BPDU Handling (Traitement des BPDU) : définit le traitement appliqué aux paquets BPDU (Bridge Protocol Data Unit) lorsque le protocole STP est désactivé sur une interface. Les valeurs possibles sont Filtering (Filtrage) et Flooding (Acheminement simultané). La valeur par défaut est Flooding (Acheminement simultané).

STP BPDU Protection (Protection des BPDU STP) : désactive un port si un nouveau commutateur tente d'accéder à la topologie STP existante. Cela empêche toute modification de la topologie STP par des commutateurs ne faisant pas partie de l'arborescence d'origine.

Si vous sélectionnez Enable (Activer), lorsqu'une BPDU est reçue sur un port d'extrémité ("edge port"), ce dernier est désactivé. Le port désactivé doit être réactivé manuellement.

Bridge Settings (Paramètres des ponts)

Priority (0-61440) (Priorité, 0-61440) : indique la valeur de priorité du pont. Les commutateurs ou les ponts exécutant le protocole STP se voient affecter un degré de priorité. Après avoir échangé des BPDU, le commutateur possédant la priorité la plus basse devient le pont racine.

Hello Time (1-10) (Délai Hello) : indique le délai (en secondes) pendant lequel le pont racine attend entre deux messages de configuration. La valeur par défaut est de 2.

Max Age (6-40) (Délai d'attente maximal, 6-40) : indique l'âge maximal du commutateur, c'est-à-dire le délai d'attente maximal (en secondes) pendant lequel le pont attend avant d'implémenter une modification de la topologie. La valeur par défaut est de 20.

Forward Delay (4-30) (Délai avant transfert, 4-30) : indique le délai d'attente avant transfert du commutateur, c'est-à-dire le délai pendant lequel un pont reste dans un état d'écoute et d'apprentissage avant de transmettre les paquets. La valeur par défaut est de 15.

État du pont racine

Bridge ID (ID du pont) : affiche l'ID du pont.

Root Bridge ID (ID du pont racine) : indique l'ID du pont racine.

Root Port (Port racine) : indique le numéro du port correspondant au chemin dont le coût est le plus faible entre ce pont et le pont racine. Ce paramètre est significatif lorsque le pont n'est pas le pont racine. La valeur par défaut est zéro.

Root Path Cost (Coût du chemin racine) : affiche le coût du chemin entre ce pont et la racine.

Topology Changes Counts (Nombre de modifications de la topologie) : affiche le nombre total de fois où l'état de la topologie STP a été modifié.

Last Topology Change (Dernière modification de la topologie) : affiche la durée totale qui s'est écoulée depuis la dernière modification de la topologie. La durée est exprimée au format jour/heures/minutes/secondes ; par exemple : 5 heures, 10 minutes et 4 secondes.

Définition des paramètres globaux STP

1. Affichez la page **STP Global Settings** (Paramètres globaux STP).
2. Sélectionnez **Enable** (Activer) dans le champ **Spanning Tree Status** (État de Spanning Tree).
3. Spécifiez le mode **STP** dans le champ **STP Operation Mode** (Mode de fonctionnement STP), et définissez les autres paramètres.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le protocole STP est activé sur le commutateur.

Modification des paramètres globaux STP

1. Affichez la page **STP Global Settings** (Paramètres globaux STP).
2. Modifiez les champs de cette page selon vos besoins.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres STP sont modifiés et le périphérique est mis à jour.

Définition des paramètres globaux STP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Spanning Tree Commands (Commandes portant sur le protocole Spanning Tree)

Paramètres des ports STP

La page **STP Port Settings** (Paramètres des ports STP) permet d'affecter des propriétés STP aux ports.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Spanning Tree** → **STP Port Settings** (Paramètres des ports STP) dans l'arborescence.

Figure 8-39 Page STP Port Settings (Paramètres des ports STP)



Cette page contient les champs suivants :

Select a Port (Sélectionner un port) : indique l'unité et le port sur lesquels le protocole STP est activé.

STP : active ou désactive le protocole STP sur le port.

Fast Link : active le mode Fast Link sur le port. Un port en mode Fast Link passe automatiquement à l'état **Forwarding** (Transfert) lorsque la liaison est active. La convergence STP peut nécessiter jusqu'à 30-60 secondes dans les réseaux de grande envergure.

Port State (État du port) : indique l'état STP actuel d'un port. L'état du port détermine l'action de transfert qui doit être appliquée au trafic. Le port peut avoir les états suivants :

Disabled (Désactivé) : le protocole STP est désactivé sur le port. Le port transfère le trafic lors de l'apprentissage des adresses MAC.

Blocking (Blocage) : le port est actuellement bloqué et ne peut pas être utilisé pour transférer le trafic ni apprendre des adresses MAC.

Listening (Écoute) : le port est actuellement en mode écoute. Il ne peut pas transférer le trafic ni apprendre des adresses MAC.

Learning (Apprentissage) : le port est actuellement en mode d'apprentissage. Il ne peut pas transférer le trafic, mais il est en mesure d'apprendre de nouvelles adresses MAC.

Forwarding (Transfert) : le port est actuellement en mode de transfert. Il peut transférer le trafic et apprendre de nouvelles adresses MAC.

STP Root Guard (Protection de la racine STP) : empêche toute modification imprévue de la racine d'une instance STP. Si une BPDU de niveau supérieur arrive sur un pont racine protégé par cette option, le port correspondant est placé dans un mode spécial signalant une incohérence de la racine, ce qui équivaut au mode d'écoute. L'utilisation du pont racine est forcée.

Role (Rôle) : affiche le rôle du port dans la topologie STP.

Speed (Vitesse) : affiche la vitesse de fonctionnement du port.

Path Cost (1-200000000) (Coût du chemin, 1-200000000) : définit la contribution du port au coût du chemin racine. Le coût du chemin est arrondi à une valeur supérieure ou inférieure. Il est utilisé pour transférer le trafic lorsqu'un chemin est réacheminé. Une valeur égale à zéro signifie que le coût du chemin est défini en fonction de la vitesse du port. La valeur par défaut est de 0.

Priority (0-240) (Priorité, 0-240) : indique la valeur de priorité du port. Cette valeur influence le choix du port lorsqu'un pont contient deux ports connectés en boucle. La valeur par défaut est de 128.

Designated Bridge ID (ID du pont désigné) : affiche l'ID du pont désigné.

Designated Port ID (ID du port désigné) : affiche l'ID du port sélectionné.

Designated Cost (Coût désigné) : affiche le coût du port participant à la topologie STP. Si le protocole détecte des boucles, le risque de blocage des ports sera moindre si leur coût est inférieur.

LAG : affiche le LAG auquel le port est rattaché.

Activation du protocole STP sur un port

1. Affichez la page **STP Port Settings** (Paramètres des ports STP).
 2. Indiquez l'unité et le port à activer dans le champ **Select a Port** (Sélectionner un port).
 3. Sélectionnez **Enable** (Activer) dans le champ **STP**.
 4. Modifiez les champs **Fast Link**, **STP Root Guard** (Protection de la racine STP), **Path Cost** (Coût du chemin) et **Priority** (Priorité) selon vos besoins.
 5. Cliquez sur **Apply Changes** (Appliquer les modifications).
- Le protocole STP est activé sur le port.

Modification des propriétés des ports STP

1. Affichez la page **STP Port Settings** (Paramètres des ports STP).
 2. Modifiez les champs **Fast Link**, **STP Root Guard** (Protection de la racine STP), **Path Cost** (Coût du chemin) et **Priority** (Priorité) selon vos besoins.
 3. Cliquez sur **Apply Changes** (Appliquer les modifications).
- Les paramètres des ports STP sont modifiés et le périphérique est mis à jour.

Affichage de la table des ports STP

1. Affichez la page **STP Port Settings** (Paramètres des ports STP).
 2. Cliquez sur **Show All** (Afficher tout).
- La page **STP Port Table** (Table des ports STP) s'affiche.

Figure 8-40. Page STP Port Table (Table des ports STP)

The screenshot shows the 'STP Port Table' interface. At the top, there are 'Unit' and 'Refresh' buttons. Below is a search bar with '1' entered. The main table has the following columns: Port, STP, Fast Link, STP Root Guard, State, Role, Path Cost, Priority, Designated Bridge ID, Designated Port ID, Designated Cost, and Edit. The table contains several rows of data, including ports 1/1g1, 1/1g2, 1/1g3, 20/11g2, 22/11g3, and 28/11g4. Each row has a dropdown menu for the 'STP' column and a checkmark in the 'Edit' column.

Port	STP	Fast Link	STP Root Guard	State	Role	Path Cost	Priority	Designated Bridge ID	Designated Port ID	Designated Cost	Edit
1/1g1	Enable	Disable	Manual Forward Disabled	Disabled	0	128	80:00:00:0:c3:90:01:45	00:00	0	0	✓
1/1g2	Enable	Disable	Disabled	Disabled	0	128	80:00:00:0:c3:90:01:45	00:00	0	0	✓
1/1g3	Enable	Disable	Manual Forward Disabled	Disabled	0	128	80:00:00:0:c3:90:01:45	00:00	0	0	✓
20/11g2	Enable	Disable	Disabled	Disabled	0	128	80:00:00:0:c3:90:01:45	00:00	0	0	✓
22/11g3	Enable	Disable	Disabled	Disabled	0	128	80:00:00:0:c3:90:01:45	00:00	0	0	✓
28/11g4	Enable	Disable	Disabled	Disabled	0	128	80:00:00:0:c3:90:01:45	00:00	0	0	✓

At the bottom of the table, there are 'Apply Changes' and 'Back' buttons.

3. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **STP Port Table** (Table des ports STP) pour les autres unités de la pile, le cas échéant.

Modification des paramètres STP pour plusieurs ports

1. Affichez la page **STP Port Settings** (Paramètres des ports STP).
 2. Cliquez sur **Show All** (Afficher tout).
- La page **STP Port Table** (Table des ports STP) s'affiche.

3. Cliquez sur **Edit** (Modifier) pour chacun des ports à modifier.
4. Modifiez les paramètres des ports STP selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des ports STP sont modifiés et le périphérique est mis à jour.

Application du mode Fast Link à un port

1. Affichez la page **STP Port Settings** (Paramètres des ports STP).

2. Cliquez sur **Show All** (Afficher tout).

La page **STP Port Table** (Table des ports STP) s'affiche.

3. Cliquez sur **Edit** (Modifier) pour chacun des ports à modifier.

4. Cochez la case **Fast Link** pour activer le mode Fast Link sur un port. Un port en mode Fast Link passe automatiquement à l'état **Forwarding** (Transfert) lorsque la liaison est active.

5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont modifiés et le périphérique est mis à jour.

Définition des paramètres des ports STP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- Spanning Tree Commands (Commandes portant sur le protocole Spanning Tree)

Paramètres des LAG STP

La page **STP LAG Settings** (Paramètres des LAG STP) permet de définir les paramètres STP des ports agrégés.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Spanning Tree** → **STP LAG Settings** (Paramètres des LAG STP) dans l'arborescence.

Figure 8-41. Page **STP LAG Settings** (Paramètres des LAG STP)



Cette page contient les champs suivants :

Select a LAG (Sélectionner un LAG) : indique le numéro du LAG dont vous souhaitez modifier les paramètres STP.

STP : active ou désactive le protocole STP sur le LAG. Le paramètre par défaut est Enable (Activer).

Fast Link : active le mode Fast Link sur le LAG. Un LAG en mode Fast Link passe automatiquement à l'état **Forwarding** (Transfert) lorsqu'il est actif. Le mode Fast Link optimise le temps nécessaire à la convergence du protocole STP. La convergence STP peut nécessiter jusqu'à 30-60 secondes dans les réseaux de grande envergure.

Port State (État du port) : affiche l'état STP actuel d'un LAG. L'état du LAG détermine l'action de transfert qui doit être appliquée au trafic. Si le pont détecte un LAG défectueux, ce dernier passe à l'état **Broken** (Interrompu). Un LAG peut avoir les états suivants :

Disabled (Désactivé) : le protocole STP est désactivé sur le LAG. Le LAG transfère le trafic et apprend des adresses MAC.

Blocking (Blocage) : le LAG est bloqué et ne peut pas être utilisé pour transférer le trafic ni apprendre des adresses MAC.

Listening (Écoute) : le LAG est en mode d'écoute et ne peut pas transférer le trafic ni apprendre des adresses MAC.

Learning (Apprentissage) : le LAG est en mode d'apprentissage et ne peut pas transférer le trafic, mais il peut apprendre de nouvelles adresses MAC.

Forwarding (Transfert) : le LAG est en mode de transfert : il peut transférer le trafic et apprendre de nouvelles adresses MAC.

Broken (Interrompu) : le LAG ne fonctionne pas correctement et ne peut pas être utilisé pour transférer le trafic.

Role (Rôle) : affiche le rôle du port dans la topologie STP.

Path Cost (1-200000000) (Coût du chemin, 1-200000000) : définit la contribution du LAG au coût du chemin racine. Le coût du chemin est arrondi à une valeur supérieure ou inférieure. Il est utilisé pour transférer le trafic lorsqu'un chemin est réacheminé. La valeur par défaut est de 0.

Priority (0-240) (Priorité, 0-240) : indique la valeur de priorité du LAG. Cette valeur influence le choix du LAG lorsqu'un pont contient deux ports connectés en boucle. Elle est comprise entre 0 et 240.

Designated Bridge ID (ID du pont désigné) : affiche l'ID du pont désigné.

Designated Port ID (ID du port désigné) : affiche l'ID du port désigné.

Designated Cost (Coût désigné) : affiche le coût du port participant à la topologie STP. Si le protocole détecte des boucles, le risque de blocage des ports sera moindre si leur coût est inférieur.

Modification des paramètres STP d'un LAG

1. Affichez la page **STP LAG Settings** (Paramètres des LAG STP).
2. Sélectionnez un LAG dans le menu déroulant **Select a LAG** (Sélectionner un LAG).
3. Modifiez les champs selon vos besoins.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont modifiés et le périphérique est mis à jour.

Affichage de la table des LAG STP

1. Affichez la page **STP LAG Settings** (Paramètres des LAG STP).
2. Cliquez sur **Show All** (Afficher tout).

La page **STP LAG Table** (Table des LAG STP) s'affiche.

Figure 8-42. Page STP LAG Table (Table des LAG STP)

Port	STP	Fast Link	STP Root Guard	State	Role	Path Cost	Priority	Designated Bridge ID	Designated Port ID	Designated Cost
S1	Enabled	Disabled	Disabled	Disabled	0	128	80:00:00:43:90:01:45	00:00	0	
S2	Enabled	Disabled	Disabled	Disabled	0	128	80:00:00:43:90:01:45	00:00	0	
S3	Enabled	Disabled	Disabled	Disabled	0	128	80:00:00:43:90:01:45	00:00	0	
S4	Enabled	Disabled	Disabled	Disabled	0	128	80:00:00:43:90:01:45	00:00	0	
S5	Enabled	Disabled	Disabled	Disabled	0	128	80:00:00:43:90:01:45	00:00	0	
S6	Enabled	Disabled	Disabled	Disabled	0	128	80:00:00:43:90:01:45	00:00	0	
S7	Enabled	Disabled	Disabled	Disabled	0	128	80:00:00:43:90:01:45	00:00	0	
S8	Enabled	Disabled	Disabled	Disabled	0	128	80:00:00:43:90:01:45	00:00	0	

3. Cette table permet d'activer et de désactiver le mode Fast Link et la protection de la racine STP pour un LAG. Pour ce faire, cliquez sur **Fast Link**, sélectionnez les options appropriées et cliquez sur **Apply Changes** (Appliquer les modifications).

Modification des paramètres STP pour plusieurs LAG

1. Affichez la page **STP LAG Settings** (Paramètres des LAG STP).
2. Cliquez sur **Show All** (Afficher tout).

La page **STP LAG Table** (Table des LAG STP) s'affiche.

3. Cochez l'option **Edit** (Modifier) pour tous les LAG à modifier.
4. Modifiez les champs selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont modifiés et le périphérique est mis à jour.

Définition des paramètres des LAG STP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

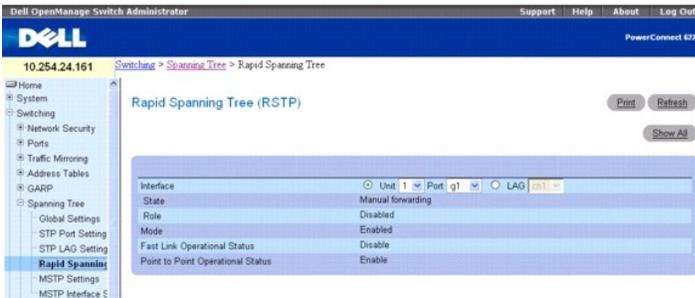
- 1 Spanning Tree Commands (Commandes portant sur le protocole Spanning Tree)

Rapid Spanning Tree (RSTP)

Le protocole Rapid Spanning Tree (RSTP) détecte et sélectionne les topologies de réseau offrant une meilleure convergence du Spanning Tree, sans pour autant créer de boucles de transfert.

Pour afficher la page **Rapid Spanning Tree**, cliquez sur **Switching** (Commutation) → **Spanning Tree** → **Rapid Spanning Tree** dans l'arborescence.

Figure 8-43. Page Rapid Spanning Tree



Cette page contient les champs suivants :

Interface : détermine si le protocole RSTP est activé sur une unité/port ou un LAG. Cliquez sur Unit/Port (Unité/Port) ou LAG pour spécifier le type d'interface, puis sélectionnez l'unité/port ou le LAG à configurer dans le menu déroulant.

State (État) : affiche l'état STP du port.

Role (Rôle) : affiche le rôle du port dans la topologie STP.

Mode : affiche le mode administratif et indique s'il est activé ou non.

Fast Link Operational Status (État opérationnel Fast Link) : indique si le mode Fast Link est activé ou désactivé pour le port ou le LAG. Si le mode Fast Link est activé pour un port, celui-ci passe automatiquement à l'état de transfert (Forwarding). Ce paramètre peut être modifié dans les pages [STP Port Settings](#) (Paramètres des ports STP) ou [STP LAG Settings](#) (Paramètres des LAG STP).

Point to Point Operational Status (État de fonctionnement point à point) : affiche l'état de fonctionnement point à point.

Pour établir des communications sur une liaison point à point, le protocole PPP émetteur envoie d'abord des paquets Link Control Protocol (LCP) pour configurer et vérifier la liaison de données. Une fois la liaison établie et les fonctions optionnelles négociées par le protocole LCP, le protocole PPP émetteur envoie des paquets Network Control Protocols (NCP) pour sélectionner et configurer un ou plusieurs protocoles de couche réseau. Lorsque tous les protocoles de couche réseau sélectionnés ont été configurés, les paquets de chaque protocole peuvent être envoyés sur la liaison. Cette dernière reste configurée pour les communications jusqu'à ce que des paquets LCP ou NCP ferment la liaison ou qu'un événement extérieur intervienne. Ce type de liaison est celui qui est utilisé par les ports du commutateur.

Affichage de la table RSTP (Rapid Spanning Tree)

1. Affichez la page **Rapid Spanning Tree (RSTP)**.
2. Cliquez sur **Show All** (Afficher tout).

La page **Rapid Spanning Tree Table** (Table Rapid Spanning Tree) s'affiche.

Figure 8-44. Page Rapid Spanning Tree Table (Table Rapid Spanning Tree)

Rapid Spanning Tree Table Print Refresh

Unit

Interface	Role	Fast Link Operational Status	Point to Point Operational Status
1	1/g1	Designated	Disabled
2	1/g2	Designated	Disabled
3	1/g3	Designated	Disabled

26	1/r/g2	Disabled	Disabled
27	1/r/g3	Disabled	Disabled
28	1/r/g4	Disabled	Disabled

LAGs			
29	ch1	Disabled	False
30	ch2	Disabled	False
31	ch3	Disabled	False
32	ch4	Disabled	False
33	ch5	Disabled	False
34	ch6	Disabled	False
35	ch7	Disabled	False
36	ch8	Disabled	False

Back

- Utilisez le menu déroulant Unit (Unité) pour afficher la page Rapid Spanning Tree Table (Table Rapid Spanning Tree) pour les autres unités de la pile, le cas échéant.

Définition des paramètres RSTP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- Spanning Tree Commands (Commandes portant sur le protocole Spanning Tree)

Paramètres MSTP

Le protocole MSTP (Multiple Spanning Tree Protocol) prend en charge plusieurs instances de l'arborescence STP afin de canaliser efficacement le trafic VLAN sur différentes interfaces. Il est compatible avec les protocoles RSTP et STP. Un pont MSTP peut en outre être configuré pour se comporter comme un pont RSTP ou STP.

Pour afficher la page MSTP Settings (Paramètres MSTP), cliquez sur Switching (Commutation) → Spanning Tree → MSTP Settings (Paramètres MSTP) dans l'arborescence.

Figure 8-45. Page MSTP Settings (Paramètres MSTP)

Dell OpenManage Switch Administrator Support Help About Log Out

DELL PowerConnect 8324

10.254.24.161 [Switching](#) > [Spanning Tree](#) > MSTP Settings

MSTP Settings Print Refresh

Show All

Global Settings

Region Name (1 - 32 characters)

Revision (0 - 65535)

Max Hops (1 - 40)

Instance ID

Instance Settings

Instance ID

Included VLANs

Priority (0 - 61440)

BridgeID

Root BridgeID

Root Port

Root Path Cost

Apply Changes

La page MSTP Settings (Paramètres MSTP) contient les champs suivants, divisés en deux sections : Global Settings (Paramètres globaux) et Instance Settings (Paramètres de l'instance) :

Region Name (1-32 Characters) (Nom de la région, 1-32 caractères) : indique le nom de la région MST définie par l'utilisateur.

Revision (0-65535) (Révision, 0-65535) : définit le chiffre 16 bits non signé identifiant le niveau de révision de la configuration MST actuelle. Le numéro de révision est indispensable à la configuration MST. La valeur par défaut est de 0.

Max Hops (1-40) (Nombre maximum de sauts, 1 à 40) : définit le nombre total de sauts effectués dans une région spécifique avant que la BPDU ne soit rejetée. Une fois la BPDU rejetée, les informations du port arrivent à expiration. La valeur par défaut est de 20.

Instance ID (ID de l'instance) : indique l'ID de l'instance STP. Les valeurs possibles sont comprises entre 1 et 15. La valeur par défaut est de 1.

Included VLANs (VLAN inclus) : mappe les VLAN sélectionnés avec l'instance sélectionnée. Chaque VLAN n'appartient qu'à une seule instance.

Priority (0-61440) (Priorité, 0-61440) : définit la priorité du commutateur pour l'instance STP sélectionnée. La valeur par défaut est de 32768.

Bridge ID (ID du pont) : indique l'ID de pont de l'instance sélectionnée.

Root Bridge ID (ID du pont racine) : ID du pont racine présentant le coût de chemin le plus faible.

Root Port (Port racine) : indique le port racine de l'instance sélectionnée.

Root Path Cost (Coût du chemin racine) : indique le coût du chemin correspondant à l'instance sélectionnée.

Modification des paramètres MSTP

1. Affichez la page **MSTP Settings (Paramètres MSTP)**.
2. Modifiez les champs des sections **Global Settings (Paramètres globaux)** et **Instance Settings (Paramètres de l'instance)** selon vos besoins.
3. Cliquez sur **Apply Changes (Appliquer les modifications)**.

Les paramètres MSTP sont modifiés et le périphérique est mis à jour.

Affichage de la table des mappages entre les VLAN et les instances MSTP

1. Affichez la page **MSTP Settings (Paramètres MSTP)**.
2. Cliquez sur **Show All (Afficher tout)**.

La table **MSTP Settings (Paramètres MSTP)** s'affiche.

Figure 8-46. Table MSTP Settings (Paramètres MSTP)

	VLAN	Instance ID (#)	Edit
1	1	0	<input type="checkbox"/>
2	3	0	<input type="checkbox"/>
3	5	0	<input type="checkbox"/>
4	7	0	<input type="checkbox"/>
5	888	0	<input type="checkbox"/>
6	2222	0	<input type="checkbox"/>

3. Pour modifier l'ID de l'instance pour un ou plusieurs VLAN, cochez la case **Edit (Modifier)** en regard des VLAN concernés.
4. Modifiez les ID d'instance selon vos besoins. Saisissez 0 pour supprimer le mappage entre un VLAN et une instance.
5. Cliquez sur **Apply Changes (Appliquer les modifications)**.

Les ID des instances sont modifiés pour les VLAN sélectionnés et le périphérique est mis à jour.

Définition d'instances MSTP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

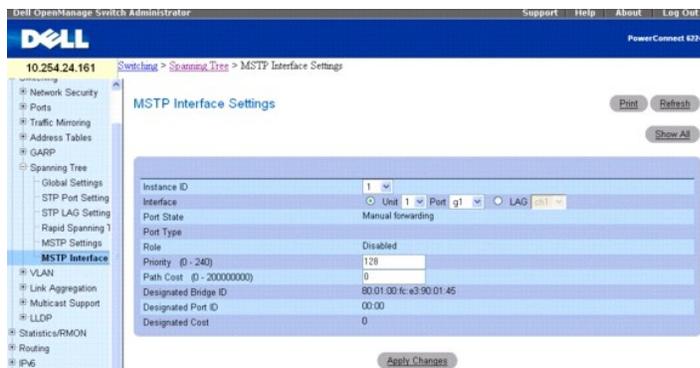
1. Spanning Tree Commands (Commandes portant sur le protocole Spanning Tree)

Paramètres des interfaces MSTP

La page **MSTP Interface Settings (Paramètres des interfaces MSTP)** permet d'affecter des paramètres MSTP à des interfaces spécifiques.

Pour afficher cette page, cliquez sur **Switching (Commutation)** → **Spanning Tree** → **MSTP Interface Settings (Paramètres des interfaces MSTP)** dans l'arborescence.

Figure 8-47. Page MSTP Interface Settings (Paramètres des interfaces MSTP)



La page **MSTP Interface Settings** (Paramètres des interfaces MSTP) contient les champs suivants :

Instance ID (ID d'instance) : sélectionne les instances MSTP configurées sur le commutateur. Les valeurs admises sont comprises entre 1 et 15.

Interface : sélectionne une unité/port ou un LAG pour cette instance MSTP.

Port State (État du port) : indique si le port est activé ou désactivé dans cette instance spécifique.

Port Type (Type de port) : indique si le protocole MSTP traite le port comme un port point à point ou connecté à un concentrateur, et s'il s'agit d'un port interne de la région MST ou d'un port frontière. Si le port est un port frontière, ce champ indique également si le commutateur situé à l'autre extrémité de la liaison fonctionne en mode RSTP ou STP.

Role (Rôle) : indique le rôle attribué au port par l'algorithme STP afin de fournir des chemins STP. Les valeurs possibles sont les suivantes :

Root (Racine) : fournit le chemin dont le coût est le plus faible pour le transfert des paquets vers le commutateur racine.

Designated (Désigné) : indique le port ou LAG sur lequel le commutateur désigné est connecté au LAN.

Alternate (Autre) : fournit un autre chemin vers le commutateur racine à partir de l'interface.

Backup (Chemin de secours) : fournit un chemin de secours vers le LAN désigné. Les ports de secours servent uniquement lorsque deux ports sont connectés en boucle par une liaison point à point, ou lorsqu'un LAN comporte deux connexions ou plus à un segment partagé.

Disabled (Désactivé) : indique que le port ne fait pas partie de la topologie Spanning Tree.

Priority (Priorité) : définit la priorité de l'interface pour l'instance spécifiée. Les priorités admises sont comprises entre 0 et 240, par incréments de 16. La valeur par défaut est de 128.

Path Cost (0-200000000) (Coût du chemin, 0-200000000) : indique la contribution du port à l'instance STP. Les valeurs admises sont comprises entre 0 et 200 000 000. La valeur par défaut est déterminée par la vitesse du port. La valeur par défaut est :

- 1 Canal du port : 20 000
- 1 1000 Mbps (giga) : 20 000
- 1 100 Mbps : 200 000
- 1 10 Mbps : 2 000 000

Designated Bridge ID (ID du pont désigné) : numéro d'ID du pont qui connecte la liaison ou le LAN partagé à la racine.

Designated Port ID (ID du port désigné) : numéro d'ID du port sur le pont désigné qui connecte la liaison ou le LAN partagé à la racine.

Designated Cost (Coût désigné) : affiche le coût du chemin entre la liaison ou le LAN partagé et la racine.

Affectation des paramètres des interfaces MSTP

1. Affichez la page **MSTP Interface Settings** (Paramètres des interfaces MSTP).
2. Sélectionnez une ID d'instance dans le menu déroulant **Instance ID**.
3. Indiquez un **port** ou un **LAG**, puis sélectionnez l'interface dans le menu déroulant associé.
4. Définissez une valeur dans les champs **Interface Priority** (Priorité de l'interface) et **Path Cost** (Coût du chemin).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de l'interface sont enregistrés et le périphérique est mis à jour.

Affichage de la table de paramètres des interfaces MSTP

1. Affichez la page **MSTP Settings** (Paramètres MSTP).
2. Cliquez sur **Show All** (Afficher tout).

La page **MSTP Interface Table** (Table des interfaces MSTP) s'affiche.

Figure 8-48. Page MSTP Interface Table (Table des interfaces MSTP)

Interface	Role	Port Priority	Path Cost	Port State	Designated Cost	Designated Bridge ID	Designated Port ID	Edit
1 1/1g1	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	8001	<input type="checkbox"/>
2 1/1g2	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	8002	<input type="checkbox"/>
3 1/1g3	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	8003	<input type="checkbox"/>

26 1/1g2	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	801A	<input type="checkbox"/>
27 1/1g3	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	801B	<input type="checkbox"/>
28 1/1g4	Enabled	128	0	Enabled	0	80:01:00:FC:E3:90:01:45	801C	<input type="checkbox"/>

3. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **MSTP Interface Table** (Table des interfaces MSTP) pour les autres unités de la pile, le cas échéant.
4. Pour modifier la priorité des ports ou le coût du chemin pour une ou plusieurs interfaces, cochez la case **Edit** (Modifier) en regard des interfaces concernées.
5. Modifiez les valeurs définies dans les colonnes **Port Priority** (Priorité des ports) ou **Path Cost** (Coût du chemin).
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les champs sont modifiés pour les interfaces sélectionnées et le périphérique est mis à jour.

Définition d'interfaces MSTP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Spanning Tree Commands (Commandes portant sur le protocole Spanning Tree)

Configuration des VLAN

L'ajout de la prise en charge des LAN virtuels (VLAN) à un commutateur de couche 2 permet de combiner certains avantages offerts par les ponts et les routeurs. En effet, à l'instar d'un pont, un commutateur inclus dans un VLAN transfère le trafic en fonction de l'en-tête de couche 2, ce qui permet de bénéficier d'une plus grande rapidité. Mais il fonctionne également comme un routeur car il partitionne le réseau en segments logiques, ce qui permet de bénéficier de fonctions améliorées en ce qui concerne l'administration, la sécurité et la gestion du trafic de multidiffusion.

Un VLAN est un ensemble regroupant des stations terminales et les ports de commutation qui les connectent. La division logique, quant à elle, peut se justifier par différents facteurs tel que l'appartenance à un projet ou à un service. Il existe une seule contrainte physique, à savoir que la station terminale et le port auquel elle est reliée doivent faire partie du même VLAN.

Chaque VLAN d'un réseau possède un ID qui apparaît dans la balise IEEE 802.1Q de l'en-tête de couche 2 figurant dans les paquets transmis sur un VLAN. Une station terminale peut omettre la balise ou la partie de la balise définissant le VLAN. Dans ce cas, le premier port de commutation recevant le paquet peut rejeter ce dernier ou y insérer une balise contenant un ID de VLAN par défaut. Un port donné peut gérer le trafic correspondant à plusieurs VLAN, mais il ne peut prendre en charge qu'un seul ID de VLAN par défaut.

Pour afficher la page **VLAN**, cliquez sur **Switching** (Commutation) → **VLAN** dans l'arborescence. Cette page contient des liens vers les fonctionnalités suivantes :

- 1 [Appartenance à un VLAN](#)
- 1 [Paramètres des ports de VLAN](#)
- 1 [Paramètres des LAG de VLAN](#)
- 1 [Liaison d'adresses MAC et de VLAN](#)
- 1 [Liaison de sous-réseau IP et de VLAN](#)
- 1 [Groupe de protocoles](#)
- 1 [Paramètres GVRP](#)

Appartenance à un VLAN

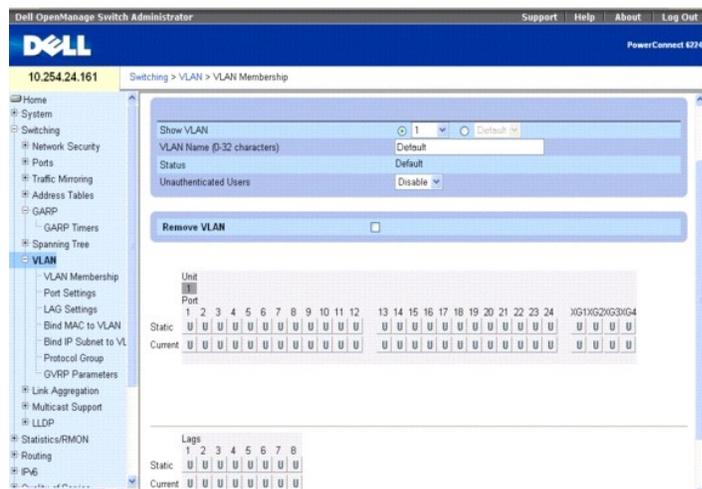
La page **VLAN Membership** (Appartenance à un VLAN) permet de définir les groupes de VLAN répertoriés dans la table d'appartenance à un VLAN. Le commutateur prend en charge jusqu'à 4094 VLAN. Cependant, vous ne pouvez réellement créer que 4092 VLAN car :

- 1 le VLAN 1 est le VLAN par défaut dont tous les ports font partie ;
- 1 le VLAN 4095 est désigné comme VLAN de rejet ("Discard VLAN").

Vous ne pouvez créer que les VLAN de 2 à 4093. Le VLAN 4094 est réservé.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **VLAN** → **VLAN Membership** (Appartenance à un VLAN) dans l'arborescence.

Figure 8-49. Page VLAN Membership (Appartenance à un VLAN)



La page **VLAN Membership** (Appartenance à un VLAN) contient deux sections. La section du haut contient les champs définissant l'appartenance au VLAN dans sa globalité. La section du bas contient des tables définissant les paramètres d'appartenance pour des ports et des LAG spécifiques de ce VLAN. Les champs de la page **VLAN Membership** (Appartenance à un VLAN) sont les suivants :

Show VLAN (Afficher le VLAN) : sélectionne le VLAN à afficher. Utilisez les menus déroulants **VLAN ID** (ID du VLAN) ou **VLAN Name** (Nom du VLAN) pour sélectionner le VLAN.

VLAN Name (0-32) (Nom du VLAN, 0-32) : indique le nom de VLAN défini par l'utilisateur. Ce champ est défini à l'aide du bouton **Add** (Ajouter). Le nom peut comprendre de 0 à 32 caractères.

Status (État) : indique le type de VLAN. Ce champ peut prendre les valeurs suivantes :

Dynamic (Dynamique) : indique que le VLAN a été créé dynamiquement via le protocole GVRP.

Static (Statique) : indique que le VLAN est défini par l'utilisateur et peut être modifié.

Default (Par défaut) : indique que le VLAN est le VLAN par défaut.

Unauthenticated Users (Utilisateurs non authentifiés) : lorsque **Enable** (Activer) est sélectionné, les commutateurs non autorisés peuvent accéder à ce VLAN.

Remove VLAN (Supprimer le VLAN) : lorsque cette case est cochée, le VLAN affiché est supprimé de la table d'appartenance à un VLAN.

La table **VLAN Membership** (Appartenance à un VLAN) affiche les ports et les LAG qui sont membres du VLAN. Elle indique également s'ils sont balisés (T, tagged), non balisés (U, untagged) ou interdits (F, forbidden). Les tables contiennent deux lignes : **Static** (Statique) et **Current** (En cours). Seule la ligne **Static** (Statique) est accessible depuis cette page. La ligne **Current** (En cours) est mise à jour dynamiquement au moyen du protocole GVRP, ou bien lorsque vous modifiez la ligne **Static** (Statique) puis cliquez sur **Apply Changes** (Appliquer les modifications).

Cette section de la page comporte deux tables :

Ports : affiche les ports appartenant à des VLAN et permet de définir des affectations. Pour affecter un port, cliquez sur **Static** (Statique) pour un port spécifique. Chaque clic permet de basculer entre U (non balisé), T (balisé) et un champ vide. Reportez-vous à la table ci-après pour connaître les définitions.

LAGs : affiche les LAG appartenant à des VLAN et permet de définir des affectations. Pour définir une affectation, cliquez sur **Static** (Statique) pour un LAG spécifique. Chaque clic permet de basculer entre U (non balisé), T (balisé) et un champ vide. Reportez-vous à la table ci-après pour connaître les définitions.

Tableau 8-1. Définitions concernant l'appartenance d'un port à un VLAN

Contrôle du port	Définition
T	Balisé (Tagged) : l'interface est membre d'un VLAN. Tous les paquets transmis par cette interface sont balisés et contiennent des informations sur le VLAN.
U	Non balisé (Untagged) : l'interface est membre d'un VLAN, Les paquets transmis par cette interface ne sont pas balisés.

F	Interdit (Forbidden) : indique que l'interface n'est pas autorisée à devenir membre d'un VLAN.
Champ vide	Champ vide : l'interface n'est pas membre d'un VLAN. Les paquets associés à cette interface ne sont pas transférés.

Ajout de nouveaux VLAN

1. Affichez la page **VLAN Membership** (Appartenance à un VLAN).
2. Cliquez sur **Add** (Ajouter).

La page **Add VLAN** (Ajouter un VLAN) s'affiche.

Figure 8-50. Page Add VLAN (Ajouter un VLAN)

3. Entrez un nouvel ID et un nom pour le VLAN.
 4. Cliquez sur **Apply Changes** (Appliquer les modifications).
- Le nouveau VLAN est ajouté et le périphérique est mis à jour.

Ajout d'un port ou d'un LAG à un VLAN

1. Affichez la page **VLAN Membership** (Appartenance à un VLAN).
2. Sélectionnez un VLAN dans le menu déroulant **VLAN ID** (ID de VLAN) ou **VLAN Name** (Nom de VLAN).
3. Dans la table **VLAN Port Membership** (Appartenance des ports à un VLAN), affectez une valeur en cliquant dans la ligne **Static** (Statique) pour un port/LAG spécifique. Chaque clic permet de basculer entre U (non balisé), T (balisé) et un champ vide (non membre).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port ou le LAG est affecté au VLAN désigné, la ligne **Current** (En cours) est actualisée avec cette désignation et le périphérique est mis à jour.

Modification des groupes d'appartenance à un VLAN

1. Affichez la page **VLAN Membership** (Appartenance à un VLAN).
2. Sélectionnez un VLAN dans le menu déroulant **VLAN ID** (ID de VLAN) ou **VLAN Name** (Nom de VLAN).
3. Modifiez les champs selon vos besoins.
4. Dans la table **VLAN Port Membership** (Appartenance des ports à un VLAN), modifiez la valeur d'un port ou d'un LAG en cliquant à l'endroit approprié dans la ligne **Static** (Statique). Chaque clic permet de basculer entre U (non balisé), T (balisé) et un champ vide (non membre).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les informations relatives à l'appartenance VLAN sont modifiées, la ligne **Current** (En cours) est actualisée et le périphérique est mis à jour.

Suppression d'un VLAN

1. Affichez la page **VLAN Membership** (Appartenance à un VLAN).
2. Sélectionnez un VLAN dans le menu déroulant **VLAN ID** (ID de VLAN) ou **VLAN Name** (Nom de VLAN).
3. Cochez la case **Remove VLAN** (Supprimer le VLAN).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le VLAN sélectionné est supprimé et le périphérique est mis à jour.

Définition des groupes d'appartenance à un VLAN et affectation de ports/LAG à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 VLAN Commands (Commandes portant sur les VLAN)

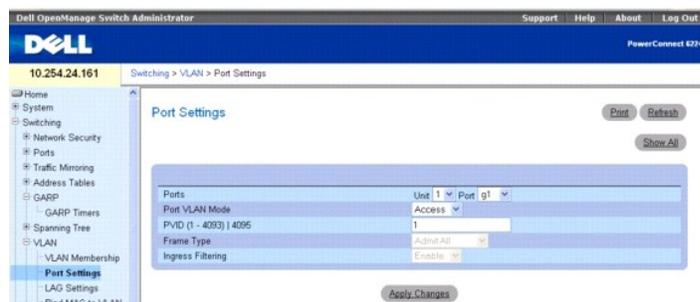
Paramètres des ports de VLAN

Dans un VLAN basé sur l'utilisation des ports, le trafic non balisé transite sur certains ports spécifiques en fonction du PVID des ports récepteurs. Ces VLAN peuvent aider à optimiser les modèles de trafic réseau car les paquets de diffusion, de multidiffusion et monodiffusion inconnus ne sont transférés que vers des ports faisant partie du VLAN. Les paquets reçus avec une balise VLAN utilisent cet ID de VLAN pour le processus de commutation.

La page **VLAN Port Settings** (Paramètres des ports de VLAN) permet d'identifier un port en tant que membre d'un VLAN et de définir et de modifier les paramètres des ports.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **VLAN** → **Port Settings** (Paramètres des ports) dans l'arborescence.

Figure 8-51. Page **Port Settings** (Paramètres des ports) pour un VLAN



Cette page contient les champs suivants :

Ports : indique l'unité et le port inclus dans le VLAN.

Port VLAN Mode (Mode VLAN du port) : indique le mode du port. Ce champ peut prendre les valeurs suivantes :

General (Général) : le port appartient à plusieurs VLAN et chaque VLAN est défini par l'utilisateur comme étant balisé ou non balisé (mode 802.1Q intégral).

Access (Accès) : le port appartient à un seul VLAN non balisé. Lorsqu'un port est en mode d'accès, les types de paquets acceptés sur le port ne peuvent pas être désignés. En outre, il est impossible d'activer ou de désactiver le filtrage en entrée sur un port d'accès.

Trunk (Tronçon) : le port appartient à plusieurs VLAN et tous les ports sont balisés (sauf dans le cas d'un seul VLAN natif).

PVID (1-4093) | 4095 (PVID, 1 à 4093 | 4095) : affecte un ID de VLAN aux paquets non balisés. Les valeurs possibles vont de 1 à 4093 ou 4095.

Frame Type (Type de trame) : indique le type de trame accepté sur le port. La valeur par défaut est **Admit All** (Accepter tout). Ce champ peut prendre les valeurs suivantes :

Admit Tag Only (Accepter uniquement les paquets balisés) : indique que seules les trames balisées sont acceptées sur le port.

Admit All (Accepter tout) : indique que les trames balisées et non balisées sont acceptées sur le port.

Ingress Filtering (Filtrage en entrée) : active ou désactive le filtrage en entrée sur le port. Le filtrage en entrée rejette les trames contenant une balise VLAN qui ne correspond pas au VLAN dont le port fait partie.

Affectation des paramètres des ports

1. Affichez la page **VLAN Port Settings** (Paramètres des ports de VLAN).
2. Sélectionnez le port à configurer dans les menus déroulant **Unit** (Unité) et **Port**.
3. Complétez les autres champs de cette page.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des ports de VLAN sont définis et le périphérique est mis à jour.

Affichage de la table des ports de VLAN

1. Affichez la page **VLAN Port Settings** (Paramètres des ports de VLAN).
2. Cliquez sur **Show All** (Afficher tout).

La page **VLAN Port Table** (Table des ports de VLAN) s'affiche.

Figure 8-52. Page VLAN Port Table (Table des ports de VLAN)

Port	Port VLAN Mode	PVID	Frame Type	Ingress Filtering	Edit
1 1/1g1	Access	1	Admit All	Enable	<input type="checkbox"/>
2 1/1g2	Access	1	Admit All	Enable	<input type="checkbox"/>
3 1/1g3	Control	3	Admit All	Enable	<input type="checkbox"/>
26 1/1g2	Access	1	Admit All	Enable	<input type="checkbox"/>
27 1/1g3	Access	1	Admit All	Enable	<input type="checkbox"/>
28 1/1g4	Access	1	Admit All	Enable	<input type="checkbox"/>

REMARQUE : Si un port **d'accès** est choisi, les types de paquets acceptés sur le port ne peuvent pas être désignés. En outre, il est impossible d'activer ou de désactiver le filtrage en entrée sur un port d'accès.

3. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **VLAN Port Table** (Table des ports de VLAN) pour les autres unités de la pile, le cas échéant.

Modification des paramètres pour plusieurs ports

1. Affichez la page **VLAN Port Settings** (Paramètres des ports de VLAN).
 2. Cliquez sur **Show All** (Afficher tout).
- La page **VLAN Port Table** (Table des ports de VLAN) s'affiche.
3. Cliquez sur **Edit** (Modifier) pour chacun des ports à modifier.
 4. Modifiez les champs selon vos besoins.
 5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des ports de VLAN sont modifiés et le périphérique est mis à jour.

Affectation de ports à des groupes de VLAN à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

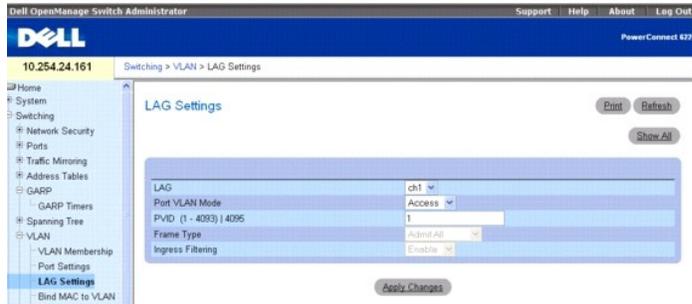
1. VLAN Commands (Commandes portant sur les VLAN)

Paramètres des LAG de VLAN

La page **VLAN LAG Settings** (Paramètres des LAG de VLAN) permet de mapper un LAG avec un VLAN. Les paquets non balisés qui arrivent sur le commutateur sont balisés à l'aide des ID de LAG spécifiés par le PVID.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **VLAN** → **LAG Settings** (Paramètres des LAG) dans l'arborescence.

Figure 8-53. Page LAG Settings (Paramètres des LAG) pour un VLAN



Cette page contient les champs suivants :

LAG : indique le numéro du LAG inclus dans le VLAN.

Port VLAN Mode (Mode VLAN du port) : indique le mode VLAN du LAG. Ce champ peut prendre les valeurs suivantes :

General (Général) : le LAG appartient à plusieurs VLAN et chaque VLAN est défini par l'utilisateur comme étant balisé ou non balisé (mode 802.1Q intégral).

Access (Accès) : le LAG appartient à un seul VLAN non balisé.

Trunk (Tronçon) : le LAG appartient à plusieurs VLAN et tous les ports sont balisés (sauf dans le cas d'un seul VLAN natif).

PVID (1-4093) | 4095 (PVID, 1 à 4093 | 4095) : affecte un ID de VLAN aux paquets non balisés. Les valeurs possibles vont de 1 à 4093 ou 4095.

Frame Type (Type de trame) : indique le type de paquets accepté par le LAG. La valeur par défaut est Admit Tag Only (Accepter uniquement les paquets balisés). Ce champ peut prendre les valeurs suivantes :

Admit Tag Only (Accepter uniquement les paquets balisés) : seuls les paquets balisés sont acceptés par le LAG.

Admit All (Accepter tout) : indique que les paquets balisés et non balisés sont acceptés par le LAG.

Ingress Filtering (Filtrage en entrée) : active ou désactive le filtrage en entrée effectué par le LAG. Le filtrage en entrée rejette les paquets contenant une balise VLAN qui ne correspond pas au VLAN dont le LAG fait partie.

Affectation des paramètres des LAG de VLAN

1. Affichez la page **VLAN LAG Settings** (Paramètres des LAG de VLAN).
2. Sélectionnez un LAG dans le menu déroulant **LAG**.
3. Complétez les autres champs de cette page.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des LAG de VLAN sont modifiés et le périphérique est mis à jour.

Affichage de la table des LAG de VLAN

1. Affichez la page **VLAN LAG Settings** (Paramètres des LAG de VLAN).
2. Cliquez sur **Show All** (Afficher tout).

La page **VLAN LAG Table** (Table des LAG de VLAN) s'affiche.

Figure 8-54. Page VLAN LAG Table (Table des LAG de VLAN)

VLAN LAG Table

Port	Port VLAN Mode	PVID	Frame Type	Ingress Filtering	Edit
1 ch1	Access	1	Admit All	Enable	<input type="checkbox"/>
2 ch2	Access	1	Admit All	Enable	<input type="checkbox"/>
3 ch3	Access	1	Admit All	Enable	<input type="checkbox"/>
4 ch4	Access	1	Admit All	Enable	<input type="checkbox"/>
5 ch5	Access	1	Admit All	Enable	<input type="checkbox"/>
6 ch6	Access	1	Admit All	Enable	<input type="checkbox"/>
7 ch7	Access	1	Admit All	Enable	<input type="checkbox"/>
8 ch8	Access	1	Admit All	Enable	<input type="checkbox"/>

Modification des paramètres pour plusieurs LAG

1. Affichez la page **VLAN LAG Settings** (Paramètres des LAG de VLAN).

2. Cliquez sur **Show All** (Afficher tout).

La page **VLAN LAG Table** (Table des LAG de VLAN) s'affiche.

3. Cliquez sur **Edit** (Modifier) pour chacun des LAG à modifier.

4. Modifiez les champs selon vos besoins.

5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des LAG de VLAN sont modifiés et le périphérique est mis à jour.

Affectation de LAG à des groupes de VLAN à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 VLAN Commands (Commandes portant sur les VLAN)

Liaison d'adresses MAC et de VLAN

La page **Bind MAC to VLAN** (Lier des adresses MAC et des VLAN) permet d'associer une entrée MAC à la table des VLAN. Une fois l'adresse MAC source et l'ID de VLAN définis, les associations correspondantes sont partagées par tous les ports du commutateur. La table des liaisons entre adresses MAC et VLAN prend en charge jusqu'à 128 entrées.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **VLAN** → **Bind MAC to VLAN** (Lier des adresses MAC et des VLAN) dans l'arborescence.

Figure 8-55. Page Bind MAC to VLAN (Lier des adresses MAC et des VLAN)



Cette page contient les champs suivants :

MAC Address (Adresse MAC) : indique l'adresse MAC à associer à un VLAN.

Bind to VLAN (1-4093) (Lier à un VLAN, 1-4093) : indique le VLAN auquel l'adresse MAC doit être associée.

Affectation des paramètres de liaison entre des adresses MAC et des VLAN

1. Affichez la page **Bind MAC to VLAN** (Lier des adresses MAC et des VLAN).

2. Entrez l'adresse MAC à associer au VLAN.

3. Entrez le VLAN auquel l'adresse MAC doit être associée.

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse MAC et le VLAN listés sont liés et le périphérique est mis à jour.

Affichage de la table des LAG de VLAN

1. Affichez la page **Bind MAC to VLAN** (Lier des adresses MAC et des VLAN).
2. Cliquez sur **Show All** (Afficher tout).

La page **MAC-VLAN Bind Table** (Table des liaisons MAC-VLAN) s'affiche.

Figure 8-56. Page MAC - VLAN Bind Table (Table des liaisons MAC-VLAN)

	MAC Address	Bind to VLAN	Remove	Edit
1	0000.6902.01FC	2	<input type="checkbox"/>	<input type="checkbox"/>
2	0000.6902.012F	110	<input type="checkbox"/>	<input type="checkbox"/>

Modification des VLAN pour plusieurs adresses MAC

1. Affichez la page **Bind MAC to VLAN** (Lier des adresses MAC et des VLAN).
 2. Cliquez sur **Show All** (Afficher tout).
- La page **MAC-VLAN Bind Table** (Table des liaisons MAC-VLAN) s'affiche.
3. Cliquez sur l'option **Edit** (Modifier) correspondant à chaque adresse MAC pour laquelle le VLAN associé doit être modifié.
 4. Modifiez les champs **Bind to VLAN** (Lier à un VLAN).
 5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de liaison MAC-VLAN sont modifiés et le périphérique est mis à jour.

Suppression d'une entrée MAC-VLAN

1. Affichez la page **Bind MAC to VLAN** (Lier des adresses MAC et des VLAN).
 2. Cliquez sur **Show All** (Afficher tout).
- La page **MAC-VLAN Bind Table** (Table des liaisons MAC-VLAN) s'affiche.
3. Cochez la case **Remove** (Supprimer) en regard de chacune des entrées à supprimer.
 4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée sélectionnée est supprimée et le périphérique est mis à jour.

Liaison d'adresses MAC et de VLAN à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. VLAN Commands (Commandes portant sur les VLAN)

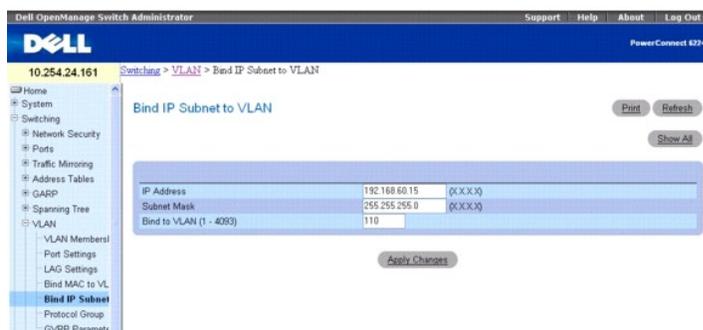
Liaison de sous-réseau IP et de VLAN

Le mappage d'un sous-réseau IP avec un VLAN est défini par une entrée dans la table IP Subnet - VLAN (Sous-réseaux IP - VLAN). Cette entrée définit une adresse IP source, un masque de réseau et l'ID du VLAN voulu. Les associations de ce type sont partagées par tous les ports du commutateur. Il est possible de configurer jusqu'à 64 entrées dans cette table.

La page **Bind IP Subnet to VLAN** (Lier un sous-réseau IP et un VLAN) permet d'associer un sous-réseau IP à un VLAN.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **VLAN** → **Bind IP Subnet to VLAN** (Lier un sous-réseau IP et un VLAN) dans l'arborescence.

Figure 8-57. Page Bind IP Subnet to VLAN (Lier un sous-réseau IP et un VLAN)



Cette page contient les champs suivants :

IP Address (Adresse IP) : indique l'adresse IP source du paquet.

Subnet Mask (Masque de sous-réseau) : indique le masque de sous-réseau correspondant à l'adresse IP source du paquet.

Bind to VLAN (1-4093) (Lier à un VLAN, 1-4093) : indique le VLAN auquel l'adresse IP est affectée.

Liaison de sous-réseaux IP et de VLAN

1. Affichez la page **Bind IP Subnet to VLAN** (Lier des sous-réseaux IP et des VLAN).
2. Entrez l'adresse IP à associer au VLAN.
3. Saisissez le sous-réseau IP associé à l'adresse IP.
4. Entrez l'ID du VLAN auquel l'adresse IP et le masque de sous-réseau sont affectés.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le sous-réseau IP et le VLAN listés sont liés et le périphérique est mis à jour.

Affichage de la table des liaisons sous-réseaux IP-VLAN

1. Affichez la page **Bind IP Subnet to VLAN** (Lier des sous-réseaux IP et des VLAN).
2. Cliquez sur **Show All** (Afficher tout).
3. La page **IP Subnet - VLAN Bind Table** (Table des liaisons sous-réseaux IP - VLAN) s'affiche.

Figure 8-58. Page IP Subnet - VLAN Bind Table (Table des liaisons sous-réseau IP - VLAN)

	IP Address	Subnet Mask	Bind to VLAN	Remove	Edit
1	192.168.12.0	255.255.255.0	110	<input type="checkbox"/>	<input type="checkbox"/>
2	192.168.13.0	255.255.255.0	110	<input type="checkbox"/>	<input type="checkbox"/>
3	192.168.60.0	255.255.255.0	110	<input type="checkbox"/>	<input type="checkbox"/>

Modification d'un VLAN associé à plusieurs adresses IP

1. Affichez la page **Bind IP Subnet to VLAN** (Lier des sous-réseaux IP et des VLAN).
2. Cliquez sur **Show All** (Afficher tout).
La page **IP Subnet - VLAN Bind Table** (Table des liaisons sous-réseaux IP - VLAN) s'affiche.
3. Cliquez sur **Edit** (Modifier) pour chaque entrée à modifier.
4. Modifiez les champs selon vos besoins.

5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de liaisons aux VLAN sont modifiés et le périphérique est mis à jour.

Suppression de l'association entre une adresse MAC et un sous-réseau IP

1. Affichez la page **Bind IP Subnet to VLAN** (Lier des sous-réseaux IP et des VLAN).
2. Cliquez sur **Show All** (Afficher tout).

La page **IP Subnet - VLAN Bind Table** (Table des liaisons sous-réseaux IP - VLAN) s'affiche.

3. Cochez la case **Remove** (Supprimer) en regard de chacune des entrées à supprimer.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée sélectionnée est supprimée et le périphérique est mis à jour.

Liaison de sous-réseaux IP et de VLAN à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. VLAN Commands (Commandes portant sur les VLAN)

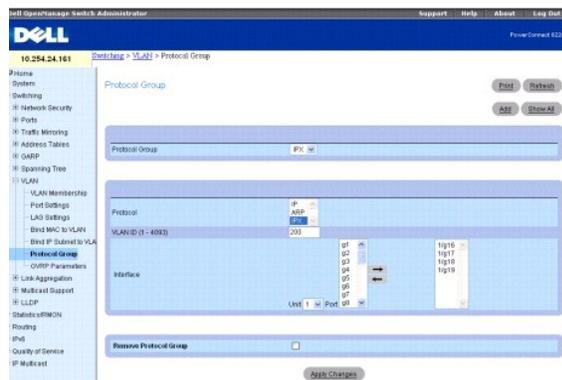
Groupe de protocoles

Dans un VLAN basé sur l'utilisation de protocoles, le trafic transite sur certains ports spécifiques, déterminés en fonction du protocole. Les critères de filtrage des paquets définis par l'utilisateur déterminent si un paquet appartient à un VLAN spécifique. Ces VLAN sont généralement utilisés dans les réseaux dont les segments contiennent des systèmes hôtes utilisant plusieurs protocoles.

La page **Protocol Group** (Groupe de protocoles) permet d'associer des types Ethernet et des VLAN et de configurer certains ports pour l'utilisation de ces paramètres.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **VLAN** → **Protocol Group** (Groupe de protocoles) dans l'arborescence.

Figure 8-59. Page Protocol Group (Groupe de protocoles)



Cette page contient les champs suivants :

Protocol Group (Groupe de protocoles) : affiche le nom associé à l'ID du groupe de protocoles. Vous pouvez créer un nouveau groupe en cliquant sur le bouton **Add** (Ajouter).

Protocol (Protocole) : indique le protocole associé à ce groupe.

VLAN ID (1-4093) (ID de VLAN, 1-4093) : indique l'ID de VLAN associé à ce groupe.

Interface : permet de sélectionner l'interface ou les interfaces à ajouter au groupe ou à supprimer. Sélectionnez les interfaces à inclure dans le groupe de protocoles et cliquez sur la flèche vers la droite. Les interfaces affichées dans la colonne de droite font partie du groupe de protocoles.

Remove Protocol Group (Supprimer un groupe de protocoles) : si vous cochez cette option, le groupe de protocoles affiché est supprimé lorsque vous cliquez sur **Apply Changes** (Appliquer les modifications). Pour supprimer plusieurs groupes simultanément, cliquez sur **Show All** (Afficher tout) et utilisez les cases à cocher **Remove** (Supprimer) disponibles dans la **table des groupes de protocoles**.

Ajout d'un groupe de protocoles

1. Affichez la page **Protocol Group** (Groupe de protocoles).
2. Cliquez sur **Add** (Ajouter).

La page **Add Protocol Group** (Ajouter un groupe de protocoles) s'affiche.

Figure 8-60. Page Add Protocol Group (Ajouter un groupe de protocoles)



3. Saisissez un nouveau nom de groupe de protocoles, ainsi que l'ID de VLAN qui sera associé à ce groupe.
4. Revenez à la page **Protocol Group** (Groupe de protocoles).
5. Sélectionnez le groupe de protocoles que vous avez ajouté, puis sélectionnez le protocole.
6. Dans la première colonne **Interface**, cliquez pour sélectionner les interfaces à ajouter au groupe de protocoles. Pour sélectionner plusieurs interfaces, cliquez tout en maintenant la touche <Maj> (pour des interfaces contiguës) ou <Ctrl> (pour des interfaces non contiguës) enfoncée.
7. Cliquez sur la flèche vers la droite.
Les interfaces sélectionnées sont déplacées dans la deuxième colonne. Toutes les interfaces de cette colonne font partie du groupe de protocoles.
8. Cliquez sur **Apply Changes** (Appliquer les modifications).
Le groupe est ajouté et le périphérique est mis à jour.

Modification des paramètres du groupe de protocoles d'un VLAN

1. Affichez la page **Protocol Group** (Groupe de protocoles).
2. Sélectionnez le protocole à modifier dans le menu déroulant **Protocol Group ID** (ID des groupes de protocoles).
3. Modifiez le protocole ou l'ID de VLAN selon vos besoins.
4. Dans la première colonne **Interface**, cliquez pour sélectionner l'interface voulue. Pour sélectionner plusieurs interfaces, cliquez tout en maintenant la touche <Maj> (pour des interfaces contiguës) ou <Ctrl> (pour des interfaces non contiguës) enfoncée.
5. Cliquez sur la flèche vers la droite.
L'interface sélectionnée est déplacée dans la deuxième colonne. Toutes les interfaces de cette colonne font partie du groupe de protocoles.
6. Pour supprimer une interface du groupe, cliquez pour sélectionner l'interface voulue dans la deuxième colonne.
7. Cliquez sur la flèche vers la gauche.
L'interface sélectionnée est supprimée de la deuxième colonne.
8. Cliquez sur **Apply Changes** (Appliquer les modifications).
Les paramètres du groupe de protocoles du VLAN sont modifiés et le périphérique est mis à jour.

Suppression de plusieurs protocoles de la table des groupes de protocoles

1. Affichez la page **Protocol Group** (Groupe de protocoles).
2. Cliquez sur **Show All** (Afficher tout).
La page **Protocol Group Table** (Table des groupes de protocoles) s'affiche.

Figure 8-61. Page Protocol Group Table (Table des groupes de protocoles)

Group Name	Protocol	VLAN ID	Interface	Remove
1	IPX	200	1/g16 1/g17 1/g18 1/g19	<input type="checkbox"/> Edit
2	IPQ2	110	1/g21 1/g22 1/g23 1/g24	<input type="checkbox"/> Edit

3. Cochez la case **Remove** (Supprimer) en regard de chaque groupe de protocoles à supprimer.

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le protocole est supprimé et le périphérique est mis à jour.

Configuration des groupes de protocole à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 VLAN Commands (Commandes portant sur les VLAN)

Paramètres GVRP

Le protocole d'enregistrement de VLAN GARP permet aux commutateurs du réseau d'enregistrer (et de désenregistrer) dynamiquement les informations d'appartenance à un VLAN correspondant aux commutateurs du même segment. Ce mécanisme permet en outre à ces informations d'être distribuées sur tous les commutateurs du réseau local prenant en charge le protocole GVRP.

Le fonctionnement de GVRP repose sur les services fournis par le protocole GARP (Generic Attribute Registration Protocol). Le protocole GVRP permet de créer jusqu'à 1024 VLAN.

La page **GVRP Global Parameters** (Paramètres globaux GVRP) permet de procéder à l'activation globale du protocole GVRP. Elle permet également d'activer ce protocole interface par interface.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **VLAN** → **GVRP Parameters** (Paramètres GVRP) dans l'arborescence.

Figure 8-62. Page GVRP Global Parameters (Paramètres globaux GVRP)



Cette page contient les champs suivants :

GVRP Global Status (État global GVRP) : active ou désactive le protocole GVRP sur le commutateur. Le protocole GVRP est désactivé par défaut.

Interface : indique l'unité et le port ou le LAG sur lesquels le protocole GVRP est activé.

GVRP State (État GVRP) : active ou désactive le protocole GVRP sur l'interface spécifiée.

Dynamic VLAN Creation (Création dynamique de VLAN) : active ou désactive la création de VLAN par le biais de GVRP.

GVRP Registration (Enregistrement GVRP) : active ou désactive l'enregistrement GVRP.

Activation du protocole GVRP sur le commutateur

1. Affichez la page **GVRP Global Parameters** (Paramètres globaux GVRP).
2. Sélectionnez **Enable** (Activer) dans le champ **GVRP Global Status** (État global GVRP).

3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le protocole GVRP est activé sur le commutateur.

Activation de l'enregistrement de VLAN par le biais du protocole GVRP

1. Affichez la page **GVRP Global Parameters** (Paramètres globaux GVRP).
2. Sélectionnez **Enable** (Activer) dans le champ **GVRP Global Status** (État global GVRP) pour l'interface voulue.
3. Sélectionnez **Enable** (Activer) dans le champ **GVRP Registration** (Enregistrement GVRP).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'enregistrement GVRP des VLAN est activé sur le port et le périphérique est mis à jour.

Affichage de la table de paramètres des ports GVRP

1. Affichez la page **GVRP Global Parameters** (Paramètres globaux GVRP).
2. Cliquez sur **Show All** (Afficher tout).

La page **GVRP Port Parameters Table** (Table de paramètres des ports GVRP) s'affiche.

Figure 8-63. Page GVRP Port Parameters Table (Table de paramètres des ports GVRP)

Interface	GVRP State	Dynamic VLAN Creation	GVRP Registration	Copy To	Edit
1	1ig1	Disable	Disable	Disable	☑
2	1ig2	Disable	Disable	Disable	☑
3	1ig3	Disable	Disable	Disable	☑

26	1hg2	Disable	Disable	Disable	☑
27	1hg3	Disable	Disable	Disable	☑
28	1hg4	Disable	Disable	Disable	☑

LAGs					
29	lag1	Disable	Disable	Disable	☑
30	lag2	Disable	Disable	Disable	☑
31	lag3	Disable	Disable	Disable	☑
32	lag4	Disable	Disable	Disable	☑
33	lag5	Disable	Disable	Disable	☑
34	lag6	Disable	Disable	Disable	☑
35	lag7	Disable	Disable	Disable	☑
36	lag8	Disable	Disable	Disable	☑

3. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **GVRP Port Parameters Table** (Table de paramètres des ports GVRP) pour les autres unités de la pile, le cas échéant.

Copie de paramètres GVRP

1. Affichez la page **GVRP Global Parameters** (Paramètres globaux GVRP).
2. Cliquez sur **Show All** (Afficher tout).
La page **GVRP Port Parameters Table** (Table de paramètres des ports GVRP) s'affiche.
3. Indiquez le port ou le LAG à partir desquels vous effectuez la copie dans **Copy Parameters From** (Copie les paramètres à partir de).
4. Cliquez sur **Copy To** (Copier vers) pour chaque interface/LAG cible.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des ports GVRP sont copiés et le périphérique est mis à jour.

Modification des paramètres GVRP pour plusieurs ports

1. Affichez la page **GVRP Global Parameters** (Paramètres globaux GVRP).
2. Cliquez sur **Show All** (Afficher tout).

La page **GVRP Port Parameters Table** (Table de paramètres des ports GVRP) s'affiche.

3. Cliquez sur **Edit** (Modifier) pour chaque interface/LAG à modifier.
4. Modifiez les champs de paramètres selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des ports GVRP sont modifiés et le périphérique est mis à jour.

Configuration de GVRP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 GVRP Commands (Commandes GVRP)

Agrégation de ports

La fonction d'agrégation des liaisons permet de regrouper des liaisons Ethernet en mode duplex intégral (FDX), de façon à former un LAG (groupe de liaisons agrégées). Le commutateur peut ainsi traiter le LAG comme s'il s'agissait d'une seule liaison.

Les LAG statiques sont pris en charge. Lorsqu'un port est ajouté à un LAG en tant que membre statique, il ne transmet pas les LACPDU et ne les reçoit pas.

Pour afficher la page **Link Aggregation** (Agrégation de liaisons), cliquez sur **Switching** (Commutation) → **Link Aggregation** (Agrégation de liaisons) dans l'arborescence. Cette page contient des liens vers les fonctionnalités suivantes :

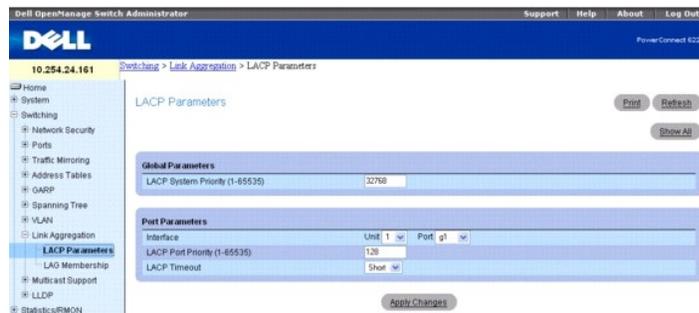
- 1 [Paramètres LACP](#)
- 1 [Appartenance à un LAG](#)
- 1 [Configuration du hachage des LAG](#)
- 1 [Récapitulatif du hachage des LAG](#)

Paramètres LACP

L'agrégation de liaisons est créée et conservée via l'échange régulier d'unités LACPDU. La page **LACP Parameters** (Paramètres LACP) permet de configurer les LAG LACP.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Link Aggregation** (Agrégation de liaisons) → **LACP Parameters** (Paramètres LACP) dans l'arborescence.

Figure 8-64. Page LACP Parameters (Paramètres LACP)



Cette page contient deux sections : Global Parameters (Paramètres globaux) et Port Parameters (Paramètres des ports). Les champs disponibles sont les suivants :

Global Parameters (Paramètres globaux)

LACP System Priority (1-65535) (Priorité système LACP, 1-65535) : priorité LACP pour les paramètres globaux. La valeur par défaut est de 1.

Port Parameters (Paramètres des ports)

Interface : indique le numéro de l'unité et du port auxquels les valeurs d'expiration et de priorité sont associées.

LACP Port Priority (1-65535) (Priorité du port LACP, 1-65535) : définit la priorité LACP pour le port indiqué. La valeur par défaut est de 1.

LACP Timeout (Délai d'expiration LACP) : indique le délai d'expiration administratif LACP. Ce champ peut prendre les valeurs suivantes :

Short (Court) : définit un délai d'expiration court

Long : définit un délai d'expiration long. Cette option est utilisée par défaut.

Définition des paramètres d'agrégation de liaisons

1. Affichez la page **LACP Parameters** (Paramètres LACP).
2. Complétez les champs selon vos besoins.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont définis et le périphérique est mis à jour.

Affichage de la table de paramètres LACP

1. Affichez la page **LACP Parameters** (Paramètres LACP).
2. Cliquez sur **Show All** (Afficher tout).

La page **LACP Parameters Table** (Table des paramètres LACP) s'affiche.

Figure 8-65. Page LACP Parameters Table (Table des paramètres LACP)

Port	Port Priority	LACP Timeout	Edit
1 1g1	128	Long	<input checked="" type="checkbox"/>
2 1g2	128	Long	<input type="checkbox"/>
3 1g3	128	Long	<input type="checkbox"/>

26 1ng2	128	Long	<input type="checkbox"/>
27 1ng3	128	Long	<input type="checkbox"/>
28 1ng4	128	Long	<input type="checkbox"/>

3. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **LACP Parameters Table** (Table des paramètres LACP) pour les autres unités de la pile, le cas échéant.

Modification des paramètres LACP pour plusieurs ports

1. Affichez la page **LACP Parameters** (Paramètres LACP).
2. Cliquez sur **Show All** (Afficher tout).

La page **LACP Parameters Table** (Table des paramètres LACP) s'affiche.

3. Cliquez sur **Edit** (Modifier) pour chacun des ports à modifier.
4. Modifiez les champs selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres LACP sont modifiés et le périphérique est mis à jour.

Configuration des paramètres LACP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

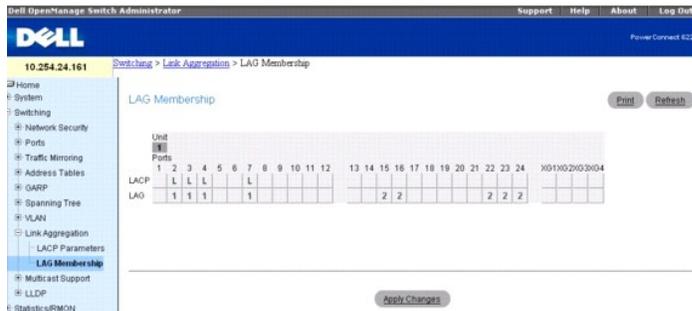
- 1 LACP Commands (Commandes LACP)

Appartenance à un LAG

Le commutateur prend en charge 18 LAG par système et huit ports par LAG. La page **LAG Membership** (Appartenance à un LAG) permet d'affecter les ports à des LAG et des LACP.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Link Aggregation** (Agrémentation de liaisons) → **LAG Membership** (Appartenance à un LAG) dans l'arborescence.

Figure 8-66. Page LAG Membership (Appartenance à un LAG)



Cette page comprend une table qui contient les champs suivants :

LACP : agrège un port de LAG à une appartenance LACP. Pour activer (valeur "on") LACP sur les ports dont le numéro figure dans la rangée LAG, vous pouvez cliquer sur la ligne **LACP**. Chaque clic permet de basculer entre L (LACP) et un champ vide (pas de LACP).

LAG : ajoute un port à un LAG et indique le LAG spécifique auquel le port appartient. Chaque clic permet de passer d'un numéro de LAG au suivant (de 1 à 18), puis à un champ vide (aucun LAG affecté).

Ajout d'un port à un LAG

1. Affichez la page **LAG Membership** (Appartenance à un LAG).
2. Cliquez sur la ligne **LAG** pour faire basculer le port sur le LAG voulu.

Le numéro du LAG s'affiche dans l'emplacement correspondant au port. Chaque clic permet de passer d'un numéro de LAG au suivant (de 1 à 18), puis à un champ vide (aucun LAG affecté).

3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port est affecté au LAG sélectionné et le périphérique est mis à jour.

Ajout d'un port de LAG à un LACP

1. Affichez la page **LAG Membership** (Appartenance à un LAG).
2. Cliquez sur la ligne **LACP** pour faire basculer le port de LAG voulu sur L.

REMARQUE : Pour pouvoir être agrégé à un LACP, le port doit avoir été affecté à un LAG.

3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port de LAG est agrégé au LACP et le périphérique est mis à jour.

Affectation de ports à des LAG et des LACP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

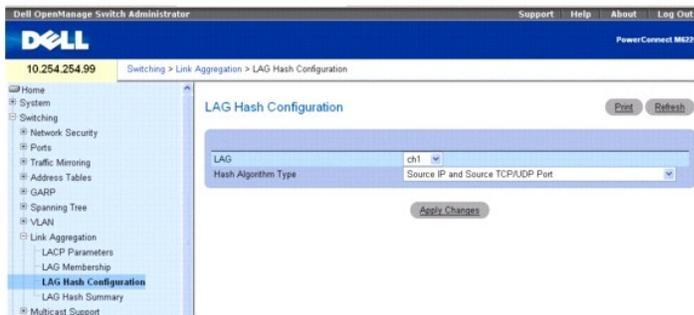
- 1 Port Channel Commands (Commandes portant sur les canaux des ports)

Configuration du hachage des LAG

Utilisez l'algorithme de hachage des LAG pour définir le mode de distribution du trafic sur la liaison d'agrégation. Le type de hachage peut être défini pour chaque tronçon.

Pour afficher la page **LAG Hash Configuration** (Configuration du hachage des LAG), cliquez sur **Switching** (Commutation) → **Link Aggregation** (Agrégation de liaisons) → **LAG Hash Configuration** (Configuration du hachage des LAG) dans l'arborescence.

Figure 8-67. Page LAG Hash Configuration (Configuration du hachage des LAG)



Cette page contient les champs suivants :

LAG : le menu déroulant répertorie les numéros de LAG.

Hash Algorithm Type (Type d'algorithme de hachage) : l'algorithme de hachage utilisé pour les flux du trafic de monodiffusion peut être de l'un des types suivants :

- 1 Adresse MAC source, VLAN, Type Ethernet, Module source et ID de port
- 1 Adresse MAC de destination, VLAN, Type Ethernet, Module source et ID de port
- 1 Adresse IP source et port TCP/UDP source (type par défaut)
- 1 Adresse IP de destination et port TCP/UDP de destination
- 1 Adresse MAC source/ de destination, VLAN, EtherType, port/MODID source
- 1 Adresse IP source/de destination et port TCP/UDP source/de destination

Configuration du hachage des LAG

1. Affichez la page **LAG Hash Configuration** (Configuration du hachage des LAG).
2. Sélectionnez le LAG à configurer et l'algorithme de hachage qui doit lui être affecté.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont modifiés et le périphérique est mis à jour.

Configuration du hachage des LAG à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Port Channel Commands (Commandes portant sur les canaux des ports)

Récapitulatif du hachage des LAG

La page **LAG Hash Summary** (Récapitulatif du hachage des LAG) répertorie les canaux du système et le type d'algorithme de hachage correspondant.

Pour afficher la page **LAG Hash Summary** (Récapitulatif du hachage des LAG), cliquez sur **Switching** (Commutation) → **Link Aggregation** (Agrégation de liaisons) → **LAG Hash Summary** (Récapitulatif du hachage des LAG) dans l'arborescence.

Figure 8-68. Page LAG Hash Summary (Récapitulatif du hachage des LAG)

LAGs	Hash Algorithm Type
1 ch1	Source IP and Source TCP/UDP Port
2 ch2	Source IP and Source TCP/UDP Port
3 ch3	Source IP and Source TCP/UDP Port
4 ch4	Source IP and Source TCP/UDP Port
5 ch5	Source IP and Source TCP/UDP Port
6 ch6	Source IP and Source TCP/UDP Port
7 ch7	Source IP and Source TCP/UDP Port
8 ch8	Source IP and Source TCP/UDP Port
9 ch9	Source IP and Source TCP/UDP Port
10 ch10	Source IP and Source TCP/UDP Port
11 ch11	Source IP and Source TCP/UDP Port
12 ch12	Source IP and Source TCP/UDP Port
13 ch13	Source IP and Source TCP/UDP Port
14 ch14	Source IP and Source TCP/UDP Port
15 ch15	Source IP and Source TCP/UDP Port
16 ch16	Source IP and Source TCP/UDP Port
17 ch17	Source IP and Source TCP/UDP Port
18 ch18	Source IP and Source TCP/UDP Port

Cette page comprend une table qui contient les champs suivants :

LAGs : répertorie les numéros de LAG.

Hash Algorithm Type (Type d'algorithme de hachage) : affiche le type d'algorithme de hachage utilisé pour les flux du trafic de monodiffusion et associé au LAG.

Affichage du récapitulatif de l'algorithme de hashage des LAG à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Port Channel Commands (Commandes portant sur les canaux des ports)

Prise en charge de la transmission multidiffusion

La base de données des transferts de multidiffusion de couche 2 est utilisée par le commutateur pour déterminer l'action de transfert à appliquer aux paquets qui arrivent avec une adresse MAC cible de multidiffusion. Le fait de limiter les multidiffusions à certains ports du commutateur permet d'éviter que le trafic ne soit envoyé à des parties du réseau lorsque cela n'est pas utile.

Lorsqu'un paquet arrive sur le commutateur, l'adresse MAC de destination est associée à l'ID de VLAN et une recherche est effectuée dans la base de données des transferts de couche 2. Si aucune correspondance n'est trouvée, le paquet est soit acheminé vers tous les ports du VLAN, soit rejeté, selon la configuration du commutateur. Si une correspondance est trouvée, le paquet est transmis uniquement aux ports membres du groupe de multidiffusion approprié.

Pour afficher la page **Multicast Support** (Prise en charge de la multidiffusion), cliquez sur **Switching** (Commutation) → **Multicast Support** (Prise en charge de la multidiffusion) dans l'arborescence. Cette page contient des liens vers les fonctionnalités suivantes :

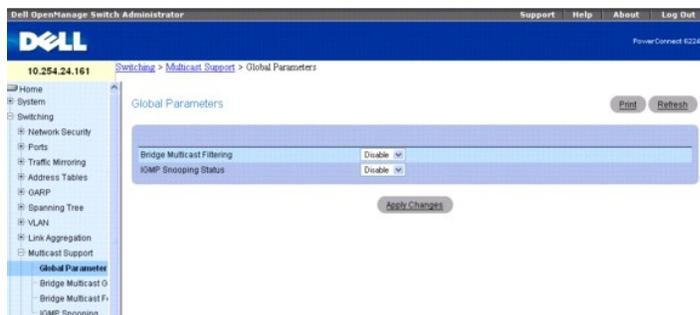
- 1 [Paramètres globaux de multidiffusion](#)
- 1 [Groupe de multidiffusion par ponts](#)
- 1 [Transfert multidiffusion par ponts](#)
- 1 [Contrôle IGMP](#)

Paramètres globaux de multidiffusion

La page **Multicast Global Parameters** (Paramètres globaux de multidiffusion) permet d'activer le filtrage de la multidiffusion par ponts ou le contrôle IGMP sur le commutateur. Les paramètres de ces fonctions peuvent être modifiés à partir des pages Web [Bridge Multicast Forward](#) (Transfert multidiffusion par ponts) et [IGMP Snooping](#) (Contrôle IGMP).

Pour afficher la page **Multicast Global Parameters** (Paramètres globaux de multidiffusion), cliquez sur **Switching** (Commutation) → **Multicast Support** (Prise en charge de la multidiffusion) → **Global Parameters** (Paramètres globaux) dans l'arborescence.

Figure 8-69. Page Global Parameters (Paramètres globaux) de la multidiffusion



Cette page contient les champs suivants :

Bridge Multicast Filtering (Filtrage de multidiffusion par ponts) : active ou désactive le filtrage de multidiffusion par ponts. La valeur par défaut est Disabled (Désactivé).

IGMP Snooping Status (État du contrôle IGMP) : active ou désactive le contrôle IGMP. La valeur par défaut est Disabled (Désactivé).

Activation du filtrage de multidiffusion par ponts sur le commutateur

1. Affichez la page **Multicast Global Parameters** (Paramètres globaux de multidiffusion).
2. Sélectionnez **Enable** (Activer) dans le champ **Bridge Multicast Filtering** (Filtrage de multidiffusion par ponts).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La multidiffusion par ponts est activée sur le commutateur.

Activation du transfert de multidiffusion et/ou du contrôle IGMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

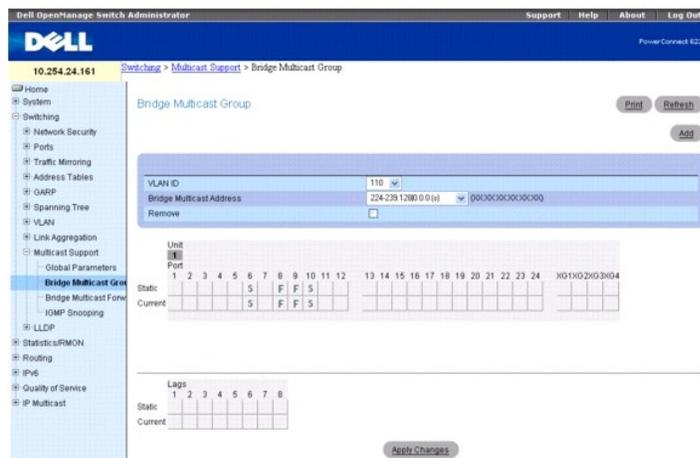
- 1 Address Table Commands (Commandes portant sur les tables d'adresses)

Groupe de multidiffusion par ponts

La page **Bridge Multicast Group** (Groupe de multidiffusion par ponts) permet de créer de nouveaux groupes de services de multidiffusion ou de modifier les ports et les LAG affectés aux groupes de services de multidiffusion existants. Les interfaces associées s'affichent dans les tables **Port** et **LAG**, ce qui reflète la façon dont chacune est jointe au groupe de multidiffusion.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Multicast Support** (Prise en charge de la multidiffusion) → **Bridge Multicast Group** (Groupe de multidiffusion par ponts) dans l'arborescence.

Figure 8-70. Page Bridge Multicast Group (Groupe de multidiffusion par ponts)



Cette page contient les champs suivants :

VLAN ID (ID de VLAN) : sélectionne le VLAN auquel le groupe de multidiffusion doit être ajouté ou dans lequel les ports d'un groupe de multidiffusion existant doivent être modifiés.

Bridge Multicast Address (Adresse de multidiffusion par ponts) : identifie l'adresse MAC ou IP du groupe de multidiffusion qui est associée à l'ID de VLAN sélectionné. Utilisez le bouton **Add** (Ajouter) pour associer une nouvelle adresse à un ID de VLAN.

Remove (Supprimer) : supprime une adresse de multidiffusion par ponts lorsque cette case est cochée.

Tables des ports et des membres de LAG

La table **Bridge Multicast Group** (Groupe de multidiffusion par ponts) affiche les ports et les LAG qui sont membres du groupe de multidiffusion. Elle indique également s'ils sont statiques (S), dynamiques (D) ou interdits (F, forbidden). Les tables contiennent deux lignes : **Static** (Statique) et **Current** (En cours). Seule la ligne **Static** (Statique) est accessible depuis cette page. La ligne **Current** (En cours) est mise à jour dynamiquement lorsque vous modifiez la ligne **Static** (Statique) puis cliquez sur **Apply Changes** (Appliquer les modifications).

La page **Bridge Multicast Group** (Groupe de multidiffusion par ponts) contient deux tables modifiables :

Units and Ports (Unités et ports) : affiche les ports appartenant à des groupes de multidiffusion et permet de définir des affectations. Pour affecter un port, cliquez sur **Static** (Statique) pour un port spécifique. Chaque clic permet de basculer entre S, F et un champ vide Reportez-vous à la table ci-après pour connaître les définitions.

LAGs : affiche les LAG appartenant à des groupes de multidiffusion et permet de définir des affectations. Pour définir une affectation, cliquez sur **Static** (Statique) pour un LAG spécifique. Chaque clic permet de basculer entre S, F et un champ vide Reportez-vous à la table ci-après pour connaître les définitions.

Le tableau suivant contient des définitions concernant les paramètres de gestion IGMP applicables aux ports et aux LAG.

Tableau 8-2. Paramètres de gestion IGMP applicables aux LAG

Contrôle du port	Définition
D	Dynamique : indique que le port/LAG a été ajouté dynamiquement au groupe de multidiffusion (s'affiche dans la ligne <i>Current</i> [En cours]).
S	Statique : rattache le port au groupe de multidiffusion en tant que membre statique (ligne <i>Static</i> [Statique]). Le port apparaît dans la ligne <i>Current</i> (En cours) lorsque vous cliquez sur Apply Changes (Appliquer les modifications).
Champ vide	Champ vide : indique que le port n'est pas rattaché à un groupe de multidiffusion.

Ajout d'adresses de multidiffusion par ponts

1. Affichez la page **Bridge Multicast Group** (Groupe de multidiffusion par ponts).
2. Cliquez sur **Add** (Ajouter).

La page **Add Bridge Multicast Group** (Ajouter un groupe de multidiffusion par ponts) s'affiche.

Figure 8-71. Page Add Bridge Multicast Group (Ajouter un groupe de multidiffusion par ponts)

The screenshot shows the configuration interface for adding a bridge multicast group. It includes a form with three main fields: VLAN ID (110), Multicast IP Address (25.0.0.0), and Multicast MAC Address (000000000000). Below the form are two tables for assigning ports and LAGs. The 'Unit' table shows units 1 through 24, with 'S' (Static) in unit 5, 'F' (Forbidden) in unit 7, and 'S' in unit 11. The 'Lags' table shows LAGs 1 through 8. At the bottom of the page are 'Apply Changes' and 'Back' buttons.

3. Sélectionnez un ID de VLAN dans le menu déroulant **VLAN ID**.
4. Indiquez la nouvelle adresse IP ou MAC de multidiffusion dans les champs **Multicast IP Address** ou **Multicast MAC Address**.
5. Dans les tables **Bridge Multicast Group** (Groupe de multidiffusion par ponts), affectez un paramètre en cliquant sur la ligne **Static** (Statique) pour un port/LAG spécifique. Chaque clic permet de basculer entre S, F et un champ vide (non membre).
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse de multidiffusion par ponts et les ports/LAG sont affectés au groupe de multidiffusion. La ligne **Current** (En cours) est mise à jour avec les paramètres de la ligne **Static** (Statique) et le périphérique est mis à jour.

Affectation d'une interface à un groupe de multidiffusion existant

1. Affichez la page **Bridge Multicast Group** (Groupe de multidiffusion par ponts).
2. Sélectionnez l'ID du VLAN dans le menu déroulant **VLAN ID**.

L'adresse de multidiffusion par ponts associée s'affiche.

3. Dans les tables **Bridge Multicast Group** (Groupe de multidiffusion par ponts), affectez un paramètre en cliquant sur la ligne **Static** (Statique) pour un port/LAG spécifique. Chaque clic permet de basculer entre S, F et un champ vide (non membre).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'interface est affectée au groupe de multidiffusion. La ligne **Current** (En cours) est mise à jour avec les paramètres de la ligne **Static** (Statique) et le périphérique est mis à jour.

Suppression d'un groupe de multidiffusion par ponts

1. Affichez la page **Bridge Multicast Group** (Groupe de multidiffusion par ponts).
2. Dans le menu déroulant **VLAN ID**, sélectionnez l'ID du VLAN associé au groupe de multidiffusion par ponts à supprimer.

L'adresse de multidiffusion par ponts et les ports/LAG associés s'affichent.

3. Cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le groupe de multidiffusion par ponts sélectionné est supprimé et le périphérique est mis à jour.

Gestion des membres du service de multidiffusion à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

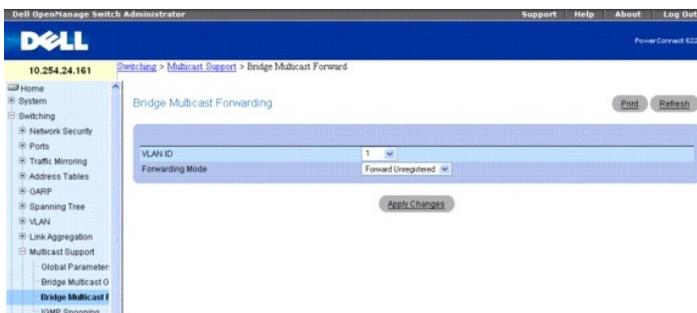
1. Address Table Commands (Commandes portant sur les tables d'adresses)

Transfert multidiffusion par ponts

La page **Bridge Multicast Forward** (Transfert multidiffusion par ponts) permet d'autoriser l'association de ports ou de LAG à un commutateur connecté à un commutateur de multidiffusion voisin. Une fois le contrôle IGMP activé, les paquets multidiffusion sont transférés au port ou VLAN approprié.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Multicast Support** (Prise en charge de la multidiffusion) → **Bridge Multicast Forwarding** (Transfert de multidiffusion par ponts) dans l'arborescence.

Figure 8-72. Page Bridge Multicast Forwarding (Transfert de multidiffusion par ponts)



La page **Bridge Multicast Forwarding** (Transfert de multidiffusion par ponts) contient deux tables modifiables, ainsi que les champs suivants :

VLAN ID (ID de VLAN) : sélectionne le VLAN à affecter.

Forwarding Mode (Mode de transfert) : définit le mode de transfert de multidiffusion pour le VLAN sélectionné. Ce champ peut prendre les valeurs suivantes :

Forward Unregistered (Transfert non enregistré) : autorise le transfert de paquets de multidiffusion IPv4 dont l'adresse de destination ne correspond à aucun des groupes répertoriés dans les rapports d'appartenance IGMP précédents.

Forward All (Transférer tout) : autorise le transfert des paquets de multidiffusion, qu'ils soient enregistrés ou non.

Filter Unregistered (Filtrer les paquets non enregistrés) : interdit le transfert de paquets de multidiffusion IPv4 dont l'adresse de destination ne correspond à aucun des groupes répertoriés dans les rapports d'appartenance IGMP précédents.

Modification du mode de transfert de la multidiffusion par ponts

1. Affichez la page **Bridge Multicast Forwarding** (Transfert de multidiffusion par ponts).
2. Sélectionnez un ID de VLAN dans le menu déroulant **VLAN ID**.
3. Sélectionnez le mode de transfert à affecter au VLAN dans le menu déroulant **Forwarding Mode**.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le VLAN est actualisé avec le paramètre **Forwarding Mode** (Mode de transfert) sélectionné et le périphérique est mis à jour.

Gestion des LAG et des ports rattachés aux routeurs multidiffusion à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1. Address Table Commands (Commandes portant sur les tables d'adresses)

Contrôle IGMP

La page **IGMP Snooping** (Contrôle IGMP) permet d'ajouter des membres IGMP.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **Multicast Support** (Prise en charge de la multidiffusion) → **IGMP Snooping** (Contrôle IGMP) dans l'arborescence.

Figure 8-73. Page **IGMP Snooping** (Contrôle IGMP)



Cette page contient les champs suivants :

Interface : sélectionne l'unité et le port à affecter.

Auto Learn (Apprentissage automatique) : active ou désactive l'apprentissage automatique sur le commutateur.

Host Timeout (Délai d'expiration de l'hôte) : indique le délai avant expiration d'une entrée de contrôle IGMP. La valeur par défaut est de 260 secondes.

Multicast Router Timeout (Délai d'expiration du routeur multidiffusion) : indique le délai avant expiration d'une entrée de routeur multidiffusion. La valeur par défaut est de 300 secondes.

Leave Timeout (Délai de sortie) : indique le délai, en secondes, entre la réception d'un message de sortie du port et l'expiration de l'entrée correspondante. Saisissez un délai d'expiration ou cliquez sur **Immediate Leave** (Sortie immédiate) pour indiquer une expiration immédiate. La valeur par défaut est de 10 secondes.

Activation du contrôle IGMP sur le commutateur

1. Affichez la page **IGMP Snooping** (Contrôle IGMP).
2. Sélectionnez l'unité et le port à configurer dans le champ **Interface**.

3. Complétez les champs de cette page selon vos besoins.
 4. Cliquez sur **Apply Changes** (Appliquer les modifications).
- Le contrôle IGMP est activé sur le commutateur.

Affichage de la page IGMP Snooping Table (Table de contrôle IGMP)

1. Affichez la page **IGMP Snooping** (Contrôle IGMP).
2. Cliquez sur **Show All** (Afficher tout).

La page **IGMP Snooping Table** (Table de contrôle IGMP) s'affiche.

Figure 8-74. Page **IGMP Snooping Table** (Table de contrôle IGMP)

Port	Auto Leaves Enable	Host Timeout	Multicast Router Timeout	Leave Timeout	Copy To	Edit
1 1/24	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
2 1/25	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
3 1/26	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
LAGs						
29 ch1	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
30 ch2	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
31 ch3	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
32 ch4	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
33 ch5	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
34 ch6	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
35 ch7	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>
36 ch8	Disable	260	300	10	<input type="checkbox"/>	<input type="checkbox"/>

Apply Changes Back

3. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **IGMP Snooping Table** (Table de contrôle IGMP) pour les autres unités de la pile, le cas échéant.

Modification des paramètres de contrôle IGMP pour plusieurs ports ou LAG

1. Affichez la page **IGMP Snooping** (Contrôle IGMP).
 2. Cliquez sur **Show All** (Afficher tout).
- La page **IGMP Snooping Table** (Table de contrôle IGMP) s'affiche.
3. Cliquez sur **Edit** (Modifier) pour chacun des ports ou LAG à modifier.
 4. Modifiez les champs de contrôle IGMP selon vos besoins.
 5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de contrôle IGMP sont modifiés et le périphérique est mis à jour.

Copie des paramètres de contrôle IGMP sur plusieurs ports ou LAG

1. Affichez la page **IGMP Snooping** (Contrôle IGMP).
 2. Cliquez sur **Show All** (Afficher tout).
- La page **IGMP Snooping Table** (Table de contrôle IGMP) s'affiche.
3. Cliquez sur **Copy Parameters From** (Copier les paramètres à partir de cet élément).
 4. Sélectionnez une unité/un port ou un LAG à utiliser comme source des paramètres voulus.

5. Cliquez sur **Copy To** (Copier vers) pour chaque unité/port ou LAG cible.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de contrôle IGMP sont modifiés et le périphérique est mis à jour.

Configuration du contrôle IGMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 IGMP Snooping Commands (Commandes de contrôle IGMP)

Configuration du protocole LLDP

Le protocole LLDP (Link Layer Discovery Protocol) est une norme IEEE 802.1AB qui permet aux stations faisant partie d'un réseau local de type 802 de déclarer leurs principales capacités et caractéristiques physiques. Ces informations peuvent être affichées par l'administrateur réseau. Elles lui permettent d'identifier la topologie du système et de détecter les configurations non valides présentes sur le réseau local.

Le protocole LLDP est un protocole unidirectionnel qui ne requiert aucune suite de requêtes/réponses. Les informations sont déclarées par les stations de transmission, puis elles sont reçues et traitées par les stations de réception. Les fonctions de transfert et de réception peuvent être activées/désactivées séparément pour chaque port. Par défaut, ces deux fonctions sont désactivées sur tous les ports. L'application est responsable du démarrage de chaque machine associée aux états de transfert et de réception, lequel doit être effectué conformément à l'état de configuration et de fonctionnement du port.

La page **LLDP** contient des liens vers les fonctionnalités suivantes :

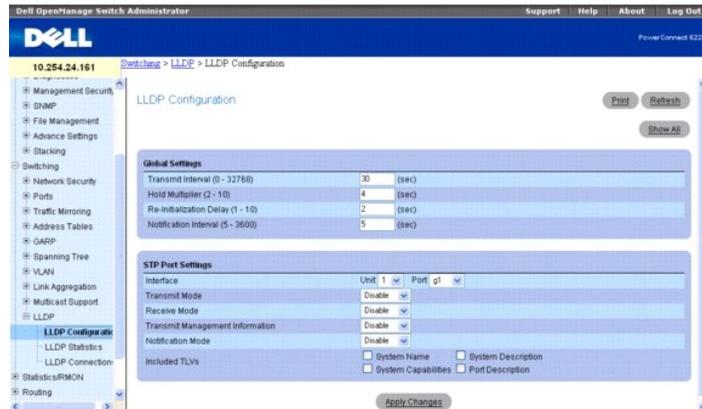
- 1 [Configuration LLDP](#)
- 1 [Statistiques LLDP](#)
- 1 [Connexions LLDP](#)

Configuration LLDP

La page **LLDP Configuration** (Configuration LLDP) permet de définir les paramètres LLDP affectant la totalité du système ou destinés à une interface spécifique.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **LLDP** → **LLDP Configuration** (Configuration LLDP) dans l'arborescence.

Figure 8-75. Page LLDP Configuration (Configuration LLDP)



Cette page contient les champs suivants :

Global Settings (Paramètres globaux)

Transmit Interval (1-32768) (Intervalle de transfert, 1-32768) : définit l'intervalle de transfert des trames. La valeur par défaut est de 30 secondes.

Hold Multiplier (2-10) (Multiplicateur pour le délai de conservation, 2-10) : définit le multiplicateur à appliquer à l'intervalle de transfert pour définir le délai d'expiration. La valeur par défaut est de 4.

Re-Initialization Delay (1-10) (Délai de réinitialisation, 1-10) : indique le temps écoulé avant la réinitialisation. La valeur par défaut est de 2 secondes.

Notification Interval (5-3600) (Intervalle de notification, 5-3600 secondes) : limite le transfert des notifications. La valeur par défaut est de 5 secondes.

Port Settings (Paramètres de port)

Interface : indique le port affecté par ces paramètres.

Transmit Mode (Mode de transfert) : active ou désactive la fonction de transfert. Le paramètre par défaut est Disabled (Désactivé).

Receive Mode (Mode de réception) : active ou désactive la fonction de réception. Le paramètre par défaut est Disabled (Désactivé).

Transmit Management Information (Transmettre les informations de gestion) : active ou désactive le transfert de l'instance de l'adresse de gestion. La valeur par défaut est Disabled (Désactivé).

Notification Mode (Mode de notification) : active ou désactive les notifications de modifications à distance. Le paramètre par défaut est Disabled (Désactivé).

Included TLVs (TLV inclus) : sélectionne les informations contenues dans les TLV qui doivent être transmises. Les informations disponibles sont les suivantes : System Name (Nom du système), System Capabilities (Capacités du système), System Description (Description du système) et Port Description (Description du port).

Modification de la configuration LLDP

1. Affichez la page **LLDP Configuration** (Configuration LLDP).
2. Complétez les champs avec les valeurs appropriées.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres LLDP sont sauvegardés sur le commutateur.

Affichage de la table de paramètres de l'interface LLDP

1. Affichez la page **LLDP Configuration** (Configuration LLDP).
2. Cliquez sur **Show All** (Afficher tout).

La page **LLDP Interface Settings Table** (Table de paramètres de l'interface LLDP) s'affiche.

Figure 8-76. Page LLDP Interface Settings Table (Table des paramètres de l'interface LLDP)

Port	Transmit	Receive	Notify	Management Info	System Name	System Description	System Capabilities	Port Description	Copy To	Edit
1/1g1	Disable	Disable	Disable	Disable						
2/1g2	Disable	Disable	Disable	Disable						
3/1g3	Disable	Disable	Disable	Disable						
26/1lg2	Disable	Disable	Disable	Disable						
27/1lg3	Disable	Disable	Disable	Disable						
28/1lg4	Disable	Disable	Disable	Disable						

3. Utilisez le menu déroulant **Unit** (Unité) pour afficher la page **LLDP Interface Settings Table** (Table des paramètres de l'interface LLDP) pour les autres unités de la pile, le cas échéant.

Copie de paramètres de l'interface LLDP

1. Affichez la page **LLDP Configuration** (Configuration LLDP).
2. Cliquez sur **Show All** (Afficher tout).

La page **LLDP Interface Settings Table** (Table de paramètres de l'interface LLDP) s'affiche.

3. Indiquez l'unité et le port à partir desquels vous effectuez la copie dans **Copy Parameters From** (Copie les paramètres à partir de).
4. Cliquez sur **Copy To** (Copier vers) pour chaque unité/port cible.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de l'interface LLDP sont copiés et le périphérique est mis à jour.

Modification des paramètres de l'interface LLDP pour plusieurs ports

1. Affichez la page **LLDP Configuration** (Configuration LLDP).
2. Cliquez sur **Show All** (Afficher tout).

La page **LLDP Interface Settings Table** (Table de paramètres de l'interface LLDP) s'affiche.

3. Cliquez sur **Edit** (Modifier) pour chaque unité/port à modifier.
4. Modifiez les champs de l'interface LLDP selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de l'interface LLDP sont modifiés et le périphérique est mis à jour.

Configuration des paramètres LLDP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. LLDP Commands (Commandes LLDP)

Statistiques LLDP

La page **LLDP Statistics** (Statistiques LLDP) permet de visualiser les statistiques relatives au protocole LLDP.

Pour afficher cette page, cliquez sur **Switching** (Commutation) → **LLDP** → **LLDP Statistics** (Statistiques LLDP) dans l'arborescence.

Figure 8-77. Page LLDP Statistics (Statistiques LLDP)

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "LLDP Statistics" and includes a "Unit" dropdown menu set to "1". Below this, there are summary statistics for LLDP:

Last Update	0d 00:00:00
Total Inserts	0
Total Deletes	0
Total Drops	0
Total Ageouts	0

Below the summary statistics is a table showing LLDP statistics for individual interfaces:

Interface	Transmit Total	Receive Total	Discards	Errors	Ageouts	TLV Discards	TLV
1/g1	0	0	0	0	0	0	0
1/g2	0	0	0	0	0	0	0
1/xg3	0	0	0	0	0	0	0
1/xg4	0	0	0	0	0	0	0

At the bottom of the table, there is a "Clear Statistics" button.

Cette page contient les champs suivants :

Statistiques sur l'ensemble du système

Last Update (Dernière mise à jour) : affiche la durée de fonctionnement du système depuis la dernière mise à jour à distance de données effectuée (création, modification ou suppression de données).

Total Inserts (Total des insertions) : affiche le nombre de fois où un ensemble complet d'informations publié par un commutateur distant a été inséré dans la table.

Total Deletes (Total des suppressions) : affiche le nombre de fois où un ensemble complet d'informations publié par un commutateur distant a été supprimé de la table.

Total Drops (Total des rejets) : affiche le nombre de fois où un ensemble complet d'informations publié par un commutateur distant n'a pas pu être inséré en raison d'une insuffisance de ressources.

Total Ageouts (Total des délais arrivés à expiration) : affiche le nombre de fois où une entrée de données distante a été supprimée en raison de l'expiration du délai (TTL, Time-To-Live).

Statistiques sur les ports

Interface : affiche l'unité et le port auxquels les statistiques figurant sur cette ligne s'appliquent.

Transmit Total (Total des transferts) : affiche le nombre total de trames LLDP transmises sur le port indiqué.

Receive Total (Total des réceptions) : affiche le nombre total de trames LLDP valides reçues sur le port indiqué.

Discards (Rejets) : affiche le nombre de trames LLDP reçues sur le port indiqué et rejetées pour une raison quelconque.

Errors (Erreurs) : affiche le nombre de trames LLDP non valides ayant été reçues sur le port indiqué.

Ageouts (Délais arrivés à expiration) : affiche le nombre de fois où une entrée de données distante associée au port indiqué a été supprimée en raison de l'expiration du délai (TTL, Time-To-Live).

TLV Discards (TLV rejetés) : affiche le nombre de TLV (ensembles Type, Longueur, Valeur) LLDP ayant été reçus sur le port indiqué et rejetés pour une raison quelconque par l'agent LLDP.

TLV Unknowns (TLV inconnus) : affiche le nombre de TLV LLDP ayant été reçus sur le port indiqué mais dont le type n'a pas été reconnu par l'agent LLDP.

Utilisez le menu déroulant **Unit (Unité)** pour afficher la page **LLDP Statistics (Statistiques LLDP)** pour les autres unités de la pile, le cas échéant.

Utilisez le bouton **Clear Statistics (Effacer les statistiques)** pour remettre les statistiques LLDP à zéro.

Affichage des statistiques LLDP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 LLDP Commands (Commandes LLDP)

Connexions LLDP

La page **LLDP Connections (Connexions LLDP)** permet d'afficher la liste des ports sur lesquels le protocole LLDP est activé. Des informations de base sur les connexions sont affichées.

Pour afficher cette page, cliquez sur **Switching (Commutation)** → **LLDP** → **LLDP Connections (Connexions LLDP)** dans l'arborescence.

Figure 8-78. Table LLDP Connections (Connexions LLDP)



Local Interface	Chassis ID	Port ID	System Name
1/g11	00 FC E3 90 01 54	00 FC E3 90 01 56	dell_141

La page **LLDP Connections (Connexions LLDP)** contient les informations suivantes sur les ports :

Local Interface (Interface locale) : désigne une unité et un port de la pile.

Chassis ID (ID du châssis) : identifie le châssis du périphérique de réseau local 802.

Port ID (ID du port) : indique le numéro du port à partir duquel l'unité de données LLDP est transmise.

System Name (Nom du système) : identifie le nom de système associé au périphérique distant.

Utilisez le menu déroulant **Unit (Unité)** pour afficher la page **LLDP Connections (Connexions LLDP)** pour les autres unités de la pile, le cas échéant.

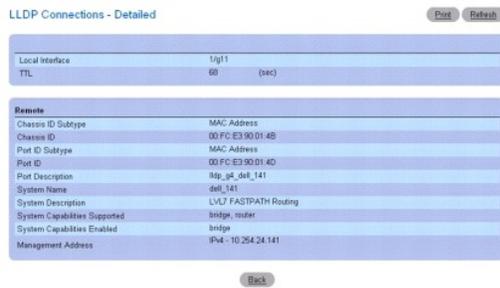
Utilisez le bouton **Clear Table** (Effacer la table) pour supprimer toutes les informations de la table **LLDP Connections** (Connexions LLDP).

Affichage d'informations détaillées sur les connexions LLDP

1. Affichez la page **LLDP Connections** (Connexions LLDP).
2. Cliquez sur une interface dans le champ **Local Interface** (Interface locale) pour afficher des informations détaillées sur le périphérique correspondant.

La page **LLDP Connections - Detailed** (Connexions LLDP - Informations détaillées) relative au périphérique concerné s'affiche.

Figure 8-79. Page LLDP Connections - Detailed (Connexions LLDP - Informations détaillées)



The screenshot shows the 'LLDP Connections - Detailed' page. At the top right, there are 'Print' and 'Refresh' buttons. The page is divided into two main sections: 'Local Interface' and 'Remote'. The 'Local Interface' section shows 'Local Interface' as 'Tig11' and 'TTL' as '60 (sec)'. The 'Remote' section lists various details for the connected device, including Chassis ID Subtype, Chassis ID, Port ID Subtype, Port ID, Port Description, System Name, System Description, System Capabilities Supported, System Capabilities Enabled, and Management Address.

Local Interface	
Local Interface	Tig11
TTL	60 (sec)

Remote	
Chassis ID Subtype	MAC Address
Chassis ID	00:FC:E3:90:01:4B
Port ID Subtype	MAC Address
Port ID	00:FC:E3:90:01:4D
Port Description	10p_g0_0/1_141
System Name	dell_141
System Description	LX7 FASTPATH Routing
System Capabilities Supported	bridge, mstc
System Capabilities Enabled	bridge
Management Address	IPv4 - 10.254.24.141

At the bottom center, there is a 'Back' button.

3. Utilisez le bouton **Back** (Précédent) pour revenir à la page **LLDP Connections** (Connexions LLDP).

Affichage des connexions LLDP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 LLDP Commands (Commandes LLDP)

[Retour au sommaire](#)

[Retour au sommaire](#)

Configuration du routage

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Protocole ARP](#)
- [Protocole IP](#)
- [Protocole OSPF](#)
- [Agent de relais BOOTP/DHCP](#)
- [Protocole RIP](#)
- [Protocole Router Discovery](#)
- [Routeur](#)
- [Routage VLAN](#)
- [Protocole VRRP](#)
- [Tunnels](#)
- [Boucles de rappel](#)

La série 6200 prend en charge la fonction de routage IP. Utilisez la page de menu **Routing** (Routage) pour configurer le routage sur les réseaux VLAN.

Lorsqu'un paquet arrive sur le commutateur, l'adresse MAC de destination est vérifiée pour déterminer si elle correspond aux interfaces de routage configurées. Si tel est le cas, le périphérique recherche dans la table des systèmes hôtes une adresse IP de destination correspondante. S'il trouve une entrée, le paquet est acheminé vers l'hôte. Dans le cas contraire, le commutateur recherche une correspondance avec le préfixe le plus long de l'adresse IP de destination. S'il trouve une entrée, le paquet est acheminé vers le saut suivant. Dans le cas contraire, le paquet est acheminé vers le saut suivant défini dans l'itinéraire par défaut. Si aucun itinéraire par défaut n'est configuré, le paquet est transmis au logiciel du PowerConnect 6200 qui lui appliquera le traitement approprié.

La table de routage peut contenir des entrées ajoutées de manière statique par l'administrateur ou de manière dynamique via le protocole RIP ou OSPF. La table des hôtes peut contenir des entrées ajoutées de manière statique par l'administrateur ou de manière dynamique via le protocole ARP.

La page **Routing** (Routage) contient des liens vers les fonctionnalités suivantes :

- 1 [Protocole ARP](#)
- 1 [Protocole IP](#)
- 1 [OSPF](#)
- 1 [Agent de relais BOOTP/DHCP](#)
- 1 [Protocole RIP](#)
- 1 [Protocole Router Discovery](#)
- 1 [Routeur](#)
- 1 [Routage VLAN](#)
- 1 [Protocole VRRP](#)
- 1 [Tunnels](#)
- 1 [Boucles de rappel](#)

 **REMARQUE :** Il n'existe aucune commande CLI pour les pages de routage.

Protocole ARP

Les systèmes de la série 6200 utilisent le protocole ARP pour associer une adresse MAC de couche 2 à une adresse IPv4 de couche 3. En outre, l'administrateur peut ajouter de manière statique des entrées à la table ARP.

Le protocole ARP est une partie obligatoire du protocole IP qui permet de convertir une adresse IP en adresse (MAC) média définie par un réseau local, par exemple Ethernet. Lorsqu'une station doit envoyer un paquet IP, elle doit apprendre l'adresse MAC de la destination IP, ou du routeur du saut suivant, si la destination n'est pas contenue dans le même sous-réseau. Pour ce faire, elle diffuse un paquet de requêtes ARP, et le destinataire renvoie une réponse ARP en monodiffusion contenant son adresse MAC. Une fois apprise, l'adresse MAC est utilisée dans le champ d'adresse de destination de l'en-tête de couche 2 ajouté au début du paquet IP.

La mémoire cache ARP est une table gérée localement dans chaque station d'un réseau. Aucune configuration spécifique n'est requise concernant la création ou la maintenance de cette mémoire cache, mais elle doit contenir au minimum les informations apprises durant le traitement des paquets du protocole ARP, qui sont désignées par le champ 0x0806 EtherType dans Ethernet. Les entrées de la mémoire cache ARP sont apprises grâce à une analyse des informations source contenues dans les champs de charge utile des paquets ARP, indépendamment du fait qu'il s'agisse d'une demande ou d'une réponse ARP. Ainsi, lorsqu'une requête ARP est diffusée à toutes les stations d'un segment LAN ou d'un réseau VLAN, chaque destinataire a la possibilité d'enregistrer les adresses IP et MAC de l'expéditeur dans sa mémoire cache ARP respective. La réponse ARP étant renvoyée en monodiffusion, elle n'est visible que par le demandeur qui enregistre les informations envoyées dans sa mémoire cache ARP. Les nouvelles informations remplacent systématiquement le contenu existant de la mémoire cache ARP.

La mémoire cache ARP peut accepter 896 entrées, mais cette taille peut être configurée par l'utilisateur sur une valeur inférieure (supérieure à 256). Lorsque plusieurs interfaces réseau sont prises en charge par un périphérique, comme c'est le cas généralement du routeur, une mémoire cache ARP unique est utilisée pour toutes les interfaces ou une mémoire cache distincte est utilisée par interface. Cette dernière solution est utile lorsqu'il existe plusieurs adressages réseau par interface, ce qui n'est pas le cas pour l'attribution d'adresses MAC Ethernet. Par conséquent, une mémoire cache ARP unique est utilisée.

Étant donné que les périphériques peuvent être déplacés dans un réseau, l'adresse IP associée à un moment donné à une certaine adresse MAC se retrouve associée à une autre adresse MAC ou peut avoir disparu complètement du réseau (celui-ci a été reconfiguré, déconnecté ou mis hors tension). De ce fait, les informations contenues dans la mémoire cache ARP deviennent obsolètes sauf si les entrées sont mises à jour pour tenir compte des nouvelles informations contenues sur le réseau, actualisées régulièrement pour déterminer si une adresse existe toujours, ou encore supprimées de la mémoire cache si l'entrée n'a pas été identifiée comme l'expéditeur d'un paquet ARP dans un intervalle d'expiration généralement défini dans la configuration.

La page de menu **ARP** contient des liens vers les pages Web permettant de configurer et d'afficher les détails ARP. Pour afficher cette page, cliquez sur **Routing** (Routage) → **ARP** dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

- 1 [Création ARP](#)

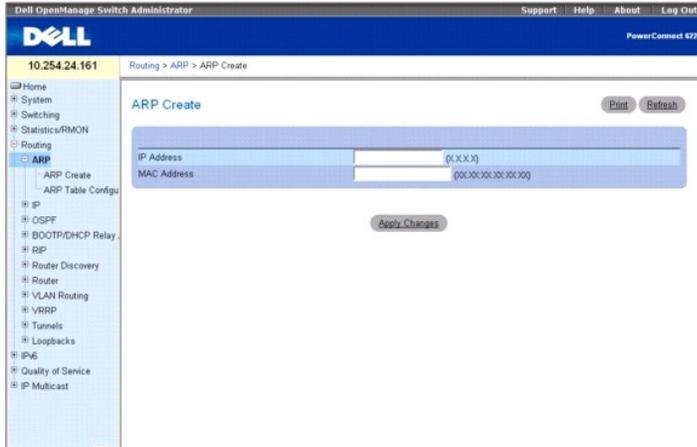
1 [Configuration de la table ARP](#)

Création ARP

La page **ARP Create** (Création ARP) permet d'ajouter une entrée à la table ARP (Address Resolution Protocol).

Pour afficher cette page, cliquez sur **Routing** (Routage) → **ARP** → **ARP Create** (Création ARP) dans l'arborescence.

Figure 10-1. Page ARP Create (Création ARP)



La page **ARP Create** (Création ARP) contient les champs suivants :

IP Address (Adresse IP) : entrez l'adresse IP à ajouter. Elle doit correspondre à l'adresse IP d'un périphérique présent dans un sous-réseau connecté à l'une des interfaces de routage existantes du commutateur.

MAC Address (Adresse MAC) : adresse MAC monodiffusion du périphérique. Elle doit comporter six nombres hexadécimaux à deux chiffres séparés par deux points, par exemple 00:06:29:32:81:40.

Ajout d'une entrée dans la table ARP

1. Affichez la page **ARP Create** (Création ARP).
2. Entrez les adresses à associer.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les adresses sont maintenant enregistrées dans la mémoire cache ARP.

Ajout d'une entrée dans la table ARP à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

1. ARP Commands (Commandes ARP)

Configuration de la table ARP

Cette page permet de modifier les paramètres de configuration de la table ARP (Address Resolution Protocol). Vous pouvez également utiliser cet écran pour afficher le contenu de la table.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **ARP** → **ARP Table Configuration** (Configuration de la table ARP) dans l'arborescence.

Figure 10-2. Page ARP Table Configuration (Configuration de la table ARP)



La page ARP Table Configuration (Configuration de la table ARP) contient les champs suivants :

Age Time (secs) (Délai d'expiration [secondes]) : entrez la valeur que le commutateur doit utiliser pour le délai d'expiration d'une entrée ARP. Vous devez entrer un nombre entier valide, qui représente le nombre de secondes avant l'expiration d'une entrée ARP. Les valeurs admises sont comprises entre 15 et 21600 secondes. La valeur par défaut est de 1200 secondes.

Response Time (secs) (Délai de réponse [secondes]) : entrez la valeur que le commutateur doit utiliser pour le délai de réponse ARP. Vous devez entrer un nombre entier valide, qui représente le délai d'attente en secondes avant que le commutateur obtienne une réponse à une requête ARP. Les valeurs admises sont comprises entre 1 et 10 secondes. La valeur par défaut est de 1 seconde.

Retries (Tentatives) : entrez un nombre entier qui représente le nombre maximum de tentatives pour une requête ARP. La plage de valeurs pour ce champ est comprise entre 0 et 10. La valeur par défaut est de 4.

Cache Size (Taille de la mémoire cache) : entrez un nombre entier qui représente le nombre maximum d'entrées pour la mémoire cache ARP. La plage de valeurs pour ce champ est comprise entre 256 et 896. La valeur par défaut est de 896.

Dynamic Renew (Renouvellement dynamique) : ce champ contrôle si le composant ARP tente automatiquement de renouveler les entrées ARP de type dynamique une fois qu'elles ont expiré. Le paramètre par défaut est Enable (Activer).

Total Entry Count (Nombre total d'entrées) : nombre total d'entrées dans la table ARP.

Peak Total Entries (Nombre maximum d'entrées) : valeur la plus élevée que peut atteindre le champ Total Entry Count (Nombre total d'entrées). Cette valeur de compteur est réinitialisée lorsque la valeur de la taille de la mémoire cache de la table ARP est modifiée.

Active Static Entries (Entrées statiques actives) : nombre total d'entrées statiques actives dans la table ARP.

Configured Static Entries (Entrées statiques configurées) : nombre total d'entrées statiques configurées dans la table ARP.

Maximum Static Entries (Entrées statiques maximales) : nombre maximum d'entrées statiques pouvant être définies.

Remove from Table (Supprimer de la table) : permet de supprimer certaines entrées de la table ARP. Les choix énumérés indiquent le type d'entrée ARP à supprimer :

- 1 All Dynamic Entries (Toutes les entrées dynamiques)
- 1 All Dynamic and Gateway Entries (Toutes les entrées dynamiques et de passerelle)
- 1 Specific Dynamic Gateway Entry (Entrée de passerelle dynamique spécifique)
- 1 Specific Static Entry (Entrée statique spécifique)

La table ARP s'affiche au bas de la page avec les champs suivants :

IP Address (Adresse IP) : adresse IP d'un périphérique faisant partie d'un sous-réseau connecté à l'une des interfaces de routage du commutateur.

MAC Address (Adresse MAC) : adresse MAC monodiffusion du périphérique. Elle doit comporter six nombres hexadécimaux à deux chiffres séparés par deux points, par exemple 00:06:29:32:81:40.

VLAN ID (ID du VLAN) : interface de routage associée à l'entrée ARP.

Type : type de l'entrée ARP.

Age (Âge) : temps écoulé depuis la dernière actualisation de l'entrée dans la table ARP. Le format est hh:mm:ss.

Configuration de la table ARP

1. Affichez la page **ARP Table Configuration** (Configuration de la table ARP).
2. Modifiez les paramètres au besoin.

3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications sont enregistrées et la table ARP est mise à jour.

Configuration de la table ARP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

1. ARP Commands (Commandes ARP)

Protocole IP

La page de menu **IP** contient des liens vers les pages Web permettant de configurer et d'afficher les données de routage IP. Pour afficher cette page, cliquez sur **Routing** (Routage) → **IP** dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

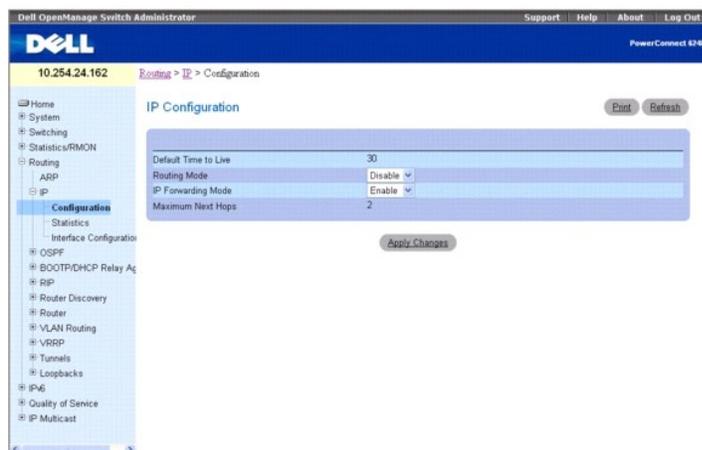
1. [Configuration IP](#)
1. [Statistiques IP](#)
1. [Configuration de l'interface IP](#)

Configuration IP

La page **IP Configuration** (Configuration IP) permet de configurer les paramètres de routage du commutateur, par opposition à une interface.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **IP** → **Configuration** dans l'arborescence.

Figure 10-3. Page **IP Configuration** (Configuration IP)



Cette page contient les champs suivants :

Default Time to Live (Durée de vie par défaut) : valeur par défaut du champ Time-To-Live (Durée de vie) figurant dans l'en-tête IP des datagrammes provenant du commutateur, si aucune valeur de durée de vie n'est fournie par le protocole de couche de transport.

Routing Mode (Mode de routage) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Vous devez activer le routage du commutateur pour pouvoir transiter par l'une des interfaces. Le routage est également activé ou désactivé par interface VLAN. La valeur par défaut est Disable (Désactiver).

IP Forwarding Mode (Mode de transfert IP) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Cela permet d'activer ou de désactiver le transfert des trames IP. La valeur par défaut est Enable (Activer).

Maximum Next Hops (Nombre maximum de sauts suivants) : nombre maximum de sauts pris en charge par le commutateur. Cette constante est définie au moment de la compilation.

Configuration des paramètres de routage IP

1. Affichez la page **IP Configuration** (Configuration IP).
2. Modifiez les paramètres au besoin.

3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications sont enregistrées et les paramètres de routage sont mis à jour.

Configuration des paramètres de routage IP à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous aux chapitres suivants du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 IP Routing Commands (Commandes de routage IP)
- 1 VLAN Commands (Commandes portant sur les VLAN)

Statistiques IP

Les statistiques contenues sur la page **IP Statistics** (Statistiques IP) sont conformes à la norme RFC 1213.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **IP** → **Statistics** (Statistiques) dans l'arborescence.

Figure 10-4. Page IP Statistics (Statistiques IP)

Metric	Value
IpInReceives	520
IpInHdrErrors	0
IpInAddrErrors	0
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	479
IpOutRequests	699
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	0
IpReasmReqds	0
IpReasmCkcs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IpMplsMpls	0
IpMplsErrors	0

Cette page contient les champs suivants :

IpInReceives : nombre total de datagrammes entrants transmis par les interfaces, y compris ceux contenant des erreurs.

IpInHdrErrors : nombre de datagrammes entrants rejetés en raison d'erreurs dans leurs en-têtes IP, notamment des sommes de contrôle incorrectes, des numéros de version incompatibles, d'autres erreurs de format, une durée de vie dépassée, des erreurs détectées durant le traitement de leurs options IP, etc.

IpInAddrErrors : nombre de datagrammes entrants rejetés car l'adresse IP figurant dans le champ de destination de leur en-tête IP était une adresse incorrecte pour cette entité. Ce nombre inclut les adresses incorrectes (par exemple 0.0.0.0) et les adresses appartenant à des catégories non prises en charge (par exemple la catégorie E). Pour les entités qui ne servent pas de passerelles IP et qui, par conséquent, ne transmettent pas de datagrammes, ce compteur inclut les datagrammes ignorés car l'adresse de destination n'était pas une adresse locale.

IpForwDatagrams : nombre de datagrammes entrants pour lesquels le système tente de rechercher un itinéraire pour les acheminer vers leur destination finale si cette entité n'était pas leur destination IP finale. Pour les entités ne servant pas de passerelles IP, ce compteur inclut uniquement les paquets ayant fait l'objet d'une action Source-Route (Itinéraire source) par le biais de cette entité, et pour lesquels le traitement de cette action s'est correctement déroulé.

IpInUnknownProtos : nombre de datagrammes adressés localement qui ont été reçus avec succès mais ignorés en raison d'un protocole inconnu ou non pris en charge.

IpInDiscards : nombre de datagrammes IP entrants dont le traitement continu s'est déroulé sans incidents, mais qui ont été rejetés (par exemple, par manque de mémoire tampon). Notez que ce compteur n'inclut pas les datagrammes rejetés pendant l'attente de leur réassemblage.

IpInDelivers : nombre total de datagrammes entrants transmis avec succès aux protocoles IP utilisateur (y compris le protocole ICMP).

IpOutRequests : nombre total de datagrammes IP fournis par les protocoles IP utilisateur locaux (y compris le protocole ICMP) au protocole IP dans les requêtes de transmission. Notez que ce compteur n'inclut pas les datagrammes dénombrés dans ipForwDatagrams.

IpOutDiscards : nombre de datagrammes IP sortants qui ont été transmis à leur destination sans incidents, mais ont été rejetés (par exemple, par manque de mémoire tampon). Notez que ce compteur inclut les datagrammes dénombrés dans ipForwDatagrams si ces paquets répondent à ce critère de rejet (conditionnel).

IpOutNoRoutes : nombre de datagrammes IP rejetés car aucun itinéraire n'a pu être trouvé pour les acheminer vers leur destination. Ce compteur inclut tous les paquets comptabilisés dans ipForwDatagrams et répondant à ce critère d'absence d'itinéraire, ainsi que les datagrammes qu'un système hôte ne peut pas acheminer car toutes ses passerelles par défaut sont indisponibles.

IpReasmTimeout : nombre maximum de secondes pendant lesquelles les fragments reçus sont conservés en attendant leur réassemblage sur cette entité.

IpReasmReqds : nombre de fragments IP reçus qui doivent être réassemblés sur cette entité.

IpReasmOKs : nombre de datagrammes IP réassemblés avec succès.

IpReasmFails : nombre d'échecs détectés par l'algorithme de réassemblage IP (pour une raison quelconque : délai expiré, erreurs, etc). Notez que ce nombre ne correspond pas forcément au nombre de fragments IP rejetés car certains algorithmes peuvent perdre la trace du nombre de fragments en les associant à leur réception.

IpFragOKs : nombre de datagrammes IP fragmentés avec succès sur cette entité.

IpFragFails : nombre de datagrammes IP rejetés car leur fragmentation sur cette entité n'a pas pu être effectuée (par exemple, parce que leur indicateur "Don't Fragment" [Ne pas fragmenter] était défini).

IpFragCreates : nombre de fragments de datagrammes IP générés suite à leur fragmentation sur cette entité.

IpRoutingDiscards : nombre d'entrées de routage rejetées bien qu'elles soient valides. Une des raisons possibles justifiant ce rejet est de libérer de l'espace dans la mémoire tampon pour les autres entrées de routage.

IcmpInMsgs : nombre total de messages ICMP reçus par l'entité. Notez que ce compteur inclut tous les messages dénombrés dans icmpInErrors.

IcmpInErrors : nombre de messages ICMP reçus par l'entité, mais contenant des erreurs propres au protocole ICMP (sommes de contrôle ICMP incorrectes, longueur incorrecte, etc.).

IcmpInDestUnreachs : nombre de messages ICMP "Destination Unreachable" (Destination inaccessible) reçus.

IcmpInTimeExcds : nombre de messages ICMP "Time Exceeded" (Délai dépassé) reçus.

IcmpInParmProbs : nombre de messages ICMP "Parameter Problem" (Problème de paramètres) reçus.

IcmpInSrcQuenchs : nombre de messages ICMP "Source Quench" (Extinction de la source) reçus.

IcmpInRedirects : nombre de messages ICMP "Redirect" (Redirection) reçus.

IcmpInEchos : nombre de messages (requête) ICMP "Echo" (Écho) reçus.

IcmpInEchoReps : nombre de messages ICMP "Echo Reply" (Réponse à l'écho) reçus.

IcmpInTimestamps : nombre de messages (requête) ICMP "Timestamp" (Horodateur) reçus.

IcmpInTimestampReps : nombre de messages ICMP "Timestamp Reply" (Réponse horodateur) reçus.

IcmpInAddrMasks : nombre de messages ICMP "Address Mask Request" (Demande de masque d'adresse) reçus.

IcmpInAddrMaskReps : nombre de messages ICMP "Address Mask Reply" (Réponse masque d'adresse) reçus.

IcmpOutMsgs : nombre total de messages ICMP que cette entité a tenté d'envoyer. Notez que ce compteur inclut tous les messages dénombrés dans icmpOutErrors.

IcmpOutErrors : nombre de messages ICMP qui n'ont pas été envoyés par cette entité en raison de problèmes détectés dans le protocole ICMP, par exemple un manque de mémoire tampon. Cette valeur ne doit pas inclure les erreurs détectées en dehors de la couche ICMP, par exemple l'incapacité du protocole IP à acheminer le datagramme résultant. Dans certaines implémentations, aucun type d'erreur n'intervient dans la valeur de ce compteur.

IcmpOutDestUnreachs : nombre de messages ICMP "Destination Unreachable" (Destination inaccessible) envoyés.

IcmpOutTimeExcds : nombre de messages ICMP "Time Exceeded" (Délai dépassé) envoyés.

IcmpOutParmProbs : nombre de messages ICMP "Parameter Problem" (Problème de paramètres) envoyés.

IcmpOutSrcQuenchs : nombre de messages ICMP "Source Quench" (Extinction de la source) envoyés.

IcmpOutRedirects : nombre de messages ICMP "Redirect" (Redirection) envoyés. Cet objet a toujours la valeur zéro pour un hôte, car les hôtes n'envoient pas de redirections.

IcmpOutEchos : nombre de messages (requête) ICMP "Echo" (Écho) envoyés.

IcmpOutEchoReps : nombre de messages ICMP "Echo Reply" (Réponse à l'écho) envoyés.

IcmpOutTimestamps : nombre de messages (requête) ICMP "Timestamp" (Horodateur) envoyés.

IcmpOutTimestampReps : nombre de messages ICMP "Timestamp Reply" (Réponse horodateur) envoyés.

IcmpOutAddrMasks : nombre de messages ICMP "Address Mask Request" (Demande de masque d'adresse) envoyés.

IcmpOutAddrMaskReps : nombre de messages ICMP "Address Mask Reply" (Réponse masque d'adresse) envoyés.

Actualisation des statistiques IP

1. Affichez la page **IP Statistics** (Statistiques IP).
2. Cliquez sur **Refresh** (Actualiser).

L'écran affiche l'état actuel des données contenues dans le commutateur.

Affichage des statistiques IP à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

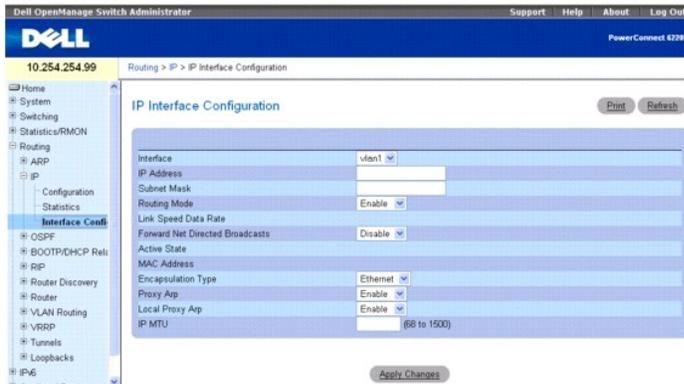
- 1 IP Routing Commands (Commandes de routage IP)

Configuration de l'interface IP

La page **IP Interface Configuration** (Configuration de l'interface IP) permet de mettre à jour les données de l'interface IP de ce commutateur.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **IP** → **Interface Configuration** (Configuration de l'interface) dans l'arborescence.

Figure 10-5. Page IP Interface Configuration (Configuration de l'interface IP)



La page **IP Interface Configuration** (Configuration de l'interface IP) contient les champs suivants :

Interface : sélectionnez l'interface à configurer dans le menu déroulant. Le menu déroulant contient les interfaces de boucles de rappel et les VLAN créés à partir de la page **Switching** (Commutation) → **VLAN** → **VLAN Membership** (Appartenance à un VLAN) → **Add** (Ajouter).

IP Address (Adresse IP) : entrez l'adresse IP de l'interface.

Subnet Mask (Masque de sous-réseau) : entrez le masque de sous-réseau de l'interface. Il est également appelé masque de sous-réseau/réseau, et définit la partie de l'adresse IP de l'interface utilisée pour identifier le réseau connecté.

Routing Mode (Mode de routage) : ce champ permet d'activer ou de désactiver le routage d'une interface. La valeur par défaut est Enable (Activer).

Link Speed Data Rate (Débit de données pour la vitesse de liaison) : nombre entier représentant le débit de données de la liaison physique pour l'interface spécifiée. Cette valeur s'applique uniquement aux interfaces physiques, et est exprimée en mégabits par seconde (Mbits/s).

Forward Net Directed Broadcasts (Envoyer les paquets de diffusion gérés par le réseau) : choisissez le mode de gestion des paquets de diffusion gérés par le réseau. Si vous sélectionnez Enable (Activer) dans le menu déroulant, les paquets de diffusion gérés par le réseau sont envoyés. Si vous sélectionnez Disable (Désactiver), ils sont abandonnés. La valeur par défaut est Disabled (Désactivé).

Active State (État d'activité) : état de l'interface spécifiée (Active ou Inactive). Une interface est considérée comme active si la liaison est activée et en état de transfert.

MAC Address (Adresse MAC) : adresse MAC de l'interface spécifiée. Elle doit comporter six nombres hexadécimaux à deux chiffres séparés par deux points, par exemple 00:06:29:32:81:40. Cette valeur s'applique aux interfaces physiques. Pour les interfaces logiques, par exemple les interfaces de routage VLAN, le champ affiche l'adresse MAC du système.

Encapsulation Type (Type d'encapsulation) : sélectionnez dans le menu déroulant le type d'encapsulation de la couche de liaison pour les paquets transmis à partir de l'interface spécifiée. Les valeurs possibles sont Ethernet et SNAP. La valeur par défaut est Ethernet.

Proxy ARP (ARP du proxy) : vous pouvez activer ou désactiver le protocole ARP du proxy pour l'interface spécifiée dans le menu déroulant.

Local Proxy ARP (ARP du proxy local) : vous pouvez activer ou désactiver le protocole ARP du proxy local pour l'interface spécifiée dans le menu déroulant.

IP MTU (MTU IP) : indique la taille MTU (Maximum Transmission Unit) des paquets IP envoyés sur une interface. La plage de valeurs admises est comprise entre 68 et 1500. La valeur par défaut est de 1500.

Modification d'une interface IP

1. Affichez la page **IP Interface Configuration** (Configuration de l'interface IP).
2. Modifiez les valeurs au besoin.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications sont enregistrées et l'interface IP est mise à jour.

Commandes CLI de configuration de l'interface IP

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous aux chapitres suivants du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 IP Addressing Commands (Commandes d'adressage IP)
 - 1 IP Routing Commands (Commandes de routage IP)
 - 1 ARP Commands (Commandes ARP)
-

Protocole OSPF

Le protocole de routage OSPF (Open Shortest Path First) est un protocole IGP (Interior Gateway Protocol). Chaque routeur OSPF crée l'arborescence du chemin le plus court pour tous les routeurs et réseaux du domaine. Les informations de routage sont acheminées par paquets LSU (Link State Update) de manière régulière et en cas de modifications de la topologie du réseau. Elles sont reçues, assimilées et enregistrées dans les bases de données OSPF de chaque routeur. Une information complète dans l'échange de bases de données comprend le numéro et les adresses IP des interfaces associées au routeur. Le protocole OSPF traite les adresses IP secondaires comme des réseaux d'extrémité connectés au routeur. Même si ces réseaux sont annoncés dans le domaine de routage OSPF, les contiguïtés n'utilisent jamais les adresses secondaires. Il est également important de noter que toutes les adresses IP secondaires doivent être contenues dans la même zone que l'adresse IP principale afin qu'elles soient annoncées par le protocole OSPF. Cela est toujours vrai dans le cas de l'implémentation des systèmes de la série 6200, car la configuration de la zone s'effectue interface par interface et non en fonction du réseau.

La page de menu **OSPF** contient des liens vers les pages Web permettant de configurer et d'afficher les paramètres et les données OSPF. Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

- 1 [Configuration OSPF](#)
- 1 [Configuration de la zone](#)
- 1 [Récapitulatif de la zone de stub](#)
- 1 [Configuration de la plage de zones](#)
- 1 [Statistiques sur les interfaces](#)
- 1 [Configuration de l'interface](#)
- 1 [Table des voisins](#)
- 1 [Configuration du routeur voisin](#)
- 1 [Base de données LSDB](#)
- 1 [Configuration des liaisons virtuelles](#)
- 1 [Récapitulatif des liaisons virtuelles](#)
- 1 [Configuration de la redistribution des itinéraires](#)
- 1 [Récapitulatif de la redistribution des itinéraires](#)

Configuration OSPF

La page **OSPF Configuration** (Configuration OSPF) permet d'activer l'interface OSPF d'un routeur et de configurer les paramètres OSPF associés.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Configuration** dans l'arborescence.

Figure 10-6. Page OSPF Configuration (Configuration OSPF)



Cette page contient les champs suivants :

Router ID (ID du routeur) : nombre entier de 32 bits à points décimaux qui identifie de manière unique le routeur dans le système autonome. Pour modifier l'ID du routeur, vous devez d'abord désactiver l'interface OSPF. Une fois que vous avez défini le nouvel ID du routeur, vous devez réactiver l'interface OSPF pour que les modifications prennent effet. La valeur par défaut est 0.0.0.0, qui n'est pas un ID de routeur correct.

OSPF Admin Mode (Mode admin OSPF) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Si vous sélectionnez Enable (Activer), l'interface OSPF est activée pour ce commutateur. La valeur par défaut est Disabled (Désactivé). Vous devez configurer un ID de routeur pour que l'interface OSPF devienne opérationnelle.

REMARQUE : Une fois l'interface OSPF activée sur le routeur, elle reste active tant que le routeur n'est pas réinitialisé.

ASBR Mode (Mode ASBR) : indique si le mode ASBR est activé ou désactivé. S'il est activé, cela signifie que le routeur est un routeur de limites de systèmes autonomes (ASBR, Autonomous System Border Router). Il devient automatiquement un routeur ASBR lorsqu'il est configuré pour redistribuer les itinéraires appris à partir d'un autre protocole.

RFC 1583 Compatibility (Compatibilité RFC 1583) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant pour indiquer les règles de préférences qui s'appliquent lorsque vous choisissez parmi plusieurs LSA externes au système autonome qui annoncent la même destination. Si vous sélectionnez Enable (Activer), les règles de préférences définies par RFC 1583 s'appliquent. Si vous sélectionnez Disable (Désactiver), les règles de préférences définies à la section 16.4.1 de la norme OSPF-2 (RFC 2328) s'appliquent, ce qui empêche le routage des boucles lorsque les LSA externes au système autonome annonçant la même destination proviennent de zones différentes. La valeur par défaut est Enable (Activer). Pour empêcher le routage des boucles, vous devez sélectionner Disable (Désactiver), mais uniquement si tous les routeurs OSPF contenus dans le domaine de routage peuvent fonctionner conformément à la RFC 2328.

ABR Status (État ABR) : les valeurs de ce champ sont Enabled (Activé) ou Disabled (Désactivé). L'option Enabled (Activé) indique que le routeur est un routeur de limite de zone. L'option Disabled (Désactivé) indique le contraire.

Exit Overflow Interval (sec) (Intervalle de sortie en cas de saturation [secondes]) : entrez le délai d'attente en secondes avant que le routeur tente de sortir de l'état de saturation, une fois cet état activé. Cela permet au routeur de créer à nouveau des LSA externes au système autonome qui ne sont pas définies par défaut. Si vous entrez la valeur 0, le routeur ne quitte pas l'état de saturation tant que le système n'est pas redémarré. Les valeurs admises sont comprises entre 0 et 2147483647 secondes.

SPF DelayTime (secs) (Délai SPF [secondes]) : entrez le délai en secondes entre le moment où l'interface OSPF reçoit un changement de topologie et le moment où elle démarre un calcul SPF. Cette valeur peut être un nombre entier compris entre 0 et 65535. La valeur par défaut est de 5 secondes. La valeur 0 indique qu'aucun délai n'est défini ; le calcul SPF est démarré immédiatement.

SPF HoldTime (secs) (Délai d'attente [secondes]) : entrez la durée minimale en secondes entre deux calculs SPF consécutifs. Cette valeur peut être un nombre entier compris entre 0 et 65535. La valeur par défaut est de 10 secondes. La valeur 0 indique qu'aucun délai n'est défini ; deux calculs SPF peuvent être effectués, l'un immédiatement après l'autre.

External LSA Count (Nombre de LSA externes) : nombre de LSA (Link State Advertisements) externes (LS de type 5) contenues dans la base de données LSDB (Link State Database).

External LSA Checksum (Somme de contrôle des LSA externes) : total des sommes de contrôle LS des LSA externes contenues dans la base de données LSDB (Link State Database). Cette valeur peut être utilisée pour déterminer si des modifications ont été apportées à la base de données LSDB d'un routeur et pour comparer les bases de données LSDB de deux routeurs. Elle est au format hexadécimal.

New LSAs Originated (Nouvelles LSA créées) : dans une zone OSPF donnée, un routeur crée plusieurs LSA. Chaque routeur crée la LSA associée à un routeur. Si le routeur correspond également au routeur désigné pour l'un des réseaux de la zone, il crée les LSA associées à ces réseaux. Cette valeur désigne le nombre de LSA créées par ce routeur.

LSAs Received (LSA reçues) : nombre de LSA (Link State Advertisements) reçues qui sont considérées comme de nouvelles instanciations. Ce nombre n'inclut pas les nouvelles instanciations des LSA créées automatiquement.

Default Metric (Métrique par défaut) : définit une valeur par défaut pour la métrique des itinéraires redistribués. Ce champ affiche la métrique par défaut si la source a déjà été définie, ou ne contient aucune valeur si elle n'a pas été configurée précédemment. Les valeurs admises sont comprises entre 1 et 16777214.

Maximum Paths (Chemins d'accès maximum) : configurez le nombre maximum de chemins d'accès que l'interface OSPF peut spécifier pour une destination donnée. Les valeurs admises sont 1 et 2.

Default Route Advertise (Annonce de routage par défaut)

Default Information Originate (Création d'informations par défaut) : activez ou désactivez l'option Default Route Advertise (Annonce de routage par défaut).

Always (Toujours) : définit l'annonce de routeur 0.0.0.0/0.0.0.0 lorsqu'elle est définie sur True (Vrai).

Metric (Métrique) : définit la métrique de l'itinéraire par défaut. Les valeurs admises sont comprises entre 1 et 16777214.

Metric Type (Type de métrique) : définit le type de métrique de l'itinéraire par défaut. Les options sont External Type 1 (Type externe 1) et External Type 2 (Type externe 2). La valeur par défaut est External Type 2 (Type externe 2).

Modification d'une configuration OSPF

1. Affichez la page **OSPF Configuration** (Configuration OSPF).
2. Modifiez les valeurs au besoin.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications sont enregistrées et l'interface OSPF est mise à jour.

Commandes CLI de configuration OSPF

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

1. OSPF Commands (Commandes OSPF)

Configuration de la zone

La page **OSPF Area Configuration** (Configuration de la zone OSPF) permet de créer une configuration de zone de stub et une configuration NSSA une fois que vous avez activé le protocole OSPF d'une interface via l'option **Routing** (Routage) → **OSPF** → **Interface Configuration** (Configuration de l'interface). L'interface OSPF d'au moins un routeur doit être activée pour que cette page Web puisse s'afficher.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Interface Configuration** (Configuration de l'interface) dans l'arborescence.

Figure 10-7. Page OSPF Area Configuration (Configuration de la zone OSPF)



La page **OSPF Area Configuration** (Configuration de la zone OSPF) contient les champs suivants :

Area (Zone) : sélectionnez la zone à afficher dans le menu déroulant. Lorsqu'une zone est sélectionnée, les champs de l'option Stub Area Information (Informations de la zone de stub) s'affichent.

Area ID (ID de zone) : zone OSPF. Cette valeur doit être un nombre entier de 32 bits à points décimaux qui identifie de manière unique la zone à laquelle une interface de routeur est connectée.

External Routing (Routage externe) : définition des fonctions du routeur pour la zone, notamment si les LSA externes au système autonome sont acheminées vers la zone. Si la zone est une zone de stub, les options possibles permettant de configurer les fonctions du routage externe sont décrites ci-dessous. Dans le cas contraire, l'unique option disponible est Import External LSAs (Importer les LSA externes).

SPF Runs (Exécutions SPF) : nombre de fois que la table de routage intra-zone a été calculée à l'aide de la base de données LSDB (Link State Database) de cette zone. Ce calcul s'effectue généralement à l'aide de l'algorithme de Dijkstra.

Area Border Router Count (Nombre de routeurs de limite de zone) : nombre total de routeurs de limite de zone accessibles dans cette zone. La valeur initiale est égale à zéro, et est calculée pour chaque passage SPF.

Area LSA Count (Nombre de LSA dans la zone) : nombre total de LSA (Link State Advertisements) contenues dans la base de données LSDB (Link State Database) de cette zone, en excluant les LSA externes au système autonome.

Area LSA Checksum (Somme de contrôle des LSA dans la zone) : total non signé de 32 bits des sommes de contrôle LS des LSA contenues dans la base de données LSDB (Link State Database) de cette zone. Cette valeur exclut les LSA (LS de type 5) externes. Elle peut être utilisée pour déterminer si des modifications ont été apportées à la base de données LSDB d'un routeur et pour comparer les bases de données LSDB de deux routeurs. Elle est au format hexadécimal.

Stub Area Information (Informations de la zone de stub)

Import Summary LSAs (Importer les LSA récapitulatives) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Si vous sélectionnez Enable (Activer), les LSA récapitulatives sont importées dans les zones de stub.

Metric Value (Valeur de métrique) : entrez la valeur de métrique que vous souhaitez appliquer pour l'itinéraire par défaut annoncé dans la zone de stub. La plage de valeurs admises est comprise entre 1 et 16 777 215.

Metric Type (Type de métrique) : sélectionnez le type de métrique défini dans le champ Metric Value (Valeur de métrique).

Translator Role (Rôle du traducteur) : attribuez au rôle du traducteur NSSA la valeur Always/Candidate (Toujours/candidat).

Translator Stability Interval (Intervalle de stabilité du traducteur) : configurez l'interface de stabilité du traducteur pour le NSSA sélectionné.

No-Redistribute Mode (Mode de non-redistribution) : configurez la redistribution des itinéraires pour le NSSA sélectionné.

Translator State (État du traducteur) : affiche l'état actuel du traducteur.

Configuration d'une zone OSPF

1. Affichez la page **OSPF Area Configuration** (Configuration de la zone OSPF).
2. Indiquez une zone à configurer.
3. Renseignez les autres champs si nécessaire.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La zone OSPF est définie et configurée.

Affichage de la configuration d'une zone OSPF

1. Affichez la page **OSPF Area Configuration** (Configuration de la zone OSPF).
2. Sélectionnez la zone OSPF à afficher dans le menu déroulant.

La configuration de la zone OSPF s'affiche dans cette zone.

Suppression de la configuration d'une zone OSPF

Suivez la procédure ci-après pour supprimer la configuration NSSA ou la configuration de la zone de stub.

1. Affichez la page **OSPF Area Configuration** (Configuration de la zone OSPF).
2. Sélectionnez la configuration de la zone OSPF à supprimer dans le menu déroulant.

La configuration s'affiche.

3. Cliquez sur **Delete** (Supprimer).

La configuration de la zone OSPF est supprimée.

Configuration d'une zone OSPF à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

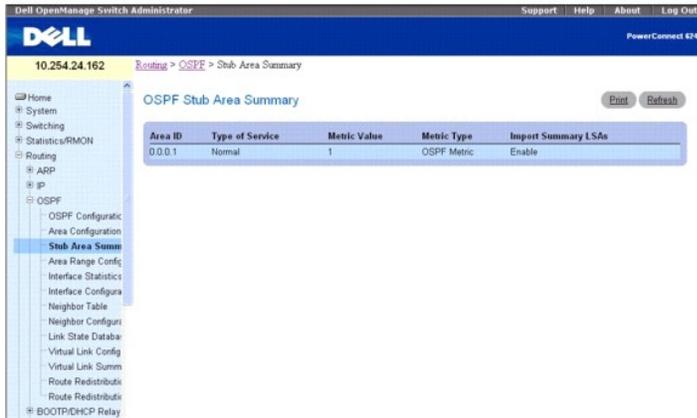
1. OSPF Commands (Commandes OSPF)

Récapitulatif de la zone de stub

La page **OSPF Stub Area Summary** (Récapitulatif de la zone de stub OSPF) permet d'afficher les détails d'une zone de stub OSPF.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Stub Area Summary** (Récapitulatif de la zone de stub) dans l'arborescence.

Figure 10-8. Page OSPF Stub Area Summary (Récapitulatif de la zone de stub OSPF)



La page **OSPF Stub Area Summary** (Récapitulatif de la zone de stub OSPF) contient les champs suivants :

Area ID (ID de zone) : ID de zone de la zone de stub.

Type of Service (Type de service) : type de service associé à la métrique du stub. Le commutateur n'accepte que la valeur Normal.

Metric Value (Valeur de métrique) : affiche la valeur de métrique configurée.

Metric Type (Type de métrique) : type de métrique associé à la zone de stub. Les types admis sont :

- 1 **OSPF Metric** (Métrique OSPF) : métrique OSPF normale
- 1 **Comparable Cost** (Coût comparable) : métriques de type externe 1 comparables à la métrique OSPF
- 1 **Non-comparable Cost** (Coût non comparable) : métriques de type externe 2 qui sont supposées être supérieures au coût de la métrique OSPF

Import Summary LSAs (Importer les LSA récapitulatives) : indique si l'importation des LSA récapitulatives est activée ou désactivée.

Affichage d'une zone de stub OSPF à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 OSPF Commands (Commandes OSPF)

Configuration de la plage de zones

La page **OSPF Area Range Configuration** (Configuration de la plage de zones OSPF) permet de configurer et d'afficher une plage de zones pour le NSSA spécifié.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Area Range Configuration** (Configuration de la plage de zones) dans l'arborescence.

Figure 10-9. Page OSPF Area Range Configuration (Configuration de la plage de zones)



La page **OSPF Area Range Configuration** (Configuration de la plage de zones OSPF) contient les champs suivants :

Area ID (ID de zone) : sélectionnez la zone dont vous voulez configurer les données dans le menu déroulant.

IP Address (Adresse IP) : entrez l'adresse IP de la plage d'adresses pour la zone sélectionnée.

Subnet Mask (Masque de sous-réseau) : entrez le masque de sous-réseau de la plage d'adresses pour la zone sélectionnée.

LSDB Type (Type de LSDB) : sélectionnez le type d'annonce de liaison associé à la zone et à la plage d'adresses spécifiées. Le type par défaut est "Network Summary" (Récapitulatif du réseau).

Advertisement (Annonce) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Si vous sélectionnez Enable (Activer), la plage d'adresses est annoncée en dehors de la zone via une LSA de type "Network Summary" (Récapitulatif du réseau). La valeur par défaut est Enable (Activer).

Add (Ajouter) : cochez la case Add (Ajouter) pour ajouter une plage de zones.

OSPF Area Range Table (Table de plages de zones OSPF)

Area ID (ID de zone) : affiche la zone OSPF.

IP Address (Adresse IP) : affiche l'adresse IP d'une plage d'adresses pour la zone.

Subnet Mask (Masque de sous-réseau) : affiche le masque de sous-réseau d'une plage d'adresses pour la zone.

LSDB Type (Type de LSDB) : affiche le type d'annonce de liaison associée à la plage d'adresses et à la zone.

Advertisement (Annonce) : affiche le mode d'annonce associé à la plage d'adresses et à la zone.

Remove (Supprimer) : supprime l'entrée de zone spécifiée.

Définition d'une plage de zones OSPF

1. Affichez la page **OSPF Area Range Configuration** (Configuration de la plage de zones OSPF).
2. Renseignez les champs **Area ID** (ID de zone), **IP Address** (Adresse IP), **Subnet Mask** (Masque de sous-réseau), **LSDB Type** (Type de LSDB) et **Advertisement** (Annonce).
3. Activez la case à cocher **Add** (Ajouter).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La plage de zones OSPF est définie et configurée. Toutes les plages de zones OSPF configurées s'affichent dans la table de la page **OSPF Area Range Configuration** (Configuration de la plage de zones OSPF).

Suppression de la configuration d'une plage de zones OSPF

1. Affichez la page **OSPF Area Range Configuration** (Configuration de la plage de zones OSPF).
2. Activez la case à cocher **Remove** (Supprimer) dans la ligne associée à **Area ID to be deleted** (ID de zone à supprimer).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La plage d'adresses est supprimée de la configuration de la zone.

Commande CLI de configuration de la plage de zones OSPF

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 OSPF Commands (Commandes OSPF)

Statistiques sur les interfaces

La page **OSPF Interface Statistics** (Statistiques sur les interfaces OSPF) permet d'afficher les statistiques de l'interface sélectionnée. Les informations ne s'affichent que si l'interface OSPF est activée.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Interface Statistics** (Statistiques sur les interfaces) dans l'arborescence.

Figure 10-10. Page OSPF Interface Statistics (Statistiques sur les interfaces OSPF)



La page **OSPF Interface Statistics** (Statistiques sur les interfaces OSPF) contient les champs suivants :

Interface : sélectionnez l'interface dont vous voulez afficher les données dans le menu déroulant.

OSPF Area ID (ID de zone OSPF) : zone OSPF à laquelle appartient l'interface du routeur sélectionnée. Cette valeur doit être un nombre entier de 32 bits à points décimaux qui identifie de manière unique la zone à laquelle l'interface est connectée.

Area Border Router Count (Nombre de routeurs de limite de zone) : nombre total de routeurs de limite de zone accessibles dans cette zone. La valeur initiale est égale à zéro, et est calculée pour chaque passage SPF.

AS Border Router Count (Nombre de routeurs de limites de systèmes autonomes) : nombre total de routeurs de limites de systèmes autonomes accessibles dans cette zone. La valeur initiale est égale à zéro, et est calculée pour chaque passage SPF.

Area LSA Count (Nombre de LSA dans la zone) : nombre total de LSA (Link State Advertisements) contenues dans la base de données LSDB (Link State Database) de cette zone, en excluant les LSA externes au système autonome.

IP Address (Adresse IP) : adresse IP de l'interface.

Interface Events (Événements de l'interface) : nombre de changements d'état ou d'erreurs enregistrés sur l'interface OSPF spécifiée.

Virtual Events (Événements virtuels) : nombre de changements d'état ou d'erreurs enregistrés sur cette liaison virtuelle.

Neighbor Events (Événements liés au voisin) : nombre de changements d'état ou d'erreurs enregistrés sur la relation de ce voisin.

External LSA Count (Nombre de LSA externes) : nombre de LSA (Link State Advertisements) externes (LS de type 5) contenues dans la base de données LSDB (Link State Database).

Affichage des statistiques sur les interfaces OSPF

1. Affichez la page **OSPF Interface Statistics** (Statistiques sur les interfaces OSPF).
2. Sélectionnez l'interface dont vous voulez afficher les données dans le menu déroulant.

Les statistiques de l'interface s'affichent.

Affichage des statistiques sur les interfaces OSPF à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

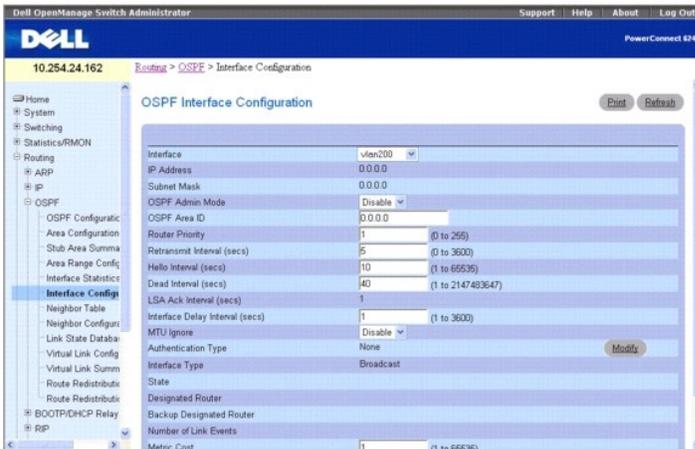
- 1 OSPF Commands (Commandes OSPF)

Configuration des interfaces

La page **OSPF Interface Configuration** (Configuration des interfaces OSPF) permet de configurer une interface OSPF.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Interface Configuration** (Configuration des interfaces) dans l'arborescence.

Figure 10-11. Page OSPF Interface Configuration (Configuration des interfaces OSPF)



La page **OSPF Interface Configuration** (Configuration des interfaces OSPF) contient les champs suivants :

Interface : sélectionnez l'interface dont vous voulez afficher ou configurer les données dans le menu déroulant.

IP Address (Adresse IP) : affiche l'adresse de l'interface VLAN.

Subnet Mask (Masque de sous-réseau) : affiche le masque de sous-réseau de l'interface VLAN.

OSPF Admin Mode (Mode admin OSPF) : vous pouvez sélectionner **Enable** (Activer) ou **Disable** (Désactiver) dans le menu déroulant. La valeur par défaut est **Disabled** (Désactivé). Vous pouvez configurer les paramètres OSPF sans activer ce mode, mais ils ne prennent effet qu'une fois ce mode activé. Les champs ci-après ne s'affichent que si l'option **Admin Mode** (Mode admin) est activée : **State** (État), **Designated Router** (Routeur désigné), **Backup Designated Router** (Routeur de sauvegarde désigné), **Number of Link Events** (Nombre d'événements de liaison), **LSA Ack Interval** (Intervalle d'accusé réception des LSA) et **Metric Cost** (Coût de métrique). Pour que l'interface OSPF soit pleinement opérationnelle, vous devez entrer une adresse IP et un masque de sous-réseau corrects dans la page **IP Interface Configuration** (Configuration de l'interface IP).

REMARQUE : Une fois l'interface OSPF activée sur le routeur, elle reste active tant que le routeur n'est pas réinitialisé.

OSPF Area ID (ID de la zone OSPF) : entrez un nombre entier de 32 bits à points décimaux qui identifie de manière unique la zone OSPF à laquelle l'interface de routeur sélectionnée est connectée. Si vous attribuez un ID de zone qui n'existe pas, la zone est créée à l'aide des valeurs par défaut.

Router Priority (Priorité du routeur) : entrez la priorité OSPF pour l'interface sélectionnée. Cette valeur doit être un nombre entier compris entre 0 et 255. La valeur par défaut est 1, qui désigne la priorité la plus élevée. La valeur 0 indique que le routeur ne peut pas être défini comme routeur désigné sur ce réseau.

Retransmit Interval (secs) (Intervalle de retransmission [secondes]) : entrez l'intervalle de retransmission OSPF pour l'interface spécifiée. Il désigne le nombre de secondes entre les LSA (Link State Advertisements) pour les contiguités appartenant à cette interface de routeur. Cette valeur est également utilisée lors de la retransmission des descriptions de base de données et des paquets LSR (Link State Request). La plage de valeurs admises est comprise entre 0 et 3600 secondes (1 heure). La valeur par défaut est de 5 secondes.

Hello Interval (secs) (Intervalle Hello [secondes]) : entrez l'intervalle Hello OSPF (en secondes) pour l'interface spécifiée. Ce paramètre doit être identique pour tous les routeurs connectés à un réseau. La plage de valeurs admises est comprise entre 1 et 65 535. La valeur par défaut est de 10 secondes.

Dead Interval (secs) (Intervalle d'inactivité [secondes]) : entrez l'intervalle d'inactivité OSPF en secondes pour l'interface spécifiée. Il désigne la durée pendant laquelle un routeur attend de recevoir des paquets Hello d'un routeur voisin avant de déclarer que ce routeur est indisponible. Ce paramètre doit être identique pour tous les routeurs connectés à un réseau. Cette valeur doit être un multiple de l'intervalle Hello (par exemple 4). La plage de valeurs admises est comprise entre 1 et 2147483647. La valeur par défaut est de 40 secondes.

LSA Ack Interval (Intervalle d'accusé réception des LSA) : nombre de secondes entre les transmissions de paquets d'accusé réception des LSA. Cette valeur doit être inférieure à l'intervalle de retransmission.

Interface Delay Interval (secs) (Intervalle de transition de l'interface [secondes]) : entrez le délai de transition OSPF pour l'interface spécifiée. Il désigne le nombre estimé de secondes pour transmettre un paquet LSU (Link State Update) sur l'interface sélectionnée. La plage de valeurs admises est comprise entre 1 et 3600 secondes (1 heure). La valeur par défaut est de 1 seconde.

MTU Ignore (Ne pas prendre en compte MTU) : désactive la détection de MTU OSPF incompatibles lors de la réception des paquets. La valeur par défaut est **Disabled** (Désactivé).

Authentication Type (Type d'authentification) : vous pouvez sélectionner un type d'authentification autre que None (Aucun) en cliquant sur le bouton **Modify** (Modifier). Une nouvelle page Web apparaît, dans laquelle vous pouvez sélectionner un type d'authentification dans le menu déroulant. Ce champ peut prendre les valeurs suivantes :

- 1 **None** (Aucun) : état initial de l'interface. Si vous sélectionnez cette option dans le menu déroulant du deuxième écran et cliquez sur **Apply Changes** (Appliquer les modifications), vous êtes renvoyé au premier écran et aucun protocole d'authentification n'est exécuté.
- 1 **Simple** : si vous sélectionnez cette option, vous êtes invité à entrer une clé d'authentification. Cette clé figure dans l'en-tête OSPF de tous les paquets envoyés sur le réseau. Tous les routeurs contenus sur le réseau doivent être configurés avec la même clé.
- 1 **Encrypt** (Crypter) : si vous sélectionnez cette option, vous êtes invité à entrer une clé d'authentification et un ID d'authentification. Le cryptage utilise l'algorithme Message-Digest MD5. Tous les routeurs contenus sur le réseau doivent être configurés avec la même clé et le même ID.

Interface Type (Type d'interface) : type d'interface OSPF, qui a toujours la valeur Broadcast (Diffusion).

State (État) : état actuel de l'interface de routeur sélectionnée. Ce champ peut prendre les valeurs suivantes :

- 1 **Down** (Inactif) : état initial de l'interface. Cet état indique que les protocoles de niveau inférieur ont signalé que l'interface est hors d'usage. Les paramètres de l'interface sont réinitialisés à leurs valeurs initiales. Toutes les horloges de l'interface sont désactivées, et aucune contiguïté n'est associée à l'interface.
- 1 **Loopback** (Boucle de rappel) : cet état indique que l'interface du routeur a effectué une boucle de rappel dans le matériel ou le logiciel. L'interface n'est pas disponible pour le transfert de données normal. Toutefois, il est toujours possible d'obtenir des informations sur la qualité de cette interface, en envoyant des commandes Ping ICMP à l'interface ou en exécutant un test d'erreurs de bits. Ainsi, il est toujours possible d'adresser des paquets IP à une interface en boucle de rappel. Pour ce faire, ces interfaces sont annoncées dans les LSA associées au routeur en tant qu'itinéraires hôtes uniques, dont la destination est l'adresse de l'interface IP.
- 1 **Waiting** (En attente) : le routeur tente de déterminer l'identité du routeur désigné (Sauvegarde) pour le réseau en contrôlant les paquets Hello reçus. Il n'est pas autorisé à sélectionner un routeur de sauvegarde désigné ou un routeur désigné tant que cet état est activé. Cela évite des modifications inutiles au routeur désigné (Sauvegarde).
- 1 **Designated Router** (Routeur désigné) : ce routeur est lui-même le routeur désigné sur le réseau connecté. Les contiguïtés sont créées pour tous les autres routeurs connectés au réseau. Le routeur doit également créer une LSA associée au nœud du réseau. Cette LSA contient les liens vers tous les routeurs (y compris le routeur désigné proprement dit) connectés au réseau.
- 1 **Backup Designated Router** (Routeur de sauvegarde désigné) : ce routeur est lui-même le routeur de sauvegarde désigné sur le réseau connecté. Il devient le routeur désigné en cas de défaillance du routeur désigné existant. Le routeur crée les contiguïtés pour tous les autres routeurs connectés au réseau. Le routeur de sauvegarde désigné exécute des fonctions légèrement différentes durant la procédure d'acheminement, par rapport au routeur désigné.
- 1 **Other Designated Router** (Autre routeur désigné) : l'interface est connectée à un réseau de diffusion ou NBMA sur lequel d'autres routeurs ont été choisis comme routeur désigné et routeur de sauvegarde désigné. Le routeur tente de créer des contiguïtés pour le routeur désigné et le routeur de sauvegarde désigné.

Le champ State (État) ne s'affiche que si l'option OSPF Admin Mode (Mode admin OSPF) est activée.

Designated Router (Routeur désigné) : identité du routeur désigné pour ce réseau, du point de vue du routeur d'annonce. Il est identifié ici par son ID de routeur. La valeur 0.0.0.0 indique qu'il n'existe aucun routeur désigné. Ce champ ne s'affiche que si l'option OSPF Admin Mode (Mode admin OSPF) est activée.

Backup Designated Router (Routeur de sauvegarde désigné) : identité du routeur désigné de sauvegarde pour ce réseau, du point de vue du routeur d'annonce. Il est identifié ici par son ID de routeur. La valeur 0.0.0.0 indique qu'il n'existe aucun routeur désigné de sauvegarde. Ce champ ne s'affiche que si l'option OSPF Admin Mode (Mode admin OSPF) est activée.

Number of Link Events (Nombre d'événements de liaison) : nombre de modifications d'état enregistrées sur l'interface OSPF spécifiée. Ce champ ne s'affiche que si l'option OSPF Admin Mode (Mode admin OSPF) est activée.

Metric Cost (Coût de métrique) : entrez la valeur du coût TOS (Type Of Service) sur cette interface. La plage de valeurs est comprise entre 1 et 65 535. Ce champ n'est configurable et ne s'affiche que si le protocole OSPF est initialisé sur l'interface.

Paramétrage de la configuration d'une interface OSPF

1. Affichez la page **OSPF Interface Configuration** (Configuration des interfaces OSPF).
2. Indiquez une interface à configurer.
3. Renseignez les autres champs si nécessaire.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'interface OSPF est configurée.

Affichage de la configuration d'une interface OSPF

1. Affichez la page **OSPF Interface Configuration** (Configuration des interfaces OSPF).
2. Sélectionnez l'interface VLAN dont vous voulez afficher les données dans le menu déroulant.

Les données de configuration de cette interface s'affichent.

Configuration d'une interface OSPF à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 OSPF Commands (Commandes OSPF)

Table des voisins

La page **OSPF Neighbor Table** (Table des voisins OSPF) permet d'afficher la liste des tables de routeurs voisins OSPF. Lorsqu'un ID de voisin spécifique est indiqué, des informations détaillées sur un voisin s'affichent. Les informations ci-dessous ne s'affichent que si l'interface OSPF est activée.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Neighbor Table** (Table des voisins) dans l'arborescence.

Figure 10-12. OSPF Neighbor Table (Table des routeurs OSPF voisins)



La page **OSPF Neighbor Table** (Table des voisins OSPF) contient les champs suivants :

Interface : sélectionnez l'interface dont vous voulez afficher les données dans le menu déroulant.

Router ID (ID du routeur) : nombre entier de 32 bits à points décimaux représentant l'interface du routeur voisin.

IP Address (Adresse IP) : adresse IP de l'interface du routeur voisin sur le réseau connecté. Elle est utilisée comme adresse IP de destination lorsque les paquets de protocole sont envoyés sous forme de paquets de monodiffusion sur cette contiguïté. Elle est également utilisée dans les LSA de routeur en tant qu'ID de liaison du réseau connecté si le routeur voisin est choisi comme routeur désigné. L'adresse IP du routeur voisin est apprise lorsque des paquets Hello sont transmis par le routeur voisin. Pour les liaisons virtuelles, cette adresse est apprise durant la procédure de création de la table de routage.

Neighbor Interface Index (Index de l'interface du routeur voisin) : interface identifiant l'index de l'interface du routeur voisin.

Affichage de la table des voisins OSPF à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 OSPF Commands (Commandes OSPF)

Configuration du routeur voisin

La page **OSPF Neighbor Configuration** (Configuration du routeur voisin OSPF) permet d'afficher la configuration du routeur voisin OSPF associée à un ID de routeur voisin sélectionné. Lorsqu'un ID de routeur voisin spécifique est saisi, des informations détaillées sur ce routeur voisin s'affichent. Les informations ci-dessous ne s'affichent que si le protocole OSPF est activé et que l'interface possède un routeur voisin. L'adresse IP est celle du voisin.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Neighbor Configuration** (Configuration du routeur voisin) dans l'arborescence.

Figure 10-13. Page OSPF Neighbor Configuration (Configuration du routeur OSPF voisin)



Cette page contient les champs suivants :

Interface : utilisez le menu déroulant pour sélectionner l'interface VLAN sur laquelle le routage est activé.

Neighbor IP Address (Adresse IP du routeur voisin) : sélectionnez l'adresse IP du routeur voisin dont vous voulez afficher les données.

Router ID (ID de routeur) : nombre entier de 32 bits à points décimaux qui identifie le routeur voisin.

Options : capacités OSPF facultatives prises en charge par le voisin. Le champ OSPF Options (Options OSPF) est disponible dans les paquets Hello, les paquets DBD (Database Description) et toutes les LSA (Link State Advertisements). Le champ Options active les routeurs OSPF pour prendre en charge ou non les capacités facultatives, et pour communiquer leur fonction aux autres routeurs. Grâce à ce mécanisme, des routeurs présentant des capacités différentes peuvent être associés dans un domaine de routage OSPF. La valeur Options est un bitmap qui désigne la capacité du routeur voisin.

Router Priority (Priorité du routeur) : affiche la priorité OSPF pour le voisin spécifié. Cette valeur doit être un nombre entier compris entre 0 et 255. La valeur 0 indique que le routeur ne peut pas être défini comme routeur désigné sur ce réseau.

State (État) : un voisin peut avoir l'un des états suivants :

- 1 **Down** (Inactif) : état initial des communications d'un voisin. Cet état indique qu'aucune information n'a été transmise par le routeur voisin. Sur les réseaux NBMA, il est toujours possible d'envoyer des paquets Hello aux voisins indisponibles, mais leur fréquence est limitée.
- 1 **Attempt** (Tentative) : cet état ne s'applique qu'aux voisins connectés aux réseaux NBMA. Il indique qu'aucune information récente n'a été transmise par le voisin, mais que des efforts plus concertés doivent être déployés pour le contacter. Pour ce faire, des paquets Hello doivent lui être envoyés à des intervalles Hello.
- 1 **Init** : cet état indique qu'un paquet Hello a été récemment transmis par le voisin. Toutefois, une communication bidirectionnelle n'a pas encore été établie avec le voisin (le routeur proprement dit n'apparaît pas dans le paquet Hello du voisin). Tous les voisins présentant cet état (ou un état supérieur) sont répertoriés dans les paquets Hello envoyés à partir de l'interface associée.
- 1 **2-Way** (Bidirectionnel) : cet état indique que la communication entre les deux routeurs est bidirectionnelle. Elle est assurée par le fonctionnement du protocole Hello. Cet état est le plus avancé, juste avant le début de la création d'une contiguïté. Le routeur désigné (sauvegarde) est sélectionné parmi l'ensemble des voisins présentant un état bidirectionnel ou supérieur.
- 1 **Exchange Start** (Démarrage de l'échange) : première étape dans la création d'une contiguïté entre les deux routeurs voisins. Elle a pour but de déterminer le routeur maître et de définir le numéro de séquence DD initial. Dans cet état ou un état supérieur, les communications des voisins sont appelées des contiguïtés.
- 1 **Exchange** (Échange) : dans cet état, le routeur décrit l'intégralité de sa base de données LSDB (Link State Database) en envoyant des paquets DBD (Database Description) au voisin. Des paquets LSU (Link State Request) peuvent également être envoyés pour demander les LSA plus récentes du voisin. Dans cet état ou un état supérieur, toutes les contiguïtés sont utilisées par la procédure d'acheminement. Elles sont pleinement capables de transmettre et de recevoir tous les types de paquets de protocole de routage OSPF.
- 1 **Loading** (En cours de chargement) : cet état indique que des paquets LSU (Link State Request) sont envoyés au voisin pour demander les LSA plus récentes détectées (mais pas encore reçues) dont l'état est Exchange (Échange).
- 1 **Full** (Complet) : cet état indique que les routeurs voisins sont totalement contigus. Ces contiguïtés apparaissent dans les LSA de routeur et de réseau.

Events (Événements) : nombre de changements d'état ou d'erreurs enregistrés sur la relation de ce voisin.

Permanence : cette variable affiche l'état de l'entrée. Les options Dynamic (Dynamique) et Permanent font référence à la manière dont le routeur voisin s'est fait connaître.

Hellos Suppressed (Paquets Hello supprimés) : indique si des paquets Hello sont supprimés pour le routeur voisin.

Retransmission Queue Length (Longueur de la file d'attente de retransmission) : longueur actuelle de la file d'attente de retransmission.

Affichage de la configuration d'un routeur voisin OSPF

1. Affichez la page **OSPF Neighbor Configuration** (Configuration des voisins OSPF).
2. Sélectionnez l'interface et l'adresse IP à afficher.

La configuration du routeur voisin s'affiche.

Affichage de la configuration d'un routeur voisin OSPF à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 OSPF Commands (Commandes OSPF)

Base de données LSDB

La page **OSPF Link State Database** (Base de données LSDB OSPF) permet d'afficher les informations sur l'état des liaisons OSPF.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Link State Database** (Base de données LSDB) dans l'arborescence.

Figure 10-14. OSPF Link State Database (Base de données LSDB OSPF)

Router ID	Area ID	LSA Type	LS ID	Age	Sequence	Checksum	Options
1.1.1.1	0.0.0.0	Router Links	1.1.1.1	336	-2147483641	0x8958	E --
2.2.2.2	0.0.0.0	Router Links	2.2.2.2	340	-2147483640	0xac41	E --
2.2.2.2	0.0.0.0	Network Links	13.1.1.2	460	-2147483647	0x64e	E --
1.1.1.1	0.0.0.0	Network Summary	17.1.1.0	355	-2147483646	0xa80	E --
2.2.2.2	0.0.0.0	Network Summary	17.1.1.0	351	-2147483646	0x426	E --
2.2.2.2	0.0.0.0	Summary ASBR	1.1.1.1	351	-2147483647	0xf652	E --
1.1.1.1	0.0.0.1	Router Links	1.1.1.1	340	-2147483644	0xb25c	E --
2.2.2.2	0.0.0.1	Router Links	2.2.2.2	341	-2147483643	0xc946	E --
2.2.2.2	0.0.0.1	Network Links	17.1.1.2	366	-2147483647	0xb27e	E --
1.1.1.1	0.0.0.1	Network Summary	13.1.1.0	365	-2147483646	0xae50	E --
2.2.2.2	0.0.0.1	Network Summary	13.1.1.0	445	-2147483645	0x74ce	E --

La page **OSPF Link State Database** (Base de données LSDB OSPF) contient les champs suivants :

Router ID (ID du routeur) : nombre entier de 32 bits à points décimaux qui identifie de manière unique le routeur dans le système autonome. Cette valeur est définie sur la page IP Configuration (Configuration IP). Pour modifier l'ID du routeur, vous devez d'abord désactiver l'interface OSPF. Une fois que vous avez défini le nouvel ID du routeur, vous devez réactiver l'interface OSPF pour que les modifications prennent effet. La valeur par défaut est 0.0.0.0, qui n'est pas un ID de routeur correct.

Area ID (ID de zone) : ID d'une zone OSPF à laquelle l'une des interfaces du routeur est connectée. Cette valeur doit être un nombre entier de 32 bits à points décimaux qui identifie de manière unique la zone à laquelle une interface est connectée.

LSA Type (Type de LSA) : format et fonction de la LSA (Link State Advertisement). Ce champ peut prendre les valeurs suivantes :

- 1 Router Links (Liaisons de routeur)
- 1 Network Links (Liaisons réseau)
- 1 Network Summary (Récapitulatif du réseau)
- 1 ASBR Summary (Récapitulatif ASBR)
- 1 AS-external (Externes au système autonome)

LS ID (ID LS) : ce champ identifie la partie du domaine de routage décrit par l'annonce. Sa valeur dépend du type LS de l'annonce.

Age (Âge) : temps écoulé (en secondes) depuis la première création de la LSA.

Sequence (Séquence) : ce numéro de séquence doit être un nombre entier signé de 32 bits. Il permet de détecter des LSA anciennes et en double. Plus le numéro de séquence est grand, plus l'annonce est récente.

Checksum (Somme de contrôle) : somme de contrôle utilisée pour détecter une altération des données dans une annonce. Cette altération peut se produire durant l'acheminement d'une annonce ou durant sa conservation dans la mémoire d'un routeur. Ce champ définit la somme de contrôle du contenu intégral de l'annonce, à l'exception du champ LS Age (Durée LS).

Options : le champ Options de l'en-tête LSA indique les capacités facultatives associées à l'annonce. Ce champ peut prendre les valeurs suivantes :

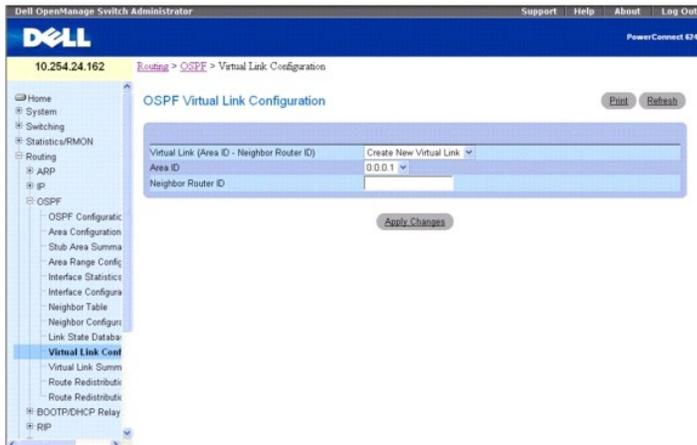
- 1 **Q** — Active la prise en charge de QoS Traffic Engineering (ingénierie du trafic QoS).
- 1 **E** — Décrit le mode d'acheminement des LSA externes au système autonome.
- 1 **MC** — Décrit le mode de transfert des datagrammes de multidiffusion IP conformément aux spécifications standard.
- 1 **O** — Indique si les LSA de type opaque sont prises en charge.
- 1 **V** — Indique si les extensions OSPF++ pour VPN/COS sont prises en charge.

Configuration des liaisons virtuelles

La page **Virtual Link Configuration** (Configuration des liaisons virtuelles OSPF) permet de créer ou de configurer les informations sur l'interface virtuelle associées à une zone et à un routeur voisin spécifiques. Une zone OSPF valide doit être configurée pour que cette page puisse s'afficher.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Virtual Link Configuration** (Configuration de liaisons virtuelles) dans l'arborescence.

Figure 10-15. Création d'une configuration de liaisons virtuelles OSPF



Les pages de configuration des liaisons virtuelles OSPF contiennent les champs suivants :

Virtual Link (Area ID - Neighbor Router ID) (Liaison virtuelle [ID de zone - ID du routeur voisin]) : sélectionnez la liaison virtuelle dont vous voulez afficher ou configurer les données. Elle comprend l'ID de zone et l'ID du routeur voisin. Pour créer une nouvelle liaison virtuelle, sélectionnez **Create New Virtual Link** (Créer une nouvelle liaison virtuelle) dans le menu déroulant. Lorsque l'option **Create New Virtual Link** (Créer une nouvelle liaison virtuelle) est sélectionnée, les champs suivants s'affichent :

Area ID (ID de zone) : cette valeur doit être un nombre entier de 32 bits à points décimaux qui identifie de manière unique la zone à laquelle une interface de routeur est connectée.

Neighbor Router ID (ID du routeur voisin) : nombre entier de 32 bits à points décimaux qui identifie de manière unique le routeur voisin faisant partie de la liaison virtuelle.

Hello Interval (Intervalle Hello) : entrez l'intervalle Hello OSPF en secondes pour l'interface spécifiée. Ce paramètre doit être identique pour tous les routeurs connectés à un réseau. La plage de valeurs admises est comprise entre 1 et 65 535. La valeur par défaut est de 10 secondes.

Dead Interval (Intervalle d'inactivité) : entrez l'intervalle d'inactivité OSPF en secondes pour l'interface spécifiée. Il désigne la durée pendant laquelle un routeur attend de recevoir des paquets Hello d'un routeur voisin avant de déclarer que ce routeur est indisponible. Ce paramètre doit être identique pour tous les routeurs connectés à un réseau. Cette valeur doit être un multiple de l'intervalle Hello (par exemple 4). La plage de valeurs admises est comprise entre 1 et 65535. La valeur par défaut est de 40 secondes.

Interface Delay Interval (secs) (Intervalle de transition de l'interface [secondes]) : délai de transition OSPF (en secondes) pour la liaison virtuelle. Il désigne le nombre estimé de secondes pour transmettre un paquet LSU (Link State Update) sur cette interface.

State (État) : état actuel de la liaison virtuelle sélectionnée. Celle-ci peut avoir l'un des états suivants :

- 1 **Down** (Inactif) : état initial de l'interface. Cet état indique que les protocoles de niveau inférieur ont signalé que l'interface est hors d'usage. Les paramètres de l'interface sont réinitialisés à leurs valeurs initiales. Toutes les horloges de l'interface sont désactivées, et aucune contiguïté n'est associée à l'interface.
- 1 **Waiting** (En attente) : le routeur tente de déterminer l'identité du routeur désigné (Sauvegarde) en contrôlant les paquets Hello reçus. Il n'est pas autorisé à sélectionner un routeur de sauvegarde désigné ou un routeur désigné tant que cet état est activé. Cela évite des modifications inutiles au routeur désigné (Sauvegarde).
- 1 **Point-to-Point** (Point à point) : l'interface est opérationnelle et connectée à la liaison virtuelle. Lorsque cet état est activé, le routeur tente de créer une contiguïté avec le routeur voisin. Les paquets Hello sont envoyés au voisin toutes les secondes de l'intervalle Hello.
- 1 **Designated Router** (Routeur désigné) : ce routeur est lui-même le routeur désigné sur le réseau connecté. Les contiguïtés sont créées pour tous les autres routeurs connectés au réseau. Le routeur doit également créer une LSA associée au nœud du réseau. Cette LSA contient les liens vers tous les routeurs (y compris le routeur désigné proprement dit) connectés au réseau.
- 1 **Backup Designated Router** (Routeur de sauvegarde désigné) : ce routeur est lui-même le routeur de sauvegarde désigné sur le réseau connecté. Il devient le routeur désigné en cas de défaillance du routeur désigné existant. Le routeur crée les contiguïtés pour tous les autres routeurs connectés au réseau. Le routeur de sauvegarde désigné exécute des fonctions légèrement différentes durant la procédure d'acheminement, par rapport au routeur désigné.
- 1 **Other Designated Router** (Autre routeur désigné) : l'interface est connectée à un réseau de diffusion ou NBMA sur lequel d'autres routeurs ont été choisis comme routeur désigné et routeur de sauvegarde désigné. Le routeur tente de créer des contiguïtés pour le routeur désigné et le routeur de sauvegarde désigné.

Neighbor State (État du voisinage) : état de la relation voisine virtuelle.

Retransmit Interval (Intervalle de retransmission) : entrez l'intervalle de retransmission OSPF pour l'interface spécifiée. Il désigne le nombre de secondes entre les LSA (Link State Advertisements) pour les contiguïtés appartenant à cette interface de routeur. Cette valeur est également utilisée lors de la retransmission des descriptions de base de données et des paquets LSR (Link State Request). La plage de valeurs admises est comprise entre

0 et 3600 secondes (1 heure). La valeur par défaut est de 5 secondes.

Authentication Type (Type d'authentification) : vous pouvez sélectionner un type d'authentification autre que None (Aucun) en cliquant sur le bouton Configure Authentication (Configurer l'authentification). Un nouvel écran apparaît, dans lequel vous pouvez sélectionner un type d'authentification dans le menu déroulant. Les choix possibles sont les suivants :

- 1 **None** (Aucun) : état initial de l'interface. Si vous sélectionnez cette option dans le menu déroulant du deuxième écran et cliquez sur **Apply Changes** (Appliquer les modifications), vous êtes renvoyé au premier écran.
- 1 **Simple** : si vous sélectionnez cette option, vous êtes invité à entrer une clé d'authentification. Cette clé figure dans l'en-tête OSPF de tous les paquets envoyés sur le réseau. Tous les routeurs contenus sur le réseau doivent être configurés avec la même clé.
- 1 **Encrypt** (Crypter) : si vous sélectionnez cette option, vous êtes invité à entrer une clé d'authentification et un ID d'authentification. Le cryptage utilise l'algorithme Message-Digest MD5. Tous les routeurs contenus sur le réseau doivent être configurés avec la même clé et le même ID.

Authentication Key (Clé d'authentification) : entrez la clé d'authentification OSPF pour l'interface spécifiée. Si vous ne sélectionnez aucun type d'authentification, vous ne serez pas invité à entrer une clé. Si vous sélectionnez Simple, la taille de la clé ne doit pas dépasser 8 caractères. Si vous sélectionnez Encrypt (Crypter), la taille de la clé peut atteindre 16 caractères. La valeur de la clé ne s'affiche que si vous possédez des droits d'accès en lecture/écriture. Sinon, elle apparaît sous forme d'astérisques.

Authentication ID (ID d'authentification) : entrez l'ID à utiliser pour l'authentification. Vous êtes invité à entrer un ID uniquement si vous sélectionnez Encrypt (Crypter) comme type d'authentification. L'ID doit être un nombre compris entre 0 et 255 inclus.

Définition d'une nouvelle liaison virtuelle

1. Affichez la page **OSPF Virtual Link Configuration** (Configuration des liaisons virtuelles OSPF).
2. Sélectionnez **Create New Virtual Link** (Créer une liaison virtuelle) dans le menu déroulant **Virtual Link (Area ID - Neighbor Router ID)** (Liaison virtuelle [ID de zone - ID du routeur voisin]).
3. Indiquez l'ID du routeur voisin associé à la nouvelle liaison virtuelle.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les autres champs s'affichent lorsque la liaison virtuelle est créée.

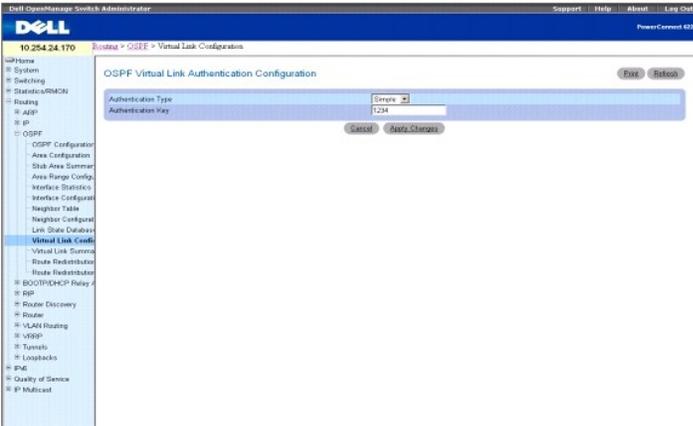
Figure 10-16. Page OSPF Virtual Link Configuration (Configuration des liaisons virtuelles OSPF)



5. Cliquez sur **Configure Authentication** (Configurer l'authentification) pour modifier l'authentification.

La page suivante s'affiche :

Figure 10-17. Page OSPF Virtual Link Authentication Configuration (Configuration de l'authentification pour une liaison virtuelle OSPF)



6. Renseignez les champs **Authentication Type** (Type d'authentification) et **Authentication Key** (Clé d'authentification).
7. Cliquez sur **Apply Changes** (Appliquer les modifications) lorsque vous avez terminé.

Configuration des données d'une liaison virtuelle

1. Affichez la page **OSPF Virtual Link Configuration** (Configuration des liaisons virtuelles OSPF).
2. Indiquez l'ID de zone et l'ID du routeur voisin à configurer.
3. Renseignez les champs si nécessaire.
4. Cliquez sur **Configure Authentication** (Configurer l'authentification) pour modifier l'authentification.
5. Cliquez sur **Apply Changes** (Appliquer les modifications) lorsque vous avez terminé.

Les données de la liaison virtuelle associées aux ID spécifiés sont configurées et le périphérique est mis à jour.

Affichage des données d'une liaison virtuelle

1. Affichez la page **OSPF Virtual Link Configuration** (Configuration des liaisons virtuelles OSPF).
2. Indiquez l'ID de zone et l'ID du routeur voisin à afficher.

Les données de la liaison virtuelle associées à ces ID s'affichent.

Suppression d'une liaison virtuelle

1. Affichez la page **OSPF Virtual Link Configuration** (Configuration des liaisons virtuelles OSPF).
2. Indiquez l'ID de zone et l'ID du routeur voisin associés à la liaison virtuelle à supprimer.

Les données de la liaison virtuelle s'affichent.

3. Cliquez sur **Delete** (Supprimer).

La liaison virtuelle est supprimée et le périphérique est mis à jour.

Configuration des données d'une liaison virtuelle à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

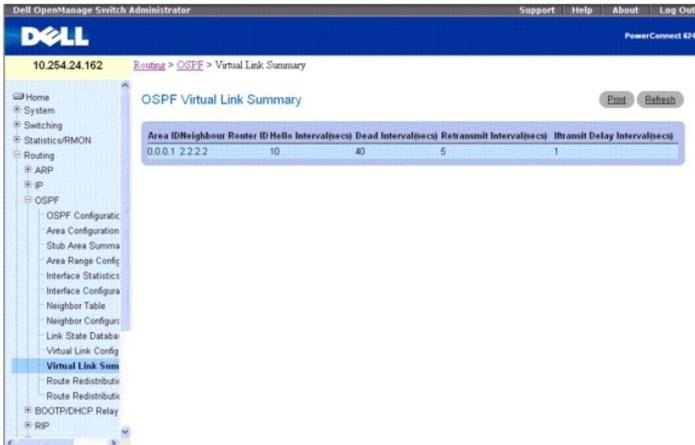
1. OSPF Commands (Commandes OSPF)

Récapitulatif des liaisons virtuelles

La page **OSPF Virtual Link Summary** (Récapitulatif des liaisons virtuelles OSPF) permet d'afficher toutes les liaisons virtuelles configurées.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Virtual Link Summary** (Récapitulatif des liaisons virtuelles) dans l'arborescence.

Figure 10-18. Page **OSPF Virtual Link Summary** (Récapitulatif des liaisons virtuelles OSPF)



Area ID	Neighbor Router ID	Hello Interval (secs)	Dead Interval (secs)	Retransmit Interval (secs)	Itransit Delay Interval (secs)
0.0.1	2.2.2	10	40	5	1

La page **OSPF Virtual Link Summary** (Récapitulatif des liaisons virtuelles OSPF) contient les champs suivants :

Area ID (ID de zone) : partie correspondant à l'ID de zone dans l'identification de la liaison virtuelle dont vous voulez afficher les données. L'ID de zone et l'ID du routeur voisin définissent ensemble une liaison virtuelle.

Neighbor Router ID (ID du routeur voisin) : partie correspondant à l'ID du routeur voisin dans l'identification de la liaison virtuelle. Des liaisons virtuelles peuvent être configurées entre une paire de routeurs de limite de zone dont les interfaces sont situées dans une zone commune (qui n'est pas un segment principal).

Hello Interval (secs) (Intervalle Hello [secondes]) : intervalle Hello OSPF (en secondes) pour la liaison virtuelle. Cette valeur doit être identique pour tous les routeurs connectés à un réseau.

Dead Interval (secs) (Intervalle d'inactivité [secondes]) : intervalle d'inactivité OSPF (en secondes) pour la liaison virtuelle. Il désigne la durée pendant laquelle un routeur attend de recevoir des paquets Hello d'un routeur voisin avant de déclarer que ce routeur est indisponible. Ce paramètre doit être identique pour tous les routeurs connectés à un réseau commun, et être un multiple de l'intervalle Hello (par exemple, 4).

Retransmit Interval (secs) (Intervalle de retransmission [secondes]) : intervalle de retransmission OSPF (en secondes) pour la liaison virtuelle. Il désigne le délai entre les LSA (Link State Advertisements) pour les contiguités appartenant à cette interface de routeur. Cette valeur est également utilisée lors de la retransmission des descriptions de base de données et des paquets LSR (Link State Request).

Itransit Delay Interval (secs) (Intervalle du délai Itransit [secondes]) : délai de transition OSPF en unités de secondes pour la liaison virtuelle. Il désigne le nombre estimé de secondes pour transmettre un paquet LSU (Link State Update) sur cette interface.

Affichage du récapitulatif des liaisons virtuelles à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 OSPF Commands (Commandes OSPF)

Configuration de la redistribution des itinéraires

La page **OSPF Route Redistribution Configuration** (Configuration de la redistribution des itinéraires OSPF) permet de configurer la redistribution dans OSPF des itinéraires appris via les options Static (Statique), Connected (Connecté) et RIP. Vous pouvez choisir de redistribuer les itinéraires appris à partir de tous ces protocoles ou de certains d'entre eux.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Route Redistribution Configuration** (Configuration de la redistribution des itinéraires) dans l'arborescence.

Figure 10-19. **OSPF Route Redistribution Configuration** (Configuration de la redistribution des itinéraires OSPF)



Cette page contient les champs suivants :

Configured Source (Source configurée) : protocole configuré permettant à OSPF de redistribuer les itinéraires appris via ce protocole. Seuls les itinéraires source qui ont été configurés pour être redistribués par OSPF sont disponibles. L'option Create (Créer) permet de configurer un nouvel itinéraire source.

Available Source (Source disponible) : protocole disponible pour la configuration permettant à OSPF de redistribuer les itinéraires. Cette option ne s'affiche que si le champ Configured Source (Source configurée) est défini sur Create (Créer). Les valeurs admises sont Static (Statique), Connected (Connecté) et RIP.

Metric (Métrique) : définit la valeur de la métrique pour les itinéraires redistribués. Ce champ affiche une valeur si la source a été préconfigurée. Les valeurs admises sont comprises entre 0 et 16777214.

Metric Type (Type de métrique) : sélectionnez le type de métrique OSPF pour les itinéraires redistribués dans le menu déroulant.

Tag (Balise) : définit le champ de balisage dans les itinéraires redistribués. Ce champ affiche une valeur si la source a été préconfigurée. Sinon, la valeur 0 s'affiche. Les valeurs admises sont comprises entre 0 et 4294967295.

Subnets (Sous-réseaux) : choisissez si les itinéraires de sous-réseau doivent être redistribués ou non dans le menu déroulant.

Distribute List (Liste de distribution) : sélectionne la liste d'accès qui filtre les itinéraires devant être redistribués par le protocole de destination. Seuls les itinéraires autorisés sont redistribués. Si cette commande fait référence à une liste d'accès inexistante, tous les itinéraires sont autorisés. Le menu déroulant répertorie les listes de contrôle d'accès (ACL) configurées à partir des pages **Switching** (Commutation) → **Network Security** (Sécurité réseau) → **Access Control Lists** (Listes de contrôle d'accès) → **IP Access Control Lists** (Listes de contrôle d'accès IP). Lorsqu'une liste d'accès est utilisée pour le filtrage du routage, les champs utilisés sont :

- 1 Source IP Address and netmask (Adresse IP et masque de réseau sources)
- 1 Destination IP Address and netmask (Adresse IP et masque de réseau de destination)
- 1 Action (Permit or Deny) (Action [Autorisation ou Refus])

Tous les autres champs (Source and Destination Port [Port source et de destination], Precedence [Précédence], Tos, etc.) ne sont pas pris en compte.

L'adresse IP source est comparée à l'adresse IP de destination de l'itinéraire. Le masque de réseau IP source dans la règle de listes d'accès est considéré comme un masque à caractères génériques, qui indique les bits de l'adresse IP source qui doivent correspondre à l'adresse de destination de l'itinéraire. (Notez que si le masque a la valeur 1, le bit d'adresse correspondant a une valeur quelconque).

Lorsqu'une règle de listes d'accès inclut une adresse IP et un masque réseau de destination (liste d'accès étendue), l'adresse IP de destination est comparée au masque réseau de la destination de l'itinéraire. Le masque réseau de destination dans la liste d'accès sert de masque à caractères génériques, qui indique les bits du masque de destination de l'itinéraire qui ont une importance pour la procédure de filtrage.

Création d'une source de redistribution des itinéraires OSPF

Lorsqu'aucune redistribution n'est configurée, le système affiche uniquement l'option Create (Créer) dans le champ Configured Source (Source configurée) et les sources possibles dans le champ Available Source (Source disponible). Lorsque vous sélectionnez une source disponible, vous devez entrer les données de configuration et cliquer sur **Apply Changes** (Appliquer les modifications). La source s'affiche dans la liste déroulante associée au champ Configure Source (Configurer la source), et elle est supprimée de la liste déroulante associée au champ Available Source (Source disponible).

1. Affichez la page **OSPF Route Redistribution Configuration** (Configuration de la redistribution des itinéraires OSPF).
2. Sélectionnez **Create** (Créer) dans le champ Configured Source (Source configurée).
3. Sélectionnez **Static** (Statique), **Connected** (Connecté) ou **RIP** dans le champ Available Source (Source disponible).
4. Cliquez sur **Apply Changes** (Appliquer les modifications) lorsque vous avez terminé.

Les données de redistribution des itinéraires sont configurées et le périphérique est mis à jour.

Modification des données de redistribution des itinéraires OSPF

1. Affichez la page **OSPF Route Redistribution Configuration** (Configuration de la redistribution des itinéraires OSPF).
2. Sélectionnez une source dans la liste déroulante associée au champ Configured Source (Source configurée).
3. Renseignez les champs si nécessaire.
4. Cliquez sur **Apply Changes** (Appliquer les modifications) lorsque vous avez terminé.

Les données de redistribution des itinéraires sont configurées et le périphérique est mis à jour.

Configuration des données de redistribution des itinéraires OSPF à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

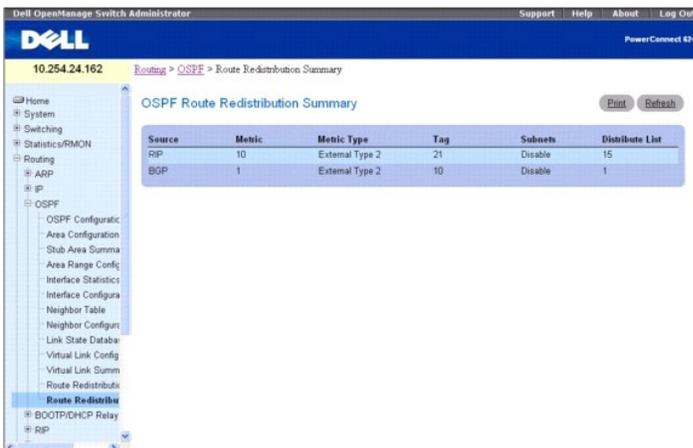
- 1 OSPF Commands (Commandes OSPF)

Récapitulatif de la redistribution des itinéraires

La page **OSPF Route Redistribution Summary** (Récapitulatif de la redistribution des itinéraires OSPF) permet d'afficher les configurations de redistribution d'itinéraires OSPF.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **OSPF** → **Route Redistribution Summary** (Récapitulatif de la redistribution des itinéraires) dans l'arborescence.

Figure 10-20. Page **OSPF Route Redistribution Summary** (Récapitulatif de la redistribution des itinéraires OSPF)



Source	Metric	Metric Type	Tag	Subnets	Distribute List
RIP	10	External Type 2	21	Disable	15
BGP	1	External Type 2	10	Disable	1

Cette page contient les champs suivants :

Source : itinéraire source devant être redistribué par le protocole OSPF.

Metric (Métrique) : métrique des itinéraires redistribués pour un itinéraire source donné. Affiche Unconfigured (Non configuré) si cette option n'est pas configurée.

Metric Type (Type de métrique) : type de métrique OSPF pour les itinéraires redistribués.

Tag (Balise) : champ de balise des itinéraires redistribués. Ce champ affiche une valeur si la source a été préconfigurée. Sinon, la valeur 0 s'affiche.

Subnets (Sous-réseaux) : indique si les itinéraires de sous-réseau doivent être redistribués ou non.

Distribute List (Liste de distribution) : liste d'accès qui filtre les itinéraires devant être redistribués par le protocole de destination.

Affichage du récapitulatif de la redistribution des itinéraires à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 OSPF Commands (Commandes OSPF)

Agent de relais BOOTP/DHCP

L'agent de relais BootP/DHCP permet aux clients et aux serveurs BootP/DHCP d'échanger des messages BootP/DHCP sur plusieurs sous-réseaux. Il reçoit les requêtes des clients et vérifie les sauts valides et les champs giaddr. Si le nombre de sauts est supérieur à la valeur configurée, il considère que le paquet a effectué une boucle sur les agents et ne le prend pas en compte. Si le champ giaddr a la valeur 0, l'agent doit entrer l'adresse IP de l'interface sur laquelle la requête a été reçue. Il envoie en monodiffusion les paquets valides vers la prochaine destination configurée. Le serveur renvoie une réponse BOOTREPLY en monodiffusion à l'agent de relais le plus proche du client indiqué dans le champ giaddr. Lorsque l'agent reçoit la réponse BOOTREPLY du serveur, il la transfère en diffusion ou en monodiffusion sur l'interface où la réponse BOOTREQUEST a été reçue. Cette interface peut être identifiée par le champ giaddr.

Le composant DHCP de la série 6200 prend également en charge les options de l'agent de relais DHCP permettant d'identifier le circuit source lorsque les clients sont connectés à Internet à l'aide d'un modem haut débit. L'agent de relais intègre ces options lors de l'envoi de la requête au serveur, et les supprime lors de l'envoi de la réponse aux clients.

Si une interface contient plusieurs adresses IP, l'agent de relais doit utiliser l'adresse IP principale configurée comme son adresse IP.

La page de menu **BOOTP/DHCP Relay Agent** (Agent de relais BOOTP/DHCP) contient des liens vers les pages Web permettant de configurer et d'afficher l'agent de relais BOOTP/DHCP. Pour afficher cette page, cliquez sur **Routing** (Routeage) → **BOOTP/DHCP Relay Agent** (Agent de relais BOOTP/DHCP) dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

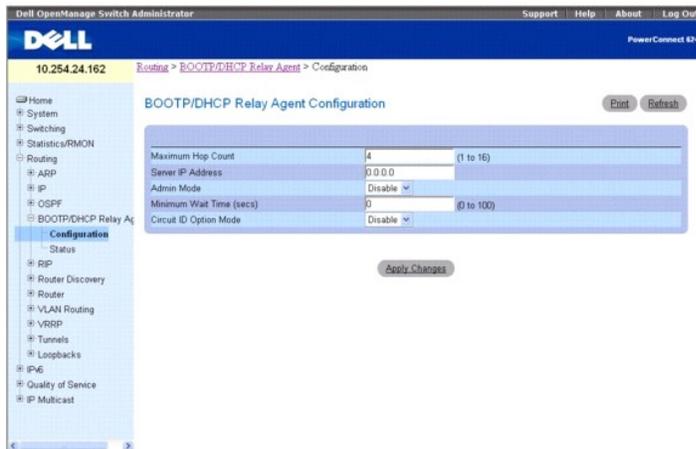
1. [Configuration de l'agent de relais BOOTP/DHCP](#)
1. [État de l'agent de relais BOOTP/DHCP](#)

Configuration de l'agent de relais BOOTP/DHCP

La page **BOOTP/DHCP Relay Agent Configuration** (Configuration de l'agent de relais BOOTP/DHCP) permet de configurer et d'afficher un agent de relais BOOTP/DHCP.

Pour afficher cette page, cliquez sur **Routing** (Routeage) → **BOOTP/DHCP Relay Agent** (Agent de relais BOOTP/DHCP) → **Configuration** dans l'arborescence.

Figure 10-21. BOOTP/DHCP Relay Agent Configuration (Configuration de l'agent de relais BOOTP/DHCP)



La page **BOOTP/DHCP Relay Agent Configuration** (Configuration de l'agent de relais BOOTP/DHCP) contient les champs suivants :

Maximum Hop Count (Nombre maximum de sauts) : entrez le nombre maximum de sauts qu'une requête client est autorisée à effectuer avant d'être rejetée.

Server IP Address (Adresse IP du serveur) : entrez l'adresse IP du serveur BOOTP/DHCP ou celle de l'agent de relais BOOTP/DHCP suivant.

Admin Mode (Mode d'administration) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Lorsque vous sélectionnez Enable (Activer), les requêtes BOOTP/DHCP sont envoyées vers l'adresse IP saisie dans le champ associé à l'adresse IP du serveur.

Minimum Wait Time (secs) (Délai d'attente minimum [secondes]) : entrez une durée en secondes. Cette valeur est comparée à l'horodateur dans les paquets de requêtes du client, et désigne le temps écoulé depuis la mise sous tension du client. Les paquets ne sont envoyés que lorsque l'horodateur dépasse le délai d'attente minimum.

Circuit ID Option Mode (Mode Option de l'ID du circuit) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Si vous sélectionnez Enable (Activer), l'agent de relais ajoute les paquets d'en-tête Option 82 aux paquets de requête DHCP avant de les envoyer au serveur, puis les supprime lors de l'envoi des réponses au client.

Configuration de l'agent de relais BOOTP/DHCP

1. Affichez la page **BOOTP/DHCP Configuration** (Configuration de l'agent de relais BOOTP/DHCP).
2. Renseignez les champs si nécessaire.

3. Cliquez sur **Apply Changes** (Appliquer les modifications) lorsque vous avez terminé.

Les données de l'agent de relais BOOTP/DHCP sont configurées et le périphérique est mis à jour.

Configuration de l'agent de relais BOOTP/DHCP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 DHCP and BOOTP Relay Commands (Commandes de relais DHCP et BOOTP)

État de l'agent de relais BOOTP/DHCP

Utilisez la page l'état de l'agent de relais **Relay Agent Status BOOTP/DHCP** pour afficher les informations de configuration et d'état de l'agent de relais BOOTP/DHCP.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **BOOTP/DHCP Relay Agent** (Agent de relais BOOTP/DHCP) → **Status** (État) dans l'arborescence.

Figure 10-22. Page BOOTP/DHCP Relay Agent Status (État de l'agent de relais BOOTP/DHCP)



Cette page contient les champs suivants :

Maximum Hop Count (Nombre maximum de sauts) : nombre maximum de sauts qu'une requête client peut effectuer sans être rejetée.

Server IP Address (Adresse IP du serveur) : adresse IP du serveur BOOTP/DHCP ou celle de l'agent de relais BOOTP/DHCP suivant.

Admin Mode (Mode admin) : mode d'administration du relais. Lorsque vous sélectionnez Enable (Activer) sur la page de configuration, les requêtes BOOTP/DHCP sont envoyées vers l'adresse IP saisie dans le champ associé à l'adresse IP du serveur.

Minimum Wait Time (secs) (Délai d'attente minimum [secondes]) : durée minimale en secondes. Cette valeur est comparée à l'horodateur dans les paquets de requêtes du client, et désigne le temps écoulé depuis la mise sous tension du client. Les paquets ne sont envoyés que lorsque l'horodateur dépasse le délai d'attente minimum.

Circuit ID Option Mode (Mode Option de l'ID du circuit) : option de l'agent de relais, qui peut être activée ou désactivée. Si vous sélectionnez Enable (Activer), l'agent de relais ajoute les paquets d'en-tête Option 82 aux paquets de requête DHCP avant de les envoyer au serveur, puis les supprime lors de l'envoi des réponses au client.

Requests Received (Requêtes reçues) : nombre total de requêtes BOOTP/DHCP transmises par tous les clients depuis la dernière réinitialisation du commutateur.

Requests Relayed (Requêtes transmises) : nombre total de requêtes BOOTP/DHCP transmises au serveur depuis la dernière réinitialisation du commutateur.

Packets Discarded (Paquets rejetés) : nombre total de paquets BOOTP/DHCP rejetés par cet agent de relais depuis la dernière réinitialisation du commutateur.

Affichage de l'agent de relais BOOTP/DHCP à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 DHCP and BOOTP Relay Commands (Commandes de relais DHCP et BOOTP)

Protocole RIP

Le protocole RIP est un protocole IGP (Interior Gateway Protocol) qui repose sur l'algorithme Bellman-Ford et cible les réseaux plus petits dont le diamètre ne dépasse pas 15 sauts. Les informations de routage sont acheminées par paquets de mise à jour RIP qui sont envoyés régulièrement et en cas de modifications de la topologie du réseau. Lorsqu'il reçoit une mise à jour RIP, le routeur peut modifier, supprimer ou ajouter l'itinéraire dans sa table de routage, selon qu'il est répertorié ou non dans la table de routage. Les préférences de routage sont envoyées par le biais d'une métrique configurable qui indique la distance de chaque destination.

La page de menu **RIP** (Protocole RIP) contient des liens vers les pages Web permettant de configurer et d'afficher les paramètres et les données RIP. Pour afficher cette page, cliquez sur **Routing** (Routage) → **RIP** dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

- 1 [Configuration RIP](#)
- 1 [Récapitulatif de l'interface RIP](#)
- 1 [Configuration de l'interface RIP](#)
- 1 [Configuration de la redistribution des itinéraires RIP](#)
- 1 [Récapitulatif de la redistribution des itinéraires RIP](#)

Configuration RIP

La page **RIP Configuration** (Configuration RIP) permet d'activer et de configurer le protocole RIP en mode Global, ou encore de le désactiver. Pour afficher cette page, cliquez sur **Routing** (Routage) → **RIP** → **Configuration** dans l'arborescence.

Figure 10-23. Page RIP Configuration (Configuration RIP)



Cette page contient les champs suivants :

RIP Admin Mode (Mode admin RIP) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant.

Si vous sélectionnez Enable (Activer), le protocole RIP est activé sur le commutateur. La valeur par défaut est Disable (Désactiver).

Split Horizon Mode (Mode Découpage de l'horizon) : sélectionnez None (Aucun), Simple ou Poison Reverse (Anti-poison) dans le menu déroulant. La valeur par défaut est Simple. Le découpage de l'horizon est une technique qui permet d'éviter les problèmes dus à l'inclusion d'un itinéraire dans les mises à jour envoyées au routeur à partir duquel l'itinéraire a été initialement appris. Les options sont :

- 1 **None** (Aucun) : aucun traitement spécial pour ce cas.
- 1 **Simple** : un itinéraire ne fait pas partie des mises à jour envoyées au routeur à partir duquel il a été appris.
- 1 **Poison Reverse** (Anti-poison) : un itinéraire est inclus dans les mises à jour envoyées au routeur à partir duquel il a été appris, mais la métrique est définie sur l'infini.

Auto Summary Mode (Mode Récapitulatif automatique) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Si vous sélectionnez Enable (Activer), les groupes d'itinéraires adjacents sont résumés en entrées uniques, afin de diminuer le nombre total d'entrées. La valeur par défaut est Enable (Activer).

Host Routes Accept Mode (Mode Accepter les itinéraires hôtes) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Si vous sélectionnez Enable (Activer), le routeur accepte les itinéraires hôtes. La valeur par défaut est Enable (Activer).

Global Route Changes (Modifications de routage globales) : affiche le nombre de modifications de routage apportées à la base de données de routage IP par le protocole RIP. Cette valeur ne tient pas compte de l'actualisation de la durée d'un itinéraire.

Global Queries (Interrogations globales) : affiche le nombre de réponses envoyées aux interrogations RIP d'autres serveurs.

Default Information Originate (Création d'informations par défaut) : activez ou désactivez l'option Default Route Advertise (Annonce de routage par défaut).

Default Metric (Métrique par défaut) : définit une valeur par défaut pour la métrique des itinéraires redistribués. Ce champ affiche la métrique par défaut si la source a déjà été définie, ou ne contient aucune valeur si elle n'a pas été configurée précédemment. Les valeurs autorisées sont comprises entre 1 et 15.

Configuration du protocole RIP

1. Affichez la page **RIP Configuration** (Configuration RIP).
2. Renseignez les champs si nécessaire.
3. Cliquez sur **Apply Changes** (Appliquer les modifications) lorsque vous avez terminé.

Le protocole RIP est configuré et le périphérique est mis à jour.

Configuration du protocole RIP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

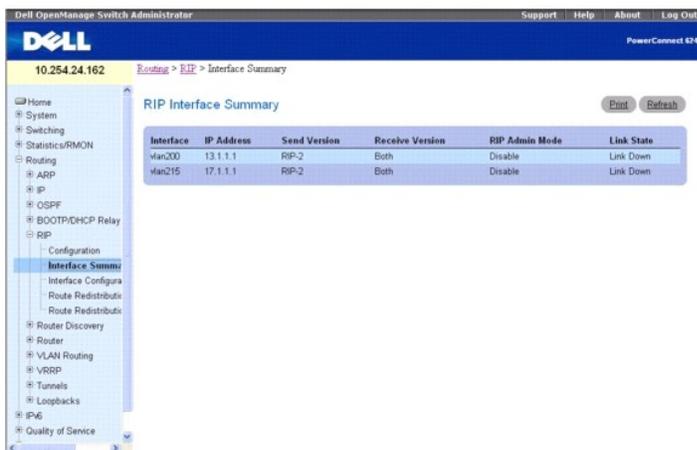
- 1 Routing Information Protocol (RIP) Commands (Commandes RIP)

Récapitulatif des interfaces RIP

La page **RIP Interface Summary** (Récapitulatif des interfaces RIP) permet d'afficher l'état de la configuration RIP sur une interface.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **RIP** → **Interface Summary** (Récapitulatif des interfaces) dans l'arborescence.

Figure 10-24. Page **RIP Interface Summary** (Récapitulatif des interfaces RIP)



Interface	IP Address	Send Version	Receive Version	RIP Admin Mode	Link State
vlan200	13.1.1.1	RIP-2	Both	Disable	Link Down
vlan215	17.1.1.1	RIP-2	Both	Disable	Link Down

Cette page contient les champs suivants :

Interface : interface, par exemple le réseau VLAN prenant en charge le routage et sur lequel le protocole RIP est activé.

IP Address (Adresse IP) : adresse IP de l'interface du routeur.

Send Version (Version d'envoi) : indique la version RIP utilisée par les paquets de contrôle RIP transmis par l'interface. La valeur par défaut est RIP-2. Les valeurs possibles sont :

- 1 **RIP-1** : les paquets au format RIP 1 sont envoyés par diffusion.
- 1 **RIP-1c** : mode de compatibilité avec la version RIP 1. Les paquets au format RIP 2 sont transmis par diffusion.
- 1 **RIP-2** : les paquets au format RIP 2 sont envoyés par multidiffusion.
- 1 **None** (Aucun) : les paquets de contrôle RIP ne sont pas transmis.

Receive Version (Version de réception) : indique la version RIP des paquets de contrôle acceptés par l'interface. La valeur par défaut est Both (Les deux). Ce champ peut prendre les valeurs suivantes :

- 1 **RIP-1** : seuls les paquets au format RIP 1 sont reçus.
- 1 **RIP-2** : seuls les paquets au format RIP 2 sont reçus.
- 1 **Both** (Les deux) : les paquets sont reçus dans les deux formats.
- 1 **None** (Aucun) : aucun paquet de contrôle RIP n'est reçu.

RIP Admin Mode (Mode admin RIP) : indique si le protocole RIP est activé ou désactivé sur l'interface.

Link State (État de la liaison) : indique si l'interface RIP est activée ou non.

Affichage du récapitulatif des interfaces RIP à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

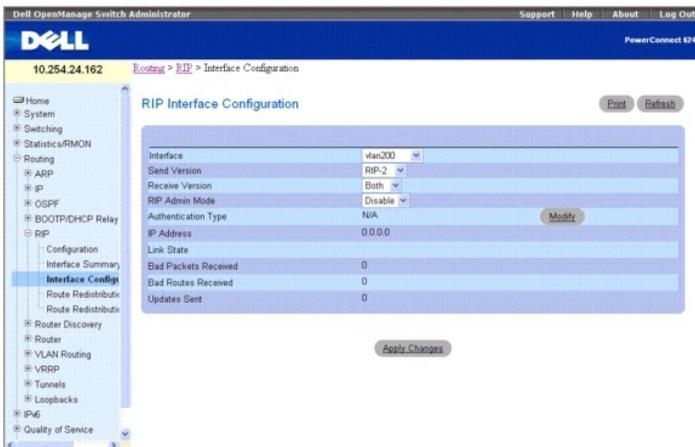
- 1 Routing Information Protocol (RIP) Commands (Commandes RIP)

Configuration de l'interface RIP

La page **RIP Interface Configuration** (Configuration de l'interface RIP) permet d'activer et de configurer le protocole RIP sur une interface spécifique, ou encore de le désactiver.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **RIP** → **Interface Configuration** (Configuration de l'interface) dans l'arborescence.

Figure 10-25. Page RIP Interface Configuration (Configuration de l'interface RIP)



Cette page contient les champs suivants :

Interface : sélectionnez l'interface dont vous voulez configurer les données dans le menu déroulant.

Send Version (Version d'envoi) : version RIP utilisée par le routeur pour envoyer ses mises à jour de routage. La valeur par défaut est RIP-2. Les valeurs possibles sont :

- 1 **RIP-1** : les paquets au format RIP 1 sont envoyés par diffusion.
- 1 **RIP-1c** : mode de compatibilité avec la version RIP 1. Les paquets au format RIP 2 sont envoyés par diffusion.
- 1 **RIP-2** : les paquets au format RIP 2 sont envoyés par multidiffusion.
- 1 **None** (Aucun) : aucun paquet de contrôle RIP n'est envoyé.

Receive Version (Version de réception) : version RIP des mises à jour de routage que le routeur doit accepter. La valeur par défaut est Both (Les deux). Ce champ peut prendre les valeurs suivantes :

- 1 **RIP-1** : seuls les paquets au format RIP 1 sont acceptés.
- 1 **RIP-2** : seuls les paquets au format RIP 2 sont acceptés.
- 1 **Both** (Les deux) : les paquets sont acceptés dans les deux formats.
- 1 **None** (Aucun) : aucun paquet de contrôle RIP n'est accepté.

RIP Admin Mode (Mode admin RIP) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Avant d'activer la version RIP 1 ou la version 1c sur une interface, vous devez d'abord activer le mode de diffusion géré par le réseau sur l'interface correspondante. La valeur par défaut est Disabled (Désactivé).

Authentication Type (Type d'authentification) : vous pouvez sélectionner un type d'authentification autre que None (Aucun) en cliquant sur le bouton **Modify** (Modifier). Un nouvel écran apparaît, dans lequel vous pouvez sélectionner un type d'authentification dans le menu déroulant. Ce champ peut prendre les valeurs suivantes :

- 1 **None** (Aucun) : état initial de l'interface. Si vous sélectionnez cette option dans le menu déroulant du deuxième écran et cliquez sur **Apply Changes** (Appliquer les modifications), vous êtes renvoyé au premier écran et aucun protocole d'authentification n'est exécuté.
- 1 **Simple** : si vous sélectionnez cette option, vous êtes invité à entrer une clé d'authentification. Cette clé figure dans l'en-tête RIP de tous les paquets envoyés sur le réseau. Tous les routeurs contenus sur le réseau doivent être configurés avec la même clé.
- 1 **Encrypt** (Crypter) : si vous sélectionnez cette option, vous êtes invité à entrer une clé d'authentification et un ID d'authentification. Le cryptage utilise l'algorithme Message-Digest MD5. Tous les routeurs contenus sur le réseau doivent être configurés avec la même clé et le même ID.

IP Address (Adresse IP) : affiche l'adresse IP de l'interface du routeur.

Link State (État de la liaison) : indique si l'interface RIP est activée ou non.

Bad Packets Received (Paquets incorrects reçus) : affiche le nombre de paquets RIP incorrects ou altérés. Cette valeur n'inclut pas explicitement les mises à jour complètes envoyées qui contiennent de nouvelles informations.

Bad Routes Received (Itinéraires incorrects reçus) : affiche le nombre d'itinéraires, dans les paquets RIP valides, qui n'ont pas été pris en compte pour une raison quelconque (nombre de mises à jour RIP déclenchées qui ont été réellement envoyées sur cette interface, etc.). Cette valeur n'inclut pas explicitement les mises à jour complètes envoyées qui contiennent de nouvelles informations.

Updates Sent (Mises à jour envoyées) : affiche le nombre de mises à jour de routage envoyées.

Configuration de l'interface RIP

1. Affichez la page **RIP Interface Configuration** (Configuration de l'interface RIP).

2. Indiquez l'interface dont vous voulez configurer les données.

3. Renseignez les champs si nécessaire :

Send Version (Version d'envoi) : dans la zone de liste déroulante, sélectionnez **None** (Aucun), **RIP-1c**, **RIP-1c** ou **RIP2**.

Receive Version (Version de réception) : dans la zone de liste déroulante, sélectionnez **None** (Aucun), **RIP-1**, **RIP-2** ou **Both** (Les deux).

RIP Admin Mode (Mode admin RIP) : sélectionnez **Enable** (Activer) ou **Disable** (Désactiver).

Authentication Type (Type d'authentification) : cliquez sur le bouton **Modify** (Modifier) pour configurer différents types d'authentification.

4. Cliquez sur **Apply Changes** (Appliquer les modifications) lorsque vous avez terminé.

L'interface RIP est configurée et le périphérique est mis à jour.

Sélection d'un mode d'authentification

1. Affichez la page **RIP Interface Configuration** (Configuration de l'interface RIP).

2. Indiquez l'interface dont vous voulez configurer le mode d'authentification.

3. Cliquez sur **Modify** (Modifier).

La page **Authentication Method** (Mode d'authentification) s'affiche.

4. Choisissez le type d'authentification (**None** [Aucun], **Simple** ou **Encrypt** [Crypter]) dans le menu déroulant.

5. Si vous sélectionnez **Simple** ou **Encrypt** (Crypter) comme type d'authentification, d'autres champs s'affichent. Entrez la clé d'authentification (Option "Simple" ou "Encrypt" [Crypter]) et l'ID de la clé d'authentification (Option "Encrypt").

6. Cliquez sur **Apply Changes** (Appliquer les modifications).

7. Le mode d'authentification et l'unité sont mis à jour.

Configuration de l'interface RIP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 Routing Information Protocol (RIP) Commands (Commandes RIP)

Configuration de la redistribution des itinéraires RIP

La page **RIP Route Redistribution Configuration** (Configuration de la redistribution des itinéraires RIP) permet de configurer les paramètres de redistribution des itinéraires RIP. Les valeurs admises pour chaque champ s'affichent en regard de celui-ci. Si des valeurs incorrectes sont saisies, un message d'alerte s'affiche, avec la liste des valeurs correctes.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **RIP** → **Route Redistribution Configuration** (Configuration de la redistribution des itinéraires) dans l'arborescence.

Figure 10-26. RIP Route Redistribution Configuration (Configuration de la redistribution des itinéraires RIP)



Cette page contient les champs suivants :

Configured Source (Source configurée) : cette zone de sélection est un sélecteur dynamique qui doit contenir uniquement les itinéraires source qui ont déjà été configurés pour être redistribués par le protocole RIP. L'option Create (Créer) vous permet de configurer un itinéraire source disponible.

Available Source (Source disponible) : cette zone de sélection est un sélecteur dynamique qui doit contenir uniquement les itinéraires source qui n'ont pas été précédemment configurés pour être redistribués par le protocole RIP. Elle s'affiche uniquement si le champ Configured Source (Source configurée) est défini sur Create (Créer). Ce champ peut prendre les valeurs suivantes :

- 1 **Static** (Statique)
- 1 **Connected** (Connecté)
- 1 **OSPF**

Metric (Métrique) : définit la valeur de métrique à utiliser pour les itinéraires redistribués. Ce champ affiche la métrique si la source a été préconfigurée et qu'elle peut être modifiée. Les valeurs admises sont comprises entre 1 et 15.

Distribute List (Liste de distribution) : définit la liste d'accès qui filtre les itinéraires devant être redistribués par le protocole de destination. Seuls les itinéraires autorisés sont redistribués.

Le menu déroulant répertorie les ACL configurées via les options **Switching** (Commutation) → **Network Security** (Sécurité du réseau) → **Access Control Lists** (Listes de contrôle d'accès) → **IP Access Control Lists** (Listes de contrôle d'accès IP). Lorsqu'une liste d'accès est utilisée pour le filtrage du routage, les champs utilisés sont :

- 1 Source IP Address and netmask (Adresse IP et masque de réseau sources)
- 1 Destination IP Address and netmask (Adresse IP et masque de réseau de destination)
- 1 Action (Permit or Deny) (Action [Autorisation ou Refus])

Tous les autres champs (Source and Destination Port [Port source et de destination], Precedence [Précédence], Tos, etc.) ne sont pas pris en compte.

L'adresse IP source est comparée à l'adresse IP de destination de l'itinéraire. Le masque de réseau IP source dans la règle de listes d'accès est considéré comme un masque à caractères génériques, qui indique les bits de l'adresse IP source qui doivent correspondre à l'adresse de destination de l'itinéraire. (Notez que si le masque a la valeur 1, le bit d'adresse correspondant a une valeur quelconque).

Lorsqu'une règle de listes d'accès inclut une adresse IP et un masque réseau de destination (liste d'accès étendue), l'adresse IP de destination est comparée au masque réseau de la destination de l'itinéraire. Le masque réseau de destination dans la liste d'accès sert de masque à caractères génériques, qui indique les bits du masque de destination de l'itinéraire qui ont une importance pour la procédure de filtrage.

Création d'une source configurée

1. Affichez la page **RIP Route Redistribution Configuration** (Configuration de la redistribution des itinéraires RIP).
2. Sélectionnez une source disponible à configurer.
3. Renseignez les autres champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La source spécifiée est configurée et le périphérique est mis à jour.

Modification d'une source configurée

1. Affichez la page **RIP Route Redistribution Configuration** (Configuration de la redistribution des itinéraires RIP).

2. Sélectionnez la source configurée à modifier.
 3. Modifiez les valeurs contenues dans cet écran si nécessaire.
 4. Cliquez sur **Apply Changes**
(Appliquer les modifications).
- Les modifications spécifiées sont enregistrées et le périphérique est mis à jour.

Configuration de la redistribution des itinéraires RIP à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 Routing Information Protocol (RIP) Commands (Commandes RIP)

Récapitulatif de la redistribution des itinéraires RIP

La page **RIP Route Redistribution Summary** (Récapitulatif de la redistribution des itinéraires RIP) permet d'afficher les configurations de redistribution des itinéraires RIP.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **RIP** → **Route Redistribution Summary** (Récapitulatif de la redistribution des itinéraires) dans l'arborescence.

Figure 10-27. Page **RIP Route Redistribution Summary** (Récapitulatif de la redistribution des itinéraires RIP)

Source	Metric	Match	Distribute List
Connected	1	N.A.	5
Static	2	N.A.	18

Cette page contient les champs suivants :

Source : itinéraire source devant être redistribué par le protocole RIP.

Metric (Métrique) : métrique des itinéraires redistribués pour un itinéraire source donné. Affiche Unconfigured (Non configuré) si cette option n'est pas configurée.

Match (Correspondance) : liste des itinéraires redistribués lorsque le protocole OSPF est sélectionné comme source. Elle peut inclure une ou plusieurs des valeurs suivantes :

- 1 Internal (Interne)
- 1 External (Externe) 1
- 1 External (Externe) 2
- 1 NSSA-External 1 (NSSA externe 1)
- 1 NSSA-External 2 (NSSA externe 2)
- 1 N.A. (Non applicable, si non OSPF)

Distribute List (Liste de distribution) : liste d'accès qui filtre les itinéraires devant être redistribués par le protocole de destination. Si la liste de distribution n'est pas configurée, ce champ est vide.

Affichage du récapitulatif de la redistribution des itinéraires RIP à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide

de référence CLI) :

- 1 Routing Information Protocol (RIP) Commands (Commandes RIP)

Protocole Router Discovery

Le protocole Router Discovery est utilisé par les hôtes pour identifier les routeurs opérationnels présents dans le sous-réseau. Il existe deux types de messages de détection de routeurs : les annonces du routeur et les sollicitations du routeur. Ce protocole exige que chaque routeur annonce régulièrement les adresses IP auxquelles il est associé. Les hôtes écoutent ces annonces et détectent les adresses IP des routeurs voisins.

La page de menu **Router Discovery** (Protocole Router Discovery) contient des liens vers les pages Web permettant de configurer et d'afficher les données de détection de routeurs. Pour afficher ce menu, cliquez sur **Routing** (Routeage) → **Router Discovery** (Protocole Router Discovery) dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

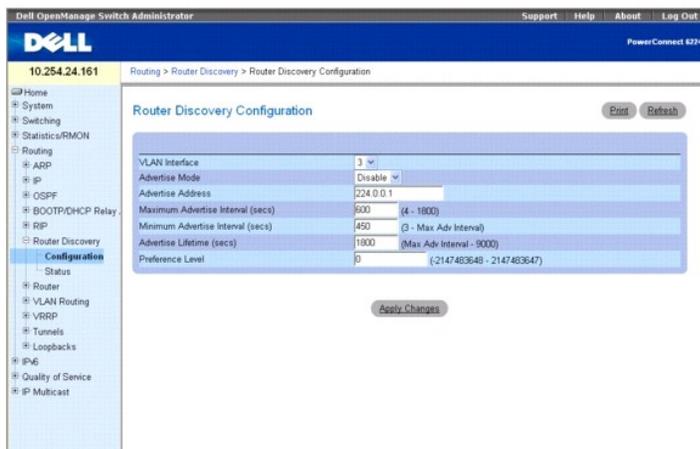
- 1 [Configuration du protocole Router Discovery](#)
- 1 [État du protocole Router Discovery](#)

Configuration du protocole Router Discovery

La page **Router Discovery Configuration** (Configuration du protocole Router Discovery) permet d'entrer ou de modifier les paramètres de détection de routeurs.

Pour afficher cette page, cliquez sur **Routing** (Routeage) → **Router Discovery** → **Configuration** dans l'arborescence.

Figure 10-28. Page Router Discovery Configuration (Configuration du protocole Router Discovery)



La page **Router Discovery Configuration** (Configuration du protocole Router Discovery) contient les champs suivants :

VLAN Interface (Interface VLAN) : sélectionnez l'interface de routeur dont vous voulez configurer les données.

Advertise Mode (Mode d'annonce) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Si vous sélectionnez Enable (Activer), les annonces du routeur sont transmises à partir de l'interface sélectionnée.

Advertise Address (Adresse de l'annonce) : entrez l'adresse IP à utiliser pour annoncer le routeur.

Maximum Advertise Interval (secs) (Intervalle d'annonce maximum [en secondes]) : entrez la durée maximale (en secondes) autorisée entre les annonces de routeur envoyées depuis l'interface.

Minimum Advertise Interval (secs) (Intervalle d'annonce minimum [en secondes]) : entrez la durée minimale (en secondes) autorisée entre les annonces de routeur envoyées depuis l'interface.

Advertise Lifetime (secs) (Durée de vie des annonces [en secondes]) : entrez la valeur (en secondes) à utiliser comme durée de vie pour les annonces de routeur envoyées depuis l'interface. Cette valeur désigne la durée maximale pendant laquelle les adresses annoncées sont considérées comme des adresses de routeur valides par les hôtes.

Preference Level (Niveau de préférence) : indiquez le niveau de préférence du routeur défini comme routeur par défaut par rapport aux autres routeurs contenus dans le même sous-réseau. Les adresses ayant des numéros élevés sont privilégiées. Vous devez entrer un nombre entier.

Configuration du protocole Router Discovery

1. Affichez la page **Router Discovery Configuration** (Configuration du protocole Router Discovery).
2. Sélectionnez l'interface de routeur à configurer.

3. Configurez les données des autres champs si nécessaire.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications de configuration spécifiées sont enregistrées et le périphérique est mis à jour.

Configuration du protocole Router Discovery à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 Router Discovery Protocol Commands (Commandes du protocole Router Discovery)

État du protocole Router Discovery

La page **Router Discovery Status** (État du protocole Router Discovery) permet d'afficher les données de détection de routeurs pour chaque port.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **Router Discovery** → **Status** (État) dans l'arborescence.

Figure 10-29. Page Router Discovery Status (État du protocole Router Discovery)

Interface	Advertise Mode	Advertise Address	Maximum Advertise Interval (secs)	Minimum Advertise Interval (secs)	Advertise Lifetime (secs)	Preference Level
Man000	Enable	224.0.0.1	600	450	1800	1
Man000	Disable	224.0.0.1	600	450	1800	0

Cette page contient les champs suivants :

Interface : interface de routeur dont vous voulez afficher les données.

Advertise Mode (Mode d'annonce) : les valeurs sont Enable (Activer) ou Disable (Désactiver). L'option Enable (Activer) indique que le protocole Router Discovery est activé sur cette interface.

Advertise Address (Adresse de l'annonce) : adresse IP utilisée pour annoncer le routeur.

Maximum Advertise Interval (secs) (Intervalle d'annonce maximum [en secondes]) : durée maximale (en secondes) autorisée entre les annonces de routeur envoyées depuis l'interface.

Minimum Advertise Interval (secs) (Intervalle d'annonce minimum [en secondes]) : durée minimale (en secondes) autorisée entre les annonces de routeur envoyées depuis l'interface.

Advertise Lifetime (secs) (Durée de vie des annonces [en secondes]) : valeur (en secondes) utilisée comme durée de vie pour les annonces de routeur envoyées depuis l'interface. Cette valeur désigne la durée maximale pendant laquelle les adresses annoncées sont considérées comme des adresses de routeur valides par les hôtes.

Preference Level (Niveau de préférence) : niveau de préférence du routeur défini comme routeur par défaut par rapport aux autres routeurs contenus dans le même sous-réseau. Les adresses ayant des numéros élevés sont privilégiées.

Affichage de l'état du protocole Router Discovery à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 Router Discovery Protocol Commands (Commandes du protocole Router Discovery)

Routeur

La page de menu **Routeur** (Routeur) contient des liens vers les pages Web permettant de configurer et d'afficher les tables de routage. Pour afficher cette page, cliquez sur **Routing** (Routage) → **Routeur** (Routeur) dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

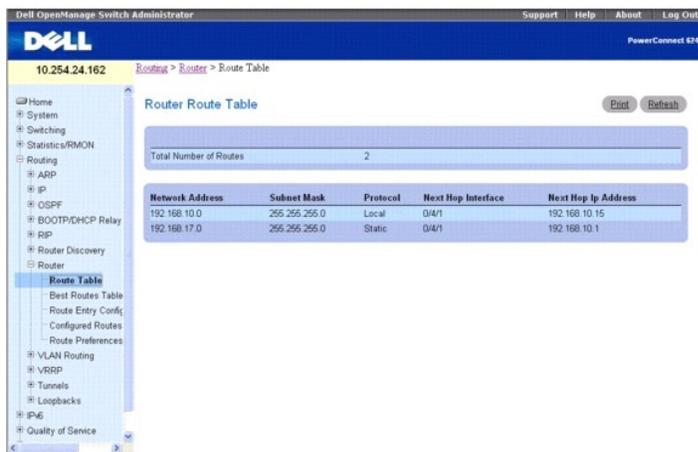
- 1 [Table de routage](#)
- 1 [Table des itinéraires recommandés](#)
- 1 [Configuration des entrées de routage](#)
- 1 [Itinéraires configurés](#)
- 1 [Configuration des préférences de routage](#)

Table de routage

La page **Router Route Table** (Table de routage du routeur) permet d'afficher la configuration de la table de routage.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **Routeur** (Routeur) → **Route Table** (Table de routage) dans l'arborescence.

Figure 10-30. Page Router Route Table (Table de routage du routeur)



Network Address	Subnet Mask	Protocol	Next Hop Interface	Next Hop Ip Address
192.168.10.0	255.255.255.0	Local	0/4/1	192.168.10.15
192.168.17.0	255.255.255.0	Static	0/4/1	192.168.10.1

La page **Router Route Table** (Table de routage du routeur) contient les champs suivants :

Total Number of Routes (Nombre total d'itinéraires) : nombre total d'itinéraires contenus dans la table de routage.

Network Address (Adresse du réseau) : préfixe de routage IP correspondant à la destination.

Subnet Mask (Masque de sous-réseau) : également appelé masque de réseau/de sous-réseau, ce champ désigne la partie de l'adresse de l'interface IP identifiant le réseau connecté.

Protocol (Protocole) : ce champ indique le protocole qui a créé l'itinéraire spécifié. Les valeurs possibles sont les suivantes :

- 1 Local
- 1 Static (Statique)
- 1 Default (Par défaut)
- 1 OSPF Intra (Intra OSPF)
- 1 OSPF Inter (Inter OSPF)
- 1 OSPF Type-1 (OSPF de type 1)
- 1 OSPF Type-2 (OSPF de type 2)
- 1 RIP

Next Hop Interface (Interface du saut suivant) : interface de sortie du routeur à utiliser lors du transfert du trafic vers la destination.

Next Hop IP Address (Adresse IP du saut suivant) : adresse IP de sortie du routeur à utiliser lors du transfert du trafic vers le routeur suivant (le cas échéant) dans le chemin d'accès vers la destination. Le prochain routeur est toujours l'un des routeurs voisins adjacents ou l'adresse IP de l'interface locale dans le cas d'un réseau directement connecté.

Affichage de la table de routage du routeur à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

Table des itinéraires recommandés

La page **Router Best Routes Table** (Table des itinéraires recommandés pour le routeur) permet d'afficher les itinéraires recommandés figurant dans la table de routage.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **Router** (Routeur) → **Best Routes Table** (Table des itinéraires recommandés) dans l'arborescence.

Figure 10-31. Page Router Best Routes Table (Table des itinéraires recommandés pour le routeur)



Network Address	Subnet Mask	Protocol	Next Hop Interface	Next Hop Ip Address
13.1.1.0	255.255.255.0	Local	loopback1	13.1.1.1
17.1.1.0	255.255.255.0	Local	loopback2	17.1.1.1

Cette page contient les champs suivants :

Total Number of Routes (Nombre total de routes) : nombre total d'itinéraires contenus dans la table de routage.

Network Address (Adresse du réseau) : préfixe de routage IP correspondant à la destination.

Subnet Mask (Masque de sous-réseau) : également appelé masque de réseau/de sous-réseau, ce champ désigne la partie de l'adresse de l'interface IP identifiant le réseau connecté.

Protocol (Protocole) : ce champ indique le protocole qui a créé l'itinéraire spécifié. Les valeurs possibles sont les suivantes :

- 1 Local
- 1 Static (Statique)
- 1 Default (Par défaut)
- 1 OSPF Intra (Intra OSPF)
- 1 OSPF Inter (Inter OSPF)
- 1 OSPF Type-1 (OSPF de type 1)
- 1 OSPF Type-2 (OSPF de type 2)
- 1 RIP

Next Hop Interface (Interface du saut suivant) : interface de sortie du routeur à utiliser lors du transfert du trafic vers la destination.

Next Hop IP Address (Adresse IP du saut suivant) : adresse IP de sortie du routeur à utiliser lors du transfert du trafic vers le routeur suivant (le cas échéant) dans le chemin d'accès vers la destination. Le prochain routeur est toujours l'un des routeurs voisins adjacents ou l'adresse IP de l'interface locale dans le cas d'un réseau directement connecté.

Affichage de la table des itinéraires recommandés à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 IP Routing Commands (Commandes de routage IP)

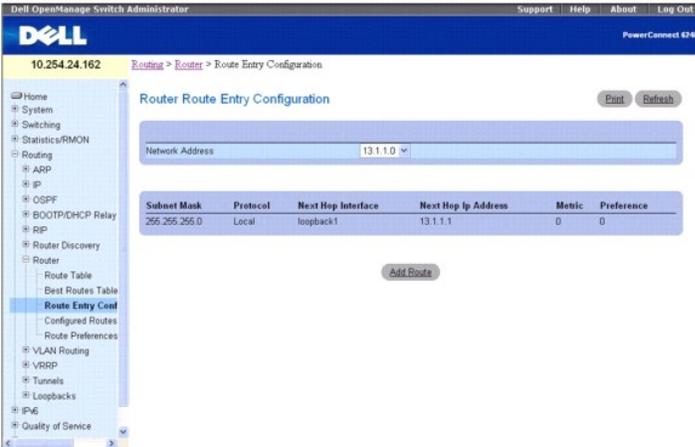
Configuration des entrées de routage

La page **Router Route Entry Configuration** (Configuration des entrées de routage du routeur) permet d'ajouter de nouveaux itinéraires et de les configurer.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **Router** (Routeur) → **Route Entry Configuration** (Configuration des entrées de routage) dans

l'arborescence.

Figure 10-32. Page Router Route Entry Configuration (Configuration des entrées de routage du routeur)



Cette page contient les champs suivants :

Network Address (Adresse du réseau) : définissez le préfixe de routage IP pour la destination dans le menu déroulant. Pour créer un itinéraire, une interface de routage valide doit exister et l'adresse IP du prochain saut doit figurer sur le même réseau que l'interface de routage. Les interfaces de routage sont créées sur la page **IP Interface Configuration** (Configuration de l'interface IP). Les adresses IP valides du prochain saut figurent sur la page **Route Table** (Table de routage).

Subnet Mask (Masque de sous-réseau) : également appelé masque de réseau/de sous-réseau, ce champ désigne la partie de l'adresse de l'interface IP identifiant le réseau connecté.

Protocol (Protocole) : ce champ indique le protocole qui a créé l'itinéraire spécifié. Ce champ peut prendre les valeurs suivantes :

- 1 Local
- 1 Static (Statique)
- 1 Default (Par défaut)
- 1 OSPF Intra (Intra OSPF)
- 1 OSPF Inter (Inter OSPF)
- 1 OSPF Type-1 (OSPF de type 1)
- 1 OSPF Type-2 (OSPF de type 2)
- 1 RIP

Next Hop Interface (Interface du saut suivant) : interface de sortie du routeur à utiliser lors du transfert du trafic vers la destination.

Next Hop IP Address (Adresse IP du saut suivant) : adresse IP de sortie du routeur à utiliser lors du transfert du trafic vers le routeur suivant (le cas échéant) dans le chemin d'accès vers la destination. Le prochain routeur est toujours l'un des routeurs voisins adjacents ou l'adresse IP de l'interface locale dans le cas d'un réseau directement connecté. Lors de la création d'un itinéraire, l'adresse IP du prochain saut doit figurer sur le même réseau que l'interface de routage. Les adresses IP valides du prochain saut figurent sur la page **Route Table** (Table de routage).

Metric (Métrique) : coût d'administration du chemin d'accès vers la destination. Si aucune valeur n'est saisie, la valeur par défaut est 1. La plage de valeurs est comprise entre 0 et 255. Ce champ ne s'affiche que lors de la création d'un itinéraire statique.

Preference (Préférence) : indique une valeur de préférence pour le prochain saut configuré.

Ajout d'un itinéraire

1. Affichez la page **Router Route Entry Configuration** (Configuration des entrées de routage du routeur).
2. Cliquez sur **Add Route** (Ajouter un itinéraire).

L'écran est actualisé et la page **Router Route Entry Configuration** (Configuration des entrées de routage du routeur) affiche de nouveaux champs, comme indiqué [Figure 10-33](#).

Figure 10-33. Ajout d'un type d'itinéraire par défaut

Router Route Entry Configuration

Route Type: Default

Next Hop IP Address: [Empty field]

Buttons: [Cancel] [Apply Changes]

3. En regard de **Route Type** (Type d'itinéraire), utilisez la liste déroulante pour ajouter un itinéraire par défaut ou statique.

Si vous sélectionnez l'option statique, la page est actualisée et de nouveaux champs apparaissent comme indiqué [Figure 10-34](#).

Default (Par défaut) : entrez l'adresse de la passerelle par défaut dans le champ **Next Hop IP Address** (Adresse IP du saut suivant).

Static (Statique) : renseignez les champs **Network Address** (Adresse du réseau), **Subnet Mask** (Masque de sous-réseau), **Next Hop IP Address** (Adresse IP du saut suivant) et **Preference** (Préférence).

Figure 10-34. Configuration des entrées de routage - Ajout d'un type d'itinéraire statique

Router Route Entry Configuration

Route Type: Static

Network Address: [Empty field]

Subnet Mask: [Empty field]

Next Hop IP Address: [Empty field]

Preference: 1 (1 to 255)

Buttons: [Cancel] [Apply Changes]

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouvel itinéraire est ajouté et vous êtes redirigé vers la page Configured Routes (Itinéraires configurés).

Ajout d'un itinéraire à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 IP Routing Commands (Commandes de routage IP)

Itinéraires configurés

La page **Configured Routes** (Itinéraires configurés) permet d'afficher les itinéraires configurés.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **Router** (Routeur) → **Configured Routes** (Itinéraires configurés) dans l'arborescence.

Figure 10-35. Page Configured Routes (Itinéraires configurés)

Configured Routes

Network Address	Subnet Mask	Next Hop IP	Preference	Remove
10.1.1.0	255.255.255.0	3.1.1.2	1	[X]
10.1.2.0	255.255.255.0	3.1.1.2	1	[X]
10.1.3.0	255.255.255.0	3.1.1.2	1	[X]

Buttons: [Apply Changes]

Cette page contient les champs suivants :

Network Address (Adresse du réseau) : préfixe de routage IP correspondant à la destination.

Subnet Mask (Masque de sous-réseau) : également appelé masque de réseau/de sous-réseau, ce champ désigne la partie de l'adresse de l'interface IP

identifiant le réseau connecté.

Next Hop IP (IP du saut suivant) : interface de sortie du routeur à utiliser lors du transfert du trafic vers la destination.

Preference (Préférence) : affiche les préférences configurées pour les itinéraires ajoutés.

Remove (Supprimer) : cochez cette case pour supprimer un itinéraire configuré.

Ajout d'un itinéraire

1. Affichez la page **Configured Routes** (Itinéraires configurés).

2. Cliquez sur **Add** (Ajouter).

La page **Router Route Entry Configuration** (Configuration des entrées de routage du routeur) représentée [Figure 10-33](#) s'affiche.

3. En regard de **Route Type** (Type d'itinéraire), utilisez la zone de liste déroulante pour ajouter un itinéraire **par défaut** ou un itinéraire **statique**.

Default (Par défaut) : entrez l'adresse de la passerelle par défaut dans le champ **Next Hop IP Address** (Adresse IP du saut suivant). La [Figure 10-33](#) montre les champs affichés lorsque la valeur du champ **Route Type** (Type d'itinéraire) est "Default" (Par défaut).

Static (Statique) : renseignez les champs **Network Address** (Adresse du réseau), **Subnet Mask** (Masque de sous-réseau), **Next Hop IP Address** (Adresse IP du saut suivant) et **Preference** (Préférence). La [Figure 10-34](#) montre les champs affichés lorsque la valeur du champ **Route Type** (Type d'itinéraire) est "Static" (Statique).

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouvel itinéraire est ajouté et la page Configured Routes (Itinéraires configurés) est rétablie.

Affichage des itinéraires configurés à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 IP Routing Commands (Commandes de routage IP)

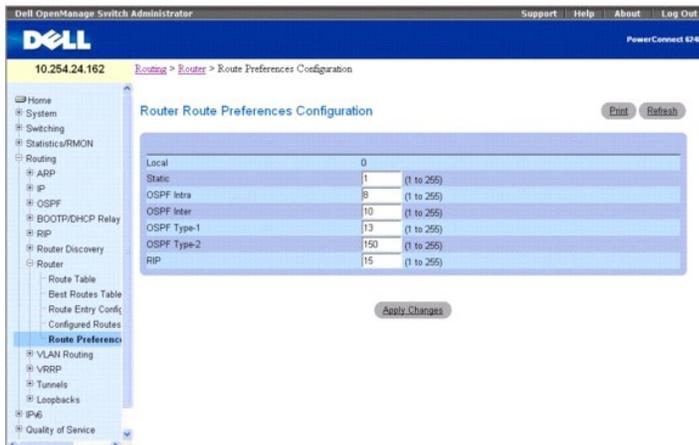
Configuration des préférences de routage

La page **Route Preferences Configuration** (Configuration des préférences de routage) permet de configurer la préférence par défaut de chaque protocole (par exemple, 60 pour les itinéraires statiques). Ces valeurs sont des valeurs arbitraires comprises entre 1 et 255 qui sont indépendantes des métriques de routage. La plupart des protocoles de routage utilisent une métrique de routage pour déterminer le chemin le plus court connu du protocole, indépendamment de tout autre protocole.

Pour choisir le meilleur itinéraire vers une destination, il faut sélectionner l'itinéraire dont la valeur de préférence est la plus faible. Lorsqu'il existe plusieurs itinéraires vers une destination, les valeurs de préférence sont utilisées pour déterminer l'itinéraire préféré. En cas d'égalité, l'itinéraire ayant la meilleure métrique de routage est choisi. Pour éviter les problèmes d'incompatibilité entre les métriques (c'est-à-dire, les métriques RIP et OSPF ne sont pas directement comparables), vous devez configurer plusieurs valeurs de préférence pour chacun des protocoles.

Pour afficher la page appropriée, cliquez sur **Routing** (Routage) → **Router** (Routeur) → **Route Preferences Configuration** (Configuration des préférences de routage) dans l'arborescence.

Figure 10-36. Page Router Route Preferences Configuration (Configuration des préférences de routage du routeur)



Cette page contient les champs suivants :

Local : valeur de préférence pour l'itinéraire local.

Static (Statique) : valeur de préférence pour l'itinéraire statique. La valeur par défaut est 1. La plage de valeurs est comprise entre 1 et 255.

OSPF Intra (Intra OSPF) : valeur de préférence pour l'itinéraire intra OSPF. La valeur par défaut est de 8. La plage de valeurs est comprise entre 1 et 255. La spécification OSPF (RFC 2328) nécessite que la préférence soit accordée aux itinéraires appris via le protocole OSPF dans l'ordre suivant : intra < inter < type-1 < type-2.

OSPF Inter (Inter OSPF) : valeur de préférence pour l'itinéraire inter OSPF. La valeur par défaut est de 10. La plage de valeurs est comprise entre 1 et 255. La spécification OSPF (RFC 2328) nécessite que la préférence soit accordée aux itinéraires appris via le protocole OSPF dans l'ordre suivant : intra < inter < type-1 < type-2.

OSPF Type-1 (OSPF de type 1) : valeur de préférence pour l'itinéraire OSPF de type 1. La valeur par défaut est de 13. La plage de valeurs est comprise entre 1 et 255. La spécification OSPF (RFC 2328) nécessite que la préférence soit accordée aux itinéraires appris via le protocole OSPF dans l'ordre suivant : intra < inter < type-1 < type-2.

OSPF Type-2 (OSPF de type 2) : valeur de préférence pour l'itinéraire OSPF de type 2. La valeur par défaut est de 150. La plage de valeurs est comprise entre 1 et 255. La spécification OSPF (RFC 2328) nécessite que la préférence soit accordée aux itinéraires appris via le protocole OSPF dans l'ordre suivant : intra < inter < type-1 < type-2.

RIP : valeur de préférence pour l'itinéraire RIP. La valeur par défaut est de 15. La plage de valeurs est comprise entre 1 et 255.

Configuration des préférences de routage

1. Affichez la page **Route Preferences Configuration** (Configuration des préférences de routage).
2. Complétez les champs appropriés de cette page.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les préférences de routage sont configurées et le périphérique est mis à jour.

Configuration des préférences de routage à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 OSPF Commands (Commandes OSPF)

Routage VLAN

Les logiciels des systèmes PowerConnect série 6200 peuvent être configurés avec des VLAN prenant en charge le routage. Vous pouvez également configurer les logiciels de façon que le trafic d'un VLAN soit traité comme si ce réseau était un port de routeur.

Lorsqu'un port est activé pour le pontage (paramètre par défaut) au lieu du routage, le traitement normal du pont est effectué pour un paquet entrant, qui est ensuite associé à un réseau VLAN. Son adresse de destination MAC et son ID de VLAN sont utilisés pour rechercher la table d'adresses MAC. Si le routage est activé pour le réseau VLAN et que l'adresse de destination MAC d'un paquet de monodiffusion entrant est celle de l'interface pont-routeur interne, le paquet est acheminé. Un paquet de multidiffusion entrant est transmis à tous les ports du réseau VLAN, plus l'interface pont-routeur interne, s'il a été reçu sur un réseau VLAN routé.

Étant donné qu'un port peut être configuré pour appartenir à plusieurs réseaux VLAN, le routage VLAN peut être activé pour tous les réseaux VLAN associés à ce port ou uniquement pour certains. Le routage VLAN permet à plusieurs ports physiques de résider sur le même sous-réseau. Il peut également être utilisé lorsqu'un réseau VLAN couvre plusieurs réseaux physiques ou lorsqu'une segmentation ou une sécurité supplémentaire est requise. Cette section indique comment configurer les logiciels des systèmes 6200 pour la prise en charge du routage VLAN. Un port peut être un port VLAN ou un port de routeur, mais pas les deux. Toutefois, un port VLAN peut faire partie d'un réseau VLAN qui est lui-même un port de routeur.

La page de menu **VLAN Routing** (Routage VLAN) contient un lien vers une page Web qui permet d'afficher les paramètres et les données de routage VLAN. Pour afficher cette page, cliquez sur **Routing** (Routage) → **VLAN Routing** (Routage VLAN) dans l'arborescence. Cette page de menu permet d'accéder à la fonction suivante :

- 1 [Récapitulatif du routage VLAN](#)

Récapitulatif du routage VLAN

La page **VLAN Routing Summary** (Récapitulatif du routage VLAN) permet d'afficher les informations sur les interfaces de routage VLAN configurées sur le système.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **VLAN Routing** (Routage VLAN) → **Summary** (Récapitulatif) dans l'arborescence.

Figure 10-37. Page VLAN Routing Summary (Récapitulatif du routage VLAN)

Dell OpenManage Switch Administrator

10.254.24.161 Routing > VLAN Routing > Summary

VLAN Routing Summary

VLANID	MAC Address	IP Address	Subnet Mask
200	00 FC E3 90 01 47	192.168.30.25	255.255.255.0
201	00 FC E3 90 01 47	10.10.10.50	255.255.255.0
300	00 FC E3 90 01 47	10.10.30.10	255.255.255.0

Cette page contient les champs suivants :

VLAN ID (ID du VLAN) : ID du réseau VLAN dont les données s'affichent dans la ligne en cours de la table.

MAC Address (Adresse MAC) : adresse MAC attribuée à l'interface de routage VLAN.

IP Address (Adresse IP) : adresse IP configurée de l'interface de routage VLAN. Notez que si un réseau VLAN est créé et que l'adresse IP n'est pas configurée, la page affiche par défaut la valeur 0.0.0.0 comme adresse IP. Pour configurer l'adresse IP, sélectionnez **IP** → **Interface Configuration** (Configuration de l'interface).

Subnet Mask (Masque de sous-réseau) : masque de sous-réseau configuré pour l'interface de routage VLAN. Ce champ a la valeur 0.0.0.0 lorsque l'interface de routage VLAN est d'abord configurée, et doit être saisie sur la page IP Interface Configuration (Configuration de l'interface IP).

Affichage du récapitulatif du routage VLAN à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous aux chapitres suivants du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 IP Addressing Commands (Commandes d'adressage IP)
- 1 Virtual LAN Routing Commands (Commandes de routage VLAN)

Protocole VRRP

Le protocole VRRP (Virtual Router Redundancy Protocol) est conçu pour gérer les défaillances du routeur par défaut en créant un schéma de sélection dynamique d'un routeur de sauvegarde. Le but était de réduire les périodes de "trou noir" causées par la panne du routeur de passerelle par défaut, durant lesquelles tout le trafic acheminé vers ce routeur est perdu tant que la panne n'est pas détectée. Bien que la configuration statique des itinéraires par défaut est courante, cette approche s'applique à un point de défaillance unique lorsque le routeur par défaut tombe en panne. Le protocole VRRP privilégie le concept de "routeur virtuel" associé à une ou plusieurs adresses IP servant de passerelles par défaut. En cas de défaillance du routeur VRRP contrôlant ces adresses IP (précédemment appelé routeur maître), le groupe d'adresses IP et le rôle de transfert par défaut sont pris en charge par un routeur VRRP de sauvegarde.

La page de menu **VRRP** (Protocole VRRP) contient des liens vers les pages Web permettant de configurer et d'afficher les paramètres et les données VRRP. Pour afficher cette page, cliquez sur **Routing** (Routage) → **VRRP** dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

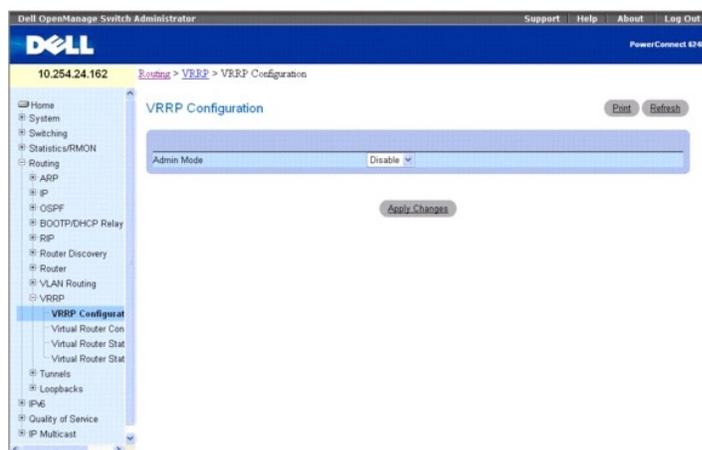
- 1 [Configuration VRRP](#)
- 1 [Configuration du routeur virtuel](#)
- 1 [État du routeur virtuel](#)
- 1 [Statistiques du routeur virtuel](#)

Configuration VRRP

La page **VRRP Configuration** (Configuration VRRP) permet d'activer ou de désactiver l'état d'administration d'un routeur virtuel.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **VRRP** → **VRRP Configuration** (Configuration VRRP) dans l'arborescence.

Figure 10-38. Page VRRP Configuration (Configuration VRRP)



Cette page contient les champs suivants :

Admin Mode (Mode admin) : ce champ active ou désactive l'état d'administration du protocole VRRP sur le routeur. Sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. La valeur par défaut est Disable (Désactiver).

Modification de l'état VRRP à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

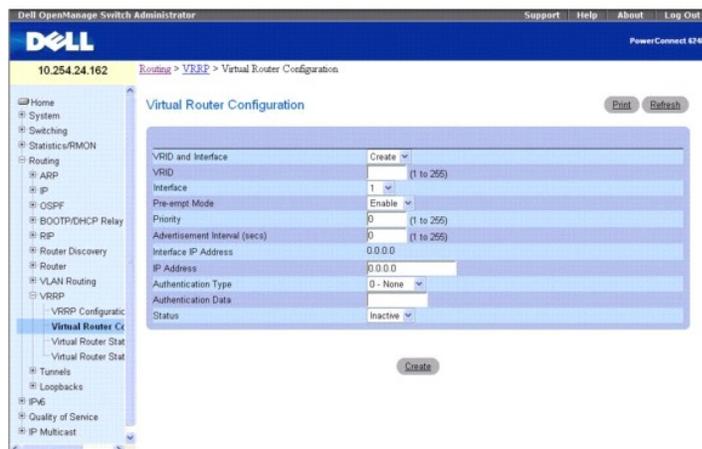
- 1 Virtual Router Redundancy Protocol Commands (Commandes VRRP)

Configuration du routeur virtuel

La page Virtual Router Configuration (Configuration du routeur virtuel) permet de créer un routeur virtuel ou de configurer un routeur virtuel existant.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **VRRP** → **Virtual Router Configuration** (Configuration du routeur virtuel) dans l'arborescence.

Figure 10-39. Page Virtual Router Configuration (Configuration du routeur virtuel)



Cette page contient les champs suivants :

VRID and Interface (VRID et interface) : cliquez sur Create (Créer) dans le menu déroulant pour configurer un nouveau routeur virtuel ou sélectionnez l'un des routeurs virtuels existants, qui sont répertoriés par numéro d'interface et VRID.

VRID : ce champ n'est configurable que si vous créez un routeur virtuel, auquel cas vous devez entrer le VRID dans la plage de valeurs comprise entre 1 et 255.

Interface : ce champ n'est configurable que si vous créez un routeur virtuel, auquel cas vous devez sélectionner l'interface du nouveau routeur virtuel dans le menu déroulant.

Pre-empt Mode (Mode préemption) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Si vous sélectionnez Enable (Activer), le routeur de sauvegarde devance le routeur maître si sa priorité est supérieure et si le routeur maître n'est pas le propriétaire de l'adresse IP du routeur virtuel. La valeur par défaut est Enable (Activer).

Priority (Priorité) : entrez la valeur de priorité que le routeur VRRP doit utiliser dans le choix du routeur virtuel maître. Si l'adresse IP virtuelle est identique à celle de l'interface, la priorité prend la valeur 255, quelle que soit votre saisie. Si vous entrez la valeur 255 alors que l'adresse IP virtuelle est différente de celle de l'interface, la priorité prend la valeur par défaut (100).

Advertisement Interval (secs) (Intervalle d'annonce [secondes]) : entrez la durée en secondes entre la transmission des paquets d'annonces par ce routeur virtuel. Ce nombre doit être compris entre 1 et 255. La valeur par défaut est de 1 seconde.

Interface IP Address (Adresse IP de l'interface) : indique l'adresse IP associée à l'interface sélectionnée.

IP Address (Adresse IP) : entrez l'adresse IP associée au routeur virtuel. La valeur par défaut est 0.0.0.0, que vous devez modifier avant d'appuyer sur **Create** (Créer).

Authentication Type (Type d'authentification) : sélectionnez le type d'authentification associé au routeur virtuel dans le menu déroulant. La valeur par défaut est **None** (Aucun). Les choix possibles sont les suivants :

- 1 **0-None** (0-Aucune) : aucune authentification n'est effectuée.
- 1 **1-Simple** : l'authentification est effectuée à l'aide d'un mot de passe textuel.

Authentication Data (Données d'authentification) : si vous avez choisi l'authentification simple, entrez le mot de passe.

Status (État) : sélectionnez **Active** (Actif) ou **Inactive** (Inactif) dans le menu déroulant ou arrêtez le fonctionnement du routeur virtuel. La valeur par défaut est **Inactive** (Inactif).

Pour configurer une deuxième adresse VRRP, vous devez d'abord configurer une adresse IP (adresse principale) pour le routeur virtuel. Vous pouvez ensuite ajouter plusieurs adresses secondaires à cette interface.

Création d'un routeur virtuel

1. Affichez la page **Virtual Router Configuration** (Configuration du routeur virtuel).
2. Sélectionnez **Create** (Créer) dans le menu déroulant associé au champ **VRID and Interface** (VRID et interface).
3. Indiquez le VRID et l'interface associés au nouveau routeur virtuel.
4. Complétez les autres champs, le cas échéant.
5. Cliquez sur **Create** (Créer).

Le nouveau routeur virtuel est enregistré et le périphérique est mis à jour.

Configuration d'un routeur virtuel

1. Affichez la page **Virtual Router Configuration** (Configuration du routeur virtuel).
2. Sélectionnez le VRID et l'interface du routeur virtuel à configurer.
3. Modifiez les champs au besoin.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration est enregistrée et le périphérique est mis à jour.

Configuration d'un routeur virtuel à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 **Virtual Router Redundancy Protocol Commands** (Commandes VRRP)

État du routeur virtuel

La page **Virtual Router Status** (État du routeur virtuel) permet d'afficher l'état d'un routeur virtuel.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **VRRP** → **Virtual Router Status** (État du routeur virtuel) dans l'arborescence.

Figure 10-40. Page Virtual Router Status (État du routeur virtuel)

VRID	VLANID	Priority	Preempt Mode	Advertisement Interval (secs)	Virtual Ip Address	Interface Ip Address	Owner	VMAC Address
20	vlan200	4	Enable	1	10.50.50.50	192.168.30.15	False	00:00:5E:00:01:20
110	vlan300	80	Disable	30	10.50.50.52	0.0.0.0	False	00:00:5E:00:01:110

Cette page contient les champs suivants :

VRID : identificateur du routeur virtuel.

VLANID : indique l'interface associée au VRID.

Priority (Priorité) : valeur de priorité utilisée par le routeur VRRP dans le choix du routeur virtuel maître.

Pre-empt Mode (Mode préemption)

- 1 **Enable (Activer)** : si le routeur virtuel est un routeur de sauvegarde, il devance le routeur maître si sa priorité est supérieure et si le routeur maître n'est pas le propriétaire de l'adresse IP du routeur virtuel.
- 1 **Disable (Désactiver)** : si le routeur virtuel est un routeur de sauvegarde, il ne devance pas le routeur maître même si sa priorité est supérieure.

Advertisement Interval (secs) (Intervalle d'annonce [secondes]) : durée en secondes entre la transmission des paquets d'annonces par ce routeur virtuel.

Virtual IP Address (Adresse IP virtuelle) : adresse IP associée au routeur virtuel.

Interface IP Address (Adresse IP de l'interface) : adresse IP réelle associée à l'interface utilisée par le routeur virtuel.

Owner (Propriétaire) : affectez la valeur True (Vrai) à ce champ si l'adresse IP virtuelle et celle de l'interface sont identiques. Sinon, affectez-lui la valeur False (Faux). Si ce paramètre a la valeur True (Vrai), le routeur virtuel est le propriétaire de l'adresse IP virtuelle, et il est toujours choisi comme routeur maître lorsqu'il est activé.

VMAC Address (Adresse VMAC) : adresse MAC virtuelle associée au routeur virtuel, qui comprend un identificateur unique de 24 bits, la constante de 16 bits identifiant le bloc d'adresses VRRP et le VRID de 8 bits. Elle se présente sous la forme 00:00:5e:00:01:XX, XX désignant le VRID.

Auth Type (Type d'authentification) : type d'authentification utilisé pour le routeur virtuel

- 1 **None (Aucun)** : indique qu'aucun type d'authentification n'est défini.
- 1 **Simple** : indique que le type d'authentification est un mot de passe textuel simple.

State (État) : état actuel du routeur virtuel :

- 1 **Initialize (Initialisation)**
- 1 **Master (Maître)**
- 1 **Backup (Sauvegarde)**

Status (Statut) : statut actuel du routeur virtuel :

- 1 **Inactive (Inactif)**
- 1 **Active (Actif)**

Secondary IP Address (Adresse IP secondaire) : adresse VRRP secondaire configurée pour le routeur VRRP maître.

Affichage de l'état du routeur virtuel à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

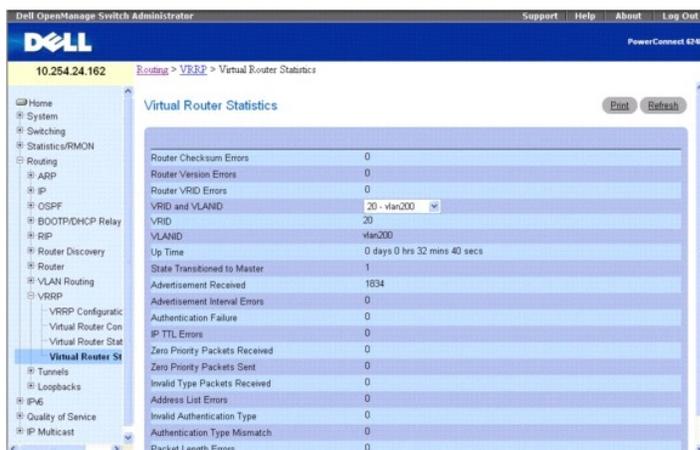
- 1 Virtual Router Redundancy Protocol Commands (Commandes VRRP)

Statistiques du routeur virtuel

La page **Virtual Router Statistics** (Statistiques du routeur virtuel) permet d'afficher les statistiques d'un routeur virtuel.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **VRRP** → **Virtual Router Statistics** (Statistiques d'un routeur virtuel) dans l'arborescence.

Figure 10-41. Page Virtual Router Statistics (Statistiques du routeur virtuel)



La page **Virtual Router Statistics** (Statistiques d'un routeur virtuel) contient les champs énumérés ci-dessous. Une grande partie de ces champs ne s'affiche que si une configuration VRRP correcte a été définie.

Router Checksum Errors (Erreurs de somme de contrôle du routeur) : nombre total de paquets VRRP reçus dont la valeur de somme de contrôle VRRP est incorrecte.

Router Version Errors (Erreurs de version du routeur) : nombre total de paquets VRRP reçus dont le numéro de version est inconnu ou n'est pas pris en charge.

Router VRID Errors (Erreurs de VRID du routeur) : nombre total de paquets VRRP reçus dont le VRID est incorrect pour ce routeur virtuel.

VRID and VLAN ID (VRID et ID du VLAN) : sélectionnez le routeur virtuel existant, répertorié par numéro d'interface et VRID, dont vous voulez afficher les statistiques.

VRID : VRID du routeur virtuel sélectionné.

VLAN ID (ID du VLAN) : interface du routeur virtuel sélectionné.

Up Time (Durée) : temps écoulé en jours, heures, minutes et secondes, depuis le passage du routeur virtuel en mode initialisé.

State Transitioned to Master (Passage en mode maître) : nombre total de passages en mode maître effectués par le routeur virtuel.

Advertisement Received (Annonces reçues) : nombre total d'annonces VRRP reçues par ce routeur virtuel.

Advertisement Interval Errors (Erreurs d'intervalle d'annonce) : nombre total de paquets VRRP reçus pour lesquels l'intervalle d'annonce est différent de celui configuré pour le routeur virtuel local.

Authentication Failure (Échec de l'authentification) : nombre total de paquets VRRP reçus qui n'ont pas réussi le contrôle d'authentification.

IP TTL Errors (Erreurs de TTL IP) : nombre total de paquets VRRP reçus par le routeur virtuel dont la valeur IP TTL (Durée de vie) n'est pas définie sur 255.

Zero Priority Packets Received (Paquets de priorité nulle reçus) : nombre total de paquets VRRP reçus par le routeur virtuel dont la priorité a la valeur 0.

Zero Priority Packets Sent (Paquets de priorité nulle envoyés) : nombre total de paquets VRRP envoyés par le routeur virtuel dont la priorité a la valeur 0.

Invalid Type Packets Received (Paquets de type incorrect reçus) : nombre de paquets VRRP reçus par le routeur virtuel dont le champ Type a une valeur incorrecte.

Address List Errors (Erreurs de liste d'adresses) : nombre total de paquets reçus dont la liste d'adresses ne correspond pas à la liste configurée localement pour le routeur virtuel.

Invalid Authentication Type (Type d'authentification incorrect) : nombre total de paquets reçus dont le type d'authentification est inconnu.

Authentication Type Mismatch (Type d'authentification incompatible) : nombre total de paquets reçus dont le type d'authentification est différent du mode d'authentification configuré localement.

Packet Length Errors (Erreurs de longueur de paquet) : nombre total de paquets reçus dont la longueur est inférieure à celle de l'en-tête VRRP.

Affichage des statistiques du routeur virtuel

1. Affichez la page **Virtual Router Statistics** (Statistiques du routeur virtuel).
2. Sélectionnez le routeur virtuel pour lequel vous souhaitez afficher des statistiques par rapport aux champs **VRID** et **VLANID**. Ces informations ne

s'affichent que si une configuration VRRP correcte a été définie.

Affichage des statistiques du routeur virtuel à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 Virtual Router Redundancy Protocol Commands (Commandes VRRP)

Tunnels

Les systèmes de la série 6200 prennent en charge la création, la suppression et la gestion des interfaces de tunnel. Ces interfaces dynamiques sont créées et supprimées par le biais d'une configuration utilisateur.

Il existe deux catégories de tunnels qui facilitent le passage d'un réseau IPv4 à un réseau IPv6 : les tunnels configurés et les tunnels automatiques. La différence réside dans le fait que les tunnels configurés sont explicitement configurés avec une destination ou un point de terminaison du tunnel. En revanche, les tunnels automatiques infèrent le point de terminaison du tunnel à partir de l'adresse de destination des paquets routés dans le tunnel.

Les systèmes de la série 6200 prennent en charge les tunnels point à point. Les interfaces point à point prennent en charge le routage basé uniquement sur l'interface (il n'est pas nécessaire d'indiquer une adresse de saut suivant explicite), et permettent de définir des interfaces non numérotés.

La page de menu **Tunnels** contient des liens vers les pages Web permettant de configurer et d'afficher les paramètres et les données des tunnels. Pour afficher cette page, cliquez sur **Routing** (Routage) → **Tunnels** dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

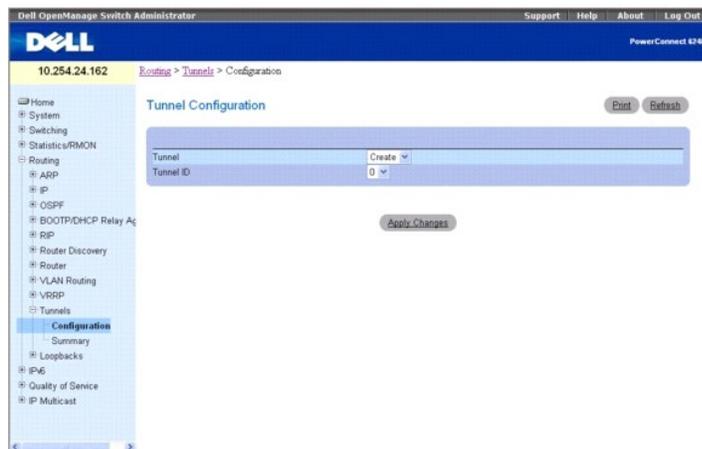
- 1 [Configuration des tunnels](#)
- 1 [Récapitulatif des tunnels](#)

Configuration des tunnels

La page **Tunnels Configuration** (Configuration des tunnels) permet de créer, de configurer et de supprimer un tunnel.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **Tunnels** → **Configuration** dans l'arborescence.

Figure 10-42. Page Tunnels Configuration (Configuration des tunnels)



Cette page contient les champs suivants :

Tunnel : utilisez le menu déroulant pour sélectionner un tunnel dans la liste des ID de tunnel actuellement configurés. Vous pouvez également utiliser l'option Create (Créer) si le nombre maximum d'interfaces de tunnel n'a pas été configuré.

Tunnel ID (ID du tunnel) : lorsque vous cliquez sur Create (Créer) dans le sélecteur de tunnel, la liste des ID de tunnel disponibles apparaît. Vous devez sélectionner un ID de tunnel à associer au nouveau tunnel et cliquer sur **Apply Changes** (Appliquer les modifications) pour que les autres champs de la page s'affichent.

Mode : sélecteur du mode Tunnel. L'option IPv6-in-IPv4 (IPv6-en-IPv4) est l'unique mode pris en charge.

Link Local Only Mode (Mode Liaison locale uniquement) : permet d'activer IPv6 sur cette interface à l'aide de l'adresse de liaison locale. Cette option doit être configurée avant de définir une adresse IPv6 explicite.

IPv6 Address (Adresse IPv6) : sélectionnez une adresse IPv6 pour l'interface de tunnel sélectionnée. Vous pouvez également utiliser l'option Add (Ajouter) si le nombre maximum d'adresses n'a pas été configuré.

IPv6 Address (Adresse IPv6) : lorsque vous cliquez sur Add (Ajouter) dans le sélecteur d'adresse IPv6, ce champ de saisie apparaît. Le format de l'adresse est préfixe/longueur.

Vous avez également la possibilité de définir l'identificateur unique étendu de 64 bits (EUI-64).

Source : sélectionnez la source de votre choix, IPv4 Address (Adresse IPv4) ou Interface. Si l'option Address (Adresse) est sélectionnée, l'adresse source de ce tunnel doit être saisie en notation à points décimaux. Si l'option Interface est sélectionnée, l'interface source de ce tunnel doit être sélectionnée. L'adresse associée à l'interface sélectionnée sert d'adresse source.

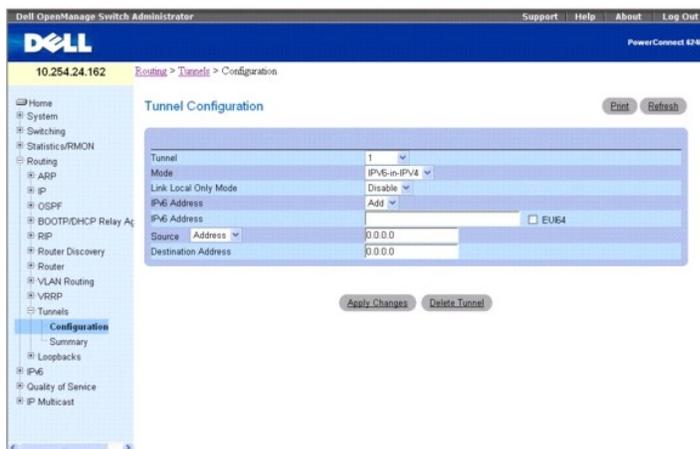
Destination Address (Adresse de destination) : adresse de destination IPv4 associée à ce tunnel, en notation décimale à points.

Création d'un tunnel

1. Affichez la page **Tunnels Configuration** (Configuration des tunnels).
2. Sélectionnez **Create** (Créer) dans le menu déroulant associé au champ **Tunnel**.
3. Entrez l'ID à utiliser dans le champ **Tunnel ID** (ID du tunnel).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le champ Tunnel ID (ID du tunnel) est supprimé et les autres champs s'affichent.

Figure 10-43. Entrée de la page Tunnel Configuration (Configuration d'un tunnel)



5. Configurez les champs si nécessaire.
6. Entrez les valeurs de votre choix dans les autres champs.
7. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau tunnel est enregistré et le périphérique est mis à jour.

Modification d'un tunnel existant

1. Affichez la page **Tunnels Configuration** (Configuration des tunnels).
2. Sélectionnez le tunnel à modifier dans le menu déroulant associé au champ **Tunnel**.
3. Modifiez les valeurs des autres champs si nécessaire.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle configuration est enregistrée et le périphérique est mis à jour.

Suppression d'un tunnel

1. Affichez la page **Tunnels Configuration** (Configuration des tunnels).

2. Sélectionnez le tunnel à supprimer dans le menu déroulant associé au champ **Tunnel**.
3. Cliquez sur **Delete Tunnel** (Supprimer le tunnel).

Le tunnel est supprimé et le périphérique est mis à jour.

Configuration d'un tunnel à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 Tunnel Interface Commands (Commandes portant sur les interfaces de tunnel)

Récapitulatif des tunnels

La page **Tunnels Summary** (Récapitulatif des tunnels) permet d'afficher le récapitulatif des tunnels configurés.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **Tunnels** → **Summary** (Récapitulatif) dans l'arborescence.

Figure 10-44. Page **Tunnels Summary** (Récapitulatif des tunnels)

Tunnel ID	Mode	Address	Source	Destination
1	IPv6-to-IPv4	3FFE.FFFF:100:F101::64 [TENT]	192.168.22.6	192.168.57.25
2	IPv6-to-IPv4	3FFE.FFFF:100:F102::64 [TENT]	192.168.22.12	192.168.57.151

Cette page contient les champs suivants :

Tunnel ID (ID du tunnel) : ID correspondant au tunnel.

Mode : mode correspondant au tunnel.

Address (Adresse) : adresse(s) IPv6 du tunnel.

Source : adresse source associée au tunnel. Si une interface a été configurée, l'interface et l'adresse s'affichent. Si aucune adresse n'est configurée pour l'interface source, le texte Unconfigured (Non configuré) s'affiche à la place de l'adresse.

Destination : adresse de destination associée au tunnel.

Affichage du récapitulatif des tunnels à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 Tunnel Interface Commands (Commandes portant sur les interfaces de tunnel)

Boucles de rappel

Les systèmes de la série 6200 prennent en charge la création, la suppression et la gestion des interfaces de boucle de rappel. Ces interfaces dynamiques sont créées et supprimées par le biais d'une configuration utilisateur. Les systèmes de la série 6200 prennent en charge plusieurs interfaces de boucle de rappel.

Une interface de boucle de rappel est toujours supposée être active. De ce fait, elle permet de configurer une adresse IP stable sur l'unité, à laquelle les autres commutateurs peuvent se référer. Cette interface définit l'adresse source des paquets envoyés, et peut recevoir des paquets locaux et distants. Elle est généralement utilisée par les protocoles de routage.

La boucle de rappel ne se comporte pas comme le port réseau d'un système de commutation. En particulier, une interface de boucle de rappel ne contient pas de routeurs voisins. Il s'agit d'un pseudo périphérique d'affectation d'adresses locales permettant au routeur de communiquer à l'aide de cette adresse, qui

est toujours activé et peut recevoir le trafic provenant des interfaces actives existantes. Ainsi, en supposant que l'accessibilité à partir d'un client distant est activée, l'adresse de la boucle de rappel permet de communiquer avec le routeur par le biais de divers services tels que telnet et ssh. L'adresse d'une boucle de rappel a un comportement identique aux adresses locales du routeur en ce qui concerne le traitement des paquets entrants.

La page de menu **Loopbacks** (Boucles de rappel) contient des liens vers les pages Web permettant de configurer et d'afficher les paramètres et les données de boucle de rappel. Pour afficher cette page, cliquez sur **Routing** (Routage) → **Loopbacks** (Boucles de rappel) dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

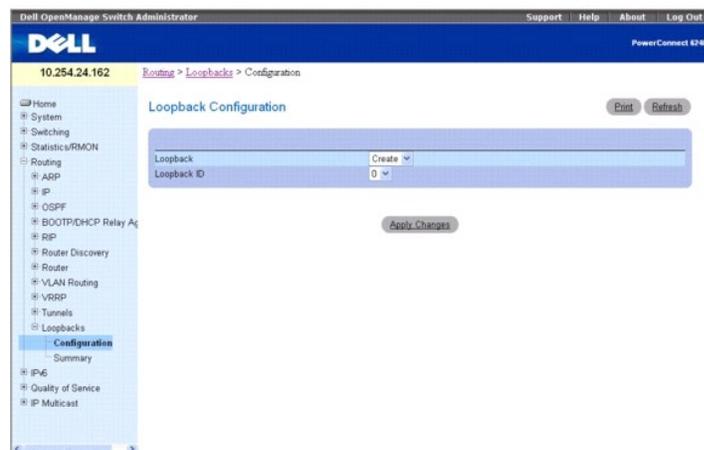
- 1 Configuration des boucles de rappel
- 1 Récapitulatif des boucles de rappel

Configuration des boucles de rappel

La page **Loopbacks Configuration** (Configuration des boucles de rappel) permet de créer, de configurer et de supprimer une interface de boucle de rappel. Vous pouvez également configurer ou supprimer une adresse secondaire associée à une boucle de rappel.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **Loopbacks** (Boucles de rappel) → **Configuration** dans l'arborescence.

Figure 10-45. Page Loopback Configuration (Configuration des boucles de rappel)



Cette page contient les champs suivants :

Loopback (Boucle de rappel) : utilisez le menu déroulant pour sélectionner une boucle de rappel dans la liste des interfaces de boucle de rappel actuellement configurées. Vous pouvez également utiliser l'option **Create** (Créer) si le nombre maximum d'interfaces de boucle de rappel n'a pas été configuré.

Loopback ID (ID de boucle de rappel) : lorsque vous cliquez sur **Create** (Créer) dans le champ **Loopback** (Boucle de rappel), la liste des ID de boucle de rappel disponibles apparaît.

Protocol (Protocole) : sélectionnez IPv4 ou IPv6 pour configurer les attributs associés de l'interface de boucle de rappel. Le protocole sélectionné affecte les champs qui s'affichent sur ce page.

Link Local Only Mode (Mode Liaison locale uniquement) : permet d'activer IPv6 sur cette interface à l'aide de l'adresse de liaison locale. Cette option ne s'affiche que si IPv6 est défini comme protocole, et doit être configurée avant de définir une adresse IPv6 explicite.

IPv6 Address (Adresse IPv6) : sélectionnez la liste des adresses IPv6 configurées pour l'interface de boucle de rappel sélectionnée. Vous pouvez également utiliser l'option **Add** (Ajouter) si le nombre maximum d'adresses n'a pas été configuré. Cette option ne s'affiche que si IPv6 est défini comme protocole.

IPv6 Address (Adresse IPv6) : lorsque vous cliquez sur **Add** (Ajouter) dans le sélecteur d'adresse IPv6, ce champ de saisie apparaît. Le format de l'adresse est préfixe/longueur. Cette option ne s'affiche que si IPv6 est défini comme protocole.

EU164 : vous avez également la possibilité de définir l'identificateur unique étendu de 64 bits (EUI-64). Cette option ne s'affiche que si IPv6 est défini comme protocole.

IPv4 Address (Adresse IPv4) : adresse IPv4 principale associée à cette interface, en notation décimale à points. Cette option ne s'affiche que si IPv4 est défini comme protocole.

IPv4 Subnet Mask (Masque de sous-réseau IPv4) : masque de sous-réseau IPv4 principal associé à cette interface en notation à points décimaux. Cette option ne s'affiche que si IPv4 est défini comme protocole.

Les champs suivants s'affichent lorsqu'une adresse principale est configurée. Vous pouvez configurer plusieurs adresses secondaires.

Secondary Address (Adresse secondaire) : sélectionnez dans le menu déroulant une adresse secondaire IPv4 configurée pour l'interface de boucle de rappel sélectionnée. Vous pouvez saisir une nouvelle adresse dans le champ **Secondary IP Address** (Adresse IP secondaire) en sélectionnant l'option **Add Secondary IP Address** (Ajouter une adresse IP secondaire) si le nombre maximum d'adresses secondaires n'a pas été configuré. Une adresse principale doit être configurée avant d'ajouter une adresse secondaire.

Secondary IP Address (Adresse IP secondaire) : adresse IP secondaire associée à cette interface en notation à points décimaux. Ce champ de saisie ne s'affiche que si l'option **Add Secondary** (Ajouter une adresse secondaire) est sélectionnée.

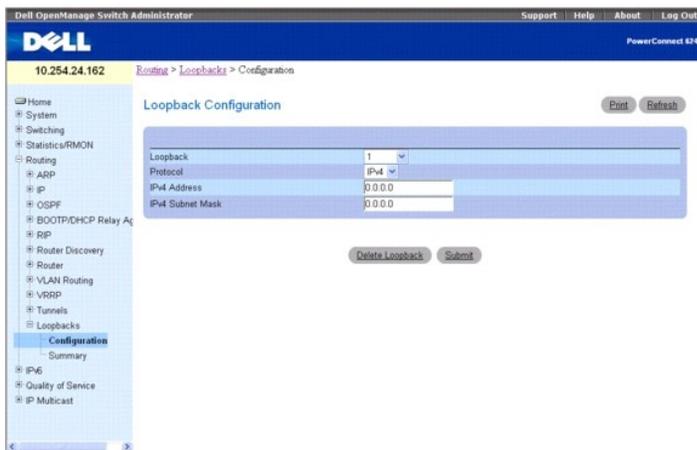
Secondary Subnet Mask (Masque de sous-réseau secondaire) : masque de sous-réseau secondaire associé à cette interface en notation à points décimaux. Ce champ de saisie ne s'affiche que si l'option **Add Secondary** (Ajouter une adresse secondaire) est sélectionnée.

Création d'une boucle de rappel (IPv4)

1. Affichez la page **Loopbacks Configuration** (Configuration des boucles de rappel).
2. Sélectionnez **Create** (Créer) dans le menu déroulant associé au champ **Loopback** (Boucle de rappel).
3. Entrez l'ID à utiliser dans le champ **Loopback ID** (ID de boucle de rappel).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le champ Loopback ID (ID de boucle de rappel) disparaît et les autres champs s'affichent.

Figure 10-46. Page Loopback Configuration (Configuration d'une boucle de rappel) - Entrée IPv4



5. Entrez **IPv4** dans le champ **Protocol** (Protocole).
6. Entrez les valeurs de votre choix dans les autres champs.
7. Cliquez sur **Submit** (Soumettre).

La nouvelle boucle de rappel est enregistrée et la page Web réapparaît, en affichant les champs de configuration de l'adresse secondaire.

Figure 10-47. Page Loopback Configuration (Configuration d'une boucle de rappel) - Ajout d'une adresse secondaire



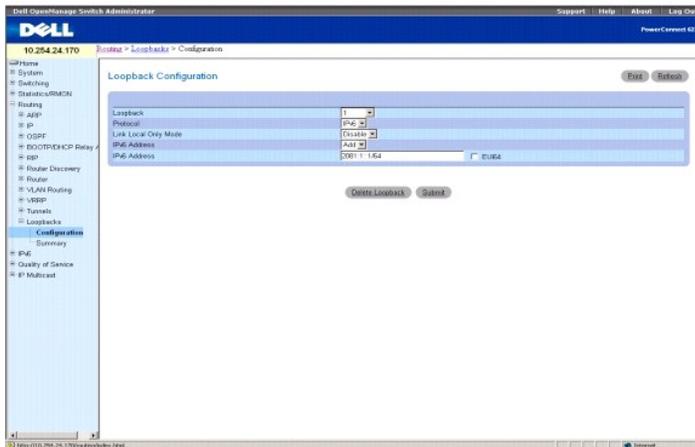
8. Renseignez les champs **Secondary Address** (Adresse secondaire), **Secondary IP Address** (Adresse IP secondaire) et **Secondary Subnet Mask** (Masque de sous-réseau secondaire).
9. Cliquez sur le bouton **Add Secondary** (Ajouter une adresse secondaire). L'adresse secondaire est enregistrée et la page Web apparaît de nouveau avec les adresses de boucle de rappel principale et secondaire.

Création d'une boucle de rappel (IPv6)

1. Affichez la page **Loopbacks Configuration** (Configuration des boucles de rappel).
2. Sélectionnez **Create** (Créer) dans le menu déroulant associé au champ **Loopback** (Boucle de rappel).
3. Entrez l'ID à utiliser dans le champ **Loopback ID** (ID de boucle de rappel).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le champ Loopback ID (ID de boucle de rappel) disparaît et les autres champs s'affichent.

Figure 10-48. Page Loopback Configuration (Configuration d'une boucle de rappel) - Entrée IPv6



5. Sélectionnez **IPv6** dans la zone de liste déroulante associée au champ **Protocol** (Protocole).
6. Ajoutez l'**adresse IPv6**.
7. Entrez les valeurs de votre choix dans les autres champs.
8. Cliquez sur **Submit** (Soumettre).

La nouvelle boucle de rappel est enregistrée et le périphérique est mis à jour.

Configuration d'une boucle de rappel existante

1. Affichez la page **Loopback Configuration** (Configuration des boucles de rappel).
2. Sélectionnez la boucle de rappel à configurer dans le menu déroulant associé au champ **Loopback** (Bouche de rappel).
3. Modifiez les valeurs des autres champs si nécessaire.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle configuration est enregistrée et le périphérique est mis à jour.

Suppression d'une boucle de rappel

1. Affichez la page **Loopback Configuration** (Configuration des boucles de rappel).
2. Sélectionnez la boucle de rappel à supprimer dans le menu déroulant associé au champ **Loopback** (Bouche de rappel).
3. Cliquez sur **Delete Loopback** (Supprimer la boucle de rappel).

La boucle de rappel est supprimée et le périphérique est mis à jour.

Suppression d'une adresse secondaire

1. Affichez la page **Loopback Configuration** (Configuration des boucles de rappel).
2. Indiquez la boucle de rappel concernée.
3. Indiquez l'adresse secondaire à supprimer.
4. Cliquez sur **Delete Selected Secondary** (Supprimer l'adresse secondaire sélectionnée).

L'adresse secondaire est supprimée et le périphérique est mis à jour.

Configuration d'une boucle de rappel à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous aux chapitres suivants du document *CLI Reference Guide* (Guide de référence CLI) :

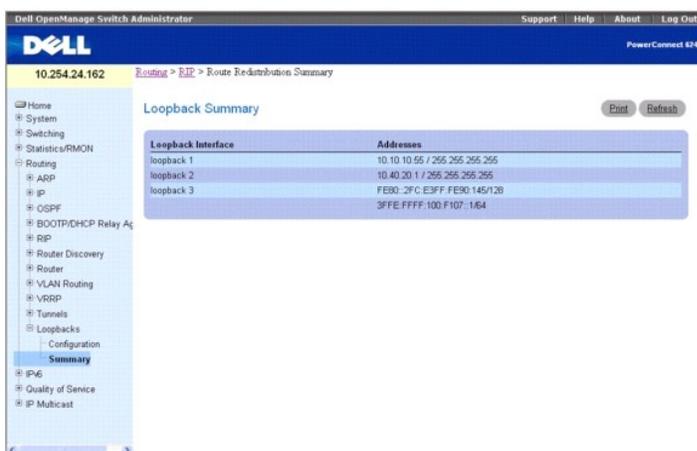
- 1 Loopback Interface Commands (Commandes de l'interface de boucle de rappel)
- 1 IP Addressing Commands (Commandes d'adressage IP)
- 1 IPv6 Routing Commands (Commandes de routage IPv6)

Récapitulatif des boucles de rappel

La page **Loopbacks Summary** (Récapitulatif des boucles de rappel) permet d'afficher le récapitulatif des boucles de rappel configurées.

Pour afficher cette page, cliquez sur **Routing** (Routage) → **Loopbacks** (Boucles de rappel) → **Summary** (Récapitulatif) dans l'arborescence.

Figure 10-49. Page **Loopbacks Summary** (Récapitulatif des boucles de rappel)



Loopback Interface	Addresses
loopback 1	10.10.10.55 / 255.255.255.255
loopback 2	10.40.20.1 / 255.255.255.255
loopback 3	FE80::2FC:E3FF:FE90:145/128 3FFE:FFFF:100:F107:164

Cette page contient les champs suivants :

Loopback Interface (Interface de boucle de rappel) : ID de l'interface de boucle de rappel configurée.

Addresses (Adresses) : liste des adresses configurées sur l'interface de boucle de rappel.

Affichage du récapitulatif des boucles de rappel à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 Loopback Interface Commands (Commandes de l'interface de boucle de rappel)

[Retour au sommaire](#)

[Retour au sommaire](#)

Configuration d'IPv6

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Configuration globale](#)
- [Configuration des interfaces](#)
- [Récapitulatif des interfaces](#)
- [Statistiques IPv6](#)
- [Table des voisins IPv6](#)
- [DHCPv6](#)
- [OSPFv3](#)
- [Itinéraires IPv6](#)

IPv6 représente la dernière génération de protocoles Internet. Avec des adresses 128 bits, contre 32 bits pour IPv4, IPv6 résout les problèmes de réduction du nombre d'adresses qui caractérisent IPv4. En outre, ce protocole supprime l'obligation de traduire les adresses réseau (NAT - Network Address Translation), conversion utilisée dans les réseaux IPv4 pour réduire le nombre d'adresses IP spécifiques à l'échelle internationale requises pour un réseau donné. Ce mécanisme d'agrégation peut réduire considérablement la taille de la table de routage globale via des combinaisons d'adresses connues. La sécurité est plus intégrée et la configuration du réseau est simplifiée mais également plus flexible.

Dans les systèmes de la série 6200, le protocole IPv6 coexiste avec le protocole IPv4. Comme avec IPv4, le routage IPv6 peut être activé sur les interfaces de boucle de rappel et de VLAN. Chaque interface de routage L3 peut être utilisée pour IPv4, IPv6 ou les deux. Les protocoles IP qui s'exécutent sous L3 (par exemple, UDP et TCP) ne changent pas avec IPv6. C'est la raison pour laquelle une seule pile de processeurs est utilisée pour le transport d'IPv4 et d'IPv6, et une interface unique de supports fournit l'accès aux deux réseaux. Les protocoles de routage peuvent calculer les itinéraires pour l'une ou les deux versions IP.

La page **IPv6** contient des liens vers les fonctionnalités suivantes :

- 1 [Configuration globale](#)
- 1 [Configuration des interfaces](#)
- 1 [Récapitulatif des interfaces](#)
- 1 [Statistiques IPv6](#)
- 1 [Table des voisins IPv6](#)
- 1 [DHCPv6](#)
- 1 [OSPFv3](#)
- 1 [Routes IPv6](#)

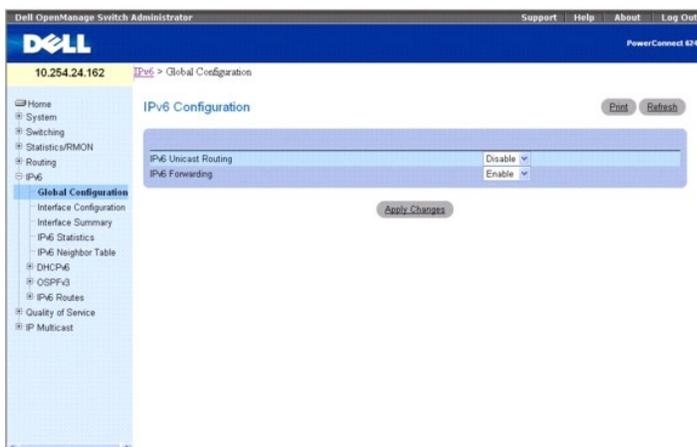
 **REMARQUE :** Certaines pages IPv6 ne correspondent à aucune commande CLI.

Configuration globale

La page **Global Configuration** (Configuration globale) permet d'activer le transfert IPv6 sur le routeur, ainsi que le transfert des datagrammes de monodiffusion IPv6.

Pour afficher cette page, cliquez sur **IPv6** → **Global Configuration** (Configuration globale) dans l'arborescence.

Figure 11-1. Configuration IPv6 globale



Cette page contient les champs suivants :

IPv6 Unicast Routing (Routage de monodiffusion IPv6) : active ou désactive globalement le routage de monodiffusion IPv6 sur le routeur. La valeur par défaut est Disable (Désactiver).

IPv6 Forwarding (Transfert IPv6) : active ou désactive le transfert des trames IPv6 sur le routeur. La valeur par défaut est Enable (Activer).

Configuration des paramètres IPv6

1. Affichez la page **IPv6 Global Configuration** (Configuration globale IPv6).
2. Activez ou désactivez le routage de monodiffusion dans le menu déroulant.
3. Activez ou désactivez le transfert des trames IPv6 dans le menu déroulant.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont enregistrés et le périphérique est mis à jour.

Configuration d'IPv6 à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 IPv6 Routing Commands (Commandes de routage IPv6)

Configuration des interfaces

La page **Interface Configuration** (Configuration des interfaces) permet de configurer les paramètres des interfaces IPv6.

Pour afficher cette page, cliquez sur **IPv6** → **Interface Configuration** (Configuration des interfaces) dans l'arborescence.

Figure 11-2. Page IPv6 Interface Configuration (Configuration des interfaces IPv6)

Field	Value
Interface	vlan1
IPv6 Mode	Disable
IPv6 Prefix	Add <input type="text"/> Delete <input type="checkbox"/> EUI64 <input type="checkbox"/>
Valid Lifetime by Prefix	0 (0 to 4294967296)
Preferred Lifetime by Prefix	0 (0 to 4294967296)
Onlink Flag by Prefix	Enable
Autonomous Flag by Prefix	Enable
Current State by Prefix	Disable
Routing Mode	Disable
IPv6 Routing Operational Mode	Disable
Interface Maximum Transmit Unit	0 (1280 to 1500) Enter 0 to unconfigure
Router Duplicate Address Detection Transmits	1 (0 to 600)
Router Advertisement NS Interval	0 (1000 to 4294967296) Enter 0 to unconfigure
Router Lifetime Interval	1800 (0 to 9000)
Router Advertisement Reachable Time	0 (0 to 3600000)
Router Advertisement Interval	600 (4 to 1000)
Router Advertisement Managed Config Flag	Disable
Router Advertisement Other Config Flag	Disable
Router Advertisement Suppress Flag	Disable

Cette page contient les champs suivants :

Interface : permet de sélectionner l'interface à configurer. Lorsque la sélection est modifiée, l'écran est réactualisé et tous les champs sont mis à jour en fonction du nouveau port. Ce champ affiche uniquement les interfaces et les tunnels prenant en charge le routage.

IPv6 Mode (Mode IPv6) : lorsque le mode IPv6 est activé, l'interface peut fonctionner en IPv6 sans adresse globale. Dans ce cas, une adresse locale-liaison EUI-64 est utilisée. Ce sélecteur répertorie les deux options pour le mode IPv6 : Enable (Activer) et Disable (Désactiver). La valeur par défaut est Disable (Désactiver).

IPv6 Prefix (Préfixe IPv6) : choisissez d'ajouter ou de supprimer un préfixe IPv6 sur cette interface. Si vous ajoutez un préfixe, indiquez-le dans le champ IPv6 Prefix (Préfixe IPv6) suivant. L'option Delete (Supprimer) permet de supprimer le préfixe IPv6 affiché.

IPv6 Prefix (Préfixe IPv6) : indique le préfixe IPv6 et sa longueur pour une interface donnée. Lorsque la sélection est modifiée, l'écran est réactualisé. Par ailleurs, la durée de vie valide, la durée de vie préférée, l'indicateur de liaison activée et l'indicateur autonome sont mis à jour en fonction de l'adresse IPv6 choisie.

EUI-64 : si cette option est cochée, elle indique le préfixe de monodiffusion 64 bits.

Valid Lifetime by Prefix (Durée de vie valide par préfixe) : valeur, en secondes, devant être saisie dans le champ **Valid Lifetime** (Durée de vie valide) de l'option **Prefix Information** (Informations sur le préfixe) dans l'annonce du routeur. Ce préfixe est valide pour la détermination de liaison activée, et uniquement pour la durée indiquée. Pendant cette durée, les systèmes hôtes qui utilisent la configuration automatique d'adresses sans état pour générer une adresse à partir de ce préfixe peuvent utiliser ces adresses. Les adresses configurées automatiquement et dont l'ancienneté est supérieure à la durée de vie préférée, mais inférieure à la durée de vie valide sont considérées comme "désapprouvées". Dans la norme RFC 2462, une adresse "désapprouvée" est une adresse attribuée à une interface dont l'utilisation est déconseillée, mais pas interdite. Une adresse désapprouvée ne doit plus être utilisée comme adresse source pour de nouvelles communications, mais les paquets envoyés à partir de ce type d'adresse ou à ce type d'adresses sont cependant livrés. Une adresse désapprouvée peut continuer à être utilisée comme adresse source dans les communications pour lesquelles le basculement vers une adresse préférée

compromet une activité de couche supérieure spécifique (par exemple, une liaison TCP existante). Les valeurs admises sont comprises entre 0 et 4294967295 secondes.

Preferred Lifetime by Prefix (Durée de vie préférée par préfixe) : valeur, en secondes, devant être saisie dans le champ **Preferred Lifetime** (Durée de vie préférée) de l'option **Prefix Information** (Informations sur le préfixe) dans une annonce de routeur. Les adresses générées à partir d'un préfixe à l'aide de la configuration automatique d'adresses sans état restent des adresses "préférées" pendant la durée indiquée. Dans la norme RFC 2462, une adresse "préférée" est une adresse attribuée à une interface dont l'utilisation par les protocoles de couche supérieure n'est pas limitée. Les adresses préférées peuvent être utilisées comme source ou comme cible des paquets envoyés à l'interface ou à partir de l'interface. Les valeurs admises sont comprises entre 0 et 4294967295 secondes.

Onlink Flag by Prefix (Indicateur de liaison activée par préfixe) : indique le préfixe choisi qui peut être utilisé pour la détermination de liaison activée. La valeur par défaut est Enable (Activer). Ce sélecteur répertorie les deux options pour l'indicateur de liaison activée : Enable (Activer) et Disable (Désactiver).

Autonomous Flag by Prefix (Indicateur autonome par préfixe) : indique le préfixe choisi qui peut être utilisé pour la configuration d'adresse autonome. La valeur par défaut est Disable (Désactiver). Ce sélecteur répertorie les deux options pour l'indicateur autonome : Enable (Activer) et Disable (Désactiver).

Current State by Prefix (État actuel par préfixe) : état de fonctionnement de l'interface pour le préfixe IPv6 choisi.

Routing Mode (Mode de routage) : indique le mode de routage d'une interface. Ce sélecteur répertorie les deux options de mode de routage : Enable (Activer) et Disable (Désactiver). La valeur par défaut est Disable (Désactiver).

IPv6 Routing Operational Mode (Mode de fonctionnement du routage IPv6) : indique l'état de fonctionnement d'une interface. La valeur par défaut est Disable (Désactiver).

Interface Maximum Transmit Unit (Unité de transmission maximale d'une interface) : indique l'unité de transmission maximale sur une interface. Si la valeur est 0, l'interface ne prend pas en charge le routage. La valeur 0 n'est pas valide si le routage est pris en charge. Les valeurs autorisées pour l'unité de transmission maximale (MTU) sont comprises entre 1280 et 1500.

Router Duplicate Address Detection Transmits (Transmissions de détection d'adresses en double du routeur) : indique le nombre de transmissions de détection d'adresses en double sur une interface. Les valeurs de transmission DAD doivent être comprises entre 0 et 600.

Router Advertisement NS Interval (Intervalle de l'annonce du routeur) : indique la durée de retransmission de l'annonce du routeur envoyée depuis l'interface. Une valeur de 0 signifie qu'aucun intervalle n'est spécifié pour ce routeur. L'intervalle de sollicitation de voisinage est compris entre 1000 et 4294967295.

Router Lifetime Interval (Intervalle de durée de vie du routeur) : indique la durée de vie de l'annonce du routeur envoyée depuis l'interface. Cette valeur doit être supérieure ou égale à l'intervalle de l'annonce maximum. La valeur 0 indique que ce routeur n'est pas utilisé comme routeur par défaut. La durée de vie d'un routeur est comprise entre 0 et 9000.

Router Advertisement Reachable Time (Durée d'accessibilité de l'annonce du routeur) : indique le délai de l'annonce du routeur pendant lequel le voisin est considéré comme joignable après la confirmation de la détection du voisinage (ND). La durée d'accessibilité est comprise entre 0 et 3600000.

Router Advertisement Interval (Intervalle de l'annonce du routeur) : indique la durée maximale autorisée entre les envois d'annonces du routeur à partir de l'interface. La valeur par défaut est de 600. L'intervalle maximal de l'annonce du routeur est compris entre 4 et 1800.

Router Advertisement Managed Config Flag (Indicateur de configuration gérée de l'annonce du routeur) : spécifie l'indicateur de configuration des adresses gérées de l'annonce du routeur. Si le paramètre est vrai, les nœuds de terminaison utilisent DHCPv6. Si le paramètre est faux, les nœuds de terminaison configurent automatiquement les adresses. La valeur par défaut de l'indicateur de configuration gérée est Disable (Désactiver).

Router Advertisement Other Config Flag (Indicateur d'autre configuration de l'annonce du routeur) : spécifie l'indicateur de configuration des autres états de l'annonce du routeur. La valeur par défaut de l'indicateur d'autre configuration est Disable (Désactiver).

Router Advertisement Suppress Flag (Indicateur de suppression de l'annonce du routeur) : indique la suppression de l'annonce du routeur sur une interface. La valeur par défaut de l'indicateur de suppression est Disable (Désactiver).

Configuration des interfaces IPv6

1. Affichez la page **IPv6 Interface Configuration** (Configuration des interfaces IPv6).
2. Modifiez les champs selon vos besoins.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications de l'interface IPv6 sont enregistrées et le périphérique est mis à jour.

Configuration des interfaces IPv6 à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 IPv6 Routing Commands (Commandes de routage IPv6)

Récapitulatif des interfaces

La page **Interface Summary** (Récapitulatif des interfaces) permet d'afficher les paramètres de toutes les interfaces IPv6.

Pour afficher cette page, cliquez sur **IPv6** → **Interface Summary** (Récapitulatif des interfaces) dans l'arborescence.

Figure 11-3. Page IPv6 Interface Summary (Récapitulatif des interfaces IPv6)

Interface	Routing Mode	Admin Mode	Operational Mode	IPv6 Prefix/Prefix Length	State	IPv6 Address	State
1/g1	Disabled	Enabled	Disabled				
1/g2	Disabled	Enabled	Disabled				
1/g3	Disabled	Enabled	Disabled				
1/g4	Disabled	Enabled	Disabled				
1/g5	Disabled	Enabled	Disabled				
1/g6	Disabled	Enabled	Disabled				
1/g7	Disabled	Enabled	Enabled				
1/g8	Disabled	Enabled	Disabled				
1/g9	Disabled	Enabled	Enabled				
1/g10	Disabled	Enabled	Disabled				
1/g11	Disabled	Enabled	Enabled				
1/g12	Disabled	Enabled	Disabled				
1/g13	Disabled	Enabled	Enabled				
1/g14	Disabled	Enabled	Disabled				
1/g15	Disabled	Enabled	Enabled				
1/g16	Disabled	Enabled	Disabled				
1/g17	Disabled	Enabled	Enabled				
1/g18	Disabled	Enabled	Disabled				
1/g19	Disabled	Enabled	Enabled				
1/g20	Disabled	Enabled	Disabled				

Cette page contient les champs suivants :

Interface : indique l'interface dont les paramètres sont affichés dans la ligne du tableau actuellement sélectionnée.

Routing Mode (Mode de routage) : indique le mode de routage de l'interface.

Admin Mode (Mode d'administration) : indique le mode d'administration de l'interface.

Operational Mode (Mode de fonctionnement) : indique le mode de fonctionnement de l'interface.

IPv6 Prefix/PrefixLength (Préfixe IPv6/Longueur du préfixe) : indique les adresses IPv6 configurées sur l'interface.

State (État) : indique si l'interface est active ou non.

Affichage du récapitulatif de l'interface IPv6 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 IPv6 Routing Commands (Commandes de routage IPv6)

Statistiques IPv6

La page **IPv6 Statistics** (Statistiques IPv6) permet d'afficher les statistiques concernant les transferts IPv6 pour une ou toutes les interfaces.

Pour afficher cette page, cliquez sur **IPv6** → **IPv6 Statistics** (Statistiques IPv6) dans l'arborescence.

Figure 11-4. Page IPv6 Statistics (Statistiques IPv6)

Interface	Total Datagrams Received	Received Datagrams Locally Delivered	Received Datagrams Discarded Due To Header Errors	Received Datagrams Discarded Due To MTU	Received Datagrams Discarded Due To No Route	Received Datagrams With Unknown Protocol	Received Datagrams Discarded Due To Invalid Address	Received Datagrams Discarded Due To Truncated Data	Received Datagrams Discarded Other	Received Datagrams Reassembly Required	Datagrams Successfully Reassembled	Datagrams Failed To Reassemble	Datagrams Forwarded	Datagrams Locally Transmitted	Datagrams Transmit Failed
All	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Cette page contient les champs suivants :

Interface : sélectionne l'interface pour laquelle les statistiques sont affichées. Lorsque la sélection est modifiée, l'écran est réactualisé et tous les champs

sont mis à jour en fonction de la nouvelle interface.

Statistiques IPv6

Total Datagrams Received (Nombre total de datagrammes reçus) : nombre total de datagrammes entrants reçus par l'interface, y compris ceux contenant des erreurs.

Received Datagrams Locally Delivered (Nombre de datagrammes transmis localement) : nombre total de datagrammes transmis avec succès aux protocoles utilisateur IPv6 (y compris le protocole ICMP). Ce compteur est incrémenté à l'interface sur laquelle ces datagrammes étaient adressés, qui n'est pas nécessairement l'interface d'entrée de certains d'entre eux.

Received Datagrams Discarded Due To Header Errors (Datagrammes reçus rejetés en raison d'erreurs dans leurs en-têtes) : nombre de datagrammes entrants rejetés en raison d'erreurs dans leurs en-têtes IPv6, notamment des incohérences dans les numéros de version, d'autres erreurs de format, un nombre de sauts dépassé, des erreurs détectées durant le traitement des options IPv6, etc.

Received Datagrams Discarded Due To MTU (Datagrammes reçus rejetés en raison de l'unité de transmission maximale) : nombre de datagrammes entrants qui n'ont pas pu être transmis car leur taille dépassait l'unité de transmission maximale (MTU - Maximum Transmission Unit) de la liaison de l'interface sortante.

Received Datagrams Discarded Due To No Route (Datagrammes reçus rejetés en raison d'absence d'itinéraire) : nombre de datagrammes entrants rejetés car aucun itinéraire n'a pu être trouvé pour les envoyer vers leur destination.

Received Datagrams With Unknown Protocol (Datagrammes reçus avec protocole inconnu) : nombre de datagrammes adressés localement qui ont été bien reçus mais rejetés en raison d'un protocole inconnu ou non pris en charge. Ce compteur est incrémenté à l'interface sur laquelle ces datagrammes étaient adressés, qui n'est pas nécessairement l'interface d'entrée de certains d'entre eux.

Received Datagrams Discarded Due To Invalid Address (Datagrammes reçus rejetés en raison d'une adresse non valide) : nombre de datagrammes entrants rejetés car l'adresse IPv6 figurant dans le champ de destination de leurs en-têtes IPv6 était une adresse incorrecte pour cette entité. Ce nombre inclut les adresses non valides (par exemple, ::0) et non prises en charge (par exemple, les adresses avec préfixes non alloués). Pour les entités qui ne sont pas des routeurs IPv6 et qui, par conséquent, ne transmettent pas de datagrammes, ce compteur inclut les datagrammes rejetés parce que l'adresse de destination n'était pas une adresse locale.

Received Datagrams Discarded Due To Truncated Data (Datagrammes reçus rejetés en raison de données tronquées) : nombre de datagrammes entrants rejetés en raison d'une insuffisance de données.

Received Datagrams Discarded Other (Datagrammes reçus rejetés pour d'autres raisons) : nombre de datagrammes IPv6 entrants dont le traitement s'est déroulé sans incidents mais qui ont été rejetés (par exemple, à cause d'un manque de mémoire tampon). Notez que ce compteur n'inclut pas les datagrammes rejetés pendant l'attente de leur réassemblage.

Received Datagrams Reassembly Required (Datagrammes reçus nécessitant un réassemblage) : nombre de fragments IPv6 reçus qui doivent être réassemblés sur cette interface. Ce compteur est incrémenté sur l'interface à laquelle ces fragments étaient adressés, qui n'est pas nécessairement l'interface d'entrée de certains d'entre eux.

Datagrams Successfully Reassembled (Datagrammes réassemblés avec succès) : nombre de datagrammes IPv6 réassemblés avec succès. Ce compteur est incrémenté sur l'interface à laquelle ces datagrammes étaient adressés, qui n'est pas nécessairement l'interface d'entrée de certains des fragments.

Datagrams Failed To Reassemble (Datagrammes non réassemblés) : nombre d'échecs détectés par l'algorithme de réassemblage IPv6, quelle qu'en soit la raison : délai expiré, erreurs, etc.). Notez que ce nombre ne correspond pas forcément au nombre de fragments IPv6 rejetés car certains algorithmes (notamment l'algorithme présent dans RFC 815) peuvent perdre la trace du nombre de fragments en les associant à leur réception. Ce compteur est incrémenté sur l'interface à laquelle ces fragments étaient adressés, qui n'est pas nécessairement l'interface d'entrée de certains d'entre eux.

Datagrams Forwarded (Datagrammes transmis) : nombre de datagrammes sortants que cette entité a reçu et acheminé vers leur destination finale. Pour les entités ne jouant pas le rôle de routeurs IPv6, ce compteur inclut uniquement les paquets renvoyés à la source par le biais de cette entité, et pour lesquels le traitement de l'itinéraire source ("Source-Route") s'est correctement déroulé. Le compteur de l'interface sortante est incrémenté pour assurer une transmission réussie du datagramme.

Datagrams Locally Transmitted (Datagrammes transmis localement) : nombre de datagrammes que cette entité a transmis avec succès à partir de cette interface de sortie.

Datagrams Transmit Failed (Datagrammes non transmis) : nombre de datagrammes que cette entité n'a pas réussi à transmettre.

Datagrams Successfully Fragmented (Datagrammes fragmentés avec succès) : nombre de datagrammes IPv6 fragmentés avec succès sur cette interface de sortie.

Datagrams Failed To Fragment (Datagrammes non fragmentés) : nombre de datagrammes de sortie qui n'ont pas pu être fragmentés sur cette interface.

Datagrams Fragments Created (Fragments de datagrammes créés) : nombre de fragments de datagrammes de sortie générés suite à leur fragmentation sur cette interface de sortie.

Multicast Datagrams Received (Datagrammes de multidiffusion reçus) : nombre de paquets de multidiffusion reçus par l'interface.

Multicast Datagrams Transmitted (Datagrammes de multidiffusion transmis) : nombre de paquets de multidiffusion transmis par l'interface.

Statistiques ICMPv6

Total ICMPv6 Messages Received (Nombre total de messages ICMPv6 reçus) : nombre total de messages ICMP reçus par l'interface, y compris les messages dénombrés dans ipv6IcmpInErrors. Cette interface est celle à laquelle les messages ICMP étaient adressés, qui n'est pas nécessairement l'interface d'entrée des messages.

ICMPv6 Messages With Errors Received (Messages ICMPv6 reçus avec erreurs) : nombre de messages ICMP reçus par l'interface, mais contenant des erreurs propres au protocole ICMP (sommets de contrôle ICMP incorrectes, longueur incorrecte, etc.)

ICMPv6 Destination Unreachable Messages Received (Messages ICMPv6 de destination inaccessible reçus) : nombre de messages ICMP "Destination inaccessible" ICMP reçus par l'interface.

ICMPv6 Messages Prohibited Administratively Received (Messages ICMPv6 interdits administrativement reçus) : nombre de messages ICMP de type "destination inaccessible" ou "communication interdite administrativement" ayant été reçus par l'interface.

ICMPv6 Time Exceeded Messages Received (Messages ICMPv6 de dépassement de délai reçus) : nombre de messages ICMP de type "dépassement de délai" reçus par l'interface.

ICMPv6 Parameter Problem Messages Received (Messages ICMPv6 reçus signalant un problème de paramètre) : nombre de messages ICMP de type

"problème de paramètre" reçus par l'interface.

ICMPv6 Packet Too Big Messages Received (Messages ICMPv6 de paquet trop volumineux reçus) : nombre de messages ICMP de type "paquet trop volumineux" reçus par l'interface.

ICMPv6 Echo Request Messages Received (Messages ICMPv6 de requête d'écho reçus) : nombre de messages (requête) ICMP de type "écho" reçus par l'interface.

ICMPv6 Echo Reply Messages Received (Messages ICMPv6 de réponse à l'écho reçus) : nombre de messages ICMP de type "réponse à l'écho" reçus par l'interface.

ICMPv6 Router Solicit Messages Received (Messages ICMPv6 de sollicitation du routeur reçus) : nombre de messages ICMP de type "sollicitation du routeur" reçus par l'interface.

ICMPv6 Router Advertisement Messages Received (Messages ICMPv6 d'annonce du routeur reçus) : nombre de messages ICMP de type "annonce de routeur" reçus par l'interface.

ICMPv6 Neighbor Solicit Messages Received (Messages ICMPv6 de sollicitation du voisinage reçus) : nombre de messages ICMP de type "sollicitation du voisinage" reçus par l'interface.

ICMPv6 Neighbor Advertisement Messages Received (Messages ICMPv6 d'annonce du voisinage reçus) : nombre de messages ICMP de type "annonce de voisinage" reçus par l'interface.

ICMPv6 Redirect Messages Received (Messages ICMPv6 de redirection reçus) : nombre de messages ICMPv6 de type "redirection" reçus par l'interface.

ICMPv6 Group Membership Query Messages Received (Messages ICMPv6 d'interrogations sur affiliation reçus) : nombre de messages ICMPv6 de type "interrogation sur l'appartenance à un groupe" reçus par l'interface.

ICMPv6 Group Membership Response Messages Received (Messages ICMPv6 de réponse sur affiliation reçus) : nombre de messages ICMPv6 de type "réponse sur l'appartenance à un groupe" reçus par l'interface.

ICMPv6 Group Membership Reduction Messages Received (Messages ICMPv6 de diminution des affiliations reçus) : nombre de messages ICMPv6 de type "diminution des affiliations" reçus par l'interface

Total ICMPv6 Messages Transmitted (Nombre total de messages ICMPv6 transmis) : nombre total de messages ICMP que cette interface a tenté d'envoyer. Notez que ce compteur inclut tous les messages dénombrés dans icmpOutErrors.

ICMPv6 Messages Not Transmitted Due To Error (Messages ICMPv6 non transmis en raison d'une erreur) : nombre de messages ICMP qui n'ont pas été envoyés par cette interface en raison de problèmes détectés dans le protocole ICMP, par exemple un manque de mémoire tampon. Cette valeur ne doit pas inclure les erreurs détectées en dehors de la couche ICMP, par exemple l'incapacité du protocole IPv6 à acheminer le datagramme résultant. Dans certaines implémentations, aucun type d'erreur n'intervient dans la valeur de ce compteur.

ICMPv6 Destination Unreachable Messages Transmitted (Messages ICMPv6 de destination inaccessible transmis) : nombre de messages ICMP de destination inaccessible envoyés par l'interface.

ICMPv6 Messages Prohibited Administratively Transmitted (Messages ICMPv6 interdits administrativement transmis) : nombre de messages ICMP de destination inaccessible/interdits administrativement envoyés.

ICMPv6 Time Exceeded Messages Transmitted (Messages ICMPv6 de délai dépassé transmis) : nombre de messages ICMP de délai dépassé envoyés par l'interface.

ICMPv6 Parameter Problem Messages Transmitted (Messages ICMPv6 de problèmes de paramètres transmis) : nombre de messages ICMP de problèmes de paramètres envoyés par l'interface.

ICMPv6 Packet Too Big Messages Transmitted (Messages ICMPv6 de paquets trop volumineux transmis) : nombre de messages ICMP de paquets trop volumineux envoyés par l'interface.

ICMPv6 Echo Request Messages Transmitted (Messages ICMPv6 de requête d'écho transmis) : nombre de messages ICMP d'écho (requête) envoyés par l'interface.

ICMPv6 Echo Reply Messages Transmitted (Messages ICMPv6 de réponse à l'écho transmis) : nombre de messages ICMP de réponse à l'écho envoyés par l'interface.

ICMPv6 Router Solicit Messages Transmitted (Messages ICMPv6 de sollicitation du routeur transmis) : nombre de messages ICMP de sollicitation du routeur envoyés par l'interface.

ICMPv6 Router Advertisement Messages Transmitted (Messages ICMPv6 d'annonce du routeur transmis) : nombre de messages ICMP d'annonce du routeur envoyés par l'interface.

ICMPv6 Neighbor Solicit Messages Transmitted (Messages ICMPv6 de sollicitation du voisinage transmis) : nombre de messages ICMP de sollicitation du voisinage envoyés par l'interface.

ICMPv6 Neighbor Advertisement Messages Transmitted (Messages ICMPv6 d'annonce du voisinage transmis) : nombre de messages ICMP d'annonce du voisinage envoyés par l'interface.

ICMPv6 Redirect Messages Transmitted (Messages ICMPv6 de redirection transmis) : nombre de messages de redirection envoyés.

ICMPv6 Group Membership Query Messages Transmitted (Messages ICMPv6 d'interrogations sur affiliation transmis) : nombre de messages ICMPv6 d'interrogations sur affiliation envoyés.

ICMPv6 Group Membership Response Messages Transmitted (Messages ICMPv6 de réponses sur affiliation transmis) : nombre de messages ICMPv6 de réponses sur affiliation envoyés.

ICMPv6 Group Membership Reduction Messages Transmitted (Messages ICMPv6 de diminution des affiliations transmis) : nombre de messages ICMPv6 de diminution des affiliations envoyés.

ICMPv6 Duplicate Address Detects (Détections ICMPv6 d'adresses en double) : nombre d'adresses en double détectées par l'interface.

Affichage des statistiques IPv6

1. Affichez la page **IPv6 Statistics** (Statistiques IPv6).
2. Sélectionnez l'interface à afficher dans le menu déroulant **Interface**.

Les statistiques concernant cette interface s'affichent.

Affichage des statistiques IPv6 et ICMPv6 à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

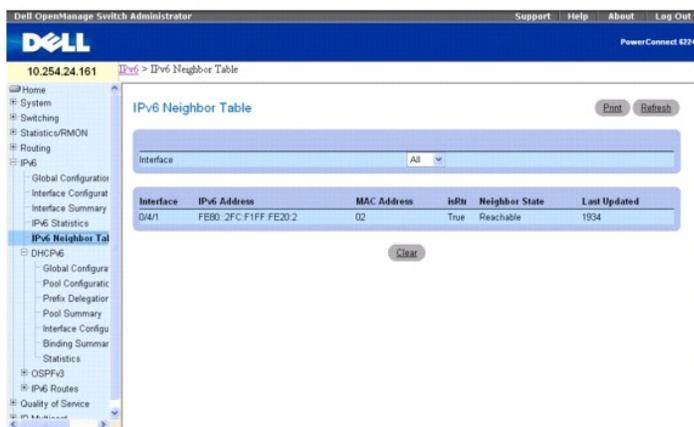
- 1 IPv6 Routing Commands (Commandes de routage IPv6)

Table des voisins IPv6

La page **IPv6 Neighbor Table** (Table des voisins IPv6) permet d'afficher les détails de voisinage IPv6 pour une interface spécifiée.

Pour afficher cette page, cliquez sur **IPv6** → **IPv6 Neighbor Table** (Table des voisins IPv6) dans l'arborescence.

Figure 11-5. Page IPv6 Neighbor Table (Table des voisins IPv6)



La page **IPv6 Neighbor Table** (Table des voisins IPv6) contient les champs suivants :

Interface : sélectionne l'interface pour laquelle les informations d'état du voisinage sont affichées.

Interface : indique l'interface dont les paramètres sont affichés dans la ligne du tableau actuellement sélectionnée.

IPv6 Address (Adresse IPv6) : indique l'adresse IPv6 du voisinage ou de l'interface.

MAC Address (Adresse MAC) : indique l'adresse MAC correspondant à l'interface.

IsRtr : indique si le voisin est un routeur. Si le voisin est un routeur, la valeur est TRUE (VRAI). Si le voisin n'est pas un routeur, la valeur est FALSE (FAUX).

Neighbor State (État du voisinage) : indique l'état de l'entrée de mémoire cache du voisinage. Les entrées dynamiques figurant dans la mémoire cache de détection du voisinage IPv6 peuvent être associées aux états suivants :

- 1 **Incmp** : une résolution d'adresse est en train d'être effectuée sur l'entrée. Un message de sollicitation du voisinage a été envoyé à l'adresse de multidiffusion du nœud sollicité de la cible, mais le message d'annonce du voisinage correspondant n'a pas encore été reçu.
- 1 **Reachable** (Accessible) : une confirmation a été reçue dans les dernières millisecondes de la durée d'accessibilité pour indiquer que le chemin de transfert menant au voisinage fonctionne correctement. Lorsqu'il est dans l'état REACH (Accès), le périphérique n'entreprend aucune action particulière lorsque les paquets sont envoyés.
- 1 **Stale** (Dépassé) : un temps supérieur à la durée d'accessibilité s'est écoulé depuis la dernière confirmation indiquant que le chemin de transfert fonctionne correctement. Lorsqu'il est dans l'état STALE (Dépassé), le périphérique n'entreprend une action que lorsqu'un paquet est envoyé.
- 1 **Delay** (Délai) : un temps supérieur à la durée d'accessibilité s'est écoulé depuis la dernière confirmation indiquant que le chemin de transfert fonctionne correctement. Un paquet a été envoyé dans les dernières secondes du DELAY_FIRST_PROBE_TIME. Si vous ne recevez aucune confirmation d'accessibilité dans les secondes du DELAY_FIRST_PROBE_TIME (suivant l'entrée de l'état DELAY, envoyez un message de sollicitation du voisinage et modifiez l'état de PROBE.
- 1 **Probe** (Capteur) : une confirmation d'accessibilité est demandée par le renvoi de messages de sollicitation du voisinage toutes les millisecondes du délai de retransmission RetransTimer.

Last Updated (Dernière mise à jour) : temps écoulé depuis que l'adresse a été confirmée comme accessible.

Affichage de la table des voisins IPv6

1. Affichez la page **IPv6 Neighbor Table** (Table des voisins IPv6).
2. Sélectionnez l'interface à afficher dans le menu déroulant **Interface**.

Des informations détaillées s'affichent.

Affichage de la table des voisins IPv6 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 IPv6 Routing Commands (Commandes de routage IPv6)

DHCPv6

DHCP est généralement utilisé entre les clients (par exemple, les systèmes hôtes) et les serveurs (par exemple, les routeurs) pour l'attribution d'adresses IP, de passerelles et d'autres définitions réseau telles que DNS, NTP, et/ou les paramètres SIP (Session Initiation Protocol). Cependant, IPv6 propose à l'origine la configuration automatique des adresses IP via IPv6 NDP et l'utilisation d'annonce du routeur. Ainsi, dans le réseau, le rôle de DHCPv6 diffère de celui de DHCPv4 dans la mesure où il est moins utilisé pour l'attribution des adresses IP.

Voici la liste des options DHCP généralement prises en charge par DHCPv4, qui doivent également être prises en charge par DHCPv6 et configurées.

 **REMARQUE :** La plus importante de ces options est DNS Server, configurée sur la page web **IPv6 → DHCPv6 → Pool Configuration** (Configuration du pool).

La page de menu **DHCPv6** contient des liens vers les pages Web permettant de définir et d'afficher les paramètres et les données DHCPv6. Pour afficher cette page, cliquez sur **IPv6 → DHCPv6** dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

- 1 [Configuration globale DHCPv6](#)
- 1 [Configuration du pool DHCPv6](#)
- 1 [Configuration de la délégation de préfixes](#)
- 1 [Récapitulatif des pools DHCPv6](#)
- 1 [Configuration des interfaces DHCPv6](#)
- 1 [Récapitulatif des liaisons du serveur DHCPv6](#)
- 1 [Statistiques DHCPv6](#)

Configuration globale DHCPv6

La page **DHCPv6 Global Configuration** (Configuration globale DHCPv6) permet de configurer les paramètres globaux DHCPv6. Pour afficher cette page, cliquez sur **IPv6 → DHCPv6 → Global Configuration** (Configuration globale) dans l'arborescence.

Figure 11-6. Configuration globale DHCPv6



La page **DHCPv6 Global Configuration** (Configuration globale DHCPv6) contient les champs suivants :

DHCPv6 Admin Mode (Mode admin DHCPv6) : détermine le fonctionnement de DHCPv6 sur le commutateur. Les valeurs possibles sont Enable (Activer) et Disable (Désactiver) ; la valeur par défaut est Disable (Désactiver).

Relay Option (Option relais) : indique la valeur de l'option Relay Agent Information (Informations de l'agent de relais). Les valeurs autorisées sont comprises entre 32 et 65535, et elles représentent la valeur échangée entre l'agent de relais et le serveur. Chaque valeur a une signification particulière et celles comprises entre 1 et 39 sont standardisées. La valeur par défaut, 32, signifie OPTION_INFORMATION_REFRESH_TIME.

Remote-id Sub-option (Sous-option Identification à distance) : permet de spécifier un nombre pour représenter le type de sous-option Remote-ID (Identification à distance) de l'option Relay Agent Information (Informations de l'agent de relais). Les valeurs autorisées sont comprises entre 1 et 65535. La valeur par défaut est de 1.

Configuration des paramètres globaux DHCPv6

1. Affichez la page **DHCPv6 Global Configuration** (Configuration globale DHCPv6).
2. Modifiez les champs selon vos besoins.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications des paramètres DHCPv6 sont enregistrées et le périphérique est mis à jour.

Configuration des paramètres globaux DHCPv6 à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. DHCPv6 Commands (Commandes DHCPv6)

Configuration du pool DHCPv6

Les clients DHCP pour IPv6 sont connectés à un serveur qui est configuré pour utiliser les paramètres d'un pool que vous définissez. Le pool est identifié à l'aide d'un nom de pool et contient les adresses IPv6 et les noms de domaine des serveurs DNS.

La page **Pool Configuration** (Configuration du Pool) permet de créer un pool et/ou de configurer les paramètres du pool.

Pour afficher cette page, cliquez sur **IPv6** → **DHCPv6** → **Pool Configuration** (Configuration des pools) dans l'arborescence.

Figure 11-7. Configuration des pools - Création

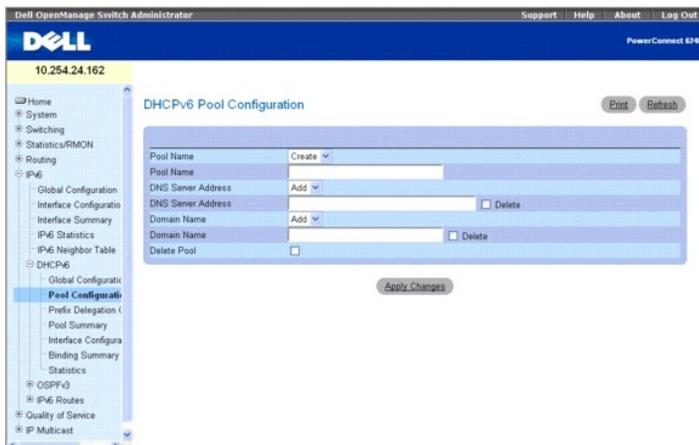


Figure 11-8. Configuration des pools - Affichage



La page **Pool Configuration** (Configuration des pools) contient les champs suivants :

Pool Name (Nom du pool) : menu déroulant qui répertorie tous les noms de pool configurés. Lorsque vous sélectionnez **Create** (Créer), les champs sur la page sont effacés pour recevoir de nouvelles informations sur le pool.

Pool Name (Nom du pool) : affiche le pool sélectionné dans le champ précédent, ou fournit l'entrée d'un nom unique pour un pool DHCPv6 lorsque **Create** (Créer) est sélectionné. Vous pouvez entrer jusqu'à 31 caractères alphanumériques.

DNS Server Address (Adresse du serveur DNS) : menu déroulant qui indique l'adresse IPv6 d'un serveur DNS dans un pool DHCPv6 spécifique. Lorsque vous sélectionnez **Add** (Ajouter) dans le menu, le champ suivant s'efface pour recevoir une nouvelle adresse.

DNS Server Address (Adresse du serveur DNS) : affiche l'adresse du serveur DNS sélectionné dans le champ précédent. Entrez ici une nouvelle adresse de serveur DNS lorsque **Add** (Ajouter) est sélectionné dans le champ précédent. Cliquez sur **Delete** (Supprimer) pour supprimer une adresse de ce pool. L'adresse est supprimée lorsque vous cliquez sur **Apply Changes** (Appliquer les modifications).

Domain Name (Nom de domaine) : menu déroulant qui répertorie les noms de domaine configurés dans un pool DHCPv6 spécifique. Lorsque vous sélectionnez **Add** (Ajouter) dans le menu, le champ suivant s'efface pour recevoir un nouveau nom.

Domain Name (Nom de domaine) : affiche le nom de domaine du serveur DNS sélectionné dans le champ précédent. Entrez un nouveau nom de domaine de serveur DNS lorsque **Add** (Ajouter) est sélectionné dans le champ précédent. Vous pouvez entrer jusqu'à 255 caractères alphanumériques. Cliquez sur **Delete** (Supprimer) pour supprimer un nom de domaine de ce pool. Le nom est supprimé lorsque vous cliquez sur **Apply Changes** (Appliquer les modifications).

Delete Pool (Supprimer le pool) : cochez cette case pour supprimer le pool affiché. Le pool est supprimé lorsque vous cliquez sur **Apply Changes** (Appliquer les modifications).

Création d'un pool DHCPv6

1. Affichez la page **Pool Configuration** (Configuration du Pool).
2. Sélectionnez **Create** (Créer) dans le menu déroulant **Pool Name** (Nom de pool).
3. Entrez un nouveau nom dans le champ **Pool Name** (Nom du pool).
4. Indiquez une adresse existante du serveur DNS à associer à ce pool, ou créez-en une nouvelle.
5. Indiquez un nom de domaine existant à associer à ce pool, ou créez-en un nouveau.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau pool est enregistré et le périphérique est mis à jour. Si une nouvelle adresse ou un nouveau nom de domaine de serveur DNS a été spécifié, il ou elle est également enregistré.

Modification des paramètres du pool DHCPv6

1. Affichez la page **Pool Configuration** (Configuration du Pool).
2. Dans le menu déroulant **Pool Name** (Nom du pool), sélectionnez le pool dont les paramètres changent.
3. Modifiez ou indiquez une nouvelle adresse de serveur DNS pour le pool spécifié.
4. Modifiez ou indiquez un nouveau nom de domaine pour le pool spécifié.

5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications des paramètres du pool DHCPv6 sont enregistrées et le périphérique est mis à jour.

Suppression d'un pool ou d'un paramètre DHCPv6

1. Affichez la page **Pool Configuration** (Configuration du Pool).
2. Dans le menu déroulant Pool Name (Nom de pool), sélectionnez le pool concerné.
3. Cochez la case Delete (Supprimer) si vous souhaitez supprimer l'adresse du serveur DNS pour ce pool.
4. Cochez la case Delete (Supprimer) si vous souhaitez supprimer le nom de domaine pour ce pool.
5. Cochez la case Delete Pool (Supprimer pool) si vous souhaitez supprimer le pool tout entier.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le pool ou ses paramètres sont supprimés, et le périphérique est mis à jour.

Configuration des paramètres du Pool DHCPv6 à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

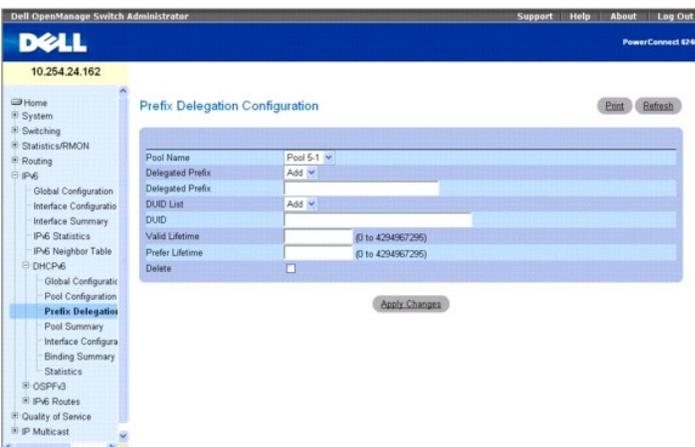
1. DHCPv6 Commands (Commandes DHCPv6)

Configuration de la délégation de préfixes

La page **Prefix Delegation Configuration** (Configuration de la délégation de préfixes) permet de configurer un préfixe délégué pour un pool. Au moins un pool doit être créé à l'aide de la fonction [Configuration du pool DHCPv6](#) pour qu'un préfixe délégué puisse être configuré.

Pour afficher cette page, cliquez sur **IPv6** → **DHCPv6** → **Prefix Delegation Configuration** (Configuration de la délégation de préfixes) dans l'arborescence.

Figure 11-9. Configuration de la délégation de préfixes



La page **Prefix Delegation Configuration** (Configuration de la délégation de préfixes) contient les champs suivants :

Pool Name (Nom du pool) : répertorie tous les pools définis. Sélectionnez le pool à configurer.

Delegated Prefix (Préfixe délégué) : menu déroulant qui indique le préfixe IPv6 délégué à associer au pool spécifié. Sélectionnez **Add** (Ajouter) pour définir un nouveau préfixe délégué pour ce pool.

Delegated Prefix (Préfixe délégué) : affiche le préfixe délégué sélectionné ou autorise la saisie d'un nouveau.

DUID List (Liste DUID) : menu déroulant qui sélectionne la valeur DUID unique du client. Sélectionnez **Add** (Ajouter) pour définir une nouvelle valeur DUID pour ce pool.

DUID : affiche la valeur DUID sélectionnée ou permet la saisie d'une nouvelle.

Valid Lifetime (Durée de vie valide) : indique la durée de vie valide en secondes du préfixe délégué.

Prefer Lifetime (Durée de vie préférée) : indique la durée de vie préférée en secondes du préfixe délégué.

Delete (Supprimer) : supprime la configuration de la délégation du préfixe du pool lorsque la case correspondante est cochée et que vous cliquez sur **Apply Changes** (Appliquer les modifications).

Configuration d'un préfixe délégué à un pool

1. Affichez la page **Prefix Delegation Configuration** (Configuration de la délégation de préfixes).
2. Sélectionnez le pool à configurer.
3. Indiquez le préfixe délégué.
4. Modifiez les autres champs selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le préfixe délégué et les paramètres sont enregistrés et le périphérique est mis à jour.

Configuration d'un préfixe délégué à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. DHCPv6 Commands (Commandes DHCPv6)

Récapitulatif des pools DHCPv6

La page **Pool Summary** (Récapitulatif des pools) permet d'afficher les paramètres de tous les pools DHCPv6. Au moins un pool doit être créé à l'aide de la fonction [Configuration du pool DHCPv6](#) pour que le récapitulatif des pools s'affiche.

Pour afficher cette page, cliquez sur **IPv6** → **DHCPv6** → **Pool Summary** (Récapitulatif des pools) dans l'arborescence.

Figure 11-10. Récapitulatif des pools



La page **Pool Summary** (Récapitulatif des pools) contient les champs suivants :

Pool Name (Nom du pool) : sélectionne le pool à afficher.

DNS Server (Serveur DNS) : affiche l'adresse IPv6 du serveur DNS associé.

Domain Name (Nom de domaine) : affiche le nom de domaine DNS.

Host IP Address (Adresse IP hôte) : affiche l'adresse et la longueur du masque IPv6 pour le préfixe délégué.

DUID : identificateur utilisé pour identifier la valeur DUID unique du client.

Valid Lifetime (Durée de vie valide) : affiche la durée de vie valide en secondes du préfixe délégué.

Prefer Lifetime (Durée de vie préférée) : affiche la durée de vie préférée en secondes du préfixe délégué.

Affichage du récapitulatif des pools l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

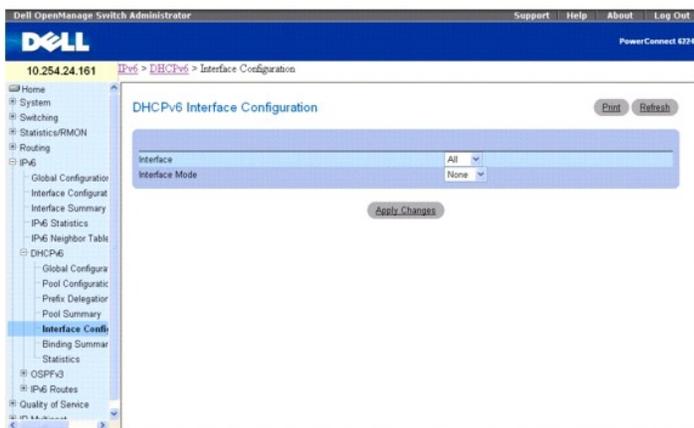
- 1 DHCPv6 Commands (Commandes DHCPv6)

Configuration des interfaces DHCPv6

La page **DHCPv6 Interface Configuration** (Configuration des interfaces DHCPv6) permet de configurer une interface DHCPv6.

Pour afficher cette page, cliquez sur **IPv6** → **DHCPv6** → **Interface Configuration** (Configuration des interfaces) dans l'arborescence.

Figure 11-11. Configuration des interfaces DHCPv6



Les pages **DHCPv6 Interface Configuration** (Configuration des interfaces DHCPv6) contiennent les champs suivants :

Interface : sélectionnez l'interface pour laquelle vous configurez le serveur DHCPv6.

Interface Mode (Mode de l'interface) : configurez le mode DHCPv6 comme Serveur ou Relais. Les fonctions du serveur DHCPv6 et du relais DHCPv6 s'excluent mutuellement.

Pool Name (Nom du pool) : sélectionne le pool DHCPv6 qui contient des paramètres sans état et/ou de délégation du préfixe. Ce champ apparaît lorsque Mode de l'interface a la valeur Serveur.

Rapid Commit (Validation rapide) : Rapid commit (Validation rapide) est un paramètre facultatif. Il est défini pour permettre des échanges abrégés entre le client et le serveur. Ce champ apparaît lorsque Mode de l'interface a la valeur Serveur.

Preference (Préférence) : sélectionne la valeur de préférence utilisée par les clients pour faire un choix entre plusieurs serveurs DHCPv6. Les valeurs autorisées sont comprises entre 0 et 4294967295. Ce champ apparaît lorsque le mode de l'interface est défini sur Serveur.

Delete (Supprimer) : cochez la case, puis cliquez sur **Apply Changes** (Appliquer les modifications) pour supprimer cette configuration. Ce champ apparaît lorsque le mode de l'interface est défini sur Serveur ou sur Relais.

Relay Interface (Interface du relais) : sélectionne l'interface permettant d'atteindre un serveur relais. Ce champ apparaît lorsque Mode de l'interface a la valeur Relais.

Destination IP Address (Adresse IP de destination) : sélectionne l'adresse IPv6 du serveur relais DHCPv6. Ce champ apparaît lorsque Mode de l'interface a la valeur Relais.

Remote ID (ID à distance) : sélectionne le choix d'informations d'agent de relais. Remote ID (ID à distance) doit être défini à partir du DUID du serveur DHCPv6 et du numéro d'interface du relais ou spécifié en tant que chaîne définie par l'utilisateur. Ce champ apparaît lorsque Mode de l'interface a la valeur Relais.

Configuration d'une interface DHCPv6 pour le mode Interface du relais

1. Affichez la page **DHCPv6 Interface Configuration** (Configuration des interfaces DHCPv6).
2. Spécifiez l'interface désirée, puis sélectionnez **Relay** (Relais) dans le menu déroulant **Interface Mode** (Mode de l'interface).

L'écran suivant apparaît :

Figure 11-12. Configuration des interfaces DHCPv6 - Relais



3. Modifiez les champs selon vos besoins.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de l'interface DHCPv6 est enregistrée et le périphérique est mis à jour.

Configuration d'une interface DHCPv6 à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 DHCPv6 Commands (Commandes DHCPv6)

Configuration d'une interface DHCPv6 pour le mode Interface du serveur

1. Affichez la page **DHCPv6 Interface Configuration** (Configuration des interfaces DHCPv6).
2. Spécifiez l'interface désirée, puis sélectionnez **Server** (Serveur) dans le menu déroulant **Interface Mode** (Mode de l'interface).

L'écran suivant apparaît :

Figure 11-13. Configuration des interfaces DHCPv6 - Serveur



3. Modifiez les champs selon vos besoins.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de l'interface DHCPv6 est enregistrée et le périphérique est mis à jour.

Configuration d'une interface DHCPv6 à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

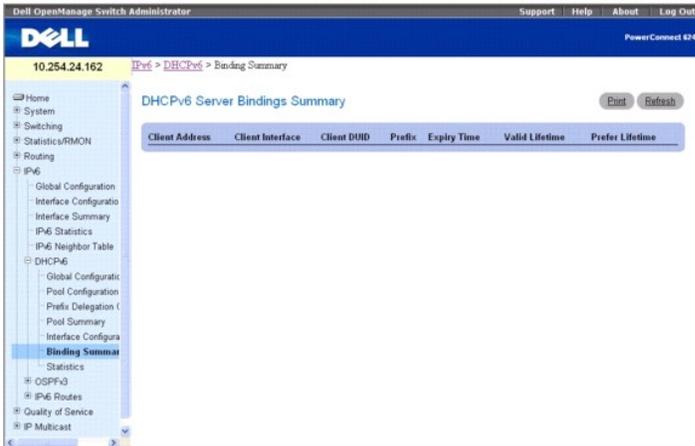
- 1 DHCPv6 Commands (Commandes DHCPv6)

Récapitulatif des liaisons du serveur DHCPv6

La page **Server Bindings Summary** (Récapitulatif des liaisons du serveur) permet d'afficher toutes les liaisons du serveur DHCPv6.

Pour afficher cette page, cliquez sur **IPv6** → **DHCPv6** → **Bindings Summary** (Récapitulatif des liaisons) dans l'arborescence.

Figure 11-14. Récapitulatif des liaisons du serveur



La page **Server Bindings Summary** (Récapitulatif des liaisons du serveur) contient les champs suivants :

Client Address (Adresse du client) : indique l'adresse IPv6 du client associé à la liaison.

Client Interface (Interface client) : indique le numéro de l'interface dans laquelle la liaison client s'est produite.

Client DUID (DUID client) : indique l'identificateur unique DHCPv6 du client.

Prefix (Préfixe) : indique le type de préfixe associé à cette liaison.

Expiry Time (Délai d'expiration) : indique le nombre de secondes avant l'expiration du préfixe associé à la liaison.

Valid Lifetime (Durée de vie valide) : indique la durée de vie valide en secondes du préfixe associé à la liaison.

Prefer Lifetime (Durée de vie préférée) : indique la durée de vie préférée en secondes du préfixe associé à la liaison.

Affichage des liaisons du serveur à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 DHCPv6 Commands (Commandes DHCPv6)

Statistiques DHCPv6

La page **DHCPv6 Statistics** (Statistiques DHCPv6) permet d'afficher les statistiques pour une ou pour toutes les interfaces.

Pour afficher cette page, cliquez sur **IPv6** → **DHCPv6** → **Statistics** (Statistiques) dans l'arborescence.

Figure 11-15. Statistiques DHCPv6

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area displays 'DHCPv6 Statistics' for interface 'g1'. A table titled 'Messages Reçus:' lists various DHCPv6 message types and their counts. All counts are currently 0.

Message Type	Count
DHCPv6 Solicit Packets Received	0
DHCPv6 Request Packets Received	0
DHCPv6 Confirm Packets Received	0
DHCPv6 Renew Packets Received	0
DHCPv6 Rebind Packets Received	0
DHCPv6 Release Packets Received	0
DHCPv6 Decline Packets Received	0
DHCPv6 Inform Packets Received	0
DHCPv6 Relay-forward Packets Received	0
DHCPv6 Relay-reply Packets Received	0
DHCPv6 Malformed Packets Received	0
Received DHCPv6 Packets Discarded	0
Total DHCPv6 Packets Received	0

La page **DHCPv6 Statistics** (Statistiques DHCPv6) contient les champs suivants :

Interface : sélectionnez l'interface pour laquelle les données doivent être affichées ou configurées. En sélectionnant **All** (Tout), vous affichez les données pour toutes les interfaces.

Messages reçus

Cette section présente l'ensemble des statistiques de niveau de toutes les interfaces pour les messages reçus.

DHCPv6 Solicit Packets Received (Paquets DHCPv6 de sollicitation reçus) : indique le nombre de sollicitations.

DHCPv6 Request Packets Received (Paquets DHCPv6 de requête reçus) : indique le nombre de requêtes.

DHCPv6 Confirm Packets Received (Paquets DHCPv6 de confirmation reçus) : indique le nombre de confirmations.

DHCPv6 Renew Packets Received (Paquets DHCPv6 de renouvellement reçus) : indique le nombre de renouvellements.

DHCPv6 Rebind Packets Received (Paquets DHCPv6 de reprise de liaison reçus) : indique le nombre de reprises de liaison.

DHCPv6 Release Packets Received (Paquets DHCPv6 de libération reçus) : indique le nombre de libérations.

DHCPv6 Decline Packets Received (Paquets DHCPv6 de refus reçus) : indique le nombre de refus.

DHCPv6 Inform Packets Received (Paquets DHCPv6 d'information reçus) : indique le nombre d'informations.

DHCPv6 Relay-forward Packets Received (Paquets DHCPv6 de transmission de relais reçus) : indique le nombre de transmission de relais.

DHCPv6 Relay-reply Packets Received (Paquets DHCPv6 de réponse de relais reçus) : indique le nombre de réponses de relais.

DHCPv6 Malformed Packets Received (Paquets DHCPv6 endommagés reçus) : indique le nombre de paquets endommagés.

Received DHCPv6 Packets Discarded (Paquets DHCPv6 rejetés reçus) : indique le nombre de paquets rejetés.

Total DHCPv6 Packets Received (Nombre total des paquets DHCPv6 reçus) : indique le nombre total de paquets reçus.

Messages envoyés

Cette section présente l'ensemble des statistiques de niveau de toutes les interfaces pour les messages envoyés.

DHCPv6 Advertisement Packets Transmitted (Paquets DHCPv6 d'annonce transmis) : indique le nombre d'annonces.

DHCPv6 Reply Packets Transmitted (Paquets DHCPv6 de réponse transmis) : indique le nombre de réponses.

DHCPv6 Reconfig Packets Transmitted (Paquets DHCPv6 de reconfiguration transmis) : indique le nombre de reconfigurations.

DHCPv6 Relay-forward Packets Transmitted (Paquets DHCPv6 de transmission de relais transmis) : indique le nombre de transmission de relais.

DHCPv6 Relay-reply Packets Transmitted (Paquets DHCPv6 de réponse de relais transmis) : indique le nombre de réponses de relais.

Total DHCPv6 Packets Sent (Total des paquets DHCPv6 envoyés) : indique le nombre total de paquets transmis.

Clear (Effacer) : réinitialise les compteurs de paquets de l'interface.

Affichage des statistiques DHCPv6

1. Affichez la page **DHCPv6 Statistics** (Statistiques DHCPv6).
2. Sélectionnez l'interface à afficher dans le menu déroulant de l'interface.

Affichage des statistiques DHCPv6 pour l'interface sélectionnée.

Affichage des statistiques DHCPv6 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 DHCPv6 Commands (Commandes DHCPv6)

OSPFv3

OSPFv3 est le protocole de routage OSPF (Open Shortest Path First) pour IPv6. Il ressemble à OSPFv2 dans son concept de base de données LSDB (Link State Database), de zone intra/inter, d'itinéraires externes AS et de liaisons virtuelles. Il diffère de son équivalent IPv4 en un certain nombre de points, notamment : L'association s'effectue via les adresses locale-liaison ; le protocole concerne la liaison plutôt que le réseau ; les sémantiques d'adressage ont été déplacées vers les LSA du noeud terminal, ce qui a finalement rendu possible son utilisation pour IPv4 et IPv6. Les liaisons point à point sont également prises en charge pour permettre son fonctionnement sous des tunnels.

Il est possible d'activer simultanément OSPF et OSPFv3. OSPF fonctionne avec IPv4 et OSPFv3 avec IPv6.

La page de menu **OSPFv3** contient des liens vers les pages Web permettant de définir et d'afficher les paramètres et les données OSPFv3. Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** dans l'arborescence.

Cette page permet d'accéder aux fonctionnalités suivantes :

- 1 [Configuration OSPFv3](#)
- 1 [Configuration de la zone OSPFv3](#)
- 1 [Récapitulatif de la zone de stub OSPFv3](#)
- 1 [Configuration de la plage de zones OSPFv3](#)
- 1 [Configuration des interfaces OSPFv3](#)
- 1 [Statistiques sur les interfaces OSPFv3](#)
- 1 [Voisins OSPFv3](#)
- 1 [Table des voisins OSPFv3](#)
- 1 [Base de données LSDB OSPFv3](#)
- 1 [Configuration des liaisons virtuelles OSPFv3](#)
- 1 [Récapitulatif des liaisons virtuelles OSPFv3](#)
- 1 [Configuration de la redistribution des itinéraires OSPFv3](#)
- 1 [Récapitulatif de la redistribution des itinéraires OSPFv3](#)

Configuration OSPFv3

La page **OSPFv3 Configuration** (Configuration OSPFv3) permet d'activer et de configurer OSPFv3 pour un commutateur.

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Configuration** dans l'arborescence.

Figure 11-16. Configuration OSPFv3



La page **OSPFv3 Configuration** (Configuration OSPFv3) contient les champs suivants :

Router ID (ID du routeur) : nombre entier de 32 bits à points décimaux qui identifie de manière unique le routeur dans le système autonome. Pour modifier l'ID du routeur, vous devez d'abord désactiver l'interface OSPFv3. Une fois que vous avez défini le nouvel ID du routeur, vous devez réactiver l'interface OSPFv3 pour que les modifications prennent effet. La valeur par défaut est 0.0.0.0 mais ce n'est pas un ID de routeur valide. Vous devez la modifier avant d'appuyer sur le bouton **Apply Changes** (Appliquer les modifications).

OSPFv3 Admin Mode (Mode Admin OSPFv3) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Si vous sélectionnez Enable (Activer), OSPFv3 est activé pour ce commutateur. La valeur par défaut est Enable (Activer). Vous devez configurer un ID de routeur pour que l'interface OSPFv3 devienne opérationnelle. L'opération peut également être effectuée en exécutant la commande CLI, `router-id` (id du routeur), dans le mode OSPF du routeur IPv6.

 **REMARQUE** : Une fois l'interface OSPFv3 activée sur le routeur, elle reste active tant que le routeur n'est pas réinitialisé.

ASBR Mode (Mode ASBR) : indique si le mode ASBR est activé ou désactivé. S'il est activé, cela signifie que le routeur est un routeur de limites de systèmes autonomes (ASBR, Autonomous System Border Router). Il devient automatiquement un routeur ASBR lorsqu'il est configuré pour redistribuer les itinéraires appris à partir d'un autre protocole.

ABR Status (État ABR) : les valeurs de ce champ sont Enabled (Activé) ou Disabled (Désactivé). Ce champ n'apparaît que si une configuration valide existe. L'option Enabled (Activé) indique que le routeur est un routeur de limite de zone. L'option Disabled (Désactivé) indique le contraire.

Exit Overflow Interval (secs) (Intervalle de sortie en cas de saturation, secondes) : entrez le délai d'attente en secondes avant que le routeur tente de sortir de l'état de saturation, une fois cet état activé. Cela permet au routeur de créer à nouveau des LSA externes au système autonome qui ne sont pas définies par défaut. Si vous entrez la valeur 0, le routeur ne quitte pas l'état de saturation tant que le système n'est pas redémarré. La plage de valeurs est comprise entre 0 et 2147483647 secondes.

External LSA Count (Nombre de LSA externes) : nombre de LSA (Link State Advertisements) externes (LS de type 5) contenues dans la base de données LSDB (Link State Database).

External LSA Checksum (Somme de contrôle des LSA externes) : total des sommes de contrôle LS des LSA externes contenues dans la base de données LSDB (Link State Database). Cette valeur peut être utilisée pour déterminer si des modifications ont été apportées à la base de données LSDB d'un routeur et pour comparer les bases de données LSDB de deux routeurs.

New LSAs Originated (Nouvelles LSA créées) : dans une zone OSPFv3 donnée, un routeur crée plusieurs LSA. Chaque routeur crée la LSA associée à un routeur. Si le routeur correspond également au routeur désigné pour l'un des réseaux de la zone, il crée les LSA associées à ces réseaux. Cette valeur désigne le nombre de LSA créées par ce routeur.

LSAs Received (LSA reçues) : nombre de LSA (Link State Advertisements) reçues qui sont considérées comme de nouvelles instanciations. Ce nombre n'inclut pas les nouvelles instanciations des LSA créées automatiquement.

External LSDB Limit (Nombre limite de LSDB externes) : nombre maximal de LSA externes qui peuvent être stockés dans la base de données. La valeur -1 indique qu'il n'y a aucune limite concernant le nombre de LSA pouvant être stockées. Les valeurs valides sont comprises entre -1 et 2147483647.

Default Metric (Métrique par défaut) : définit une métrique par défaut pour les itinéraires redistribués. Ce champ affiche la métrique par défaut si une a déjà été définie, ou il ne contient aucune valeur s'il n'a pas été configuré précédemment. Les valeurs autorisées sont comprises entre 1 et 16777214.

Maximum Paths (Chemins d'accès maximum) : configurez le nombre maximum de chemins d'accès que l'interface OSPFv3 peut spécifier pour une destination donnée. Les valeurs autorisées sont comprises entre 1 et 2.

Default Information Originate (Création d'informations par défaut) : activez ou désactivez l'option Default Route Advertise (Annonce de routage par défaut). Les valeurs de Always (Toujours), Metric (Métrique) et Metric Type (Type de valeur) ne peuvent être configurées que lorsque l'option Default Information Originate (Création d'informations par défaut) a la valeur Enable (Activer). Si l'option Default Information Originate (Création d'informations par défaut) a la valeur Enable (Activer) et que les valeurs de Always (Toujours), Metric (Métrique) et Metric Type (Type de métrique) sont déjà configurées, le paramétrage de Default Information Originate (Création d'informations par défaut) sur Disable (Désactiver) entraîne l'application des valeurs par défaut pour Always (Toujours), Metric (Métrique) et Metric Type (Type de métrique).

Always (Toujours) : définit l'annonce `::/0` lorsqu'elle est définie sur True (Vrai).

Metric (Métrique) : définit la métrique de l'itinéraire par défaut. Les valeurs autorisées sont comprises entre 0 et 16777214.

Metric Type (Type de métrique) : définit le type de métrique de l'itinéraire par défaut. Les valeurs autorisées sont External Type 1 (Type externe 1) et External Type 2 (Type externe 2).

Configuration de OSPFv3

1. Affichez la page **OSPFv3 Configuration** (Configuration OSPFv3).
2. Modifiez les champs selon vos besoins.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration OSPFv3 est enregistrée et le périphérique est mis à jour.

Configuration de OSPFv3 à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

Configuration de la zone OSPFv3

La page **OSPFv3 Area Configuration** (Configuration de la zone OSPFv3) permet de créer et de configurer une zone OSPFv3.

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Area Configuration** (Configuration de la zone) dans l'arborescence.

Figure 11-17. Configuration de la zone OSPFv3



La page **OSPFv3 Area Configuration** (Configuration de la zone OSPFv3) contient les champs suivants :

Area ID (ID de zone) : zone OSPFv3. Cette valeur doit être un nombre entier de 32 bits à points décimaux qui identifie de manière unique la zone à laquelle une interface de routeur est connectée.

External Routing (Routage externe) : définition des capacités du routeur pour la zone, notamment si les LSA externes au système autonome sont acheminés vers la zone. Si la zone est une zone de stub, les options possibles permettant de configurer les capacités de routage externe sont décrites ci-dessous. Dans le cas contraire, l'unique option disponible est Import External LSAs (Importer les LSA externes).

SPF Runs (Exécutions SPF) : nombre de fois que la table de routage intra-zone a été calculée à l'aide de la base de données LSDB (Link State Database) de cette zone. Ce calcul s'effectue généralement à l'aide de l'algorithme de Dijkstra.

Area Border Router Count (Nombre de routeurs de limite de zone) : nombre total de routeurs de limite de zone accessibles dans cette zone. La valeur initiale est égale à zéro, et est calculée pour chaque passage SPF.

Area LSA Count (Nombre de LSA dans la zone) : nombre total de LSA (Link State Advertisements) contenues dans la base de données LSDB (Link State Database) de cette zone, en excluant les LSA externes au système autonome.

Area LSA Checksum (Somme de contrôle des LSA dans la zone) : total non signé de 32 bits des sommes de contrôle LS des LSA contenues dans la base de données LSDB (Link State Database) de cette zone. Cette valeur exclut les LSA (LS de type 5) externes. Elle peut être utilisée pour déterminer si des modifications ont été apportées à la base de données LSDB d'un routeur et pour comparer les bases de données LSDB de deux routeurs. Elle est au format hexadécimal.

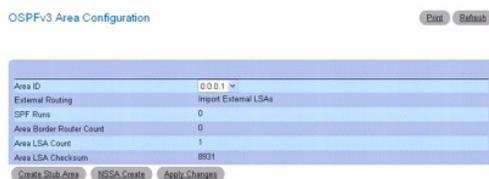
Configuration de la zone OSPFv3

1. Affichez la page **OSPFv3 Area Configuration** (Configuration de la zone OSPFv3).
2. Modifiez les champs selon vos besoins.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration est enregistrée et le périphérique est mis à jour.

La page Web réapparaît avec les boutons **Create Stub Area** (Créer une zone de stub) et **NSSA Create** (Créer NSSA).

Figure 11-18. Configuration de la zone OSPFv3 - Créer une zone de stub et Créer NSSA



Configuration de la zone de stub OSPFv3

1. Affichez la page **OSPFv3 Area Configuration** (Configuration de la zone OSPFv3).
2. Modifiez les champs selon vos besoins.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La page Web réapparaît avec les boutons **Create Stub Area** (Créer une zone de stub) et **NSSA Create** (Créer NSSA). Voir la [Figure 11-18](#).

4. Cliquez sur **Create Stub Area** (Créer une zone de stub).

Les champs **Stub Area Information** (Informations sur la zone de stub) s'affichent.

Figure 11-19. Configuration de la zone de stub OSPFv3

The screenshot shows the 'OSPFv3 Area Configuration' page with the 'Stub Area Information' section expanded. The fields are as follows:

Area ID	0.0.0.1
External Routing	Import No LSAs
SPF Runs	8
Area Border Router Count	0
Area LSA Count	4
Area LSA Checksum	106098
Stub Area Information	
Import Summary LSAs	Enable
Metric Value	1 (1 to 16777215)

Buttons: **Delete Stub Area**, **Apply Changes**

5. Complétez les autres champs.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les informations de la zone de stub sont enregistrées et le périphérique est mis à jour.

Configuration de la zone NSSA OSPFv3

1. Affichez la page **OSPFv3 Area Configuration** (Configuration de la zone OSPFv3).
2. Modifiez les champs selon vos besoins.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La page Web réapparaît avec les boutons **Create Stub Area** (Créer une zone de stub) et **NSSA Create** (Créer NSSA). Voir la [Figure 11-18](#).

4. Cliquez sur **NSSA Create** (Créer NSSA) sur la page Web **OSPFv3 Area Configuration** (Configuration de la zone OSPFv3).

La page Web réapparaît avec les options pour la configuration NSSA.

Figure 11-20. Configuration de la zone OSPFv3 - NSSA

The screenshot shows the 'OSPFv3 Area Configuration' page with the 'NSSA Specific Information' section expanded. The fields are as follows:

Area ID	0.0.0.1
External Routing	Import NSSAs
SPF Runs	10
Area Border Router Count	0
Area LSA Count	3
Area LSA Checksum	98443
NSSA Specific Information	
Import Summary LSAs	Enable
Default Information Originate	False
Default Metric	10 (1 to 16777214)
Default Metric Type	Non-comparable Cost
Translator Role	Candidate
Translator Stability Interval	30 (0 to 3600)
No-Redistribute Mode	Enable
Translator State	Elected

Buttons: **NSSA Delete**, **Apply Changes**

5. Complétez les autres champs.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les informations NSSA sont enregistrées et le périphérique est mis à jour.

Suppression des informations de la zone de stub OSPFv3

1. Affichez la page **OSPFv3 Area Configuration** (Configuration de la zone OSPFv3) avec les informations de la zone de stub configurées.
2. Cliquez sur **Delete Stub Area** (Supprimer une zone de stub).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Suppression des informations NSSA OSPFv3

1. Affichez la page **OSPFv3 Area Configuration** (Configuration de la zone OSPFv3) avec les informations NSSA configurées.
2. Cliquez sur **NSSA Delete** (Supprimer NSSA).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Configuration de la zone OSPFv3 à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

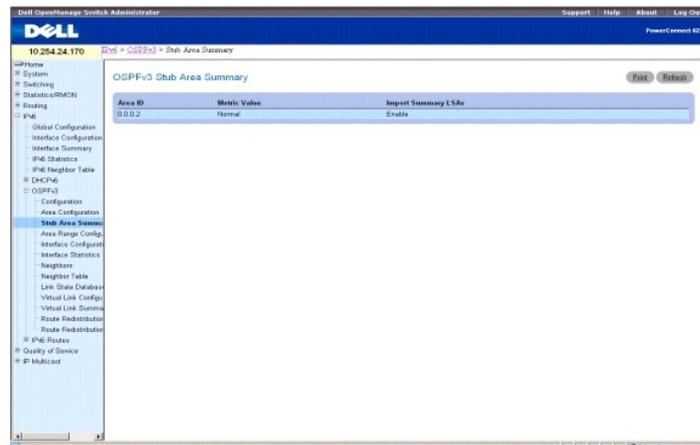
- 1 OSPFv3 Commands (Commandes OSPFv3)

Récapitulatif de la zone de stub OSPFv3

La page **OSPFv3 Stub Area Summary** (Récapitulatif de la zone de stub OSPFv3) permet d'afficher les détails d'une zone de stub OSPFv3.

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Stub Area Summary** (Récapitulatif de la zone de stub) dans l'arborescence.

Figure 11-21. Récapitulatif de la zone de stub OSPFv3



Area ID	Metric Value	Import Summary LSAs
0.0.0.2	Normal	Enable

La page **OSPFv3 Stub Area Summary** (Récapitulatif de la zone de stub OSPFv3) contient les champs suivants :

Area ID (ID de zone) : ID de zone de la zone de stub.

Metric Value (Valeur de métrique) : valeur de métrique appliquée à l'itinéraire par défaut annoncé dans la zone.

Import Summary LSAs (Importer les LSA récapitulatives) : indique si l'importation des LSA récapitulatives est activée ou désactivée.

Affichage du récapitulatif de la zone de stub OSPFv3 à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

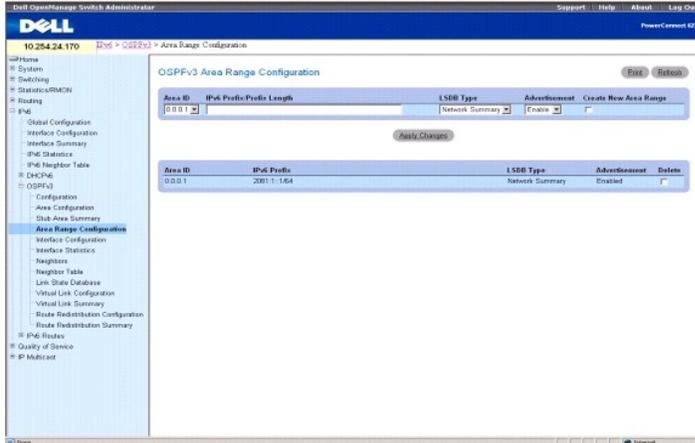
- 1 OSPFv3 Commands (Commandes OSPFv3)

Configuration de la plage de zones OSPFv3

La page **OSPFv3 Area Range Configuration** (Configuration de la plage de zones OSPFv3) permet de configurer les plages de zone OSPFv3.

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Area Range Configuration** (Configuration de la plage de zones) dans l'arborescence.

Figure 11-22. Configuration de la plage de zones OSPFv3



La page **OSPFv3 Area Range Configuration** (Configuration de la plage de zones OSPFv3) contient les champs suivants :

Area ID (ID de zone) : sélectionnez la zone pour laquelle vous souhaitez configurer les données.

IPv6 Prefix/Prefix Length (Préfixe IPv6/Longueur du préfixe) : saisissez le préfixe IPv6/la longueur du préfixe de la plage d'adresses pour la zone sélectionnée.

LSDB Type (Type de LSDB) : sélectionnez le type d'annonce de liaison associée à la zone et à la plage d'adresses spécifiées. Le type par défaut est Network Summary (Récapitulatif du réseau).

Advertisement (Annonce) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Si vous sélectionnez Enable (Activer), la plage d'adresses est annoncée en dehors de la zone par le biais d'une LSA de type Network Summary (Récapitulatif du réseau). La valeur par défaut est Enable (Activer).

Create New Area Range (Créer une nouvelle plage de zones) : cochez la case pour créer une nouvelle plage de zones OSPFv3 avec les valeurs spécifiées.

Area ID (ID de zone) : zone OSPFv3.

IPv6 Prefix (Préfixe IPv6) : préfixe IPv6 d'une plage d'adresses pour la zone.

LSDB Type (Type de LSDB) : type d'annonce de liaison associée à la plage d'adresses et à la zone.

Advertisement (Annonce) : mode d'annonce associé à la plage d'adresses et à la zone.

Delete (Supprimer) : cochez la case pour supprimer la plage de zones OSPFv3 spécifiée.

Configuration de la plage de zones OSPFv3

1. Affichez la page **OSPFv3 Area Range Configuration** (Configuration de la plage de zones OSPFv3).
2. Modifiez les champs selon vos besoins.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La plage de zones OSPFv3 est enregistrée et le périphérique est mis à jour.

Configuration de la plage de zones OSPFv3 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. OSPFv3 Commands (Commandes OSPFv3)

Configuration des interfaces OSPFv3

La page **OSPFv3 Interface Configuration** (Configuration des interfaces OSPFv3) permet de créer et de configurer des interfaces OSPFv3.

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Interface Configuration** (Configuration des interfaces) dans l'arborescence.

Figure 11-23. Configuration des interfaces OSPFv3



La page **OSPFv3 Interface Configuration** (Configuration des interfaces OSPFv3) contient les champs suivants :

Interface : sélectionnez l'interface pour laquelle les données doivent être affichées ou configurées.

IP Address (Adresse IP) : adresse IPv6 de l'interface.

OSPFv3 Admin Mode (Mode admin OSPFv3) : vous pouvez sélectionner **Enable** (Activer) ou **Disable** (Désactiver) dans le menu déroulant. La valeur par défaut est **Disabled** (Désactivé). Vous pouvez configurer les paramètres OSPFv3 sans activer ce mode, mais ils ne prennent effet qu'une fois ce mode activé. Les champs ci-après ne s'affichent que si l'option Admin Mode (Mode admin) est activée : **State** (État), **Designated Router** (Routeur désigné), **Backup Designated Router** (Routeur de sauvegarde désigné), **Number of Link Events** (Nombre d'événements de liaison), **LSA Ack Interval** (Intervalle d'accusé réception des LSA) et **Metric Cost** (Coût de métrique). Pour que OSPFv3 soit totalement opérationnel, l'interface doit disposer d'un préfixe IPv6 et d'une longueur de préfixe valides. L'opération peut être effectuée via l'interface de ligne de commande (CLI) à l'aide de la commande `ipv6 address` (adresse ipv6) dans le mode de configuration de l'interface.

Une fois l'interface OSPFv3 activée sur le routeur, elle reste active tant que le routeur n'est pas réinitialisé.

OSPFv3 Area ID (ID de zone OSPFv3) : entrez un nombre entier de 32 bits à points décimaux qui identifie de manière unique la zone OSPFv3 à laquelle l'interface de routeur sélectionnée est connectée. Si vous attribuez un ID de zone qui n'existe pas, la zone est créée à l'aide des valeurs par défaut.

Router Priority (Priorité du routeur) : entrez la priorité OSPFv3 pour l'interface sélectionnée. Cette valeur doit être un nombre entier compris entre 0 et 255. La valeur par défaut est 1, qui désigne la priorité la plus élevée. La valeur 0 indique que le routeur ne peut pas être défini comme routeur désigné sur ce réseau.

Retransmit Interval (secs) (Intervalle de retransmission [secondes]) : entrez l'intervalle de retransmission OSPFv3 pour l'interface spécifiée. Il désigne le nombre de secondes entre les LSA (Link State Advertisements) pour les contiguités appartenant à cette interface de routeur. Cette valeur est également utilisée lors de la retransmission des descriptions de base de données et des paquets LSR (Link State Request). La plage de valeurs admises est comprise entre 0 et 3600 secondes (1 heure). La valeur par défaut est de 5 secondes.

Hello Interval (secs) (Intervalle Hello [secondes]) : entrez l'intervalle hello OSPFv3 en secondes pour l'interface spécifiée. Ce paramètre doit être identique pour tous les routeurs connectés à un réseau. La plage de valeurs admises est comprise entre 1 et 65 535. La valeur par défaut est de 10 secondes.

Dead Interval (secs) (Intervalle d'inactivité [secondes]) : entrez l'intervalle d'inactivité OSPFv3 en secondes pour l'interface spécifiée. Il désigne la durée pendant laquelle un routeur attend de recevoir des paquets Hello d'un routeur voisin avant de déclarer que ce routeur est hors service. Ce paramètre doit être identique pour tous les routeurs connectés à un réseau. Cette valeur doit être un multiple de l'intervalle hello (par exemple 4). La plage de valeurs admises est comprise entre 1 et 2147483647. La valeur par défaut est de 40 secondes.

LSA Ack Interval (Intervalle d'accusé réception des LSA) : nombre de secondes entre les transmissions de paquets d'accusé réception des LSA. Cette valeur doit être inférieure à l'intervalle de retransmission.

Interface Delay Interval (secs) (Intervalle de transition de l'interface [secondes]) : entrez le délai de transition OSPFv3 pour l'interface spécifiée. Il désigne le nombre estimé de secondes pour transmettre un paquet LSU (Link State Update) sur l'interface sélectionnée. La plage de valeurs admises est comprise entre 1 et 3600 secondes (1 heure). La valeur par défaut est de 1 seconde.

MTU Ignore (Ignorer MTU) : désactive la détection de MTU OSPFv3 incompatibles lors de la réception des paquets. La valeur par défaut est **Disabled** (Désactivé).

Interface Type (Type d'interface) : entrez le type d'interface, qui peut être défini en mode diffusion ou en mode point à point. Le type d'interface par défaut est le mode diffusion.

State (État) : état actuel de l'interface de routeur sélectionnée. Celle-ci peut avoir l'un des états suivants :

- 1 **Down** (Hors service) : état initial de l'interface. Cet état indique que les protocoles de niveau inférieur ont signalé que l'interface est inutilisable. Les paramètres de l'interface sont réinitialisés à leurs valeurs initiales. Toutes les horloges de l'interface sont désactivées, et aucune contiguité n'est associée à l'interface.
- 1 **Loopback** (Boucle de rappel) : cet état indique que l'interface du routeur a effectué une boucle de rappel dans le matériel ou le logiciel. L'interface n'est pas disponible pour le transfert de données normal. Toutefois, il est toujours possible d'obtenir des informations sur la qualité de cette interface, en

envoyant des commandes Ping ICMP à l'interface ou en exécutant un test d'erreurs de bits. Ainsi, il est toujours possible d'adresser des paquets IP à une interface en boucle de rappel. Pour ce faire, ces interfaces sont annoncées dans les LSA associées au routeur en tant qu'itinéraires hôtes uniques, dont la destination est l'adresse de l'interface IP.

- 1 **Waiting (En attente)** : le routeur tente de déterminer l'identité du routeur désigné (Sauvegarde) pour le réseau en contrôlant les paquets Hello reçus. Il n'est pas autorisé à sélectionner un routeur de sauvegarde désigné ou un routeur désigné tant que cet état est activé. Cela évite des modifications inutiles au routeur désigné (Sauvegarde).
- 1 **Designated Router (Routeur désigné)** : ce routeur est lui-même le routeur désigné sur le réseau connecté. Les contiguïtés sont créées pour tous les autres routeurs connectés au réseau. Le routeur doit également créer une LSA associée au nœud du réseau. Cette LSA contient les liens vers tous les routeurs (y compris le routeur désigné proprement dit) connectés au réseau.
- 1 **Backup Designated Router (Routeur de sauvegarde désigné)** : ce routeur est lui-même le routeur de sauvegarde désigné sur le réseau connecté. Il devient le routeur désigné en cas de défaillance du routeur désigné existant. Le routeur crée les contiguïtés pour tous les autres routeurs connectés au réseau. Le routeur de sauvegarde désigné exécute des fonctions légèrement différentes durant la procédure d'acheminement, par rapport au routeur désigné.
- 1 **Other Designated Router (Autre routeur désigné)** : l'interface est connectée à un réseau de diffusion ou NBMA sur lequel d'autres routeurs ont été choisis comme routeur désigné et routeur de sauvegarde désigné. Le routeur tente de créer des contiguïtés pour le routeur désigné et le routeur de sauvegarde désigné.

Le champ State (État) ne s'affiche que si l'option OSPF Admin Mode (Mode admin OSPF) est activée.

Designated Router (Routeur désigné) : identité du routeur désigné pour ce réseau, du point de vue du routeur d'annonce. Il est identifié ici par son ID de routeur. La valeur 0.0.0.0 indique qu'il n'existe aucun routeur désigné. Ce champ ne s'affiche que si l'option OSPFv3 Admin Mode (Mode admin OSPF) est activée.

Backup Designated Router (Routeur de sauvegarde désigné) : identité du routeur désigné de sauvegarde pour ce réseau, du point de vue du routeur d'annonce. Il est identifié ici par son ID de routeur. La valeur 0.0.0.0 indique qu'il n'existe aucun routeur désigné de sauvegarde. Ce champ ne s'affiche que si l'option OSPFv3 Admin Mode (Mode admin OSPF) est activée.

Number of Link Events (Nombre d'événements de liaison) : nombre de modifications d'état enregistrées sur l'interface OSPFv3 spécifiée. Ce champ ne s'affiche que si l'option OSPFv3 Admin Mode (Mode admin OSPF) est activée.

Metric Cost (Coût de métrique) : entrez la valeur du coût TOS (Type Of Service) sur cette interface. La plage de valeurs est comprise entre 1 et 65535. Ce champ ne peut être configuré que si le protocole OSPFv3 est initialisé sur l'interface.

Configuration d'une interface OSPFv3

1. Affichez la page **OSPFv3 Interface Configuration** (Configuration des interfaces OSPFv3).
2. Sélectionnez l'interface sur laquelle vous voulez configurer OSPFv3.
3. Modifiez les autres champs selon vos besoins.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'interface est configurée pour OSPFv3 et le périphérique est mis à jour.

Configuration d'une interface OSPFv3 à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

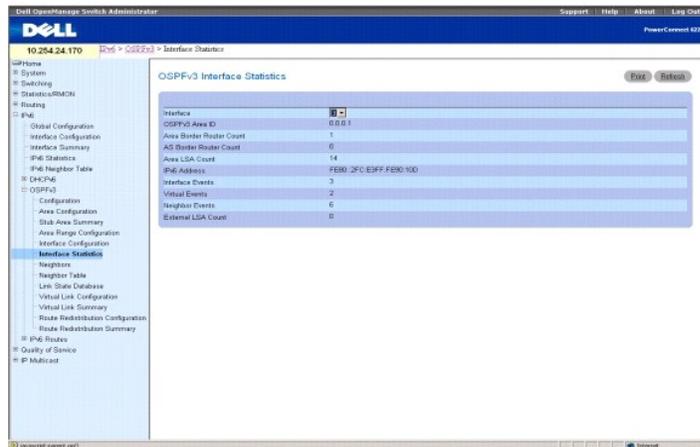
- 1 OSPFv3 Commands (Commandes OSPFv3)

Statistiques sur les interfaces OSPFv3

La page **OSPFv3 Interface Statistics** (Statistiques sur les interfaces OSPFv3) permet d'afficher les statistiques sur les interfaces OSPFv3. Les informations ne s'affichent que si l'interface OSPF est activée.

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Interface Statistics** (Statistiques sur les interfaces) dans l'arborescence.

Figure 11-24. Statistiques sur les interfaces OSPFv3



La page **OSPFv3 Interface Statistics** (Statistiques sur les interfaces OSPFv3) contient les champs suivants :

Interface : sélectionnez l'interface pour laquelle les données doivent être affichées.

OSPF Area ID (ID de zone OSPF) : zone OSPF à laquelle appartient l'interface du routeur sélectionnée. Cette valeur doit être un nombre entier de 32 bits à points décimaux qui identifie de manière unique la zone à laquelle l'interface est connectée.

Area Border Router Count (Nombre de routeurs de limite de zone) : nombre total de routeurs de limite de zone accessibles dans cette zone. La valeur initiale est égale à zéro, et est calculée pour chaque passage SPF.

AS Border Router Count (Nombre de routeurs de limites de systèmes autonomes) : nombre total de routeurs de limites de systèmes autonomes accessibles dans cette zone. La valeur initiale est égale à zéro, et est calculée pour chaque passage SPF.

Area LSA Count (Nombre de LSA dans la zone) : nombre total de LSA (Link State Advertisements) contenues dans la base de données LSDB (Link State Database) de cette zone, en excluant les LSA externes au système autonome.

IPv6 Address (Adresse IPv6) : adresse IP de l'interface.

Interface Events (Événements de l'interface) : nombre de changements d'état ou d'erreurs enregistrés sur l'interface OSPF spécifiée.

Virtual Events (Événements virtuels) : nombre de changements d'état ou d'erreurs enregistrés sur cette liaison virtuelle.

Neighbor Events (Événements liés au voisin) : nombre de changements d'état ou d'erreurs enregistrés sur la relation de ce voisin.

External LSA Count (Nombre de LSA externes) : nombre de LSA (Link State Advertisements) externes (LS de type 5) contenues dans la base de données LSDB (Link State Database).

Affichage des statistiques sur les interfaces OSPFv3

1. Affichez la page **OSPFv3 Interface Statistics** (Statistiques sur les interfaces OSPFv3).
2. Sélectionnez l'interface à afficher dans le menu déroulant **Interface**.

Les statistiques de l'interface s'affichent.

Affichage des statistiques sur les interfaces OSPFv3 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

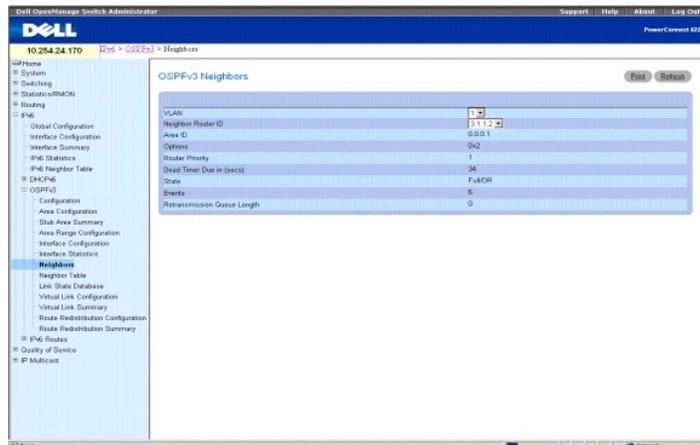
- 1 OSPFv3 Commands (Commandes OSPFv3)

Voisins OSPFv3

La page **OSPFv3 Neighbors** (Voisins OSPFv3) permet d'afficher la configuration des voisins OSPF pour un ID de voisin sélectionné. Lorsqu'un ID de voisin spécifique est indiqué, des informations détaillées sur ce voisin s'affichent. Les informations sur les voisins ne s'affichent que si le protocole OSPF est activé et que l'interface possède un voisin. L'adresse IP est celle du voisin.

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Neighbors** (Voisins) dans l'arborescence.

Figure 11-25. Voisins OSPFv3



La page **OSPFv3 Neighbors** (Voisins OSPFv3) contient les champs suivants :

Interface : permet de sélectionner l'interface pour laquelle les données doivent être affichées ou configurées.

Neighbor Router ID (ID du routeur voisin) : sélectionne l'adresse IP du voisin pour lequel vous souhaitez afficher les données.

Area ID (ID de zone) : nombre entier de 32 bits à points décimaux qui identifie le routeur voisin.

Options : capacités OSPF facultatives prises en charge par le voisin. Les capacités OSPF facultatives du voisin sont également répertoriées dans ses paquets Hello. Ce qui permet le rejet des paquets Hello reçus (les relations voisines ne débutent même pas) en cas de problème de comptabilité pour certaines capacités OSPF cruciales.

Router Priority (Priorité du routeur) : affiche la priorité OSPF pour le voisin spécifié. Cette valeur doit être un nombre entier compris entre 0 et 255. La valeur 0 indique que le routeur ne peut pas être défini comme routeur désigné sur ce réseau.

Dead Timer Due in (secs) (Temporisateur de panne, en secondes) : si les paquets Hello n'arrivent pas, indiquez la durée qui s'est écoulée avant que le voisin ne soit déclaré mort.

State (État) : un voisin peut avoir l'un des états suivants :

- 1 **Down** (Hors service) : état initial des communications d'un voisin. Cet état indique qu'aucune information n'a été transmise par le voisin. Sur les réseaux NBMA, il est toujours possible d'envoyer des paquets Hello aux voisins hors service, mais leur fréquence est limitée.
- 1 **Attempt** (Tentative) : cet état ne s'applique qu'aux voisins connectés aux réseaux NBMA. Il indique qu'aucune information récente n'a été transmise par le voisin, mais que des efforts plus concertés doivent être déployés pour le contacter. Pour ce faire, des paquets Hello doivent lui être envoyés à des intervalles Hello.
- 1 **Init** : cet état indique qu'un paquet Hello a été récemment transmis par le voisin. Toutefois, une communication bidirectionnelle n'a pas encore été établie avec le voisin (le routeur proprement dit n'apparaît pas dans le paquet Hello du voisin). Tous les voisins présentant cet état (ou un état supérieur) sont répertoriés dans les paquets Hello envoyés à partir de l'interface associée.
- 1 **2-Way** (Bidirectionnel) : cet état indique que la communication entre les deux routeurs est bidirectionnelle. Elle est assurée par le fonctionnement du protocole Hello. Cet état est le plus avancé, juste avant la début de la création d'une contiguïté. Le routeur désigné (sauvegarde) est sélectionné parmi l'ensemble des voisins présentant un état bidirectionnel ou supérieur.
- 1 **Exchange Start** (Démarrage de l'échange) : première étape dans la création d'une contiguïté entre les deux routeurs voisins. Elle a pour but de déterminer le routeur maître et de définir le numéro de séquence DD initial. Dans cet état ou un état supérieur, les communications des voisins sont appelées des contiguïtés.
- 1 **Exchange** (Échange) : dans cet état, le routeur décrit l'intégralité de sa base de données LSDB (Link State Database) en envoyant des paquets DBD (Database Description) au voisin. Des paquets LSU (Link State Request) peuvent également être envoyés pour demander les LSA plus récentes du voisin. Dans cet état ou un état supérieur, toutes les contiguïtés sont utilisées par la procédure d'acheminement. Elles sont pleinement capables de transmettre et de recevoir tous les types de paquets de protocole de routage OSPF.
- 1 **Loading** (En cours de chargement) : cet état indique que des paquets LSU (Link State Request) sont envoyés au voisin pour demander les LSA plus récentes détectées (mais pas encore reçues) dont l'état est Exchange (Échange).
- 1 **Full** (Complet) : cet état indique que les routeurs voisins sont totalement contigus. Ces contiguïtés apparaissent désormais dans les LSA associées au routeur et au réseau.

Events (Événements) : nombre de changements d'état ou d'erreurs enregistrés sur la relation de ce voisin.

Retransmission Queue Length (Longueur de la file d'attente de retransmission) : longueur actuelle de la file d'attente de retransmission.

Affichage des voisins OSPFv3

1. Affichez la page **OSPFv3 Neighbors** (Voisins OSPFv3).
2. Sélectionnez l'interface à afficher dans le menu déroulant **Interface**.
3. Sélectionnez **Neighbor Router ID** (ID du routeur voisin) à afficher.

Statistiques pour l'affichage de **Neighbor ID** (ID de voisin) de l'interface sélectionnée.

Affichage des voisins OSPFv3 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

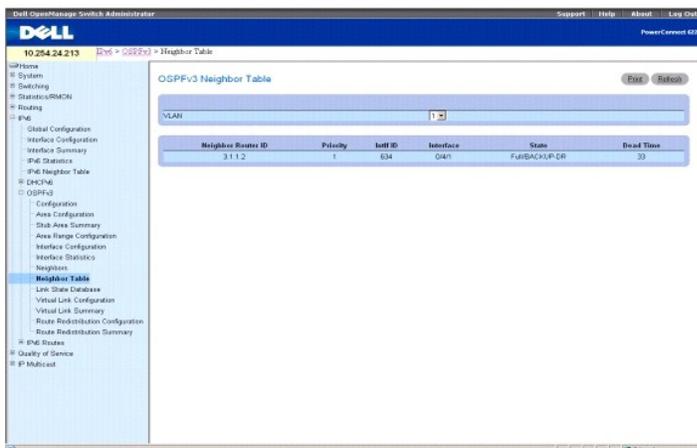
- 1 OSPFv3 Commands (Commandes OSPFv3)

Table des voisins OSPFv3

La page **OSPFv3 Neighbor Table** (Table des voisins OSPFv3) permet d'afficher la liste des tables des voisins OSPF. Lorsqu'un ID de voisin spécifique est indiqué, des informations détaillées sur un voisin s'affichent. La table des voisins ne s'affiche que si l'interface OSPF est activée.

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Neighbor Table** (Table des voisins) dans l'arborescence.

Figure 11-26. Table des voisins OSPFv3



La page **OSPFv3 Neighbor Table** (Table des voisins OSPFv3) contient les champs suivants :

Interface : permet de sélectionner l'interface pour laquelle les données doivent être affichées ou configurées.

Neighbor Router ID (ID du routeur voisin) : nombre entier de 32 bits à points décimaux représentant l'interface voisine.

Priority (Priorité) : priorité de ce voisin dans l'algorithme d'élection du routeur désigné. La valeur 0 indique que le voisin ne peut pas être défini comme routeur désigné sur ce réseau.

Hello ID : ID de l'interface que le voisin annonce dans ses paquets Hello sur cette liaison.

Interface : connecteur/port qui identifie l'index de l'interface voisine.

State (État) : état de la relation avec ce voisin.

Dead Time (Délai d'inactivité) : nombre de secondes écoulées depuis la dernière transmission Hello des voisins contigus. Définissez cette valeur sur 0 pour les voisins se trouvant dans un état égal ou inférieur à Init.

Affichage de la table des voisins OSPFv3

1. Affichez la page **OSPFv3 Neighbor Table** (Table des voisins OSPFv3).
2. Sélectionnez l'interface à afficher dans le menu déroulant **Interface**.

La table des voisins OSPF pour l'interface sélectionnée s'affiche.

Affichage de la table des voisins OSPFv3 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 OSPFv3 Commands (Commandes OSPFv3)

Base de données LSDB OSPFv3

La page OSPFv3 Link State Database (Base de données LSDB OSPFv3) permet d'afficher la base de données LSDB.

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Link State Database** (Base de données LSDB) dans l'arborescence.

Figure 11-27. Base de données LSDB OSPFv3

Adv. Router	Area ID	LSA Type	Link ID	Age	Sequence	Checksum	Options	Rtr Opt.
10.250.14.14	0.0.0.0	Intra Prefix	0	147	80000001	c50b		

La page **OSPFv3 Link State Database** (Base de données LSDB OSPFv3) contient les champs suivants :

Adv. Router (Routeur annoncé) : nombre entier de 32 bits à points décimaux qui identifie de manière unique le routeur dans le système autonome. L'ID du routeur est défini dans la page Configuration OSPFv3.

Area ID (ID de la zone) : ID d'une zone OSPF à laquelle l'une des interfaces du routeur est connectée. Cette valeur doit être un nombre entier de 32 bits à points décimaux qui identifie de manière unique la zone à laquelle une interface est connectée.

LSA Type (Type de LSA) : format et fonction de la LSA (Link State Advertisement). Les types (définis dans la section A.4 de la norme RFC 2740) peuvent être les suivants :

- 1 Router-LSA (LSA de routeur)
- 1 Network-LSA (LSA de réseau)
- 1 Inter-Area-Prefix-LSA (LSA de préfixe inter-zone)
- 1 Inter-Area-Router-LSA (LSA de routeur inter-zone)
- 1 AS-External-LSA (LSA externes au système)
- 1 Type-7-LSA (LSA de type 7)
- 1 Link-LSA (LSA de liaison)
- 1 Intra-Area-Prefix-LSA (LSA de préfixe intra-zone)

Link ID (ID de la liaison) : ce champ identifie la partie du domaine de routage décrit par l'annonce. Sa valeur dépend du type LS de l'annonce.

Age (Âge) : temps écoulé (en secondes) depuis la création de la LSA.

Sequence (Séquence) : ce numéro de séquence doit être un nombre entier signé de 32 bits. Il permet de détecter des LSA anciennes et en double. Plus le numéro de séquence est grand, plus l'annonce est récente.

Checksum (Somme de contrôle) : somme de contrôle utilisée pour détecter une altération des données dans une annonce. Cette altération peut se produire durant l'acheminement d'une annonce ou durant sa conservation dans la mémoire d'un routeur. Ce champ définit la somme de contrôle du contenu intégral de l'annonce, à l'exception du champ LS Age (Durée LS).

Options : le champ Options de l'en-tête LSA indique les capacités facultatives associées à l'annonce. Les options sont :

- 1 V6 : lorsque cette option est désactivée, la liaison est exclue des calculs de routage IPv6.
- 1 E : décrit la façon dont les LSA externes au système sont acheminés.
- 1 MC : indique si les datagrammes de multidiffusion IP sont transférés conformément aux spécifications.
- 1 N : décrit le traitement appliqué aux LSA de type 7.
- 1 R : indique si le demandeur est un routeur actif. L'option R représente le bit du routeur. Si elle n'est pas sélectionnée, les itinéraires qui transitent par le nœud d'annonce ne peuvent pas être calculés.
- 1 DC : décrit la façon dont le système traite les circuits de demande.

Rtr Opt. (Options du routeur) : affiche les options spécifiques au routeur.

Affichage de la base de données LSDB OSPFv3 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

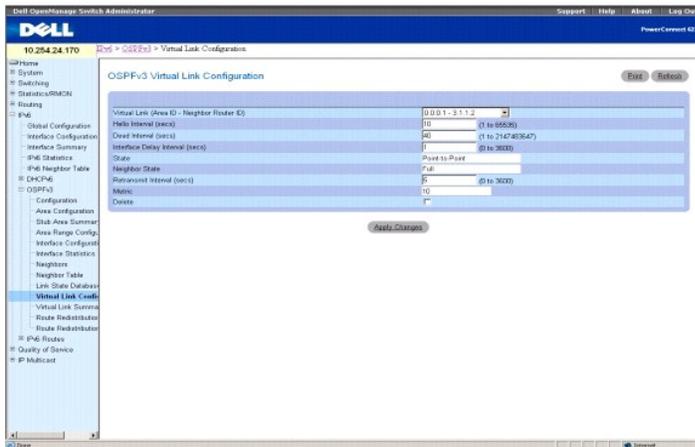
- 1 OSPFv3 Commands (Commandes OSPFv3)

Configuration des liaisons virtuelles OSPFv3

La page **OSPFv3 Virtual Link Configuration** (Configuration des liaisons virtuelles OSPFv3) permet de configurer un lien virtuel existant ou d'en définir un nouveau. Pour que vous puissiez afficher cette page, une zone OSPFv3 valide doit être définie dans la page **OSPFv3 Area Configuration** (Configuration de zone OSPFv3).

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Virtual Link Configuration** (Configuration des liaisons virtuelles) dans l'arborescence.

Figure 11-28. Configuration des liaisons virtuelles OSPFv3



La page **OSPFv3 Virtual Link Configuration** (Configuration des liaisons virtuelles OSPFv3) contient les champs suivants :

Create New Virtual Link (Créer une liaison virtuelle) : sélectionnez cette option dans le menu déroulant pour définir une nouvelle liaison virtuelle. La partie correspondant à la zone dans l'identification de la liaison virtuelle est fixe : vous êtes invité à entrer l'ID du routeur voisin dans un autre écran.

Virtual Link (Area ID - Neighbor Router ID) (Liaison virtuelle [ID de zone - ID du routeur voisin]) : sélectionnez la liaison virtuelle dont vous voulez afficher ou configurer les données. Elle comprend l'ID de zone et l'ID du routeur voisin.

Hello Interval (secs) (Intervalle Hello, secondes) : entrez l'intervalle Hello OSPFv3 pour l'interface spécifiée en secondes. Ce paramètre doit être identique pour tous les routeurs connectés à un réseau. La plage de valeurs admises est comprise entre 1 et 65 535. La valeur par défaut est de 10 secondes.

Dead Interval (secs) (Intervalle de mise hors service, secondes) : entrez l'intervalle OSPF de mise hors service (en secondes) correspondant à l'interface indiquée. Il désigne la durée pendant laquelle un routeur attend de recevoir des paquets Hello d'un routeur voisin avant de déclarer que ce routeur est hors service. Ce paramètre doit être identique pour tous les routeurs connectés à un réseau. Cette valeur doit être un multiple de l'intervalle Hello (par exemple 4). La plage de valeurs admises est comprise entre 1 et 2147483647. La valeur par défaut est de 40 secondes.

Interface Delay Interval (secs) (Intervalle de délai de l'interface, secondes) : entrez le délai de transition OSPFv3 pour l'interface spécifiée. Il désigne le nombre estimé de secondes pour transmettre un paquet LSU (Link State Update) sur l'interface sélectionnée. La plage de valeurs admises est comprise entre 1 et 3600 secondes (1 heure). La valeur par défaut est de 1 seconde.

State (État) : état actuel de la liaison virtuelle sélectionnée. Celle-ci peut avoir l'un des état suivants :

- 1 **Down** (Hors service) : état initial de l'interface. Cet état indique que les protocoles de niveau inférieur ont signalé que l'interface est inutilisable. Les paramètres de l'interface sont réinitialisés à leurs valeurs initiales. Toutes les horloges de l'interface sont désactivées, et aucune contiguïté n'est associée à l'interface.
- 1 **Waiting** (En attente) : le routeur tente de déterminer l'identité du routeur désigné (Sauvegarde) en contrôlant les paquets Hello reçus. Il n'est pas autorisé à sélectionner un routeur de sauvegarde désigné ou un routeur désigné tant que cet état est activé. Cela évite des modifications inutiles au routeur désigné (Sauvegarde).
- 1 **Point-to-Point** (Point à point) : l'interface est opérationnelle et connectée à la liaison virtuelle. Lorsque cet état est activé, le routeur tente de créer une contiguïté avec le routeur voisin. Les paquets Hello sont envoyés au voisin toutes les secondes de l'intervalle Hello.
- 1 **Designated Router** (Routeur désigné) : ce routeur est lui-même le routeur désigné sur le réseau connecté. Les contiguïtés sont créées pour tous les autres routeurs connectés au réseau. Le routeur doit également créer une LSA associée au nœud du réseau. Cette LSA contient les liens vers tous les routeurs (y compris le routeur désigné proprement dit) connectés au réseau.
- 1 **Backup Designated Router** (Routeur de sauvegarde désigné) : ce routeur est lui-même le routeur de sauvegarde désigné sur le réseau connecté. Il devient le routeur désigné en cas de défaillance du routeur désigné existant. Le routeur crée les contiguïtés pour tous les autres routeurs connectés au réseau. Le routeur de sauvegarde désigné exécute des fonctions légèrement différentes durant la procédure d'acheminement, par rapport au routeur désigné.
- 1 **Other Designated Router** (Autre routeur désigné) : l'interface est connectée à un réseau de diffusion ou NBMA sur lequel d'autres routeurs ont été choisis comme routeur désigné et routeur de sauvegarde désigné. Le routeur tente de créer des contiguïtés pour le routeur désigné et le routeur de sauvegarde désigné.

Neighbor State (État du voisinage) : état de la relation voisine virtuelle.

Retransmit Interval (Intervalle de retransmission) : entre l'intervalle de retransmission OSPF pour l'interface spécifiée. Il désigne le nombre de secondes entre les LSA (Link State Advertisements) pour les contiguités appartenant à cette interface de routeur. Cette valeur est également utilisée lors de la retransmission des descriptions de base de données et des paquets LSR (Link State Request). La plage de valeurs admises est comprise entre 1 et 3600 secondes (1 heure). La valeur par défaut est de 5 secondes.

Metric (Métrique) : métrique utilisée par la liaison virtuelle.

Delete (Supprimer) : supprime la liaison virtuelle spécifiée de la configuration du routeur.

Création d'une liaison virtuelle

1. Affichez la page **OSPFv3 Virtual Link Configuration** (Configuration des liaisons virtuelles OSPFv3).
2. Sélectionnez **Create New Virtual Link** (Créer une liaison virtuelle) dans le menu déroulant pour définir une nouvelle liaison virtuelle.
3. Entrez une valeur pour **Neighbor Router ID** (ID du routeur voisin).
4. Cliquez sur **Create** (Créer).

La liaison est créée et vous êtes renvoyé sur la page Virtual Link Configuration (Configuration des liaisons virtuelles).

Configuration de liaison virtuelle

1. Affichez la page **OSPFv3 Virtual Link Configuration** (Configuration des liaisons virtuelles OSPFv3).
2. Sélectionnez la liaison virtuelle à configurer.
3. Modifiez les autres champs selon vos besoins.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).
5. La liaison virtuelle est configurée pour OSPFv3 et le périphérique est mis à jour.

Configuration des liaisons virtuelles OSPFv3 à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 OSPFv3 Commands (Commandes OSPFv3)

Récapitulatif des liaisons virtuelles OSPFv3

La page **OSPFv3 Virtual Link Summary** (Récapitulatif des liaisons virtuelles OSPFv3) permet d'afficher les données sur la liaison virtuelle par Area ID (ID de zone) et Neighbor Router ID (ID du routeur voisin).

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Virtual Link Summary** (Récapitulatif des liaisons virtuelles) dans l'arborescence.

Figure 11-29. Récapitulatif des liaisons virtuelles OSPFv3

Area ID	Neighbor Router ID	Hello Interval (secs)	Dead Interval (secs)	Retransmit Interval (secs)	Interface Delay Interval (secs)
0.0.0.1	3.1.1.2	10	40	5	1

La page **OSPFv3 Virtual Link Summary** (Récapitulatif des liaisons virtuelles OSPFv3) contient les champs suivants :

Area ID (ID de zone) : partie correspondant à l'ID de zone dans l'identification de la liaison virtuelle dont vous voulez afficher les données. L'ID de zone et l'ID du routeur voisin définissent ensemble une liaison virtuelle.

Neighbor Router ID (ID du routeur voisin) : partie correspondant à l'ID du routeur voisin dans l'identification de la liaison virtuelle. Des liaisons virtuelles peuvent être configurées entre une paire de routeurs de limite de zone dont les interfaces sont situées dans une zone commune (qui n'est pas un segment principal).

Hello Interval (secs) (Intervalle Hello, secondes) : intervalle Hello d'OSPF (en secondes) correspondant à la liaison virtuelle. Cette valeur doit être identique pour tous les routeurs connectés à un réseau.

Dead Interval (secs) (Intervalle avant mise hors service, secondes) : intervalle d'inactivité OSPF (en secondes) correspondant à la liaison virtuelle. Il désigne la durée pendant laquelle un routeur attend de recevoir des paquets Hello d'un routeur voisin avant de déclarer que ce routeur est hors service. Ce paramètre doit être identique pour tous les routeurs connectés à un réseau commun, et être un multiple de l'intervalle Hello (par exemple, 4).

Retransmit Interval (secs) (Intervalle de retransmission, secondes) : intervalle de retransmission OSPF (en secondes) pour la liaison virtuelle. Il désigne le délai entre les LSA (Link State Advertisements) pour les contiguïtés appartenant à cette interface de routeur. Cette valeur est également utilisée lors de la retransmission des descriptions de base de données et des paquets LSR (Link State Request).

Interface Delay Interval (secs) (Intervalle de transition de l'interface, secondes) : délai de transition OSPF en unités de secondes pour la liaison virtuelle. Il désigne le nombre estimé de secondes pour transmettre un paquet LSU (Link State Update) sur cette interface.

Affichage du récapitulatif des liaisons virtuelles OSPFv3 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 OSPFv3 Commands (Commandes OSPFv3)

Configuration de la redistribution des itinéraires OSPFv3

La page **OSPFv3 Route Redistribution Configuration** (Configuration de la redistribution des itinéraires OSPFv3) permet de configurer la redistribution des itinéraires.

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Route Redistribution Configuration** (Configuration de la redistribution des itinéraires) dans l'arborescence.

Figure 11-30. Configuration de la redistribution des itinéraires OSPFv3



La page **OSPFv3 Route Redistribution Configuration** (Configuration de la redistribution des itinéraires OSPFv3) contient les champs suivants :

Configured Source (Source configurée) : ce menu déroulant est un sélecteur dynamique qui contient uniquement les itinéraires source configurés pour être redistribués par le protocole OSPF. **Create** (Créer) est l'option du haut dans la zone de sélection. Elle permet de configurer un autre itinéraire source parmi les itinéraires source disponibles. Les valeurs correctes sont **Static** (Statique), **Connected** (Connecté) et **Create** (Créer).

Available Source (Source disponible) : ce menu déroulant est un sélecteur dynamique qui contient uniquement les itinéraires source qui n'ont pas déjà été configurés pour être redistribués par le protocole OSPF. Ce menu ne s'affiche que si vous sélectionnez l'option **Create** (Créer) comme **Configured Source** (Source configurée). Les valeurs correctes sont **Static** (Statique) et **Connected** (Connecté).

Metric (Métrique) : définit la valeur de métrique à utiliser pour les itinéraires redistribués. Ce champ affiche la métrique si la source a été préconfigurée et qu'elle peut être modifiée. Les valeurs autorisées sont comprises entre 0 et 16777214.

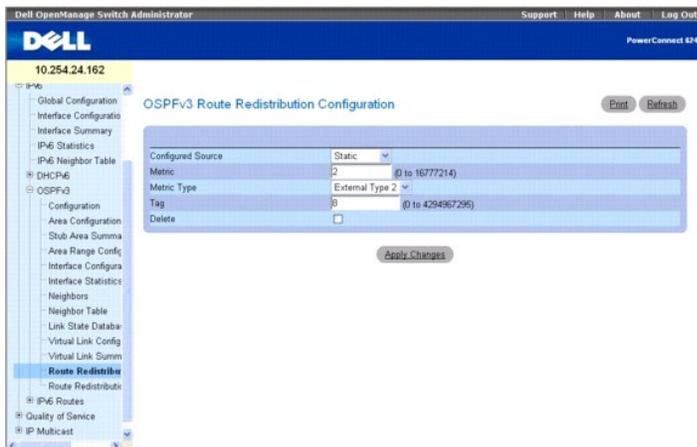
Metric Type (Type de métrique) : définit le type de métrique OSPF pour les itinéraires redistribués.

Tag (Numéro) : définit le champ des numéros dans les itinéraires redistribués. Ce champ présente le numéro si la source était préconfigurée, sinon la valeur 0 s'affiche. Les valeurs admises sont comprises entre 0 et 4294967295.

Configuration de la redistribution des itinéraires OSPFv3

1. Affichez la page **OSPFv3 Route Redistribution Configuration** (Configuration de la redistribution des itinéraires OSPFv3).
2. Spécifiez **Create** (Créer) pour définir une nouvelle source. Sélectionnez **Connected** (Connecté) ou **Static** (Statique) pour modifier une source existante.

Figure 11-31. Configuration de la redistribution des itinéraires OSPFv3 - Source configurée



3. Définissez ou modifiez les champs si nécessaire.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La redistribution des itinéraires sélectionnée est configurée pour OSPFv3 et le périphérique est mis à jour.

Configuration de la redistribution des itinéraires OSPFv3 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 OSPFv3 Commands (Commandes OSPFv3)

Récapitulatif de la redistribution des itinéraires OSPFv3

La page **OSPFv3 Route Redistribution Summary** (Récapitulatif de la redistribution des itinéraires OSPFv3) permet d'afficher les paramètres de la redistribution des itinéraires par la source.

Pour afficher cette page, cliquez sur **IPv6** → **OSPFv3** → **Route Redistribution Summary** (Récapitulatif de la redistribution des itinéraires) dans l'arborescence.

Figure 11-32. Récapitulatif de la redistribution des itinéraires OSPFv3

Source	Metric	Metric Type	Tag
Connected	2	External Type 2	5
Static	2	External Type 2	8

La page **OSPFv3 Route Redistribution Summary** (Récapitulatif de la redistribution des itinéraires OSPFv3) contient les champs suivants :

Source : itinéraire source devant être redistribué par le protocole OSPF.

Metric (Métrique) : métrique des itinéraires redistribués pour l'itinéraire source donné. Affiche Unconfigured (Non configuré) si cette option n'est pas configurée.

Metric Type (Type de métrique) : type de métrique OSPF pour les itinéraires redistribués.

Tag (Numéro) : champ des numéros dans les itinéraires redistribués. Ce champ présente le numéro si la source était préconfigurée, sinon la valeur 0 s'affiche.

Affichage du récapitulatif de la redistribution des itinéraires OSPFv3 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 OSPFv3 Commands (Commandes OSPFv3)

Itinéraires IPv6

La page de menu **IPv6 Routes** (Itinéraires IPv6) contient des liens vers les pages Web permettant de définir et d'afficher les paramètres et les données des itinéraires IPv6. Pour afficher cette page, cliquez sur **IPv6** → **IPv6 Routes** (Itinéraires IPv6) dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

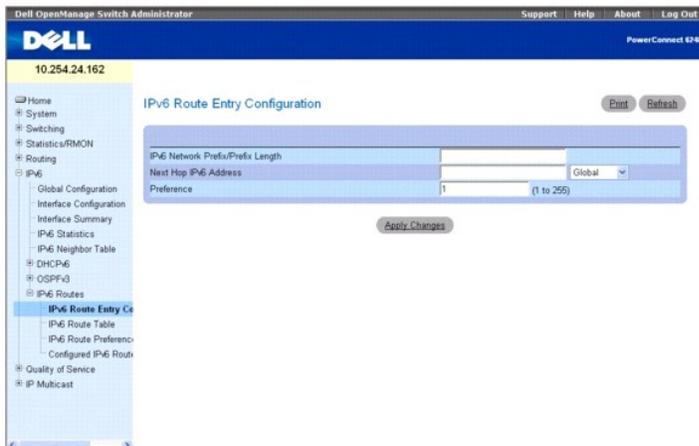
- 1 [Configuration des entrées de routage IPv6](#)
- 1 [Table de routage IPv6](#)
- 1 [Préférences de routage IPv6](#)
- 1 [Itinéraires IPv6 configurés](#)

Configuration des entrées de routage IPv6

La page **IPv6 Route Entry Configuration** (Configuration des entrées de routage IPv6) permet de configurer les informations pour les itinéraires IPv6.

Pour afficher cette page, cliquez sur **IPv6** → **IPv6 Routes** (Itinéraires IPv6) → **IPv6 Route Entry Configuration** (Configuration des entrées de routage IPv6) dans l'arborescence.

Figure 11-33. Configuration des entrées de routage IPv6



La page **IPv6 Route Entry Configuration** (Configuration des entrées de routage IPv6) contient les champs suivants :

IPv6 Network Prefix/PrefixLength (Préfixe réseau IPv6/Longueur du préfixe) : entrez une adresse réseau et un préfixe IPv6 valides.

Next Hop IPv6 Address (Adresse IPv6 du saut suivant) : entrez une adresse IPv6 pour le saut suivant. Si l'adresse IPv6 du saut suivant spécifiée est une adresse IPv6 locale-liaison, spécifiez l'interface pour l'adresse IPv6 du saut suivant de la liaison locale. Sélectionnez **Global** ou **Link-local** (Locale-liaison) dans le menu déroulant pour l'appliquer à cette adresse.

Preference (Préférence) : entrez une valeur de préférence pour l'itinéraire donné. Les valeurs correctes sont comprises entre 1 et 255, 1 étant la valeur par défaut.

Configuration des entrées de routage IPv6

1. Affichez la page **IPv6 Route Entry Configuration** (Configuration des entrées de routage IPv6).
2. Modifiez les champs selon vos besoins.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée de routage est configurée pour IPv6 et le périphérique est mis à jour.

Configuration de l'entrée de routage avec la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

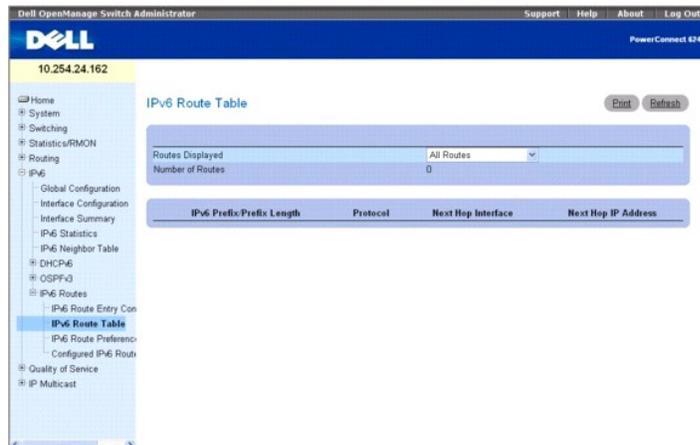
- 1 IPv6 Routing Commands (Commandes de routage IPv6)

Table de routage IPv6

La page **IPv6 Route Table** (Table de routage IPv6) permet d'afficher tous les itinéraires IPv6 actifs ainsi que leurs paramètres.

Pour afficher cette page, cliquez sur **IPv6** → **IPv6 Routes** (Itinéraires IPv6) → **IPv6 Route Table** (Table de routage IPv6) dans l'arborescence.

Figure 11-34. Table de routage IPv6



La page **IPv6 Route Table** (Table de routage IPv6) contient les champs suivants :

Routes Displayed (Itinéraires affichés) : sélectionnez cette option pour afficher les itinéraires configurés (Configured Routes), les meilleurs itinéraires (Best Routes) ou tous les itinéraires (All Routes) dans le menu déroulant.

Number of Routes (Nombre d'itinéraires) : affiche le nombre total d'itinéraires actifs/meilleurs itinéraires dans la table de routage pour le type d'itinéraire sélectionné.

IPv6 Prefix/Prefix Length (Préfixe IPv6/Longueur du préfixe) : affiche le préfixe de réseau et la longueur du préfixe pour l'itinéraire actif.

Protocol (Protocole) : affiche le type de protocole pour l'itinéraire actif.

Next Hop Interface (Interface du saut suivant) : affiche l'interface sur laquelle l'itinéraire est actif.

Next Hop IP Address (Adresse IP du saut suivant) : affiche l'adresse IPv6 du saut suivant pour l'itinéraire actif.

Affichage de la table de routage IPv6

1. Affichez la page **IPv6 Route Table** (Table de routage IPv6).
2. Sélectionnez le type d'itinéraire à afficher dans le champ **Routes Displayed** (Itinéraires affichés).

Les itinéraires sélectionnés s'affichent.

Affichage de la table de routage IPv6 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

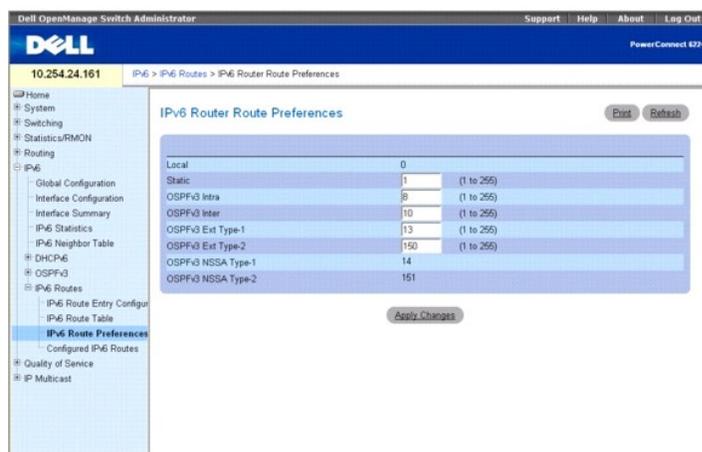
- 1 IPv6 Routing Commands (Commandes de routage IPv6)

Préférences de routage IPv6

La page **IPv6 Route Preferences** (Préférences de routage IPv6) permet de configurer les préférences par défaut pour chaque protocole. Ces valeurs sont des valeurs arbitraires comprises entre 1 et 255 qui sont indépendantes des métriques de routage. La plupart des protocoles de routage utilisent une métrique de routage pour déterminer le chemin le plus court connu du protocole, indépendamment de tout autre protocole. Pour choisir le meilleur itinéraire vers une destination, il faut sélectionner l'itinéraire dont la valeur de préférence est la plus faible. Lorsqu'il existe plusieurs itinéraires vers une destination, les valeurs de préférence sont utilisées pour déterminer l'itinéraire préféré. En cas d'égalité, l'itinéraire ayant la meilleure métrique de routage est choisi. Pour éviter les problèmes d'incompatibilité entre les métriques, vous devez configurer plusieurs valeurs de préférence pour chacun des protocoles.

Pour afficher cette page, cliquez sur **IPv6** → **IPv6 Routes** (Itinéraires IPv6) → **IPv6 Route Preferences** (Préférences de routage IPv6) dans l'arborescence.

Figure 11-35. Préférences de routage IPv6



La page **IPv6 Route Preferences** (Préférences de routage IPv6) contient les champs suivants. Dans chaque cas, les valeurs les plus faibles indiquent les plus grandes préférences.

Local : affiche la préférence locale. Ce champ n'est pas configurable. La valeur est 0, qui représente la préférence la plus élevée.

Static (Statique) : valeur de préférence pour l'itinéraire statique. La valeur par défaut est 1. La plage de valeurs est comprise entre 1 et 255.

OSPFv3 Intra (OSPFv3 intra-itinéraire) : valeur de préférence OSPFv3 intra-itinéraire associée au routeur. La valeur par défaut est de 8. Les valeurs admises sont comprises entre 1 et 255. La spécification OSPFv3 nécessite que la préférence soit accordée aux itinéraires appris via le protocole OSPFv3 dans l'ordre suivant : intra < inter < type-1 < type-2.

OSPFv3 Inter (OSPFv3 inter-itinéraire) : valeur de préférence OSPFv3 inter-itinéraire associée au routeur. La valeur par défaut est de 10. Les valeurs admises sont comprises entre 1 et 255. La spécification OSPFv3 nécessite que la préférence soit accordée aux itinéraires appris via le protocole OSPFv3 dans l'ordre suivant : intra < inter < type-1 < type-2.

OSPFv3 Type-1 : valeur de préférence pour l'itinéraire OSPFv3 de type 1. La valeur par défaut est de 13. Les valeurs admises sont comprises entre 1 et 255. La spécification OSPFv3 nécessite que la préférence soit accordée aux itinéraires appris via le protocole OSPFv3 dans l'ordre suivant : intra < inter < type-1 < type-2.

OSPFv3 Type-2 : valeur de préférence pour l'itinéraire OSPFv3 de type 2. La valeur par défaut est de 150. Les valeurs admises sont comprises entre 1 et 255. La spécification OSPFv3 nécessite que la préférence soit accordée aux itinéraires appris via le protocole OSPFv3 dans l'ordre suivant : intra < inter < type-1 < type-2.

OSPFv3 NSSA Type-1 : affiche la valeur de préférence pour l'itinéraire OSPFv3 NSSA de type 2.

OSPFv3 NSSA Type-2 : affiche la valeur de préférence pour l'itinéraire OSPFv3 NSSA de type 1.

Configuration des préférences de routage IPv6

1. Affichez la page **IPv6 Route Preferences** (Préférences de routage IPv6).
2. Configurez les préférences par défaut pour chaque protocole.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les préférences de routage sont configurées pour IPv6 et le périphérique est mis à jour.

Configuration des préférences de routage IPv6 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

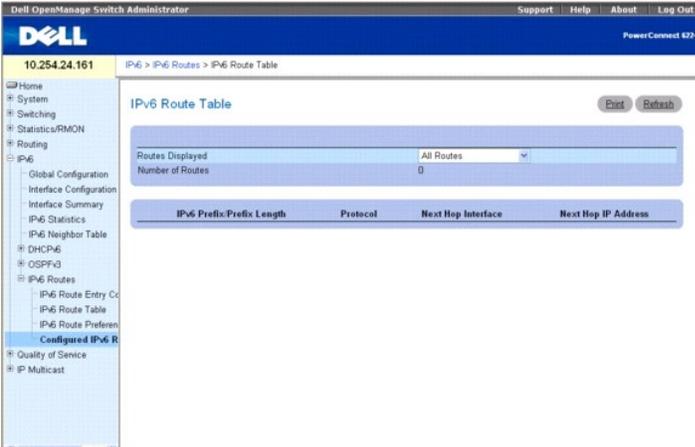
- 1 IPv6 Routing Commands (Commandes de routage IPv6)

Itinéraires IPv6 configurés

La page **Configured IPv6 Routes** (Itinéraires IPv6 configurés) permet d'afficher les itinéraires IPv6 sélectionnés.

Pour afficher cette page, cliquez sur **IPv6** → **IPv6 Routes** (Itinéraires IPv6) → **Configured IPv6 Routes** (Itinéraires IPv6 configurés) dans l'arborescence.

Figure 11-36. Itinéraires IPv6 configurés



La page **Configured IPv6 Routes** (Itinéraires IPv6 configurés) contient les champs suivants :

Routes Displayed (Itinéraires affichés) : sélectionnez cette option pour afficher les itinéraires configurés (Configured Routes), les meilleurs itinéraires (Best Routes) ou tous les itinéraires (All Routes).

Lorsque l'option Configured Routes (Itinéraires configurés) est sélectionnée, les champs suivants s'affichent :

IPv6 Prefix/Prefix Length (Préfixe IPv6/Longueur du préfixe) : affiche le préfixe de réseau et la longueur du préfixe pour l'itinéraire configuré.

Next Hop IP (IP du saut suivant) : affiche l'adresse IPv6 du saut suivant pour l'itinéraire configuré.

Next Hop Interface (Interface du saut suivant) : affiche l'interface du saut suivant pour l'itinéraire configuré.

Preference (Préférence) : affiche la préférence de routage pour l'itinéraire configuré.

Delete (Supprimer) : cliquez sur cette case et sur le bouton Refresh (Actualiser) pour supprimer l'itinéraire affiché.

Lorsque les options Best Routes (Meilleurs itinéraires) ou All Routes (Tous les itinéraires) sont sélectionnées, les champs suivants s'affichent :

Number of Routes (Nombre d'itinéraires) : indique le nombre de meilleurs itinéraires ou de l'ensemble des itinéraires.

IPv6 Prefix/Prefix Length (Préfixe IPv6/Longueur du préfixe) : affiche le préfixe de réseau et la longueur du préfixe pour l'itinéraire configuré.

Protocol (Protocole) : indique le protocole utilisé pour les itinéraires configurés.

Next Hop Interface (Interface du saut suivant) : affiche l'interface du saut suivant pour l'itinéraire configuré.

Next Hop IP Address (Adresse IP du saut suivant) : affiche l'adresse IPv6 du saut suivant pour l'itinéraire configuré.

Affichage des itinéraires IPv6

1. Affichez la page **Configured IPv6 Routes** (Itinéraires IPv6 configurés).
2. Sélectionnez les itinéraires à afficher dans le menu déroulant **Routes Displayed** (Itinéraires affichés).

Les itinéraires sélectionnés et leurs configurations s'affichent.

Affichage des itinéraires IPv6 à l'aide de la commande CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 IPv6 Routing Commands (Commandes de routage IPv6)

[Retour au sommaire](#)

[Retour au sommaire](#)

Configuration de la qualité de service

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Présentation de la qualité de service](#)
- [Configuration des services différenciés](#)
- [Classe de service](#)

Cette section présente un aperçu de la qualité de service (QoS). Elle décrit les fonctions accessibles à partir de la page Quality of Service (Qualité de service) : Differentiated Services (Services différenciés) et Class of Service (Classe de service).

Présentation de la qualité de service

Dans un commutateur type, chaque port physique est constitué d'une ou plusieurs files d'attente destinées à la transmission des paquets sur le réseau connecté. Un port offre souvent plusieurs files d'attente permettant de privilégier certains paquets par rapport à d'autres, en fonction de critères définis par l'utilisateur. Lorsqu'un paquet est mis en file d'attente avant d'être transmis, la vitesse à laquelle il est traité dépend de la configuration de la file d'attente et, éventuellement, du trafic présent dans les autres files d'attente du port. Si un délai est nécessaire, les paquets sont maintenus en file d'attente jusqu'à ce que le planificateur autorise leur transmission. Lorsque les files d'attente sont saturées, les paquets ne peuvent plus y être placés ; ils sont alors éliminés par le commutateur.

QoS assure une transmission cohérente et prévisible des données en différenciant les paquets urgents de ceux qui peuvent tolérer un léger retard. Dans un réseau prenant en charge QoS, les paquets urgents bénéficient d'un "traitement spécial". Pour que cela soit possible, tous les éléments du réseau doivent prendre en charge QoS. La présence d'au moins un noeud ne prenant pas en charge QoS crée une déficience dans le réseau, laquelle peut compromettre les performances de tout le flux de paquets.

Pour afficher la page appropriée, cliquez sur **Quality of Service** (Qualité de service) dans l'arborescence. Deux liens présents sur cette page correspondent aux deux types de QoS disponibles. Ces liens sont les suivants :

- 1 [Configuration des services différenciés](#)
 - 1 [Classe de service](#)
-

Configuration des services différenciés

Présentation de DiffServ

La fonction QoS prend en charge les services différenciés (DiffServ). Ces derniers permettent d'organiser le trafic en différents flux et de les traiter en fonction des actions définies pour chaque saut individuel.

Les réseaux IP standard sont conçus pour fournir des services de transmission de données "au mieux". Avec ce mode de transmission, les données sont envoyées dans les meilleurs délais possibles, mais sans garantie de livraison. Lors des périodes de trafic intense, les paquets peuvent être retardés, envoyés de façon irrégulière ou éliminés. Dans le cas des applications Internet courantes telles que la messagerie électronique et le transfert de fichiers, une légère diminution des performances est acceptable et peut parfois même passer inaperçue. À l'inverse, les applications ayant des exigences élevées en termes de délais (applications vocales ou multimédia, par exemple), ne tolèrent aucune baisse de performances.

Définition de DiffServ

Avant d'utiliser DiffServ pour QoS, vous devez définir les catégories et critères suivants à partir des pages Web accessibles via la page **Differentiated Services** (Services différenciés) :

1. **Classe** : création de classes et définitions des critères associés
2. **Stratégie** : création de stratégies, association de classes et définition des règles correspondantes
3. **Service** : ajout d'une stratégie à une interface d'entrée

Les paquets sont classés et traités en fonction des critères définis. Les critères de classification sont définis par une classe. Le traitement est défini par les attributs d'une stratégie. Les attributs d'une stratégie peuvent être définis pour chaque instance de classe. Ce sont ces attributs qui sont appliqués en cas de correspondance. Une stratégie peut contenir plusieurs classes. Lorsqu'une stratégie est active, les actions entreprises dépendent de la classe à laquelle correspond le paquet.

Le traitement des paquets débute par une mise en comparaison des critères associés aux paquets et aux classes. Lorsque les critères d'un paquet correspondent à une classe, celle-ci est appliquée au paquet.

La page de menus **Differentiated Services** (Services différenciés) comporte plusieurs liens vers les différentes fonction d'affichage et de configuration de DiffServ.

Pour afficher cette page, cliquez sur **Quality of Service** (Qualité de service) → **Differentiated Services** (Services différenciés) dans l'arborescence. La page correspondante contient des liens vers les fonctionnalités suivantes :

- 1 [Configuration de DiffServ](#)

- 1 [Configuration des classes](#)
- 1 [Critères des classes](#)
- 1 [Configuration d'une stratégie](#)
- 1 [Définition des classes d'une stratégie](#)
- 1 [Configuration d'un service](#)
- 1 [Statistiques détaillées sur un service](#)

Configuration de DiffServ

Utilisez la page **DiffServ Configuration** (Configuration des services différenciés) pour afficher des informations d'état générales sur DiffServ telles que le mode administratif en cours et le nombre maximal de lignes dans chaque table MIB privée DiffServ.

Pour afficher cette page, cliquez sur **Quality of Service** (Qualité de service) → **Differentiated Services** (Services différenciés) → **DiffServ Configuration** (Configuration de DiffServ) dans l'arborescence.

Figure 12-1. Page DiffServ Configuration (Configuration de DiffServ)



Cette page contient les champs suivants :

DiffServ Admin Mode (Mode administratif DiffServ) : permet d'activer et de désactiver le mode administratif. Lorsqu'il est désactivé, la configuration de DiffServ est conservée et peut être modifiée, mais elle n'est pas active. Lorsqu'il est activé, les services différenciés sont actifs.

Table MIB

Class Table (Table de classe) : affiche le nombre de lignes en cours et maximal de la table de classes.

Class Rule Table (Table des règles de classes) : affiche le nombre de lignes en cours et maximal de la table des règles de classes.

Policy Table (Table des stratégies) : affiche le nombre de lignes en cours et maximal de la table des stratégies.

Policy Instance Table (Table des instances de stratégies) : affiche le nombre de lignes en cours et maximal de la table des instances de stratégies.

Policy Attributes Table (Table des attributs de stratégies) : affiche le nombre de lignes en cours et maximal de la table des attributs de stratégies.

Service Table (Table des services) : affiche le nombre de lignes en cours et maximal de la table des services.

Modification du mode administratif de DiffServ

1. Affichez la page **DiffServ Configuration** (Configuration de DiffServ).
2. Sélectionnez **Enable** (Activer) ou **Disable** (Désactiver) dans le menu déroulant en regard du champ **DiffServ Admin Mode** (Mode Admin DiffServ).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mode administratif de DiffServ est modifié et le périphérique est mis à jour.

Affichage des tables MIB à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

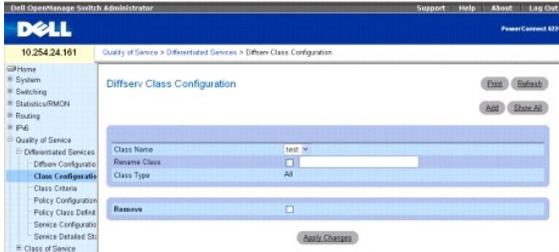
- 1 QoS Commands (Commandes QoS)

Configuration des classes

Utilisez la page **DiffServ Class Configuration** (Configuration des classes DiffServ) pour ajouter un nouveau nom de classe DiffServ, ou pour renommer ou supprimer une classe existante.

Pour afficher cette page, cliquez sur **Quality of Service** (Qualité de service) → **Differentiated Services** (Services différenciés) → **Class Configuration** (Configuration des classes) dans l'arborescence.

Figure 12-2. Page DiffServ Class Configuration (Configuration des classes DiffServ)



Cette page contient les champs suivants :

Class Name (Nom de classe) : permet de sélectionner un nom de classe à renommer ou supprimer. Cliquez sur **Add** (Ajouter) pour définir un nouveau nom de classe.

Rename Class (Renommer une classe) : permet de renommer la classe affichée (vous devez cocher la case et entrer un nouveau nom).

Class Type (Type de classe) : répertorie tous les types de classe. À ce jour, le matériel ne prend en charge que la valeur **All** (Tous).

All (Tous) : tous les critères de correspondance définis pour la classe doivent être satisfaits pour qu'une correspondance soit établie. **All** représente l'opérateur logique **AND** (et).

Remove (Supprimer) : supprime le nom de classe affiché (vous devez cocher la case et cliquer sur **Apply Changes** [Appliquer les modifications]).

Changement de nom d'une configuration de classe

1. Affichez la page **Class Configuration** (Configuration des classes).
2. Sélectionnez le nom de classe à modifier dans le menu déroulant **Class Name** (Nom de classe).
3. Cochez la case **Rename Class** (Renommer la classe) et saisissez le nouveau nom dans le champ adjacent.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de classe est renommée et le périphérique est mis à jour.

Ajout d'une configuration de classe DiffServ

1. Affichez la page **Class Configuration** (Configuration des classes).
2. Cliquez sur **Add** (Ajouter).

La page **Add DiffServ Class** (Ajouter une classe DiffServ) s'affiche.

Figure 12-3. Page Add DiffServ Class (Ajouter une classe DiffServ)



3. Saisissez le nouveau nom dans le champ **Class Name** (Nom de classe).

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nom de classe est ajouté et le périphérique est mis à jour.

Suppression d'une configuration de classe

1. Affichez la page **Class Configuration** (Configuration des classes).
2. Sélectionnez le nom de classe à supprimer dans le menu déroulant **Class Name** (Nom de classe).
3. Cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de classe associée est supprimée et le périphérique est mis à jour.

Affichage des configurations de classe

1. Affichez la page **Class Configuration** (Configuration des classes).
2. Cliquez sur **Show All** (Afficher tout).

La page **DiffServ Class Summary** (Récapitulatif des classes DiffServ) répertorie toutes les configurations de classe existantes.

Figure 12-4. Page DiffServ Class Summary (Récapitulatif des classes DiffServ)

	Class Name	Class Type	Reference Class
1	Class B	All	Class A
2	Class A	All	Class A
3	Class C	All	Class B

Ajout d'une configuration de classe à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

1. QoS Commands (Commandes QoS)

Critères des classes

Utilisez la page **DiffServ Class Criteria** (Critères des classes DiffServ) pour définir les critères à associer à une classe DiffServ. À mesure que les paquets sont reçus, ces classes DiffServ sont utilisées pour leur affecter une priorité.

Pour afficher cette page, cliquez sur **Quality of Service** (Qualité de service) → **Differentiated Services** (Services différenciés) → **Class Criteria** (Critères des classes) dans l'arborescence.

Figure 12-5. Page DiffServ Class Criteria (Critères des classes DiffServ)

Cette page contient les champs suivants :

Class Name (Nom de classe) : permet de sélectionner le nom de la classe pour laquelle vous définissez les critères.

Class Type (Type de classe) : affiche le type de classe. La seule option configurable est **All** (Tous).

Attributs de correspondance

Utilisez les champs suivants pour faire correspondre les paquets à une classe. Cochez la case correspondant à chaque critère voulu et saisissez des informations dans le champ adjacent. Une même classe peut comporter plusieurs critères de correspondance. Les critères sont associés entre eux par l'opérateur booléen "logical-and" (ET logique).

Source IP Address (Adresse IP source) : l'adresse IP du port source associé à un paquet doit correspondre à l'adresse indiquée ici.

Subnet Mask (Masque de sous-réseau) : indique le masque de sous-réseau associé à l'adresse IP source. Ce champ doit être renseigné lorsque la case **Source IP Address** (Adresse IP source) est cochée.

Destination IP Address (Adresse IP de destination) : l'adresse IP du port de destination associé à un paquet doit correspondre à l'adresse indiquée ici.

Subnet Mask (Masque de sous-réseau) : indique le masque de sous-réseau associé à l'adresse IP de destination. Ce champ doit être renseigné lorsque la case **Destination IP Address** (Adresse IP de destination) est cochée.

Source L4 Port (Port L4 source) : le port source TCP/UDP d'un paquet doit correspondre au port indiqué ici. Choisissez l'une des options suivantes :

Select From List (Sélectionner dans la liste) : cliquez pour sélectionner un port source dans une liste de ports source connus avec lesquels les paquets sont mis en correspondance.

Match to Port (Comparer avec le port) : cliquez pour ajouter un ID de port défini par l'utilisateur avec lequel les paquets sont mis en correspondance.

Destination L4 Port (Port L4 de destination) : le port TCP/UDP de destination d'un paquet doit correspondre au port indiqué ici. Choisissez l'une des options suivantes :

Select From List (Sélectionner dans la liste) : cliquez pour sélectionner un port de destination dans une liste de ports source connus avec lesquels les paquets sont mis en correspondance.

Match to Port (Comparer avec le port) : cliquez pour ajouter un ID de port défini par l'utilisateur avec lequel les paquets sont mis en correspondance.

Protocol (Protocole) : le protocole d'un paquet doit correspondre au protocole indiqué. Choisissez l'une des options suivantes :

Select from List (Sélectionner dans la liste) : permet d'effectuer une sélection dans la liste déroulante répertoriant les protocoles.

Match to Protocol ID (Comparer avec un ID de protocole) : entrez un ID de protocole avec lequel les paquets doivent être comparés.

EtherType : le type Ethernet d'une trame doit correspondre à la valeur indiquée ici. Choisissez l'une des options suivantes :

Select from List (Sélectionner dans la liste) : permet d'effectuer une sélection dans la liste déroulante répertoriant les types Ethernet.

Match to Port (Comparer avec un port) : entrez un ID de type Ethernet avec lequel les paquets doivent être comparés.

Class of Service (CoS) (Classe de service) : la classe de service des paquets entrants doit correspondre à la valeur indiquée ici.

Source MAC Address (Adresse MAC source) : l'adresse MAC source des paquets entrants doit correspondre à l'adresse indiquée ici.

Source MAC Mask (Masque de l'adresse MAC source) : définit le masque à caractères génériques correspondant à l'adresse MAC source. Les masques à caractères génériques déterminent les bits qui sont utilisés et ceux qui sont ignorés. Un masque à caractères génériques de 255.255.255.255 signifie qu'aucun bit n'est important. Un masque à caractères génériques de 0.0.0.0 indique que tous les bits sont importants. Ce champ doit être renseigné lorsque la case **Source MAC Address** (Adresse MAC source) est cochée.

Destination MAC Address (Adresse MAC de destination) : l'adresse MAC de destination des paquets entrants doit correspondre à l'adresse indiquée ici.

Destination MAC Mask (Masque de l'adresse MAC de destination) : définit le masque à caractères génériques correspondant à l'adresse MAC de destination. Les masques à caractères génériques déterminent les bits qui sont utilisés et ceux qui sont ignorés. Un masque à caractères génériques de 255.255.255.255 signifie qu'aucun bit n'est important. Un masque à caractères génériques de 0.0.0.0 indique que tous les bits sont importants. Ce champ doit être renseigné lorsque la case **Destination MAC Address** (Adresse MAC de destination) est cochée.

VLAN ID (ID de VLAN) : l'ID de VLAN associé aux paquets entrants doit correspondre à celui indiqué ici.

Secondary VLAN ID (ID de VLAN secondaire) : l'ID de VLAN secondaire associé aux paquets entrants doit correspondre à celui indiqué ici.

Reference Class (Classe de référence) : sélectionne une classe à utiliser pour activer le référencement des critères. Cochez la case **Add DiffServ Class** (Ajouter une classe DiffServ) et sélectionnez une classe DiffServ précédemment configurée à partir du menu déroulant associé.

Critères des types de service

Sélectionnez l'un des champs de correspondance suivants afin de l'utiliser pour la mise en correspondance des paquets et des critères de classe :

IP DSCP (DSCP IP) : compare le code DSCP du paquet avec le critère de la classe. Sélectionnez le type DSCP dans le menu déroulant ou entrez la valeur DSCP à utiliser pour la comparaison.

IP Precedence (Précédence IP) : lorsque cette option est sélectionnée et que vous entrez une valeur, le système compare la valeur de précédence IP du paquet avec le critère de la classe.

IP TOS Bits (Bits du type de service IP) : lorsque cette option est sélectionnée et que vous entrez une valeur, le système compare les bits du type de service figurant dans l'en-tête IP du paquet avec le critère de la classe.

Match Every (Comparer tous les critères) : exige du paquet qu'il réponde à tous les critères.

Définition des critères d'une classe

1. Affichez la page **DiffServ Class Criteria** (Critères des classes DiffServ).
2. Utilisez le menu déroulant **Class Name** (Nom de la classe) pour sélectionner la classe pour laquelle vous souhaitez définir des attributs de comparaison.
3. Sélectionnez les attributs à comparer pour cette classe et définissez les critères correspondants.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les critères sont ajoutés à la classe et le périphérique est mis à jour.

Configuration des critères d'une classe à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

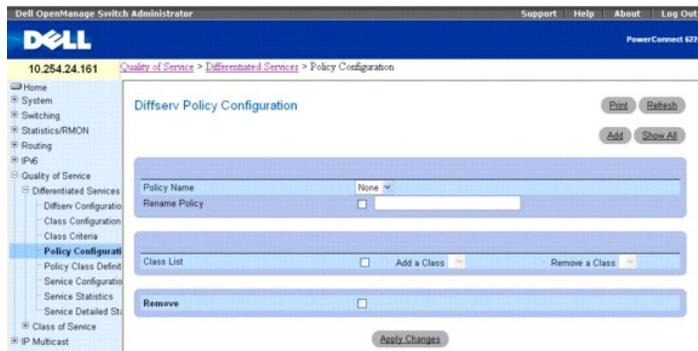
1. QoS Commands (Commandes QoS)

Configuration des stratégies

Utilisez la page **DiffServ Policy Configuration** (Configuration des stratégies DiffServ) pour associer un ensemble de classes à une ou plusieurs règles de stratégies.

Pour afficher cette page, cliquez sur **Quality of Service** (Qualité de service) → **Differentiated Services** (Services différenciés) → **Policy Configuration** (Configuration des stratégies) dans l'arborescence.

Figure 12-6. Page DiffServ Policy Configuration (Configuration des stratégies DiffServ)



Cette page contient les champs suivants :

Policy Name (Nom de la stratégie) : permet de sélectionner le nom de la stratégie à associer aux classes.

Rename Policy (Renommer une stratégie) : permet de renommer une stratégie. La modification est effectuée lorsque vous cliquez sur **Apply Changes** (Appliquer les modifications).

Class List (Liste de classes) : permet de définir les associations de classes correspondant à la stratégie.

Add a Class (Ajouter une classe) : permet d'associer la classe sélectionnée dans le menu déroulant à une stratégie.

Remove a Class (Supprimer une classe) : permet de supprimer la classe sélectionnée de la stratégie.

Remove (Supprimer) : supprime la stratégie sélectionnée du périphérique.

Association d'une classe à une stratégie et suppression d'une association

1. Affichez la page **DiffServ Policy Configuration** (Configuration des stratégies DiffServ).
2. Sélectionnez le nom de la stratégie à associer à la classe dans le champ **Policy Name** (Nom de la stratégie).
3. Dans le champ **Class List** (Liste des classes), cochez la case et cliquez sur le bouton radio **Add a Class** (Ajouter une classe) ou **Remove a Class** (Retirer une classe). Sélectionnez ensuite la classe voulue dans le menu déroulant approprié.

L'option **Add a Class** (Ajouter une classe) permet d'associer une classe à la stratégie. L'option **Remove a Class** (Retirer une classe) permet de retirer la classe de la stratégie.

4. Sélectionnez la classe concernée dans le menu déroulant approprié.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La stratégie modifiée est enregistrée et le périphérique est mis à jour.

Changement de nom d'une stratégie

1. Affichez la page **DiffServ Policy Configuration** (Configuration des stratégies DiffServ).
2. Sélectionnez le nom de la stratégie à renommer dans le champ **Policy Name** (Nom de la stratégie).
3. Pour renommer la stratégie, cochez l'option **Rename Policy** (Renommer une stratégie) et entrez le nouveau nom dans le champ adjacent.

Le nom de stratégie modifié est enregistré et le périphérique est mis à jour.

Ajout d'une nouvelle stratégie

1. Affichez la page **DiffServ Policy Configuration** (Configuration des stratégies DiffServ).
2. Cliquez sur **Add** (Ajouter).

La page **Add DiffServ Policy** (Ajouter une stratégie DiffServ) s'affiche.

Figure 12-7. Page Add DiffServ Policy (Ajouter une stratégie DiffServ)

Add DiffServ Policy

Print Refresh

Policy Name (1 - 31 alphanumeric characters)

Apply Changes Back

3. Complétez le champ **Policy name** (Nom de la stratégie) en indiquant le nom de la nouvelle stratégie.
 4. Cliquez sur **Apply Changes** (Appliquer les modifications).
- La nouvelle stratégie est enregistrée et le périphérique est mis à jour.

Affichage du récapitulatif des stratégies

1. Affichez la page **Policy Configuration** (Configuration des stratégies).
2. Cliquez sur **Show All** (Afficher tout).

La page **DiffServ Policy Summary** (Récapitulatif des stratégies DiffServ) affiche le nom de toutes les stratégies, ainsi que leur type et les classes qui en font partie.

Figure 12-8. Page **DiffServ Policy Summary** (Récapitulatif des stratégies DiffServ)

DiffServ Policy Summary

Print Refresh

	Policy Name	Member Classes
1	Policy1	
2	Policy2	

Back

Suppression d'une configuration de stratégie

1. Affichez la page **DiffServ Policy Configuration** (Configuration des stratégies DiffServ).
2. Sélectionnez le nom de la stratégie à supprimer dans le menu déroulant **Policy Name** (Nom de la stratégie).
3. Cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de stratégie associée est supprimée et le périphérique est mis à jour.

Définition des configurations de stratégies à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

1. QoS Commands (Commandes QoS)

Définition des classes d'une stratégie

La page **DiffServ Policy Class Definition** (Définition des classes d'une stratégie DiffServ) permet d'associer une classe à une stratégie et de définir les attributs de l'instance correspondante.

Pour afficher cette page, cliquez sur **Quality of Service** (Qualité de service) → **Differentiated Services** (Services différenciés) → **Policy Class Definition** (Définition des classes d'une stratégie) dans l'arborescence.

Figure 12-9. Page **DiffServ Policy Class Definition** (Définition des classes d'une stratégie DiffServ)



Cette page contient les champs suivants :

Policy Name (Nom de la stratégie) : le menu déroulant permet de sélectionner la stratégie à associer à une classe membre.

Member Classes (Classes membres) : le menu déroulant permet de sélectionner la classe à associer avec la stratégie.

Drop Packets (Rejeter les paquets) : sélectionnez ce champ pour rejeter les paquets correspondant à cette classe de stratégie.

Assign Queue (Affecter à une file d'attente) : les paquets correspondant à cette classe de stratégie sont ajoutés à une file d'attente. Les valeurs admises sont comprises entre 0 et 6.

Traffic Conditioning (Conditionnement de trafic) : lorsque cette option est cochée, elle permet d'affecter un type de conditionnement de trafic correspondant à la condition sélectionnée dans le menu déroulant. Ce champ détermine le traitement appliqué au trafic correspondant à cette classe de stratégie. Les options disponibles sont **None** (Aucun), **Marking** (Marquage) et **Policing** (Vérification de conformité). Lorsque les options **Marking** (Marquage) et **Policing** (Vérification de conformité) sont sélectionnées, l'écran change pour afficher les champs appropriés.

- 1 **None** (Aucun) : indique qu'aucun conditionnement du trafic n'est effectué lors du traitement des paquets. Cette option est utilisée par défaut.
- 1 **Marking** (Marquage) : permet de marquer l'un des champs suivants du paquet : IP DSCP (Code DSCP IP), IP Precedence (Précédence IP), Class of Service (Classe de service). Pour plus d'informations sur les champs qui s'affichent lorsque l'option **Marking** (Marquage) est sélectionnée, voir [Conditionnement du trafic par marquage des paquets](#).
- 1 **Policing** (Vérification de conformité) : permet de définir les modalités d'application de la stratégie, ainsi que le traitement appliqué aux paquets considérés comme conformes ou non-conformes. Pour plus d'informations sur les champs qui s'affichent lorsque l'option **Policing** (Vérification de conformité) est sélectionnée, voir [Conditionnement du trafic par vérification de la conformité](#).

Redirect Interface (Interface de redirection) : permet d'indiquer si l'interface de redirection s'applique à cette classe de stratégie et de définir l'interface ou le LAG à utiliser.

Flow Based Mirroring (Mise en miroir basée sur les flux) : permet d'indiquer si la mise en miroir basée sur les flux s'applique à cette classe de stratégie et de définir l'interface ou le LAG à utiliser.

Définition d'une instance de classe de stratégie

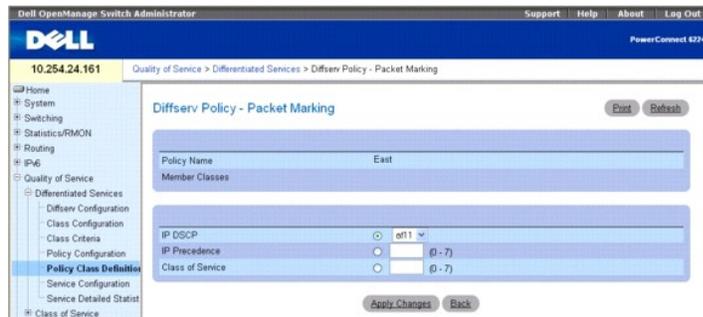
1. Affichez la page **DiffServ Policy Class Definition** (Définition des classes de stratégies DiffServ).
2. Sélectionnez une stratégie et une classe membre à associer.
3. Utilisez les autres champs de cette page pour définir les attributs à appliquer à cette instance de classe de stratégie.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La classe de stratégie est définie et le périphérique est mis à jour.

Conditionnement du trafic par marquage des paquets

Lorsque l'option **Marking** (Marquage) est sélectionnée dans le champ **Traffic Conditioning** (Conditionnement du trafic), la page suivante s'affiche :

Figure 12-10. Définition d'une classe de stratégie - Marquage des paquets



Cette page contient les champs suivants :

Policy Name (Nom de la stratégie) : indique la stratégie associée à une classe membre.

Member Classes (Classes membres) : affiche la classe membre associée à ce nom de stratégie.

Les champs pouvant être marqués sont les suivants :

IP DSCP (Code DSCP IP) : permet de sélectionner le code DSCP IP à marquer. Vous pouvez effectuer une sélection dans le menu déroulant ou compléter le champ User Value (Valeur utilisateur).

IP Precedence (Précédence IP) : permet de sélectionner le numéro de file d'attente de priorité IP à marquer.

Class of Service (Classe de service) : permet de sélectionner le numéro de file d'attente CoS (Classe de service) à marquer.

Configuration du marquage des paquets pour une instance de classe de stratégie

1. Sélectionnez **Marking** (Marquage) dans le menu déroulant **Traffic Conditioning** (Conditionnement du trafic) de la page **DiffServ Policy Class Definition** (Définition d'une classe de stratégie DiffServ).

La page **Packet Marking** (Marquage de paquets) représentée [Figure 12-10](#) s'affiche.

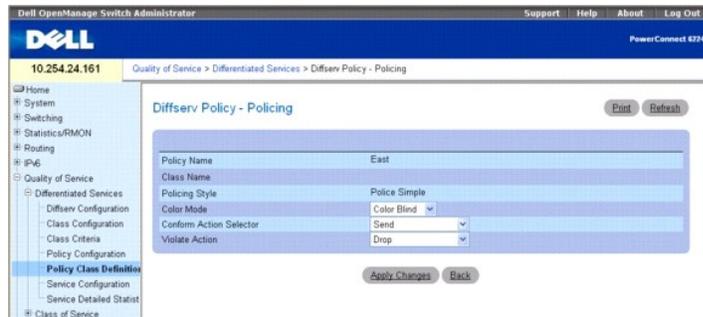
2. Sélectionnez le code DSCP IP, la priorité IP ou la classe de service à marquer pour cette classe de stratégie.
3. Sélectionnez une valeur ou entrez-la dans le champ.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La classe de stratégie est définie et le périphérique est mis à jour.

Conditionnement du trafic par vérification de la conformité

Lorsque l'option **Policing** (Vérification de conformité) est sélectionnée dans le champ **Traffic Conditioning** (Conditionnement du trafic), la page suivante s'affiche :

Figure 12-11. Définition d'une classe de stratégie - Vérification de conformité



Cette page contient les champs suivants :

Policy Name (Nom de la stratégie) : indique la stratégie pour laquelle vous définissez la vérification de conformité.

Class Name (Nom de la classe) : affiche la classe membre associée à cette stratégie.

Policing Style (Style de vérification de conformité) : indique le style de vérification de conformité utilisé.

Color Mode (Mode de coloration) : permet de sélectionner le type de coloration utilisé. Choisissez Color Blind (Non sensible à la couleur) ou Color Aware (Sensible à la couleur) dans le menu déroulant.

Conform Action Selector (Action en cas de conformité) : permet de sélectionner l'action à appliquer aux paquets considérés comme conformes, c'est-à-dire n'excédant pas les limites définies pour cette stratégie. Les options disponibles sont Send (Envoyer), Drop (Rejeter), Mark CoS (Marquer la classe de service), Mark IP DSCP (Marquer le code DSCP IP), Mark IP Precedence (Marquer la préférence IP).

Violate Action (Action en cas de violation) : permet de sélectionner l'action à appliquer aux paquets considérés comme non-conformes, c'est-à-dire excédant les limites définies pour cette stratégie. Les options disponibles sont Send (Envoyer), Drop (Rejeter), Mark CoS (Marquer la classe de service), Mark IP DSCP (Marquer le code DSCP IP), Mark IP Precedence (Marquer la préférence IP).

Configuration de la vérification de conformité pour une instance de classe de stratégie

1. Sélectionnez **Policing** (Vérification de conformité) dans le menu déroulant **Traffic Conditioning** (Conditionnement du trafic) de la page **DiffServ Policy Class Definition** (Définition d'une classe de stratégie DiffServ).

La page **DiffServ Policy - Policing** (Stratégie DiffServ - Vérification de conformité) représentée [Figure 12-11](#) s'affiche.

2. Cochez un ou plusieurs critères de vérification à utiliser pour cette classe de stratégie.
3. Dans chaque champ, sélectionnez une valeur ou saisissez-la directement.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La page suivante s'affiche :

Figure 12-12. Configuration des critères d'une stratégie

Field	Value
Policy Name	East
Class Name	test
Color Mode	Color Blind
Committed Rate (kpbs)	(1 to 4294967295) kbps
Committed Burst Size (KB)	(1 to 128) KBytes
Conform Action	Send
Violate Action	Drop

5. Entrez les valeurs de critères voulues dans les champs Committed Rate (Débit prévu au contrat) et/ou Committed Burst Size (Taille de rafale prévue au contrat).
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

La vérification de conformité est activée pour l'instance de classe de stratégie indiquée et le périphérique est mis à jour.

Définition des classes de stratégies à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

1. QoS Commands (Commandes QoS)

Configuration d'un service

La page **DiffServ Service Configuration** (Configuration d'un service DiffServ) permet d'activer une stratégie sur un port donné.

Pour afficher cette page, cliquez sur **Quality of Service** (Qualité de service) → **Differentiated Services** (Services différenciés) → **Service Configuration** (Configuration d'un service) dans l'arborescence.

Figure 12-13. Page DiffServ Service Configuration (Configuration d'un service DiffServ)



Cette page contient les champs suivants :

Interface : sélectionnez l'interface (unité/port, LAG ou option All [Tous]) à affecter dans les menus déroulants.

Policy In (Stratégie associée) : utilisez le menu déroulant pour sélectionner la stratégie à associer au port.

Activation d'une stratégie sur un port

1. Affichez la page **DiffServ Service Configuration** (Configuration d'un service DiffServ).
2. Sélectionnez l'interface voulue dans les menus déroulants.
3. Sélectionnez la stratégie voulue dans le menu déroulant.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La stratégie est activée sur l'interface et le périphérique est mis à jour.

Affichage du récapitulatif des services DiffServ

1. Affichez la page **DiffServ Service Configuration** (Configuration d'un service DiffServ).
2. Cliquez sur **Show All** (Afficher tout).

La page **DiffServ Service Summary** (Récapitulatif des services DiffServ) s'affiche.

Figure 12-14. Page **DiffServ Service Summary** (Récapitulatif des services DiffServ)

Interface	Direction	Operation Status	Policy Name
1/1	In	Down	East

Affectation d'une stratégie à un port à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

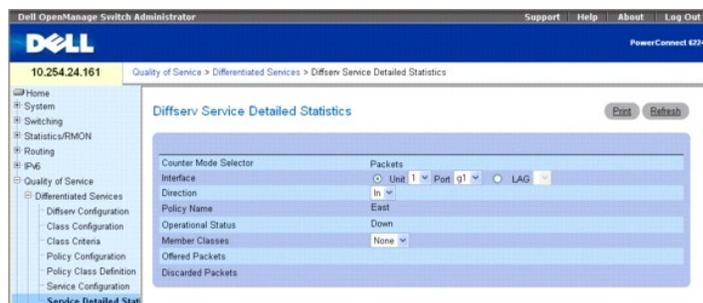
1. QoS Commands (Commandes QoS)

Statistiques détaillées sur un service

La page **DiffServ Service Detailed Statistics** (Statistiques détaillées sur un service DiffServ) permet d'afficher des informations détaillées concernant un port et une classe spécifiques.

Pour afficher cette page, cliquez sur **Quality of Service** (Qualité de service) → **Differentiated Services** (Services différenciés) → **Service Detailed Statistics** (Statistiques détaillées sur un service) dans l'arborescence.

Figure 12-15. Page **DiffServ Service Detailed Statistics** (Statistiques détaillées sur un service DiffServ)



Cette page contient les champs suivants :

Counter Mode Selector (Mode de comptage) : type de statistiques à afficher. Le seul type disponible est Packets (Paquets).

Interface : permet de sélectionner l'unité et le port ou le LAG correspondant aux statistiques de service à afficher.

Direction : permet de sélectionner la direction des paquets pour lesquels les statistiques de service doivent être affichées.

Policy Name (Nom de la stratégie) : indique la stratégie associée à l'interface sélectionnée.

Operational Status (État de fonctionnement) : indique si la stratégie est active ou non sur cette interface.

Member Classes (Classes membres) : permet de sélectionner la classe membre correspondant aux statistiques à afficher.

Offered Packets (Paquets présentés) : indique le nombre de paquets conformes à la stratégie.

Discarded Packets (Paquets rejetés) : indique le nombre de paquets rejetés par la stratégie.

Affichage de statistiques sur les services

1. Affichez la page **DiffServ Service Detailed Statistics** (Statistiques détaillées sur un service DiffServ).
2. Complétez les champs selon vos besoins.

Le système affiche les statistiques sur les paquets correspondant à l'interface, la direction et la classe indiquées.

Configuration de statistiques sur les services à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 QoS Commands (Commandes QoS)

Classe de service

La fonction de mise en file d'attente Classe de service (CoS) permet de configurer directement certains aspects de la mise en file d'attente sur le commutateur. Le comportement QoS voulu peut ainsi être associé à différents types de trafic réseau lorsque les fonctions plus complexes offertes par les services DiffServ ne sont pas requises. Une table de mappage peut être utilisée pour diriger les paquets arrivant sur une interface vers la file d'attente CoS de sortie appropriée. Les caractéristiques des files d'attente CoS affectant le mappage des files d'attente (bande passante minimale garantie, lissage des débits de transmission, etc.) peuvent être configurées par l'utilisateur au niveau de la file d'attente ou du port.

Le nombre de files d'attente prises en charge pour chaque port est de sept. Bien que le matériel prenne en charge huit files d'attente, l'une d'elles est toujours réservée à une utilisation interne par le sous-système d'empilage.

Pour afficher la page appropriée, cliquez sur **Quality of Service** (Qualité de service) → **Class of Service** (Classe de service) dans l'arborescence. La page **Class of Service** (Classe de service) contient des liens vers les fonctionnalités suivantes :

- 1 [Configuration de la table de mappage](#)
- 1 [Configuration des interfaces](#)
- 1 [Configuration des files d'attente des interfaces](#)

Configuration de la table de mappage

Chaque port du commutateur peut être configuré pour considérer l'un des champs des paquets (802.1p, précedence IP ou code DSCP IP) comme digne de confiance ("trusted" ou sécurisé), ou au contraire pour considérer comme non digne de confiance ("untrusted" ou non sécurisé) toute désignation de priorité du paquet. Si le port est défini sur un mode de confiance, il fait appel à une table de mappage correspondant au champ sécurisé utilisé. La table de mappage

indique la file d'attente CoS à laquelle le paquet devrait être transmis sur le ou les ports de sortie appropriés. Pour que la table de mappage ait une quelconque utilité, ce champ sécurisé doit effectivement exister dans le paquet. Si tel n'est pas le cas, des actions par défaut sont effectuées. Ces actions impliquent la redirection du paquet vers le niveau de CoS spécifique configuré pour le port d'entrée au niveau global. Cette redirection est basée sur la priorité par défaut du port mappée avec une classe de trafic dans la table de mappage 802.1p en cours.

Inversement, lorsqu'un port est considéré comme non sécurisé, il ne se base pas sur la désignation de priorité des paquets entrants mais utilise sa propre priorité par défaut. Tous les paquets qui arrivent sur un port non sécurisé sont dirigés vers la file d'attente CoS spécifique associé au(x) port(s) de sortie approprié(s), conformément avec la priorité par défaut définie pour le port d'entrée. Ce processus est également utilisé lorsque le mappage d'un port sécurisé ne peut pas être honoré, par exemple lorsqu'un paquet non IP arrive sur un port configuré pour se baser sur la valeur du code DSCP IP.

La page **Mapping Table Configuration** (Configuration de la table de mappage) permet de définir la façon dont une classe de service est affectée à un paquet.

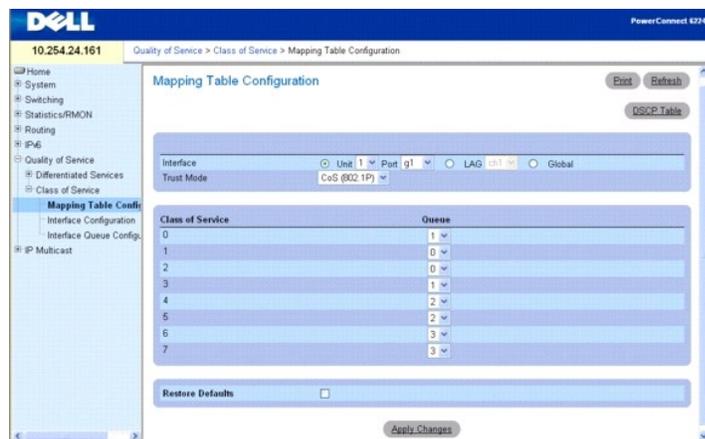
Pour afficher cette page, cliquez sur **Quality of Service** (Qualité de service) → **Class of Service** (Classe de service) → **Mapping Table Configuration** (Configuration de la table de mappage) dans l'arborescence.

Le mode de confiance sélectionné dans la page **Mapping Table Configuration** (Configuration de la table de mappage) conditionne l'affichage de la page et les champs auxquels elle permet d'accéder. Les trois modes de confiance disponibles à partir de cette page sont les suivants :

- 1 Untrusted (None) (Non sécurisé, Aucun)
- 1 CoS(802.1P)
- 1 IP DSCP (Code DSCP IP)

CoS(802.1P) étant le mode par défaut, la page correspondante s'affiche lorsque vous sélectionnez **Mapping Table Configuration** (Configuration de la table de mappage) dans la page **Class of Service** (Classe de service).

Figure 12-16. Page Mapping Table Configuration (Configuration de la table de mappage) - CoS (802.1P)



Mode CoS (802.1P) sécurisé

La page **CoS (802.1P) Mapping Table Configuration** (Configuration de la table de mappage - CoS 802.1P) contient les champs suivants :

Interface : sélectionnez l'interface à laquelle la configuration de la classe de service est appliquée. Sélectionnez une unité et un port ou unLAG, ou bien sélectionnez l'option Global pour appliquer la configuration à toutes les interfaces.

Trust Mode (Mode sécurisé) : permet de sélectionner le mode sécurisé à appliquer. L'option par défaut est **CoS (802.1P)**.

Class of Service (Classe de service) : chaque classe de service figure sur une ligne distincte et peut donc être associée à une file d'attente différente.

Queue (File d'attente) : permet de sélectionner une file d'attente pour chaque classe de service dans le menu déroulant. Les files d'attente par défaut sont affichées initialement.

Restore Defaults (Restaurer les valeurs par défaut) : permet de restaurer les valeurs par défaut. La modification est prise en compte lorsque vous cliquez sur **Apply Changes** (Appliquer les modifications).

Configuration du mode de confiance CoS (802.1P)

1. Affichez la page **Mapping Table Configuration** (Configuration de la table de mappage).
2. Sélectionnez l'unité et le port ou LAG concernés, ou bien sélectionnez l'option Global pour appliquer les paramètres à toutes les interfaces.
3. Sélectionnez un mode de confiance dans le champ **Trust Mode**.
4. Dans le champ **Queue** (File d'attente), sélectionnez une file d'attente à associer à chaque classe de service.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les modifications sont appliquées aux interfaces sélectionnées et le périphérique est mis à jour.

Restauration des paramètres par défaut des files d'attente

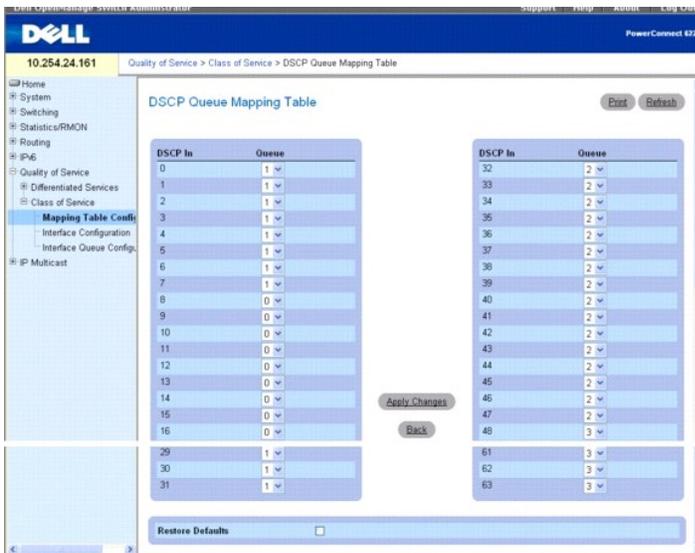
1. Affichez la page **Mapping Table Configuration** (Configuration de la table de mappage).
2. Cochez la case **Restore Defaults** (Restaurer les valeurs par défaut).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les files d'attente retrouvent les paramètres par défaut pour chaque classe de service et le périphérique est mis à jour.

Configuration de la table DSCP IP

Pour accéder à la page **DSCP Queue Mapping Table** (Table de mappage des files d'attente DSCP), cliquez sur **Quality of Service (Qualité de service)** → **Class of Service (Classe de service)** → **Mapping Table Configuration (Configuration de la table de mappage)** dans l'arborescence, puis cliquez sur le lien **DSCP Table (Table DSCP)**.

Figure 12-17. Page DSCP Queue Mapping Table (Table de mappage des files d'attente DSCP)



Cette page contient les champs suivants :

DSCP In (DSCP en entrée) : cochez cette option pour sélectionner ce critère, puis indiquez le code DSCP à utiliser pour les paquets. Ce champ détermine la file d'attente à laquelle le paquet est envoyé.

Queue ID (ID de file d'attente) : permet de sélectionner la file d'attente à laquelle le paquet est envoyé.

Restauration des paramètres par défaut des files d'attente

1. Affichez la page **DSCP Queue Mapping Table** (Table de mappage des files d'attente DSCP).
2. Cochez la case **Restore Defaults** (Restaurer les valeurs par défaut).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les files d'attente retrouvent leurs valeurs par défaut et le périphérique est mis à jour.

Configuration de la table de mappage à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

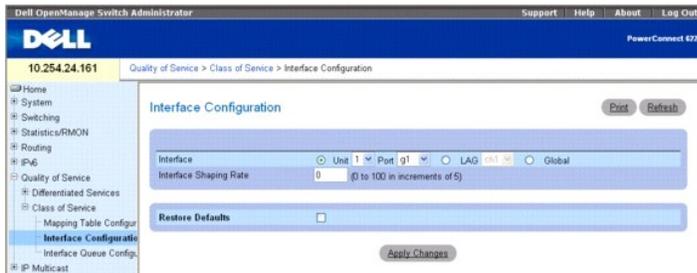
1. QoS Commands (Commandes QoS)

Configuration des interfaces

La page **Interface Configuration** (Configuration des interfaces) permet de définir la configuration CoS de chaque port et d'appliquer un lissage aux interfaces correspondant aux ports sélectionnés.

Pour afficher la page **Interface Configuration** (Configuration de l'interface), cliquez sur **Quality of Service** (Qualité de service) → **Class of Service** (Classe de service) → **Interface Configuration** (Configuration des interfaces) dans l'arborescence.

Figure 12-18. Page Interface Configuration (Configuration des interfaces)



Cette page contient les champs suivants :

Interface : permet de sélectionner l'interface à laquelle le taux de lissage doit être appliqué.

Interface Shaping Rate (Taux de lissage de l'interface) : définit la quantité maximale de trafic autorisée à quitter un port. La valeur indiquée représente un pourcentage de la bande passante maximale négociée. Les valeurs admises vont de 0 à 100 par incréments de 5.

Restore Defaults (Restaurer les valeurs par défaut) : restaure le taux de lissage par défaut sur les interfaces sélectionnées.

Définition de la configuration des interfaces

1. Affichez la page **Interface Configuration** (Configuration des interfaces).
2. Sélectionnez l'unité et le port ou LAG concernés, ou bien sélectionnez l'option Global pour appliquer les paramètres à toutes les interfaces.
3. Complétez le champ **Interface Shaping Rate** (Taux de lissage de l'interface) en indiquant le taux de lissage à appliquer à ces ports.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le taux de lissage modifié est appliqué aux interfaces sélectionnées et le périphérique est mis à jour.

Restauration du taux de lissage par défaut

1. Affichez la page **Interface Configuration** (Configuration des interfaces).
2. Cochez la case **Restore Defaults** (Restaurer les valeurs par défaut).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les ports retrouvent le taux de lissage par défaut et le périphérique est mis à jour.

Définition de la configuration des interfaces à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

1. QoS Commands (Commandes QoS)

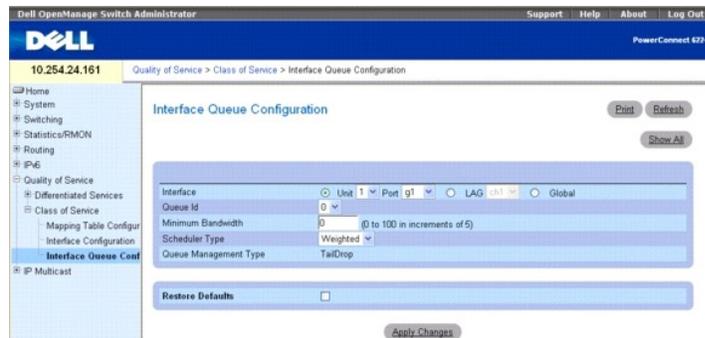
Configuration des files d'attente des interfaces

Utilisez la page **Interface Queue Configuration** (Configuration des files d'attente des interfaces) pour définir le comportement d'une file d'attente donnée en configurant les files d'attente de sortie du commutateur. Des paramètres pouvant être définis par l'utilisateur contrôlent la quantité de bande passante utilisée par la file d'attente, la profondeur de cette dernière pendant les périodes d'encombrement et la planification de la transmission des paquets à partir de toutes les files d'attente d'un port. Chaque port dispose de sa propre configuration de file d'attente CoS.

Chaque paramètre de file d'attente CoS peut être configuré globalement ou port par port, ce qui simplifie la procédure de configuration. Les modifications de configuration globales sont appliquées automatiquement à tous les ports du système.

Pour afficher la page **Interface Queue Configuration** (Configuration des files d'attente des interfaces), cliquez sur **Quality of Service (Qualité de service)** → **Class of Service (Classe de service)** → **Interface Queue Configuration** (Configuration des files d'attente des interfaces) dans l'arborescence.

Figure 12-19. Page Interface Queue Configuration (Configuration des files d'attente des interfaces)



Cette page contient les champs suivants :

Interface : indique l'unité/le port ou le LAG affectés. Vous pouvez également sélectionner l'option Global.

Queue ID (ID de la file d'attente) : sélectionnez l'interface à configurer dans le menu déroulant.

Minimum Bandwidth (Bande passante minimale) : sélectionnez un pourcentage de la bande passante maximale négociée pour le port. Les valeurs admises vont de 0 à 100 par incréments de 5.

Scheduler Type (Type de planificateur) : sélectionnez le type de traitement des files d'attente dans le menu déroulant. Les valeurs possibles sont **Weighted** (Pondéré) et **Strict**. La configuration file d'attente par file d'attente permet à l'utilisateur de créer les caractéristiques de service voulues pour différents types de trafic.

Weighted (Pondéré) : associe une pondération à chaque file d'attente. Il s'agit du comportement par défaut.

Strict : le trafic ayant la priorité la plus élevée est traité en premier.

Queue Management Type (Type de gestion de file d'attente) : indique le type de gestion utilisé pour tous les paquets, c'est-à-dire "Taildrop" (suppression des paquets en fin de file d'attente). Tous les paquets en file d'attente sont conservés, mais si cette dernière arrive à saturation, tous les paquets supplémentaires sont rejetés.

Configuration d'une file d'attente d'interface

1. Affichez la page **Interface Queue Configuration** (Configuration des files d'attente des interfaces).
2. Sélectionnez le port concerné dans les menus déroulants **Interface**, **Unit** (Unité) et **Port**.
3. Utilisez les autres champs pour configurer la file d'attente et ses paramètres pour ce port.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La file d'attente est configurée et le périphérique est mis à jour.

Affichage des paramètres des files d'attente des interfaces

1. Affichez la page **Interface Queue Configuration** (Configuration des files d'attente des interfaces).
2. Cliquez sur **Show All** (Afficher tout).
La page **Interface Queue Status** (État des files d'attente des interfaces) s'affiche.
3. Sélectionnez **Unit / Port** (Unité/Port), **LAG** ou **Global**.

Figure 12-20. Page Interface Queue Status (État des files d'attente des interfaces)

Dell OpenManage Switch Administrator Support Help About Log Out
DELL PowerConnect 6724

10.254.24.161 Quality of Service > Class of Service > Interface Queue Status

Home System Switching Statistics/RMON Routing IPG Quality of Service Differentiated Services Class of Service Mapping Table Conf Interface Configurat Interface Queue Con IP Multicast

Interface Queue Status Print Refresh

Interface Unit Port LAG ch1 Global

Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
0	0	weighted	taildrop
1	0	weighted	taildrop
2	0	weighted	taildrop
3	0	weighted	taildrop
4	0	weighted	taildrop
5	0	weighted	taildrop
6	0	weighted	taildrop

Back

Configuration d'une file d'attente d'interface à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 QoS Commands (Commandes QoS)

[Retour au sommaire](#)

[Retour au sommaire](#)

Configuration de la multidiffusion IP

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [DVMRP](#)
- [IGMP](#)
- [Multidiffusion](#)
- [PIM-DM](#)
- [PIM-SM](#)

Les protocoles de multidiffusion permettent de transmettre des paquets de multidiffusion depuis une source vers plusieurs récepteurs. Ils améliorent l'utilisation de la bande passante et réduisent les traitements liés à l'hôte et au routeur, ce qui les rend particulièrement adaptés aux applications d'audio et de visioconférence, aux outils de tableau blanc, aux messages de distribution d'actions, etc.

Les applications de multidiffusion envoient un exemplaire d'un paquet à plusieurs destinataires (adresse de groupe de multidiffusion) plutôt qu'à un seul (adresse de monodiffusion). Le réseau est chargé de transmettre les paquets uniquement aux réseaux et hôtes qui doivent le recevoir.

Les routeurs activés pour la multidiffusion acheminent les paquets de multidiffusion en fonction des itinéraires définis dans la base MRIB (Multicast Routing Information Base). Ces itinéraires sont définis dans la base au cours de la création des arborescences de distribution de multidiffusion par les protocoles de multidiffusion qui s'exécutent sur le routeur. Les techniques utilisées pour créer les arborescences de distribution de la multidiffusion diffèrent selon les protocoles de multidiffusion IP.

Si le trafic de multidiffusion doit être acheminé via une partie du réseau qui ne prend pas en charge la multidiffusion (routeurs non activés pour la multidiffusion), les paquets de multidiffusion sont encapsulés dans un datagramme IP et envoyés comme des paquets de monodiffusion. Lorsque le routeur de multidiffusion situé à l'autre extrémité du tunnel reçoit le paquet, il supprime l'encapsulation IP et transmet le paquet comme paquet de multidiffusion IP. Le processus d'encapsulation des paquets de multidiffusion est appelé tunnelisation.

Pour afficher la page **IP Multicast** (Multidiffusion IP), cliquez sur **IP Multicast** (Multidiffusion IP) dans l'arborescence. Cette page contient des liens vers les informations suivantes :

- 1 [DVMRP](#)
- 1 [IGMP](#)
- 1 [Multidiffusion](#)
- 1 [PIM-DM](#)
- 1 [PIM-SM](#)

DVMRP

DVMRP échange des paquets de vérification avec tous les routeurs prenant en charge DVMRP, il établit des relations de voisinage bidirectionnelles et crée une table de voisins. Il échange des paquets de rapport et crée une table de topologie de monodiffusion, qu'il utilise pour créer la table de routage de multidiffusion. Celle-ci permet d'acheminer les paquets de multidiffusion. Chaque routeur DVMRP utilise le même protocole de routage de monodiffusion, ce qui permet d'éviter les boucles de routage.

La page **DVMRP** contient des liens vers des pages Web qui définissent et affichent les paramètres et les données DVMRP. Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **DVMRP** dans l'arborescence.

Cette page permet d'accéder aux fonctionnalités suivantes :

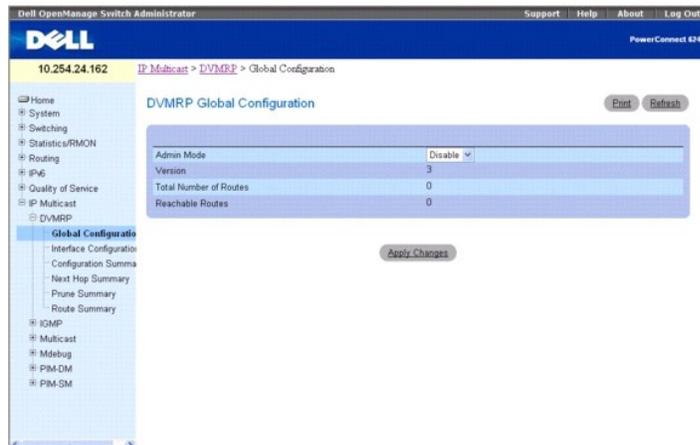
- 1 [Configuration globale DVMRP](#)
- 1 [Configuration de l'interface DVMRP](#)
- 1 [Récapitulatif de la configuration DVMRP](#)
- 1 [Informations sur le saut suivant](#)
- 1 [Récapitulatif d'élagage](#)
- 1 [Récapitulatif des itinéraires](#)

Configuration globale DVMRP

La page **DVMRP Global Configuration** (Configuration globale DVMRP) permet de configurer les paramètres DVMRP globaux.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **DVMRP** → **Global Configuration** (Configuration globale) dans l'arborescence.

Figure 13-1. Page DVMRP Global Configuration (Configuration globale DVMRP)



La page **DVMRP Global Configuration** (Configuration globale DVMRP) contient les champs suivants :

Admin Mode (Mode d'administration) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant. Cela permet d'activer ou de désactiver l'état administratif de DVMRP. La valeur par défaut est Disable (Désactiver).

Version : valeur en cours de la chaîne de version de DVMRP.

Total Number of Routes (Nombre total d'itinéraires) : nombre d'itinéraires dans la table de routage DVMRP.

Reachable Routes (Itinéraires accessibles) : nombre d'itinéraires de la table de routage DVMRP qui ont une métrique non infinie.

Définition du mode Admin DVMRP

1. Affichez la page **DVMRP Global Configuration** (Configuration globale DVMRP).
2. Sélectionnez Enable (Activer) ou Disable (Désactiver) dans le champ **Admin Mode** (Mode Admin) pour activer ou désactiver DVMRP.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration DVMRP est enregistrée et le périphérique est mis à jour.

Configuration de DVMRP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

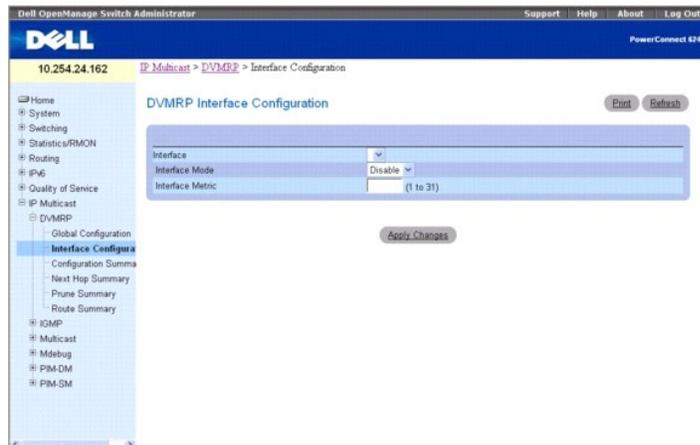
- 1 DVMRP Commands (Commandes DVMRP)

Configuration de l'interface DVMRP

Utilisez la page **DVMRP Interface Configuration** (Configuration de l'interface DVMRP) pour configurer une interface DVMRP. Vous devez configurer au moins une interface de routeur pour pouvoir configurer une interface DVMRP. Dans le cas contraire, un message indiquant qu'aucune interface de routeur n'est disponible s'affiche et vous n'avez pas accès à l'écran de configuration.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **DVMRP** → **Interface Configuration** (Configuration de l'interface DVMRP) dans l'arborescence.

Figure 13-2. Page DVMRP Interface Configuration (Configuration de l'interface DVMRP)



La page **DVMRP Interface Configuration** (Configuration de l'interface DVMRP) contient les champs suivants :

Interface : sélectionnez l'interface pour laquelle les données doivent être configurées. Vous devez configurer au moins une interface de routeur pour pouvoir configurer une interface DVMRP.

Interface Mode (Mode de l'interface) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant pour définir le mode administratif de l'interface de routage DVMRP sélectionnée.

Interface Metric (Métrique de l'interface) : entrez la métrique DVMRP de l'interface sélectionnée. Cette valeur est transmise dans les messages DVMRP en tant que coût d'accès au réseau. Les valeurs valides sont comprises entre 1 et 31.

Configuration d'une interface DVMRP

1. Affichez la page **DVMRP Interface Configuration** (Configuration de l'interface DVMRP).
2. Sélectionnez l'interface à configurer dans le champ **Interface**.
3. Modifiez les autres champs selon vos besoins.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de l'interface est enregistrée et le périphérique est mis à jour.

Configuration d'une interface DVMRP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

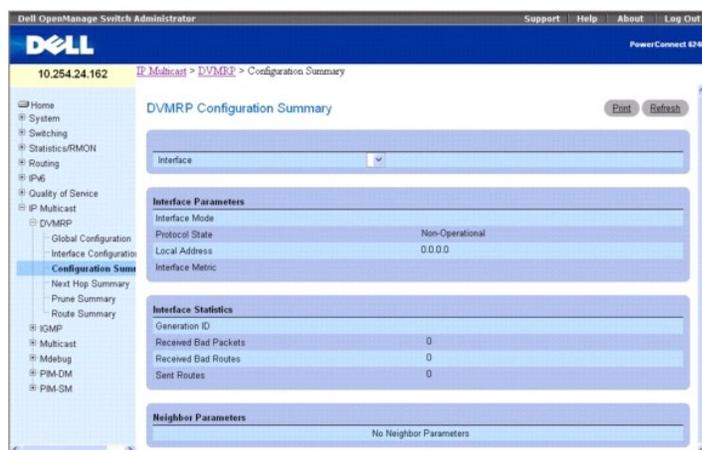
1. DVMRP Commands (Commandes DVMRP)

Récapitulatif de la configuration DVMRP

Utilisez la page **DVMRP Configuration Summary** (Récapitulatif de la configuration DVMRP) pour afficher ou imprimer la configuration et les données DVMRP d'une interface sélectionnée. Vous devez configurer au moins une interface de routeur pour pouvoir afficher les données d'une interface DVMRP. Dans le cas contraire, un message indiquant qu'aucune interface de routeur n'est disponible s'affiche et vous n'avez pas accès à l'écran de récapitulatif de la configuration.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **DVMRP** → **Configuration Summary** (Récapitulatif de la configuration DVMRP) dans l'arborescence.

Figure 13-3. Page DVMRP Configuration Summary (Récapitulatif de la configuration DVMRP)



La page **DVMRP Configuration Summary** (Récapitulatif de la configuration DVMRP) contient les champs suivants :

Interface : sélectionnez l'interface dont vous voulez afficher les données. Vous devez configurer au moins une interface de routeur pour pouvoir afficher les données d'une interface DVMRP.

Interface Parameters (Paramètres de l'interface)

Interface Mode (Mode de l'interface) : indique le mode administratif de l'interface de routage DVMRP sélectionnée, à savoir Enable (Activer) ou Disable (Désactiver).

Protocol State (État du protocole) : affiche l'état opérationnel du protocole DVMRP sur l'interface sélectionnée, à savoir Operational (Opérationnel) ou Non-operational (Non opérationnel).

Local Address (Adresse locale) : indique l'adresse IP utilisée comme adresse source dans les paquets envoyés à partir de l'interface sélectionnée.

Interface Metric (Métrique de l'interface) : affiche la métrique utilisée pour calculer les vecteurs de distance pour l'interface sélectionnée.

Interface Statistics (Statistiques sur les interfaces)

Generation ID (ID de génération) : affiche l'ID de génération DVMRP utilisé par le routeur pour l'interface sélectionnée. Cette valeur est réinitialisée chaque fois qu'une interface est (re)démarrée et placée dans les messages d'élagage. La modification de l'ID de génération informe les routeurs voisins que les précédentes informations relatives à ce routeur doivent être supprimées.

Received Bad Packets (Paquets incorrects reçus) : nombre de paquets non valides reçus sur l'interface sélectionnée.

Received Bad Routes (Itinéraires incorrects reçus) : nombre d'itinéraires non valides reçus sur l'interface sélectionnée.

Sent Routes (Itinéraires envoyés) : nombre d'itinéraires envoyés sur l'interface sélectionnée.

Neighbor Parameters (Paramètres du voisin)

Neighbor IP (Adresse IP du voisin) : adresse IP du voisin dont les informations sont affichées.

State (État) : état du routeur voisin spécifié sur l'interface sélectionnée (actif ou inactif).

Neighbor Uptime (Temps de fonctionnement du voisin) : durée de fonctionnement DVMRP du voisin spécifié sur l'interface sélectionnée. Il s'agit de la durée écoulée depuis l'apprentissage de l'entrée du voisin.

Neighbor Expiry Time (Délai avant expiration du voisin) : délai DVMRP avant expiration du voisin spécifié sur l'interface sélectionnée. Il s'agit de la durée restante avant que l'entrée du voisin arrive à expiration ; elle ne s'applique pas aux voisins inactifs.

Generation ID (ID de génération) : ID de génération DVMRP du voisin spécifié sur l'interface sélectionnée.

Major Version (Version majeure) : version majeure DVMRP du voisin spécifié sur l'interface sélectionnée.

Minor Version (Version mineure) : version mineure DVMRP du voisin spécifié sur l'interface sélectionnée.

Capabilities (Capacités) : capacités DVMRP du voisin spécifié sur l'interface sélectionnée.

Received Routes (Itinéraires reçus) : nombre d'itinéraires reçus pour le voisin spécifié sur l'interface sélectionnée.

Received Bad Packets (Paquets incorrects reçus) : nombre de paquets non valides reçus pour le voisin spécifié sur l'interface sélectionnée.

Received Bad Routes (Itinéraires incorrects reçus) : nombre d'itinéraires non valides reçus pour le voisin spécifié sur l'interface sélectionnée.

Affichage du récapitulatif de la configuration DVMRP à l'aide des commandes CLI

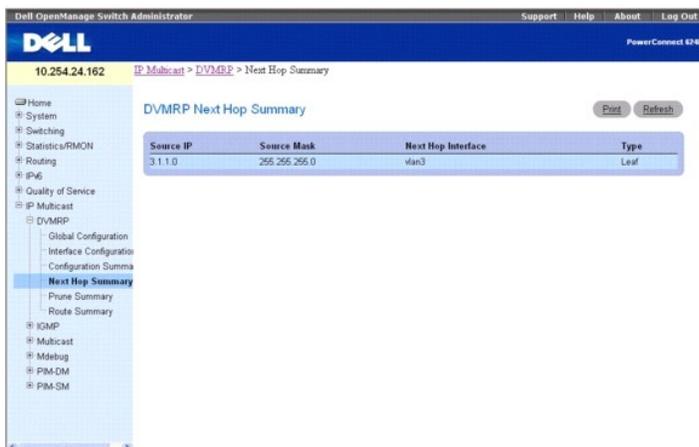
Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

Informations sur le saut suivant

Utilisez la page **Next Hop Summary** (Informations sur le saut suivant) pour afficher ou imprimer les informations sur le saut suivant par adresse IP source.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **DVMRP** → **Next Hop Summary** (Récapitulatif du saut suivant) dans l'arborescence.

Figure 13-4. Page **Next Hop Summary** (Récapitulatif du saut suivant)



Source IP	Source Mask	Next Hop Interface	Type
3.1.1.0	255.255.255.0	vlan3	Leaf

La page **Next Hop Summary** (Récapitulatif du saut suivant) contient les champs suivants :

Source IP (Adresse IP source) : affiche l'adresse IP utilisée avec le masque source pour identifier le réseau source pour cette entrée de la table.

Source Mask (Masque source) : masque de réseau utilisé avec l'adresse IP source.

Next Hop Interface (Interface du saut suivant) : affiche l'interface de sortie du saut suivant.

Type : type du saut suivant. Leaf (Feuille) indique qu'aucun voisin dépendant en aval n'existe sur l'interface de sortie. Sinon, le type Branch (Branche) est utilisé.

Affichage du récapitulatif sur le saut suivant à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 DVMRP Commands (Commandes DVMRP)

Récapitulatif d'élagage

Utilisez la page **Prune Summary** (Récapitulatif d'élagage) pour afficher ou imprimer le récapitulatif d'élagage par adresse IP de groupe.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **DVMRP** → **Prune Summary** (Récapitulatif d'élagage) dans l'arborescence.

Figure 13-5. Page **Prune Summary** (Récapitulatif d'élagage)

Dell OpenManage Switch Administrator

10.254.24.162 IP Multicast > DVMRP > Prune Summary

DVMRP Prune Summary

Group IP	Source IP	Source Mask	Expiry Time (secs)
224.2.2.24	3.1.1.0	255.255.255.0	532

La page **Prune Summary** (Récapitulatif d'élagage) contient les champs suivants :

Group IP (Adresse IP de groupe) : adresse IP de groupe élaguée.

Source IP (Adresse IP source) : adresse de la source ou du réseau source élagué.

Source Mask (Masque source) : masque de sous-réseau à combiner à l'adresse IP source pour identifier la source ou le réseau source élagué.

Expiry Time (secs) (Délai d'expiration [secondes]) : durée restante avant l'expiration de l'élément élagué au niveau du voisin en amont. Si aucun message d'élagage n'a été reçu des voisins en aval, cette valeur est celle du temporisateur d'élagage par défaut ; sinon, c'est la plus petite valeur reçue ou celle du temporisateur par défaut qui est définie (la valeur inférieure est retenue).

Affichage du récapitulatif d'élagage à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 DVMRP Commands (Commandes DVMRP)

Récapitulatif des itinéraires

Utilisez la page **Route Summary** (Récapitulatif des itinéraires) pour afficher ou imprimer le récapitulatif des itinéraires DVMRP.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **DVMRP** → **Route Summary** (Récapitulatif des itinéraires) dans l'arborescence.

Figure 13-6. Page **Route Summary** (Récapitulatif des itinéraires)

Dell OpenManage Switch Administrator

10.254.24.162 IP Multicast > DVMRP > Route Summary

DVMRP Route Summary

Source Address	Source Mask	Upstream Neighbor	Interface	Metric	Expiry Time (secs)	UP Time (secs)
9.0.0.0	255.0.0.0	0.0.0.0	vlan0	0	0	224
16.0.0.0	255.0.0.0	0.0.0.0	vlan10	0	0	224
20.20.15.0	255.255.255.0	9.1.1.3	vlan0	4	0	205
20.20.20.0	255.255.255.0	9.1.1.3	vlan0	4	0	205

La page **Route Summary** (Récapitulatif des itinéraires) contient les champs suivants :

Source Address (Adresse source) : adresse réseau combinée au masque source pour identifier les sources de cette entrée.

Source Mask (Masque source) : masque de sous-réseau combiné à l'adresse source pour identifier les sources de cette entrée.

Upstream Neighbor (Voisin en amont) : adresse du voisin en amont (RPF, par exemple) depuis lequel les datagrammes IP provenant de ces sources sont reçus.

Interface : interface sur laquelle les datagrammes IP envoyés par ces sources sont reçus. La valeur 0 indique généralement que l'itinéraire est un agrégat pour lequel il n'existe pas d'interface de saut suivant.

Metric (Métrique) : distance (en nombre de sauts) par rapport au sous-réseau source.

Expiry Time (Délai d'expiration) : délai minimum restant avant expiration de cette entrée.

Up Time (Temps de fonctionnement) : temps écoulé depuis l'apprentissage par le routeur de l'itinéraire représenté par cette entrée.

Affichage du récapitulatif des itinéraires DVMRP à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 DVMRP Commands (Commandes DVMRP)

IGMP

Le protocole IGMP (Internet Group Management Protocol) permet à des systèmes en IPv4 (hôtes et routeurs) de déclarer les groupes de multidiffusion IP auxquels ils appartiennent aux routeurs multidiffusion avoisinants. Les systèmes de la série 6200 assument le rôle de routeurs de multidiffusion du protocole IGMP ; ils collectent les informations d'appartenance nécessaires au routage de multidiffusion actif. Actuellement, les protocoles de routage de multidiffusion pris en charge par la série 6200 sont DVMRP, PIM-DM et PIM-SM.

Les systèmes de la série 6200 prennent en charge IGMP version 3. Cette version met en oeuvre le filtrage des sources, qui représente la possibilité pour un système de signaler qu'il souhaite recevoir des paquets provenant uniquement de certaines adresses source, comme l'exige la multidiffusion SSM (Source-Specific Multicast), ou provenant de toutes les adresses source sauf certaines, dont les paquets doivent être envoyés à une adresse de multidiffusion donnée. La version 3 est conçue pour être compatible avec les versions 1 et 2.

La page **IGMP** contient des liens vers des pages Web qui définissent et affichent les paramètres et les données IGMP. Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **IGMP** dans l'arborescence.

Cette page permet d'accéder aux fonctionnalités suivantes :

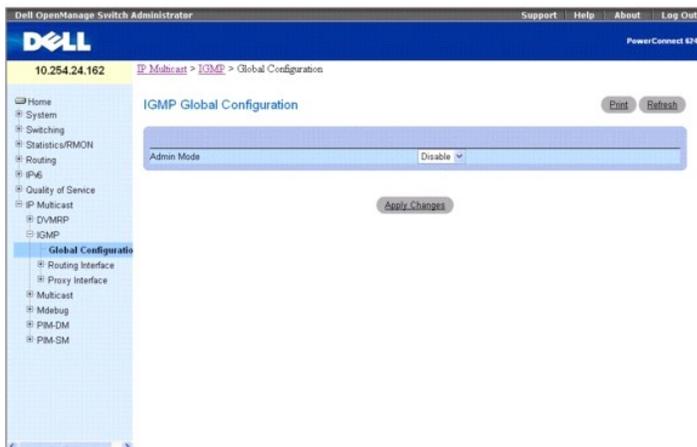
- 1 [Configuration globale IGMP](#)
- 1 [Interface de routage](#)
- 1 [Interface du proxy](#)

Configuration globale IGMP

Utilisez la page **IGMP Global Configuration** (Configuration globale IGMP) pour définir IGMP comme actif ou inactif sur le système.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **IGMP** → **Global Configuration** (Configuration globale) dans l'arborescence.

Figure 13-7. Page IGMP Global Configuration (Configuration globale IGMP)



La page **IGMP Global Configuration** (Configuration globale IGMP) contient les champs suivants :

Admin Mode (Mode Admin) : sélectionnez **Enable** (Activer) ou **Disable** (Désactiver) dans le menu déroulant pour définir l'état administratif d'IGMP sur le routeur comme actif ou inactif. La valeur par défaut est **Disable** (Désactiver).

Définition du mode IGMP

1. Affichez la page **IGMP Global Configuration** (Configuration globale IGMP).
2. Sélectionnez Enable (Activer) ou Disable (Désactiver) dans le champ **Admin Mode** (Mode Admin) pour activer ou désactiver IGMP.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration d'IGMP est enregistrée et le périphérique est mis à jour.

Définition du mode IGMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 IGMP Commands (Commandes IGMP)

Interface de routage

La page **Routing Interface** (Interface de routage) contient des liens vers des pages Web qui configurent et affichent les paramètres et les données du routage IGMP. Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **IGMP** → **Routing Interface** (Interface de routage) dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

- 1 [Configuration de l'interface IGMP](#)
- 1 [Récapitulatif de la configuration IGMP](#)
- 1 [Informations sur la mémoire cache IGMP](#)
- 1 [Informations d'appartenance détaillées pour l'interface IGMP](#)

Configuration de l'interface IGMP

Utilisez la page **IGMP Interface Configuration** (Configuration de l'interface IGMP) pour configurer et/ou afficher les paramètres de l'interface du routeur. Pour pouvoir accéder à cette page et configurer le protocole de multidiffusion IP IGMP, vous devez configurer au moins une interface de routage valide.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **IGMP** → **Routing Interface** (Interface de routage) → **Interface Configuration** (Configuration de l'interface) dans l'arborescence.

Figure 13-8. Page IGMP Interface Configuration (Configuration de l'interface IGMP)



La page **IGMP Interface Configuration** (Configuration de l'interface IGMP) contient les champs suivants :

Interface : sélectionnez l'interface dont vous voulez afficher ou configurer les données dans le menu déroulant.

Interface Mode (Mode de l'interface) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant pour définir l'état administratif d'IGMP sur l'interface sélectionnée. La valeur par défaut est Disable (Désactiver).

Version : entrez la version d'IGMP à configurer sur l'interface sélectionnée. Les valeurs valides vont de 1 à 3 (3 est la valeur par défaut). Ce champ ne peut être configuré que si le mode de l'interface IGMP est activé.

Robustness (Robustesse) : entrez la valeur de robustesse. Cette variable permet de prendre en compte les pertes de paquets prévues sur un sous-réseau. Si vous vous attendez à des pertes importantes, vous devez augmenter la valeur de ce paramètre. IGMP prend en charge (variable de robustesse - 1) paquets

perdus. Les valeurs valides vont de 1 à 255. La valeur par défaut est de 2.

Query Interval (secs) (Intervalle entre requêtes [secondes]) : entrez la fréquence (en secondes) selon laquelle les paquets de requête hôte IGMP doivent être transmis sur l'interface. Les valeurs valides vont de 1 à 3600. La valeur par défaut est de 125.

Query Max Response Time (1/10 of a second) (Délai maximal de réponse à une requête [dixièmes de seconde]) : entrez le délai de réponse maximal pour l'annonce de requêtes IGMPv2 sur cette interface, en dixièmes de seconde. La valeur par défaut est de 100. Les valeurs valides vont de 0 à 255.

Startup Query Interval (secs) (Intervalle entre requêtes de démarrage [secondes]) : entrez le nombre de secondes entre la transmission des requêtes de démarrage sur l'interface sélectionnée. Les valeurs valides vont de 1 à 300. La valeur par défaut est de 31.

Startup Query Count (Nombre de requêtes de démarrage) : entrez le nombre de requêtes à envoyer au démarrage. Les valeurs valides vont de 1 à 20. La valeur par défaut est de 2.

Last Member Query Interval (1/10 of a second) (Intervalle entre requêtes du dernier membre [dixièmes de seconde]) : entrez l'intervalle de requête du dernier membre, en dixièmes de seconde. Il s'agit du délai de réponse maximal à insérer dans les requêtes de groupe envoyées en réponse aux messages de sortie de groupe, ainsi que du délai entre les messages de requête de groupe. Les valeurs valides vont de 0 à 255. La valeur par défaut est de 10. Cette valeur n'est pas utilisée pour IGMP version 1.

Last Member Query Count (Nombre de requêtes du dernier membre) : entrez le nombre de requêtes à envoyer lorsqu'un rapport de sortie de groupe est reçu. Les valeurs valides vont de 1 à 20. La valeur par défaut est de 2.

Configuration d'une interface de routage IGMP

1. Affichez la page **IGMP Interface Configuration** (Configuration de l'interface IGMP).
2. Sélectionnez l'interface à configurer dans le champ **Interface**.
3. Modifiez les autres champs selon vos besoins.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de l'interface est enregistrée et le périphérique est mis à jour.

Configuration d'une interface de routage IGMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

1. IGMP Commands (Commandes IGMP)

Récapitulatif de la configuration IGMP

Utilisez la page **IGMP Configuration Summary** (Récapitulatif de la configuration IGMP) pour afficher les paramètres et les données de routage IGMP. Pour pouvoir accéder à cette page, vous devez configurer au moins une interface de routeur IGMP.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **IGMP** → **Routing Interface** (Interface de routage) → **Configuration Summary** (Récapitulatif de la configuration) dans l'arborescence.

Figure 13-9. Page **IGMP Configuration Summary** (Récapitulatif de la configuration IGMP)

The screenshot displays the Dell OpenManage Switch Administrator web interface. The breadcrumb navigation shows: IP Multicast > IGMP > Routing Interface > Configuration Summary. The main content area is titled "IGMP Configuration Summary" and includes a dropdown menu for the interface, currently set to "vlan3". Below this, there are two tables: "Interface Parameters" and "Interface Statistics".

Interface Parameters	
Interface Mode	Enable
IP Address	3.1.1.2
Subnet Mask	255.255.255.0
Protocol State	Operational
Version	3
Query Interval (secs)	125
Query Max Response Time (1/10 of a second)	100
Robustness	2
Startup Query Interval (secs)	31
Startup Query Count	2
Last Member Query Interval (1/10 of a second)	10
Last Member Query Count	2

Interface Statistics	
Querier	3.1.1.2
Querier Status	Querier
Querier Up Time (secs)	1832
Querier Expiry Time (secs)	0
Wrong Version Queues	0
Number of Joins	0
Number of Groups	0

La page **IGMP Configuration Summary** (Récapitulatif de la configuration IGMP) contient les champs suivants :

Interface : sélectionnez l'interface dont vous voulez afficher les données.

Interface Parameters (Paramètres de l'interface)

Interface Mode (Mode de l'interface) : état administratif d'IGMP sur l'interface sélectionnée.

IP Address (Adresse IP) : adresse IP de l'interface sélectionnée.

Subnet Mask (Masque de sous-réseau) : masque de sous-réseau correspondant à l'adresse IP de l'interface sélectionnée.

Protocol State (État du protocole) : état opérationnel d'IGMP sur l'interface sélectionnée.

Version : version du protocole IGMP configuré sur l'interface sélectionnée.

Query Interval (secs) (Intervalle d'interrogation [secondes]) : fréquence selon laquelle les paquets de requête hôte IGMP doivent être transmis sur l'interface sélectionnée.

Query Max Response Time (1/10 of a second) (Délai maximal de réponse à une requête [dixièmes de seconde]) : délai de réponse maximal annoncé dans les requêtes IGMPv2 envoyées depuis l'interface sélectionnée.

Robustness (Robustesse) : paramètre de robustesse de l'interface sélectionnée. Cette variable permet de prendre en compte les pertes de paquets prévues sur un sous-réseau. Si vous vous attendez à des pertes importantes, vous pouvez augmenter la variable de robustesse. IGMP prend en charge (variable de robustesse - 1) paquets perdus.

Startup Query Interval (secs) (Intervalle entre requêtes de démarrage [secondes]) : intervalle d'envoi des requêtes de démarrage sur l'interface sélectionnée.

Startup Query Count (Nombre de requêtes de démarrage) : nombre de requêtes à envoyer au démarrage.

Last Member Query Interval (1/10 of a second) (Intervalle entre requêtes du dernier membre [dixièmes de seconde]) : il s'agit du délai de réponse maximal inséré dans les requêtes de groupe envoyées en réponse aux messages de sortie de groupe, ainsi que du délai entre les messages de requête de groupe. Cette valeur peut être réglée pour modifier la latence de sortie du réseau. La diminution de cette valeur réduit le délai de détection de la sortie du dernier membre d'un groupe. Cette valeur n'est pas utilisée pour IGMP version 1.

Last Member Query Count (Nombre de requêtes du dernier membre) : nombre de requêtes à envoyer lorsqu'un rapport de sortie de groupe est reçu.

Interface Statistics (Statistiques sur les interfaces)

Querier (Demandeur) : adresse du demandeur IGMP sur le sous-réseau IP auquel l'interface sélectionnée est rattachée.

Querier Status (État du demandeur) : indique si l'interface sélectionnée est en mode demandeur ou non demandeur.

Querier Up Time (secs) (Temps de fonctionnement du demandeur [secondes]) : durée (en secondes) depuis la dernière modification du demandeur d'interface IGMP.

Querier Expiry Time (secs) (Délai avant expiration du demandeur [secondes]) : délai (en secondes) avant expiration du temporisateur de l'autre demandeur. Si le système local est le demandeur, cette valeur est égale à zéro.

Wrong Version Queries (Requêtes avec version incorrecte) : nombre de requêtes reçues sur l'interface sélectionnée, avec une version IGMP ne correspondant pas à celle configurée pour l'interface, pendant la durée de vie de l'entrée. IGMP exige que tous les routeurs d'un réseau local soient configurés pour exécuter la même version d'IGMP. En conséquence, une erreur de configuration est renvoyée lorsqu'une requête effectuée avec un numéro de version incorrect est reçue.

Number of Joins (Nombre d'adhésions) : nombre de fois qu'une appartenance au groupe a été ajoutée sur l'interface sélectionnée (nombre d'ajouts d'entrées pour cette interface dans la table de cache). Cette valeur fournit une indication de l'intensité de l'activité IGMP sur l'interface.

Number of Groups (Nombre de groupes) : nombre d'entrées en cours pour l'interface sélectionnée dans la table de cache.

Affichage de la configuration du routage IGMP à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

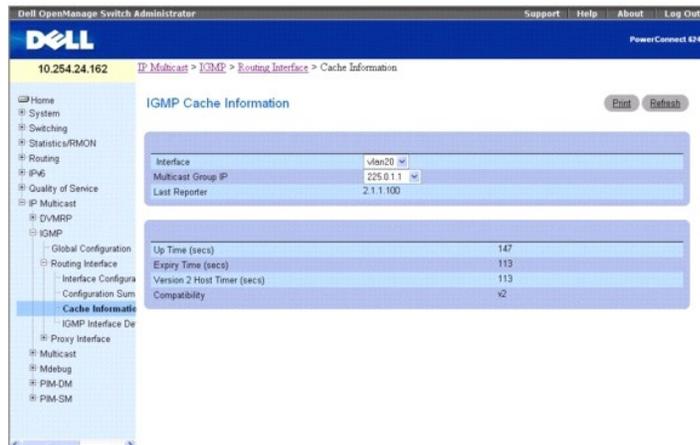
1 IGMP Commands (Commandes IGMP)

Informations sur la mémoire cache IGMP

Utilisez la page **IGMP Cache Information (Informations sur la mémoire cache IGMP)** pour afficher les paramètres et les données de cache pour une adresse de groupe de multidiffusion IP. Pour pouvoir accéder à cette page, vous devez configurer au moins une interface de routeur IGMP. Pour que des données s'affichent, des rapports d'appartenance de groupe doivent également avoir été reçus sur l'interface sélectionnée.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **IGMP** → **Routing Interface** (Interface de routage) → **Cache Information** (Informations sur la mémoire cache) dans l'arborescence.

Figure 13-10. Page IGMP Cache Information (Informations sur la mémoire cache IGMP)



La page **IGMP Cache Information** (Informations sur la mémoire cache IGMP) contient les champs suivants :

Interface : sélectionnez l'interface dont vous voulez afficher les données.

Multicast Group IP (Adresse IP du groupe de multidiffusion) : sélectionnez l'adresse IP du groupe de multidiffusion pour laquelle les données doivent être affichées. Si aucun rapport d'appartenance de groupe n'a été reçu sur l'interface sélectionnée, vous ne pouvez pas choisir cette option ; la page ne contient pas de données.

Last Reporter (Dernier émetteur de rapport) : adresse IP de la source du dernier rapport d'appartenance reçu pour l'adresse de groupe de multidiffusion IP sur l'interface sélectionnée.

Up Time (Temps de fonctionnement) : durée écoulée depuis la création de l'entrée.

Expiry Time (Délai d'expiration) : délai minimum restant avant expiration de cette entrée.

Version 1 Host Timer (Temporisateur hôte version 1) : délai restant avant que le routeur local suppose que le sous-réseau IP rattaché à cette interface ne contient plus aucun membre IGMP version 1. Lorsqu'un rapport d'appartenance IGMPv1 est reçu, ce temporisateur est réinitialisé en fonction du temporisateur d'appartenance du groupe. Lorsque ce temporisateur est différent de zéro, le routeur local ignore les messages de sortie de groupe IGMPv2 reçus sur l'interface sélectionnée. Ce champ s'affiche uniquement si l'interface est configurée pour IGMP version 1.

Version 2 Host Timer (Temporisateur hôte version 2) : délai restant avant que le routeur local suppose que le sous-réseau IP rattaché à cette interface ne contient plus aucun membre IGMP version 2. Lorsqu'un rapport d'appartenance IGMPv2 est reçu, ce temporisateur est réinitialisé en fonction du temporisateur d'appartenance du groupe. Lorsque ce temporisateur est différent de zéro, le routeur local ignore les messages de sortie de groupe IGMPv1 et IGMPv3 reçus sur l'interface sélectionnée. Ce champ s'affiche uniquement si l'interface est configurée pour IGMP version 2.

Compatibility (Compatibilité) : ce paramètre indique le mode de compatibilité de groupe (v1, v2 et v3) de ce groupe sur l'interface spécifiée.

Filter Mode (Mode de filtrage) : mode de filtrage source (Include/Exclude/NA) du groupe spécifié sur cette interface. Ce champ est vide lorsque le mode NA est actif.

Affichage des informations sur la mémoire cache à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

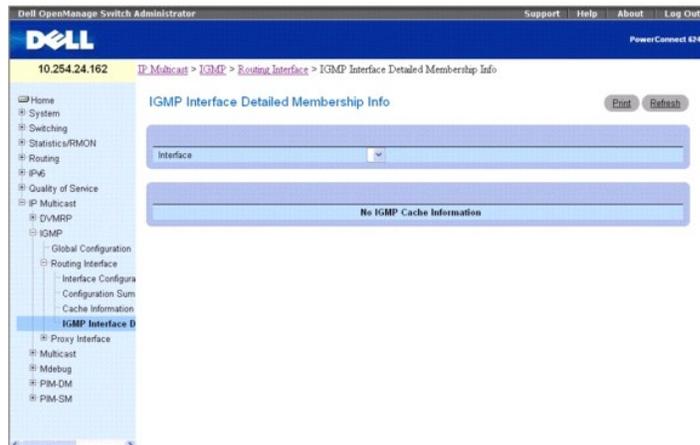
- 1 IGMP Commands (Commandes IGMP)

Informations d'appartenance détaillées pour l'interface IGMP

Utilisez la page **IGMP Interface Detailed Membership Info** (Informations d'appartenance détaillées pour l'interface IGMP) pour afficher des informations d'appartenance détaillées pour une interface. Pour pouvoir accéder à cette page, vous devez configurer au moins une interface de routeur IGMP. Pour que des données s'affichent, des rapports d'appartenance de groupe doivent également avoir été reçus sur l'interface sélectionnée.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **IGMP** → **Routing Interface** (Interface de routage) → **IGMP Interface Detailed Membership Info** (Informations d'appartenance détaillées pour l'interface IGMP) dans l'arborescence.

Figure 13-11. Page IGMP Interface Detailed Membership Info (Informations d'appartenance détaillées pour l'interface IGMP)



La page **IGMP Interface Detailed Membership Info** (Informations d'appartenance détaillées pour l'interface IGMP) contient les champs suivants :

Interface : sélectionnez l'interface dont vous voulez afficher les données.

Multicast Group IP (Adresse IP du groupe de multidiffusion) : sélectionnez l'adresse IP du groupe de multidiffusion pour laquelle les données doivent être affichées. Si aucun rapport d'appartenance de groupe n'a été reçu sur l'interface sélectionnée, vous ne pouvez pas choisir cette option ; les autres champs ne s'affichent pas.

Interface : interface sur laquelle les paquets de multidiffusion sont transmis.

Group Compatibility Mode (Mode de compatibilité du groupe) : mode de compatibilité de groupe (v1, v2 et v3) de ce groupe sur l'interface spécifiée.

Source Filter Mode (Mode de filtrage source) : mode de filtrage source (Include/Exclude/NA) du groupe spécifié sur cette interface.

Source Hosts (Hôtes source) : adresses source appartenant à cette adresse de multidiffusion.

Expiry Time (Délai d'expiration) : intervalle avant expiration de chaque adresse source appartenant à ce groupe de multidiffusion. Passé ce délai, l'entrée arrive à expiration.

Affichage des informations d'appartenance détaillées pour l'interface IGMP

1. Affichez la page **IGMP Interface Detailed Membership Info** (Informations d'appartenance détaillées pour l'interface IGMP).
2. Sélectionnez l'interface à afficher dans le menu déroulant **Interface**.
3. Sélectionnez la valeur voulue dans **Multicast Group IP** (Adresse du groupe de multidiffusion IP).

Des informations d'appartenance détaillées pour cette interface et l'adresse du groupe de multidiffusion IP s'affichent.

Affichage des informations d'appartenance détaillées pour l'interface IGMP à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 IGMP Commands (Commandes IGMP)

Interface du proxy

Le but du proxy IGMP est de permettre à un routeur de multidiffusion d'assimiler (apprendre) des informations d'appartenance de groupe de multidiffusion et de transmettre les paquets de multidiffusion en fonction de ces informations. Le proxy IGMP ne peut fonctionner que dans certaines topologies non dépendantes des protocoles MRP (Multicast Routing Protocols) tels que DVMRP, PIM-DM et PIM-SM, et structurées en arborescence. En effet, certaines fonctions telles que l'arbre de recouvrement destiné à éviter les boucles, ne sont pas prises en charge.

La page **Proxy Interface** (Interface du proxy) contient des liens vers des pages Web qui définissent et affichent les paramètres et les données de l'interface du proxy. Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **IGMP** → **Proxy Interface** (Interface du proxy) dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

- 1 [Configuration de l'interface du proxy IGMP](#)
- 1 [Récapitulatif de la configuration du proxy IGMP](#)
- 1 [Informations d'appartenance relatives à l'interface du proxy IGMP](#)
- 1 [Informations d'appartenance détaillées relatives à l'interface du proxy IGMP](#)

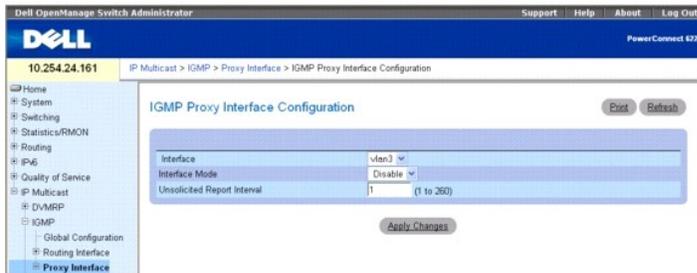
Configuration de l'interface du proxy IGMP

Le proxy IGMP est utilisé par le routeur IGMP (système IPv4) pour permettre au système d'émettre des messages hôte IGMP pour le compte d'hôtes détectés par le système via les interfaces de routeur IGMP standard. Cette fonction permet au système de faire office de proxy pour tous les hôtes résidant sur ses interfaces de routeur.

Utilisez la page **IGMP Proxy Interface Configuration** (Configuration de l'interface du proxy IGMP) pour configurer le proxy IGMP pour une interface. Pour pouvoir configurer ou afficher les données pour une interface de proxy IGMP, vous devez avoir configuré au moins une interface de routeur non IGMP.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **IGMP** → **Proxy Interface** (Interface du proxy) → **Interface Configuration** (Configuration de l'interface) dans l'arborescence.

Figure 13-12. Page IGMP Proxy Interface Configuration (Configuration de l'interface du proxy IGMP)



La page **IGMP Proxy Interface Configuration** (Configuration de l'interface du proxy IGMP) contient les champs suivants :

Interface : sélectionnez le port dont vous voulez afficher ou configurer les données dans le menu déroulant. Pour pouvoir configurer ou afficher les données pour une interface de proxy IGMP, vous devez avoir configuré au moins une interface de routeur non IGMP. Ce champ ne peut être configuré que lorsque le mode de l'interface est désactivé.

Interface Mode (Mode de l'interface) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant pour définir l'état administratif du proxy IGMP sur l'interface sélectionnée. La valeur par défaut est Disable (Désactiver). Les modes d'administration Routing (Routage), IGMP et Multicast (Multidiffusion) doivent être activés pour que le mode d'interface du proxy IGMP puisse être activé.

Unsolicited Report Interval (Intervalle entre rapports non sollicités) : entrez l'intervalle entre rapports non sollicités, en secondes. Il s'agit du délai entre les répétitions du rapport initial d'appartenance à un groupe émis par un hôte. Les valeurs valides vont de 1 à 260. La valeur par défaut est de 1.

Configuration de l'interface du proxy IGMP

1. Affichez la page **IGMP Proxy Interface Configuration** (Configuration de l'interface du proxy IGMP).
2. Sélectionnez l'interface à afficher dans le menu déroulant **Interface**.
3. Modifiez les autres champs selon vos besoins.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de l'interface du proxy est enregistrée et le périphérique est mis à jour.

Configuration de l'interface du proxy IGMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

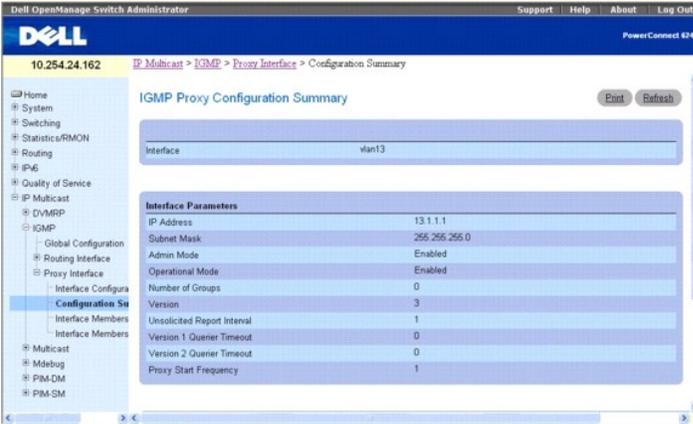
- 1 IGMP Proxy Commands (Commandes de proxy IGMP)

Récapitulatif de la configuration du proxy IGMP

Utilisez la page **IGMP Proxy Configuration Summary** (Récapitulatif de la configuration du proxy IGMP) pour afficher les configurations correspondant à chaque interface du proxy. Pour que cette page contienne des données, vous devez avoir configuré au moins une interface de routeur.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **IGMP** → **Proxy Interface** (Interface du proxy) → **Configuration Summary** (Récapitulatif de la configuration) dans l'arborescence.

Figure 13-13. Page IGMP Proxy Configuration Summary (Récapitulatif de la configuration du proxy IGMP)



La page **IGMP Proxy Configuration Summary** (Récapitulatif de la configuration du proxy IGMP) contient les champs suivants :

Interface : affiche l'interface sur laquelle le proxy IGMP est activé. Il ne peut y avoir qu'une interface du proxy IGMP.

IP Address (Adresse IP) : adresse IP de l'interface du proxy IGMP.

Subnet Mask (Masque de sous-réseau) : masque de sous-réseau correspondant à l'adresse IP de l'interface du proxy IGMP.

Admin Mode (Mode admin) : état administratif du proxy IGMP sur l'interface sélectionnée.

Operational Mode (Mode opérationnel) : état opérationnel de l'interface du proxy IGMP.

Number of Groups (Nombre de groupes) : nombre d'entrées correspondant à des groupes de multidiffusion pour l'interface du proxy IGMP dans la table de la mémoire cache.

Version : version du protocole IGMP configuré sur l'interface du proxy IGMP.

Unsolicited Report Interval (Intervalle entre rapports non sollicités) : délai entre les répétitions du rapport initial d'appartenance à un groupe émis par un hôte. La valeur par défaut est de 1 seconde.

Version 1 Querier Timeout (Délai d'attente du demandeur version 1) : valeur du délai d'attente (en secondes) pour le demandeur IGMP version 1. Il s'agit du délai maximal pour faire repasser un hôte en mode IGMPv3 lorsqu'une requête adressée à une version précédente est émise. Dès réception de ce type de requête, les hôtes définissent leur paramètre Older Version Querier Present Timer (temporisateur de demandeur de version précédente) en fonction du paramètre Older Version Querier Interval (intervalle du demandeur de version précédente).

Version 2 Querier Timeout (Délai d'attente du demandeur version 2) : valeur du délai d'attente (en secondes) pour le demandeur IGMP version 2.

Proxy Start Frequency (Fréquence de démarrage du proxy) : nombre de fois où le proxy a été démarré.

Proxy Interface Statistics (Statistiques relatives à l'interface du proxy) : nombre de requêtes reçues, nombre de rapports reçus/envoyés, nombre de rapports de sortie reçus/envoyés.

Affichage des configurations d'interface du proxy IGMP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

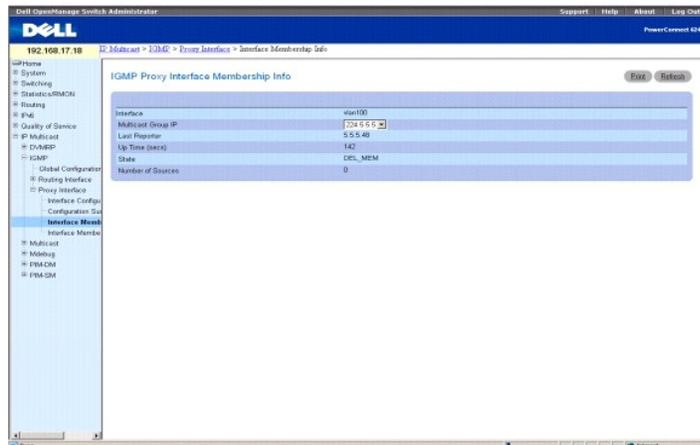
- 1 IGMP Proxy Commands (Commandes de proxy IGMP)

Informations d'appartenance relatives à l'interface du proxy IGMP

Utilisez la page **IGMP Proxy Interface Membership Info** (Informations d'appartenance relatives à l'interface du proxy IGMP) pour afficher les données d'appartenance de l'interface correspondant à une adresse IP de groupe de multidiffusion spécifique. Pour pouvoir afficher les informations d'appartenance de l'interface, vous devez avoir configuré au moins une interface de routeur non IGMP. Pour que cette page contienne des données, des rapports d'appartenance de groupe doivent avoir été reçus sur l'interface sélectionnée.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **IGMP** → **Proxy Interface** (Interface du proxy) → **Interface Membership Info** (Informations d'appartenance relatives à l'interface) dans l'arborescence.

Figure 13-14. Page IGMP Proxy Interface Membership Info (Informations d'appartenance relatives à l'interface du proxy IGMP)



La page **IGMP Proxy Interface Membership Info** (Informations d'appartenance relatives à l'interface du proxy IGMP) contient les champs suivants :

Interface : affiche l'interface sur laquelle le proxy IGMP est activé.

Multicast Group IP (Adresse IP du groupe de multidiffusion) : sélectionnez l'adresse IP du groupe de multidiffusion pour laquelle les données doivent être affichées. Si aucun rapport d'appartenance de groupe n'a été reçu sur l'interface sélectionnée, vous ne pouvez pas choisir cette option ; la page ne contient aucune des données ci-dessous.

Last Reporter (Dernier émetteur de rapport) : adresse IP de la source du dernier rapport d'appartenance reçu pour l'adresse de groupe de multidiffusion IP sur l'interface de proxy IGMP sélectionnée.

Up Time (secs) (Temps de fonctionnement [secondes]) : durée écoulée depuis la création de l'entrée.

State (État) : état de l'entrée correspondant au système hôte. Un système hôte peut se trouver dans différents états. L'état "Non-Member" (non membre) indique que le membre n'appartient pas au groupe associé à l'interface. L'état "Delaying Member" (Membre en attente) indique que le système hôte appartient au groupe associé à l'interface et que le temporisateur de rapport s'exécute. Ce temporisateur est utilisé pour envoyer les rapports. L'état "Idle" (Inactif) indique que le système hôte appartient au groupe associé à l'interface mais qu'aucun temporisateur de rapport ne s'exécute.

Number of Sources (Nombre de sources) : nombre d'hôtes source appartenant au groupe de multidiffusion sélectionné.

Affichage des informations d'appartenance relatives à l'interface du proxy IGMP à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

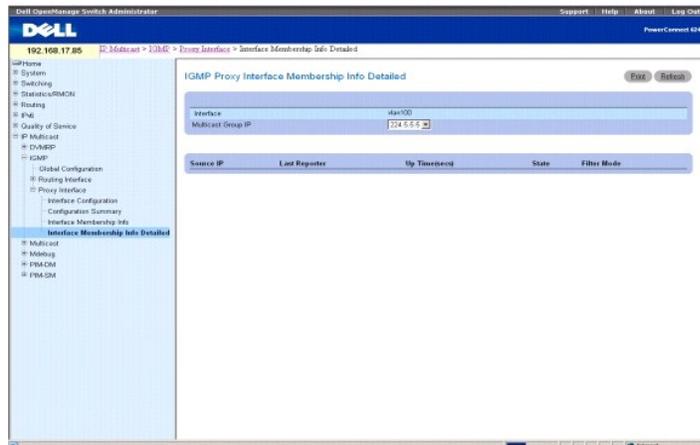
- 1 IGMP Proxy Commands (Commandes de proxy IGMP)

Informations d'appartenance détaillées relatives à l'interface du proxy IGMP

Utilisez la page **IGMP Proxy Interface Membership Info Detailed** (Informations d'appartenance détaillées relatives à l'interface du proxy IGMP) pour afficher les données d'appartenance détaillées relatives à l'interface. Pour pouvoir afficher les informations détaillées d'appartenance de l'interface, vous devez avoir configuré au moins une interface de routeur non IGMP. Pour que des données s'affichent, des rapports d'appartenance de groupe doivent avoir été reçus sur l'interface sélectionnée.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **IGMP** → **Proxy Interface** (Interface du proxy) → **Interface Membership Info Detailed** (Informations d'appartenance détaillées relatives à l'interface) dans l'arborescence.

Figure 13-15. IGMP Proxy Interface Membership Info Detailed (Informations d'appartenance détaillées relatives à l'interface du proxy IGMP)



La page **IGMP Proxy Interface Membership Info Detailed** (Informations d'appartenance détaillées relatives à l'interface du proxy IGMP) contient les champs suivants :

Interface : sélectionnez l'interface dont vous voulez afficher les données.

Multicast Group IP (Adresse IP du groupe de multidiffusion) : sélectionnez l'adresse IP du groupe de multidiffusion pour laquelle les données doivent être affichées. Si aucun rapport d'appartenance de groupe n'a été reçu sur l'interface sélectionnée, vous ne pouvez pas choisir cette option ; les données ne pouvant pas être configurées ne s'affichent pas.

Source IP (Adresse IP source) : adresses source appartenant à cette adresse de multidiffusion.

Last Reporter (Dernier émetteur de rapport) : adresse IP de la source du dernier rapport d'appartenance reçu pour l'adresse de groupe de multidiffusion IP de l'interface sélectionnée.

UpTime (secs) (Temps de fonctionnement [secondes]) : délai écoulé depuis la création de l'entrée dans la table de la mémoire cache.

State (État) : état de l'entrée correspondant au système hôte. Un hôte peut se trouver dans l'un des états suivants :

Non-member State (Non membre) : l'hôte n'appartient pas au groupe associé à l'interface.

Delaying Member State (Membre en attente) : indique que le système hôte appartient au groupe associé à l'interface et que le temporisateur de rapport s'exécute. Ce temporisateur est utilisé pour envoyer les rapports.

Idle Member State (Membre inactif) : indique que le système hôte appartient au groupe associé à l'interface mais qu'aucun temporisateur de rapport ne s'exécute.

Filter Mode (Mode de filtrage) : mode de filtrage de groupe (Include/Exclude/None) du groupe spécifié sur l'interface du proxy IGMP.

Affichage des informations d'appartenance détaillées relatives à l'interface du proxy IGMP

1. Affichez la page **IGMP Proxy Interface Membership Info Detailed** (Informations d'appartenance détaillées relatives à l'interface du proxy IGMP)
2. Sélectionnez l'interface à afficher dans le menu déroulant **Interface**.
3. Sélectionnez la valeur voulue dans **Multicast Group IP** (Adresse IP du groupe de multidiffusion).

Des données d'appartenance détaillées pour cette interface et l'adresse IP du groupe de multidiffusion s'affichent.

Affichage des informations d'appartenance détaillées relatives à l'interface du proxy IGMP à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

1. IGMP Proxy Commands (Commandes de proxy IGMP)

Multidiffusion

La page **Multicast** (Multidiffusion) contient des liens vers des pages Web qui définissent et affichent les paramètres et les données de **multidiffusion**. Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **Multicast** (Multidiffusion IP) dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

1. [Configuration globale de la multidiffusion](#)

- 1 [Configuration de l'interface de multidiffusion](#)
- 1 [Récapitulatif de la multidiffusion pour Mroute](#)
- 1 [Configuration d'itinéraires statiques de multidiffusion](#)
- 1 [Récapitulatif des itinéraires statiques de multidiffusion](#)
- 1 [Configuration des limites administratives de la multidiffusion](#)
- 1 [Récapitulatif des limites administratives de la multidiffusion](#)

Configuration globale de la multidiffusion

Utilisez la page **Multicast Global Configuration** (Configuration globale de la multidiffusion) pour configurer l'état administratif de la transmission de multidiffusion dans le routeur, et pour afficher les paramètres globaux de multidiffusion.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **Multicast** (Multidiffusion) → **Global Configuration** (Configuration globale) dans l'arborescence.

Figure 13-16. Page Multicast Global Configuration (Configuration globale de la multidiffusion)



La page **Multicast Global Configuration** (Configuration globale de la multidiffusion) contient les champs suivants :

Admin Mode (Mode Admin) : sélectionnez Enable (Activer) ou Disable (Désactiver) pour définir l'état administratif de la transmission de multidiffusion dans le routeur. La valeur par défaut est Disable (Désactiver).

Protocol State (État du protocole) : état opérationnel du module de transmission multidiffusion.

Table Maximum Entry Count (Nombre maximal d'entrées dans la table) : nombre maximal d'entrées dans la table de routage de multidiffusion IP.

Number Of Packets For Which Source Not Found (Nombre de paquets avec source introuvable) : nombre de paquets de multidiffusion censés être acheminés mais pour lesquels la vérification RPF a échoué.

Number Of Packets For Which Group Not Found (Nombre de paquets avec groupe introuvable) : nombre de paquets de multidiffusion censés être acheminés mais pour lesquels aucun itinéraire de multidiffusion n'a été trouvé.

Protocol (Protocole) : protocole de routage de multidiffusion actuellement activé sur le routeur, le cas échéant.

Table Entry Count (Nombre d'entrées dans la table) : nombre d'entrées de routage de multidiffusion actuellement présentes dans la table de routage de multidiffusion.

Table Highest Entry Count (Nombre maximal d'entrées dans la table) : nombre maximal d'entrées de routage de multidiffusion dans la table de routage de multidiffusion.

Configuration du mode administratif de la transmission de multidiffusion

1. Affichez la page **Multicast Global Configuration** (Configuration globale de la multidiffusion).
2. Sélectionnez Enable (Activer) ou Disable (Désactiver) dans le champ **Admin Mode** (Mode Admin).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration globale de la multidiffusion est enregistrée et le périphérique est mis à jour.

Configuration/affichage des paramètres de transmission de multidiffusion à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

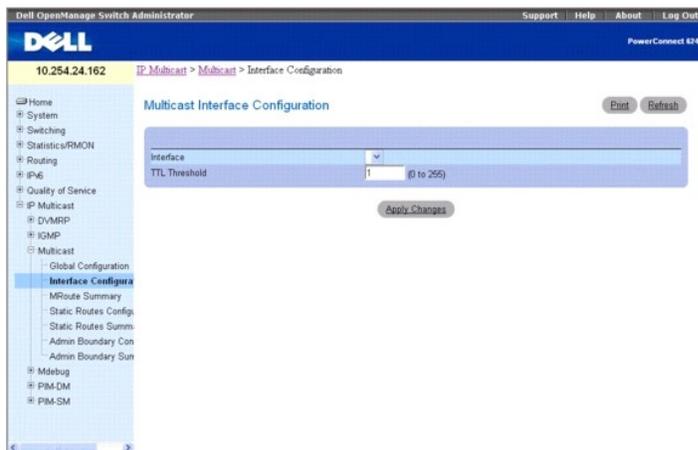
- 1 Multicast Commands (Commandes de multidiffusion)

Configuration de l'interface de multidiffusion

Utilisez la page **Multicast Interface Configuration** (Configuration de l'interface de multidiffusion) pour configurer le seuil TTL d'une interface de multidiffusion. Pour que cette page contienne des champs, vous devez configurer au moins une interface de routeur.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **Multicast** (Multidiffusion) → **Interface Configuration** (Configuration de l'interface) dans l'arborescence.

Figure 13-17. Page Multicast Interface Configuration (Configuration de l'interface de multidiffusion)



La page **Multicast Interface Configuration** (Configuration de l'interface de multidiffusion) contient les champs suivants :

Interface : sélectionnez dans le menu déroulant l'interface de routage à configurer.

TTL Threshold (Seuil TTL) : entrez le seuil TTL en-deçà duquel un paquet de données de multidiffusion n'est pas transmis à partir de l'interface sélectionnée. Indiquez un nombre compris entre 0 et 255. Si vous entrez 0, tous les paquets de multidiffusion pour l'interface sélectionnée sont transmis. Pour que ce champ s'affiche, vous devez configurer au moins une interface de routeur.

Configuration d'une interface de multidiffusion

1. Affichez la page **Multicast Interface Configuration** (Configuration de l'interface de multidiffusion).
2. Sélectionnez l'interface à configurer dans le menu déroulant **Interface**.
3. Entrez une valeur dans le champ **TTL Threshold** (Seuil TTL).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de l'interface de multidiffusion est enregistrée et le périphérique est mis à jour.

Configuration d'une interface de multidiffusion à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 Multicast Commands (Commandes de multidiffusion)

Récapitulatif de la multidiffusion pour MRoute

Utilisez la page **MRoute Summary** (Récapitulatif MRoute) pour afficher les données relatives à MRoute.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **Multicast** (Multidiffusion) → **MRoute Summary** (Récapitulatif MRoute) dans l'arborescence.

Figure 13-18. Page Multicast MRoute Summary (Récapitulatif de la multidiffusion pour MRoute)

Source IP	Group IP	Incoming Interface	Outgoing Interfaces	Up Time (secs)	Expiry Time (secs)	RPF Neighbour	Protocol	Flags
3.1.1.100	255.0.2.2	vlan30	vlan10	520	182	0.0.0.0	PIMDM	----

La page **Multicast MRoute Summary** (Récapitulatif de la multidiffusion pour MRoute) contient les champs suivants :

Source IP (Adresse IP source) : adresse IP de la source du paquet de multidiffusion qui, associée à l'adresse IP du groupe, identifie une entrée de la table MRoute.

Group IP (Adresse IP du groupe) : adresse IP du groupe de destination.

Incoming Interface (Interface d'entrée) : interface d'entrée sur laquelle arrivent les paquets de multidiffusion pour cette source/ce groupe.

Outgoing Interfaces (Interfaces de sortie) : liste des interfaces de sortie sur lesquelles sont transmis les paquets de multidiffusion pour cette source/ce groupe.

Up Time (secs) (Temps de fonctionnement [secondes]) : durée en secondes écoulée depuis la création de l'entrée.

Expiry Time (secs) (Délai d'expiration [secondes]) : délai en secondes avant que cette entrée arrive à expiration et soit supprimée de la table.

RPF Neighbor (Voisin RPF) : adresse IP du voisin RPF (Reverse Path Forwarding).

Protocol (Protocole) : protocole de routage de multidiffusion ayant créé cette entrée. Les valeurs possibles sont les suivantes :

- 1 PIM-DM
- 1 PIM-SM
- 1 DVMRP

Flags (Indicateurs) : la valeur de ce champ est valide si le protocole de routage de multidiffusion en cours d'exécution est PIM-SM. Les valeurs possibles sont RPT et SPT. Pour les autres protocoles, "-----" s'affiche.

Affichage du récapitulatif MRoute à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

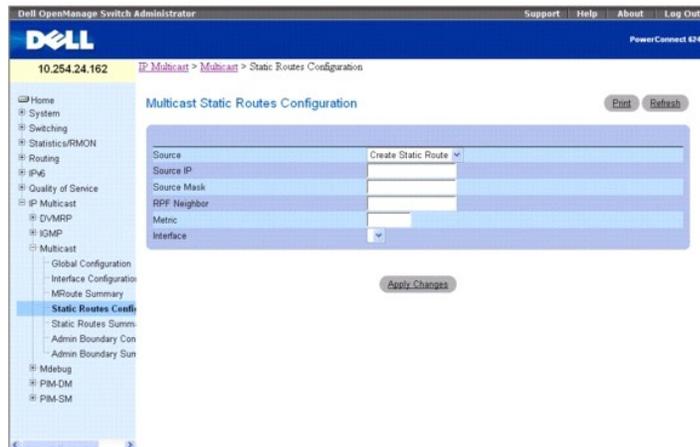
- 1 Multicast Commands (Commandes de multidiffusion)

Configuration des itinéraires statiques de multidiffusion

Utilisez la page **Multicast Static Routes Configuration** (Configuration des itinéraires statiques de multidiffusion) pour configurer une nouvelle entrée statique dans la table MRoute ou pour modifier une entrée existante.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **Multicast** (Multidiffusion) → **Static Routes Configuration** (Configuration des itinéraires statiques) dans l'arborescence.

Figure 13-19. Page Multicast Static Routes Configuration (Configuration des itinéraires statiques de multidiffusion)



La page **Multicast Static Routes Configuration** (Configuration des itinéraires statiques de multidiffusion) contient les champs suivants :

Source : sélectionnez **Create Static Route** (Créer un itinéraire statique) pour configurer une nouvelle entrée statique dans la table MRoute, ou bien sélectionnez une entrée existante dans le menu déroulant.

Source IP (Adresse IP source) : entrez l'adresse IP qui identifie la source des paquets de multidiffusion pour l'entrée en cours de création.

Source Mask (Masque source) : entrez le masque de sous-réseau à appliquer à l'adresse IP source.

RPF Neighbor (Voisin RPF) : entrez l'adresse IP du routeur voisin sur le chemin vers la source.

Metric (Métrique) : entrez le coût des liaisons du chemin vers la source de multidiffusion. Les valeurs possibles vont de 0 à 255 ; la valeur par défaut est de 1. Vous pouvez modifier la métrique d'un itinéraire configuré en sélectionnant l'itinéraire statique et en modifiant ce champ.

Interface : sélectionnez le numéro d'interface dans le menu déroulant. Il s'agit de l'interface de connexion au routeur voisin pour l'adresse IP source donnée.

Configuration d'un itinéraire statique

1. Affichez la page **Static Routes** (Itinéraires statiques).
2. Sélectionnez **Create Static Route** (Créer un itinéraire statique) dans le champ **Source** pour configurer une nouvelle entrée statique, ou bien sélectionnez une entrée existante.
3. Modifiez les autres champs selon vos besoins.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'itinéraire statique nouveau ou modifié est enregistré et le périphérique est mis à jour.

Configuration d'un itinéraire statique à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 Multicast Commands (Commandes de multidiffusion)

Récapitulatif des itinéraires statiques de multidiffusion

Utilisez la page **Multicast Static Routes Summary** (Récapitulatif des itinéraires statiques de multidiffusion) pour afficher les itinéraires statiques et leur configuration.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **Multicast** (Multidiffusion) → **Static Routes Summary** (Récapitulatif des itinéraires statiques) dans l'arborescence.

Figure 13-20. Page Multicast Static Routes Summary (Récapitulatif des itinéraires statiques de multidiffusion)

Dell OpenManage Switch Administrator

10.254.24.162 IP Multicast > Multicast > Static Routes Summary

Multicast Static Routes Summary

Source IP	Source Mask	RPF Address	Metric	VLANID
3.1.1.1	255.255.255.0	6.1.1.1	1	vlan3

La page **Multicast Static Routes Summary** (Récapitulatif des itinéraires statiques de multidiffusion) contient les champs suivants :

Source IP (Adresse IP source) : adresse IP qui identifie la source des paquets de multidiffusion pour cette route.

Source Mask (Masque source) : masque de sous-réseau appliqué à l'adresse IP source.

RPF Address (Adresse RPF) : adresse IP du voisin RPF.

Metric (Métrique) : coût des liaisons du chemin vers la source de multidiffusion. La plage est comprise entre 0 et 255.

VLANID : numéro du VLAN d'entrée dont l'adresse IP est utilisée comme RPF pour l'adresse IP source donnée.

Affichage du récapitulatif des itinéraires statiques à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 Multicast Commands (Commandes de multidiffusion)

Configuration des limites administratives de la multidiffusion

La définition d'une limite administrative permet de stopper le trafic de multidiffusion entrant et sortant pour une plage spécifique d'adresses de multidiffusion sur une interface de routage donnée. Utilisez la page **Multicast Admin Boundary Configuration** (Configuration des limites administratives de la multidiffusion) pour configurer une limite administrative nouvelle ou existante. Pour que cette page s'affiche, vous devez avoir configuré une interface de routage valide et la multidiffusion.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **Multicast** (Multidiffusion) → **Admin Boundary Configuration** (Configuration des limites administratives) dans l'arborescence.

Figure 13-21. Page Multicast Admin Boundary Configuration (Configuration des limites administratives de la multidiffusion)

Dell OpenManage Switch Administrator

10.254.24.162 IP Multicast > Multicast > Admin Boundary Configuration

Multicast Admin Boundary Configuration

Group: Create Boundary

Interface: [text box]

Group IP: [text box]

Group Mask: [text box]

Apply Changes

La page **Multicast Admin Boundary Configuration** (Configuration des limites administratives de la multidiffusion) contient les champs suivants :

Group (Groupe) : sélectionnez **Create Boundary** (Créer une limite) dans le menu déroulant pour créer une nouvelle limite administrative, ou bien sélectionnez

une limite existante pour afficher ou mettre à jour sa configuration.

Interface : sélectionnez l'interface de routeur pour laquelle la limite administrative doit être configurée.

Group IP (Adresse IP du groupe) : entrez l'adresse du groupe de multidiffusion correspondant au début de la plage d'adresses à exclure. Cette adresse doit être comprise entre 239.0.0.0 et 239.255.255.255.

Group Mask (Masque de groupe) : entrez le masque à appliquer à l'adresse du groupe de multidiffusion. La combinaison du masque et de l'adresse IP du groupe représente la plage d'adresses administratives de l'interface sélectionnée.

Configuration d'une limite administrative

1. Affichez la page **Multicast Admin Boundary Configuration** (Configuration des limites administratives de la multidiffusion).
2. Sélectionnez **Create Boundary** (Créer une limite) dans le champ **Group IP** (Adresse IP du groupe) pour configurer une nouvelle limite administrative, ou bien sélectionnez l'une des entrées existantes.
3. Modifiez les autres champs selon vos besoins.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La limite administrative nouvelle ou modifiée est enregistrée et le périphérique est mis à jour.

Configuration d'une limite administrative à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

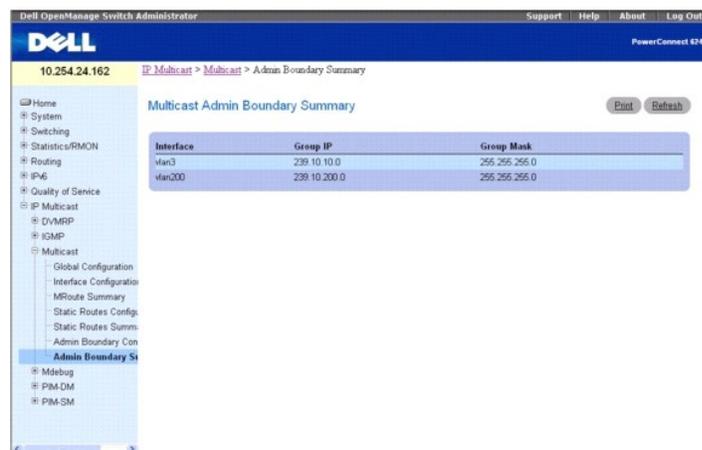
1. Multicast Commands (Commandes de multidiffusion)

Récapitulatif des limites administratives de la multidiffusion

Utilisez la page **Multicast Admin Boundary Summary** (Récapitulatif des limites administratives de la multidiffusion) pour afficher les limites administratives existantes.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **Multicast** (Multidiffusion) → **Admin Boundary Summary** (Récapitulatif des limites administratives) dans l'arborescence.

Figure 13-22. Page **Multicast Admin Boundary Summary** (Récapitulatif des limites administratives de la multidiffusion)



Interface	Group IP	Group Mask
lan3	239.10.10.0	255.255.255.0
lan200	239.10.200.0	255.255.255.0

La page **Multicast Admin Boundary Summary** (Récapitulatif des limites administratives de la multidiffusion) contient les champs suivants :

Interface : interface de routeur à laquelle la plage d'adresses administratives est appliquée.

Group IP (Adresse IP du groupe) : adresse du groupe de multidiffusion correspondant au début de la plage d'adresses à exclure.

Group Mask (Masque de groupe) : masque à appliquer à l'adresse du groupe de multidiffusion. La combinaison du masque et de l'adresse IP du groupe représente la plage d'adresses administratives de l'interface sélectionnée.

Affichage du récapitulatif des limites administratives de la multidiffusion à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 Multicast Commands (Commandes de multidiffusion)

PIM-DM

PIM-DM est un protocole de routage de multidiffusion simple et indépendant des autres protocoles. Il utilise une table de routage de monodiffusion existante et un mécanisme Join/Prune/Graft (adhésion/élagage/greffage) pour créer un arbre. PIM-DM crée des arbres de distribution basés sur le plus court chemin jusqu'à la source faisant appel à RPF. Il ne peut pas être utilisé pour créer un arbre de distribution partagé, contrairement à PIM-SM. PIM-DM part du principe que, lorsqu'un expéditeur commence à envoyer des données, tous les routeurs et les hôtes en aval souhaitent recevoir un datagramme de multidiffusion. Au départ, PIM-DM diffuse le trafic de multidiffusion sur tout le réseau. Les routeurs qui n'ont pas de voisins en aval élaguent le trafic non sollicité. Outre les messages d'élagage (PRUNE), PIM-DM utilise des messages de greffage (graft) et d'assertion (assert). Les messages d'élagage sont utilisés lorsqu'un nouvel hôte souhaite adhérer au groupe. Les messages d'assertion permettent d'arrêter les flux redondants sur un réseau à accès multiple.

Il existe deux versions de PIM-DM. La version 2 n'utilise pas le message IGMP ; elle fait appel à un message encapsulé dans un paquet IP, avec le numéro de protocole 103. Dans la version 2, le message Hello remplace le message de requête.

PIM-DM peut être utilisé dans les cas suivants :

- 1 Forte densité de récepteurs
- 1 Peu d'expéditeurs pour de nombreux récepteurs (en raison de diffusions fréquentes)
- 1 Volume élevé de trafic de multidiffusion
- 1 Flux de trafic constant

La page **PIM-DM** contient des liens vers des pages Web qui définissent et affichent les paramètres et les données de **PIM-DM**. Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **PIM-DM** dans l'arborescence.

Cette page permet d'accéder aux fonctionnalités suivantes :

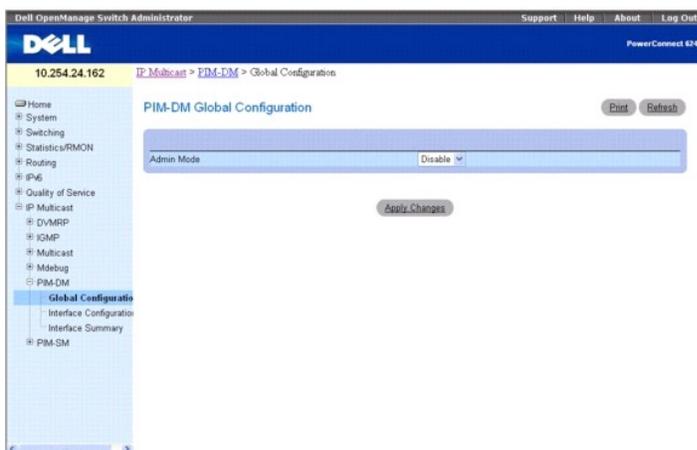
- 1 [Configuration globale PIM-DM](#)
- 1 [Configuration des interfaces PIM-DM](#)
- 1 [Récapitulatif des interfaces PIM-DM](#)

Configuration globale PIM-DM

Utilisez la page **PIM-DM Global Configuration** (Configuration globale PIM-DM) pour configurer l'état administratif de PIM-DM sur ce système.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **PIM-DM** → **Global Configuration** (Configuration globale) dans l'arborescence.

Figure 13-23. Page PIM-DM Global Configuration (Configuration globale PIM-DM)



La page **PIM-DM Global Configuration** (Configuration globale PIM-DM) contient le champ suivant :

Admin Mode (Mode Admin) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant pour définir l'état administratif de PIM-DM sur le système. La valeur par défaut est Disable (Désactiver).

Configuration de PIM-DM

1. Affichez la page **PIM-DM Global Configuration** (Configuration globale PIM-DM).

2. Sélectionnez **Enable (Activer)** ou **Disable (Désactiver)** dans le champ **Admin Mode (Mode Admin)** pour activer ou désactiver PIM-DM.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de PIM-DM est enregistrée et le périphérique est mis à jour.

Configuration de PIM-DM à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

1. PIM-DM Commands (Commandes PIM-DM)

Configuration des interfaces PIM-DM

Utilisez la page **PIM-DM Interface Configuration** (Configuration des interfaces PIM-DM) pour configurer des interfaces spécifiques à l'aide de PIM-DM. Pour que cette page de configuration s'affiche, PIM-DM doit être activé dans la page **PIM-DM Global Configuration** (Configuration globale PIM-DM).

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **PIM-DM** → **Interface Configuration** (Configuration de l'interface) dans l'arborescence.

Figure 13-24. Page PIM-DM Interface Configuration (Configuration des interfaces PIM-DM)



La page **PIM-DM Interface Configuration** (Configuration des interfaces PIM-DM) contient les champs suivants :

Interface : sélectionnez l'interface dont vous souhaitez afficher ou configurer les données. Pour pouvoir configurer ou afficher les données relatives à une interface PIM-DM, vous devez avoir configuré au moins une interface de routeur ; dans le cas contraire, un message d'erreur s'affiche.

Interface Mode (Mode de l'interface) : sélectionnez **Enable (Activer)** ou **Disable (Désactiver)** dans le menu déroulant pour définir l'état administratif de PIM-DM pour l'interface sélectionnée. La valeur par défaut est **Disable (Désactiver)**.

Hello Interval (secs) (Intervalle entre messages Hello [secondes]) : entrez le nombre de secondes devant s'écouler entre les messages Hello PIM transmis à partir de l'interface sélectionnée. La valeur par défaut est de 30. Les valeurs valides vont de 10 à 3600.

Configuration de PIM-DM pour une interface

1. Affichez la page **PIM-DM Interface Configuration** (Configuration des interfaces PIM-DM).
2. Sélectionnez l'interface à configurer dans le champ **Interface**.
3. Modifiez les autres champs selon vos besoins.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de l'interface est enregistrée et le périphérique est mis à jour.

Configuration de PIM-DM pour une interface à l'aide des commandes CLI

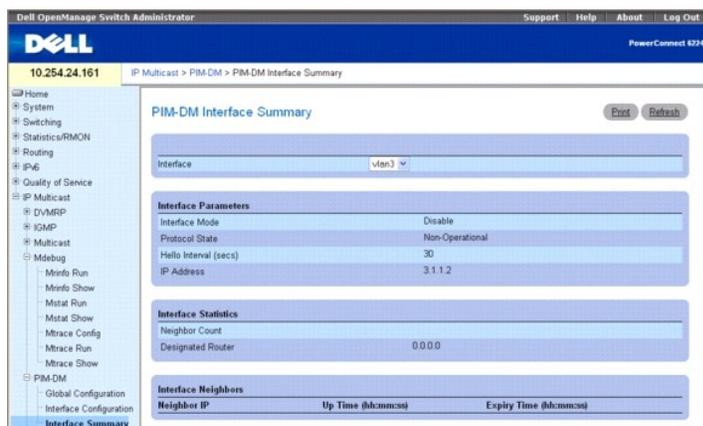
Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

Récapitulatif des interfaces PIM-DM

Utilisez la page **PIM-DM Interface Summary** (Récapitulatif des interfaces PIM-DM) pour afficher une interface PIM-DM et les paramètres correspondants. Pour que cette page s'affiche, au moins une interface de ce routeur doit être définie comme PIM-DM.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **PIM-DM** → **Interface Summary** (Récapitulatif de l'interface) dans l'arborescence.

Figure 13-25. PIM-DM Interface Summary (Récapitulatif des interfaces PIM-DM)



La page **PIM-DM Interface Summary** (Récapitulatif des interfaces PIM-DM) contient les champs suivants :

Interface : sélectionnez l'interface dont vous voulez afficher les données. Pour pouvoir afficher les données relatives à une interface PIM-DM, vous devez avoir configuré au moins une interface de routeur ; dans le cas contraire, un message d'erreur s'affiche.

Interface Parameters (Paramètres de l'interface)

Interface Mode (Mode de l'interface) : indique l'état administratif de PIM-DM pour l'interface sélectionnée. La valeur par défaut est Disable (Désactiver).

Protocol State (État du protocole) : état opérationnel du protocole PIM-DM sur cette interface.

Hello Interval (secs) (Intervalle entre messages Hello [secondes]) : fréquence selon laquelle les messages Hello PIM sont transmis sur l'interface sélectionnée.

IP Address (Adresse IP) : adresse IP de l'interface sélectionnée.

Interface Statistics (Statistiques sur les interfaces)

Neighbor Count (Nombre de voisins) : nombre de voisins PIM sur l'interface sélectionnée.

Designated Router (Routeur désigné) : routeur désigné sur l'interface PIM sélectionnée. Pour les interfaces point à point, la valeur est 0.0.0.0.

Interface Neighbors (Voisins de l'interface)

Neighbor IP (Adresse IP du voisin) : adresse IP du voisin PIM sur lequel cette entrée contient des informations.

Up Time (hh:mm:ss) (Temps de fonctionnement [hh:mm:ss]) : durée écoulée depuis que ce voisin PIM est devenu un voisin du routeur local.

Expiry Time (hh:mm:ss) (Délai d'expiration [hh:mm:ss]) : délai minimal restant avant que ce voisin PIM arrive à expiration.

Affichage du récapitulatif des interfaces PIM-DM à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

PIM-SM

PIM-SM permet d'acheminer efficacement le trafic de multidiffusion vers des groupes de multidiffusion pouvant appartenir à plusieurs réseaux étendus (WAN), lorsque la bande passante constitue une contrainte. Par défaut, ce protocole utilise des arborescences partagées ; il implémente des arborescences basées sur la source pour une plus grande efficacité. Le basculement d'une arborescence à l'autre se fait en fonction du seuil défini pour le débit des données. PIM-SM suppose que seuls les hôtes qui en font la demande explicite souhaitent recevoir le trafic de multidiffusion. Il crée un arbre de distribution partagé axé sur un

point de rendez-vous (RP) défini, à partir duquel le trafic source est transmis aux récepteurs. Tout d'abord, les expéditeurs envoient les données de multidiffusion au RP, lequel les transmet ensuite aux récepteurs via l'arbre partagé. Les arbres partagés axés sur un RP (point de rendez-vous) ne déterminent pas obligatoirement le chemin le plus court/optimal. Dans ce type de cas, PIM-SM permet de passer à des arbres spécifiques à une source plus efficaces.

La page **PIM-SM** contient des liens vers des pages Web qui définissent et affichent les paramètres et les données de PIM-SM. Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **PIM-SM** dans l'arborescence.

Cette page permet d'accéder aux fonctionnalités suivantes :

- 1 [Configuration globale PIM-SM](#)
- 1 [État global de PIM-SM](#)
- 1 [Configuration des interfaces PIM-SM](#)
- 1 [Récapitulatif des interfaces PIM-SM](#)
- 1 [Récapitulatif des composants](#)
- 1 [Récapitulatif des RP définis](#)
- 1 [Récapitulatif des RP candidats](#)
- 1 [Configuration des RP statiques](#)

Configuration globale PIM-SM

Utilisez la page **PIM-SM Global Configuration** (Configuration globale PIM-SM) pour configurer les paramètres PIM-SM globaux pour ce système.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **PIM-SM** → **Global Configuration** (Configuration globale) dans l'arborescence.

Figure 13-26. Page PIM-SM Global Configuration (Configuration globale PIM-SM)



La page **PIM-SM Global Configuration** (Configuration globale PIM-SM) contient les champs suivants :

Admin Mode (Mode Admin) : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant pour définir l'état administratif de PIM-SM sur le système. Pour pouvoir activer PIM-SM, vous devez activer IGMP. La valeur par défaut est Disable (Désactiver).

Join/Prune Interval (secs) (Intervalle entre messages Join/Prune [adhésion/élagage] : entrez l'intervalle (en secondes) entre les transmissions des messages Join/Prune (adhésion/élagage) PIM-SM. Les valeurs valides sont comprises entre 10 et 3600 secondes. La valeur par défaut est de 60.

Data Threshold Rate (Kbps) (Seuil de débit de données, Kbps) : entrez le débit de données source minimal, en kilobits par seconde, au-delà duquel le routeur du dernier saut passe à un arbre correspondant à une source spécifique utilisant un chemin plus court. Les valeurs valides vont de 0 à 2000 Kbps. La valeur par défaut est de 50.

Register Threshold Rate (Kbps) (Seuil de débit d'enregistrement, Kbps) : entrez le débit de données source minimal, en kilobits par seconde, au-delà duquel le routeur du point de rendez-vous passe à un arbre correspondant à une source spécifique utilisant un chemin plus court. Les valeurs valides vont de 0 à 2000 Kbps. La valeur par défaut est de 50.

Configuration de PIM-SM

1. Affichez la page **PIM-SM Global Configuration** (Configuration globale PIM-SM).
2. Sélectionnez Enable (Activer) ou Disable (Désactiver) dans le champ **Admin Mode** (Mode Admin) pour activer ou désactiver PIM-SM.
3. Modifiez les autres champs selon vos besoins.

4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de l'interface est enregistrée et le périphérique est mis à jour.

Configuration de PIM-SM à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 PIM-SM Commands (Commandes PIM-SM)

État global de PIM-SM

Utilisez la page **PIM-SM Global Status** (État global de PIM-SM) pour afficher les paramètres globaux sélectionnés sur la page **PIM-SM Global Configuration** (Configuration globale PIM-SM).

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **PIM-SM** → **Global Status** (État global) dans l'arborescence.

Figure 13-27. Page **PIM-SM Global Status** (État global de PIM-SM)



La page **PIM-SM Global Status** (État global PIM-SM) contient les champs suivants :

Admin Mode (Mode Admin) : état administratif de PIM-SM dans le routeur. Cet état peut être Enable (Activer) ou Disable (Désactiver).

Join/Prune Interval (secs) (Intervalle entre messages Join/Prune [adhésion/élagage]) : intervalle (en secondes) entre les transmissions des messages Join/Prune (adhésion/élagage) PIM-SM.

Data Threshold Rate (Kbps) (Seuil de débit de données, Kbps) : débit de données source minimal, en kilobits par seconde, au-delà duquel le routeur du dernier saut passe à un arbre correspondant à une source spécifique utilisant un chemin plus court.

Register Threshold Rate (Kbps) (Seuil de débit d'enregistrement, Kbps) : débit de données source minimal, en kilobits par seconde, au-delà duquel le routeur du point de rendez-vous passe à un arbre correspondant à une source spécifique utilisant un chemin plus court.

Affichage de l'état global de PIM-SM à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

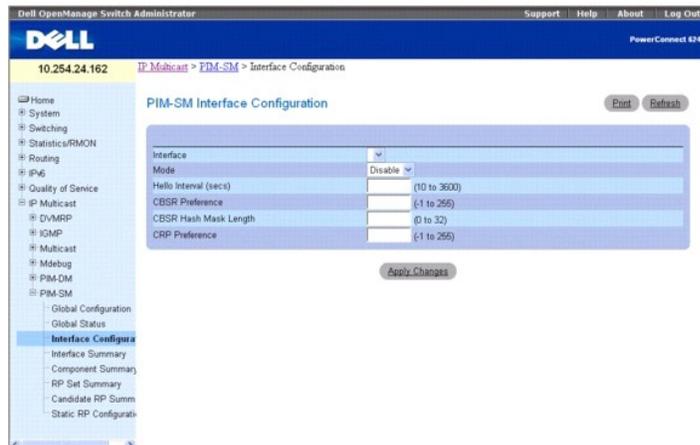
- 1 PIM-SM Commands (Commandes PIM-SM)

Configuration des interfaces PIM-SM

Utilisez la page **PIM-SM Interface Configuration** (Configuration des interfaces PIM-SM) pour configurer PIM-SM pour une interface. Pour que cette page de configuration s'affiche, PIM-SM doit être activé dans la page **PIM-SM Global Configuration** (Configuration globale PIM-SM).

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **PIM-SM** → **Interface Configuration** (Configuration de l'interface) dans l'arborescence.

Figure 13-28. Page **PIM-SM Interface Configuration** (Configuration des interfaces PIM-SM)



La page **PIM-SM Interface Configuration** (Configuration des interfaces PIM-SM) contient les champs suivants :

Interface : sélectionnez l'interface dont vous souhaitez afficher ou configurer les données. Pour que les données puissent être affichées ou configurées, il doit exister au moins une interface de routage.

Mode : sélectionnez Enable (Activer) ou Disable (Désactiver) dans le menu déroulant pour définir l'état administratif de PIM-SM sur cette interface. La valeur par défaut est Disable (Désactiver).

Hello Interval (secs) (Intervalle entre messages Hello [secondes]) : entrez le délai (en secondes) entre les transmissions de messages Hello PIM sur cette interface. Les valeurs valides sont comprises entre 10 et 3600 secondes. La valeur par défaut est de 30.

CBSR Preference (Préférence CBSR) : entrez la valeur de préférence de l'interface locale en tant que routeur BSR (bootstrap) candidat. La valeur -1 indique que l'interface locale n'est pas une interface BSR candidate. Les valeurs valides vont de -1 à 255. La valeur par défaut est de 0.

CBSR Hash Mask Length (Longueur du masque de hachage CBSR) : entrez la longueur du masque de hachage CBSR à annoncer dans les messages bootstrap si cette interface est élue comme routeur BSR. La longueur du masque de hachage est utilisée dans l'algorithme de hachage pour sélectionner le RP pour un groupe donné. Les valeurs valides vont de 0 à 32. La valeur par défaut est de 30.

CRP Preference (Préférence CRP) : entrez la valeur de préférence de l'interface locale en tant que routeur BSR (bootstrap) candidat. La valeur -1 indique que l'interface locale n'est pas une interface BSR candidate. Les valeurs valides vont de -1 à 255. La valeur par défaut est de 0.

Configuration de PIM-SM pour une interface

1. Affichez la page **PIM-SM Interface Configuration** (Configuration des interfaces PIM-SM).
2. Sélectionnez l'interface à configurer dans le champ **Interface**.
3. Sélectionnez **Enable** (Activé) dans le champ **Mode**.
4. Modifiez les autres champs selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La configuration de l'interface est enregistrée et le périphérique est mis à jour.

Configuration de PIM-SM pour une interface à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 PIM-SM Commands (Commandes PIM-SM)

Récapitulatif des interfaces PIM-SM

Utilisez la page **PIM-SM Interface Summary** (Récapitulatif des interfaces PIM-SM) pour afficher une interface PIM-SM et les paramètres correspondants. Pour que cette page s'affiche, au moins une interface de ce routeur doit être définie comme PIM-SM.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **PIM-SM** → **Interface Summary** (Récapitulatif des interfaces) dans l'arborescence.

Figure 13-29. PIM-SM Interface Summary (Récapitulatif des interfaces PIM-SM)



La page **PIM-SM Interface Summary** (Récapitulatif des interfaces PIM-SM) contient les champs suivants :

Interface : sélectionnez l'interface dont vous voulez afficher les données.

Mode : état administratif de PIM-SM dans le routeur. Cet état peut être Enable (Activer) ou Disable (Désactiver).

Protocol State (État du protocole) : affiche l'état opérationnel du protocole PIM-SM sur l'interface sélectionnée, à savoir Operational (Opérationnel) ou Non-operational (Non opérationnel).

IP Address (Adresse IP) : adresse IP de l'interface PIM sélectionnée.

Net Mask (Masque de réseau) : masque de réseau correspondant à l'adresse IP de l'interface PIM sélectionnée.

Designated Router (Routeur désigné) : routeur désigné sur l'interface PIM sélectionnée. Pour les interfaces point à point, cet objet a la valeur 0.0.0.0.

Hello Interval (secs) (Intervalle entre messages Hello [secondes]) : fréquence selon laquelle les messages Hello PIM sont transmis sur l'interface sélectionnée.

CBSR Preference (Préférence CBSR) : valeur de préférence de l'interface locale en tant que routeur BSR (bootstrap) candidat. La valeur -1 indique que l'interface locale n'est pas une interface BSR candidate.

CBSR Hash Mask Length (Longueur du masque de hachage CBSR) : longueur du masque de hachage CBSR à annoncer dans les messages bootstrap si cette interface est élue comme routeur BSR. La longueur du masque de hachage est utilisée dans l'algorithme de hachage pour sélectionner le RP pour un groupe donné.

CRP Preference (Préférence CRP) : valeur de préférence de l'interface locale en tant que routeur BSR (bootstrap) candidat. La valeur -1 indique que l'interface locale n'est pas une interface BSR candidate.

Neighbor Count (Nombre de voisins) : nombre de voisins PIM sur l'interface sélectionnée.

IP Address (Adresse IP) : adresse IP du voisin PIM de cette entrée.

Up Time (hh:mm:ss) (Temps de fonctionnement [hh:mm:ss]) : durée écoulée depuis que ce voisin PIM est devenu un voisin du routeur local.

Expiry Time (hh:mm:ss) (Délai d'expiration [hh:mm:ss]) : délai minimal restant avant que ce voisin PIM arrive à expiration.

Affichage du récapitulatif des interfaces PIM-SM

1. Affichez la page **PIM-SM Interface Summary** (Récapitulatif des interfaces PIM-SM).
2. Sélectionnez l'interface à afficher dans le menu déroulant **Interface**.

Les données de configuration PIM-SM de cette interface s'affichent.

Affichage du récapitulatif des interfaces PIM-SM à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 PIM-SM Commands (Commandes PIM-SM)

Récapitulatif des composants

Utilisez la page **Component Summary** (Récapitulatif des composants) pour afficher les données relatives aux composants PIM-SM.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **PIM-SM** → **Component Summary** (Récapitulatif des composants) dans l'arborescence.

Figure 13-30. Page Component Summary (Récapitulatif des composants)

Component Index	Component BSR Address	Component BSR Expiry Time (hh:mm:ss)	Component CRP Hold Time (hh:mm:ss)
1	3.1.1.2	00:00:20	00:00:20

La page **Component Summary** (Récapitulatif des composants) contient les champs suivants :

Component Index (Index du composant) : numéro unique identifiant l'index du composant.

Component BSR Address (Adresse BSR du composant) : adresse IP du routeur BSR de la région PIM locale.

Component BSR Expiry Time (hh:mm:ss) (Délai d'expiration BSR du composant [hh:mm:ss]) : délai minimal restant avant la déclaration du routeur BSR du domaine local.

Component CRP Hold Time (hh:mm:ss) (Temps d'attente CRP du composant [hh:mm:ss]) : temps d'attente du composant, lorsque celui-ci est un point de rendez-vous candidat dans le domaine local.

Affichage du récapitulatif des composants PIM-SM à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 PIM-SM Commands (Commandes PIM-SM)

Récapitulatif des RP définis

Utilisez la page **PIM-SM RP Set Summary** (Récapitulatif des RP PIM-SM définis) pour afficher les informations relatives aux points de rendez-vous statiques du routeur PIM-SM.

Pour afficher cette page, cliquez sur **IP Multicast** (Récapitulatif des interfaces PIM-SM) → **PIM-SM** → **RP Set Summary** (Récapitulatif des RP définis) dans l'arborescence.

Figure 13-31. Page PIM-SM RP Set Summary (Récapitulatif des RP PIM-SM définis)

Group Address	Group Mask	Address	Hold Time (hh:mm:ss)	Expiry Time (hh:mm:ss)	Component
224.0.0.0	240.0.0.0	3.1.1.2	00:01:40	00:02:30	1

La page **PIM-SM RP Set Summary** (Récapitulatif des RP PIM-SM définis) contient les champs suivants dans un tableau :

Group Address (Adresse du groupe) : adresse IP du groupe de multidiffusion.

Group Mask (Masque du groupe) : masque d'adresse du groupe de multidiffusion.

Address (Adresse) : adresse IP du RP candidat.

Hold Time (hh:mm:ss) (Temps d'attente [hh:mm:ss]) : temps d'attente d'un RP candidat. Si le routeur local n'est pas le BSR, la valeur 0 est indiquée.

Expiry Time (hh:mm:ss) (Délai d'expiration [hh:mm:ss]) : délai minimal restant avant que le RP candidat soit déclaré indisponible.

Component (Composant) : numéro qui identifie le composant de manière unique. Chaque instance de protocole connectée à un domaine séparé doit avoir une valeur d'index distincte.

Affichage du récapitulatif des RP définis à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

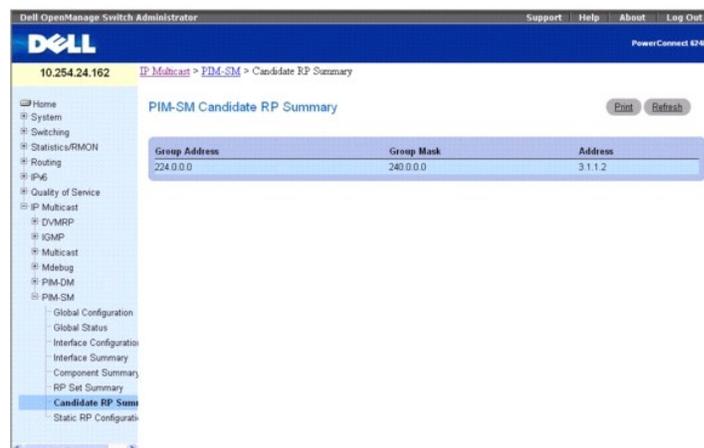
- 1 PIM-SM Commands (Commandes PIM-SM)

Récapitulatif des RP candidats

La page **PIM-SM Candidate RP Summary** (Récapitulatif des RP PIM-SM candidats) affiche les informations PIM relatives aux points de rendez-vous candidats pour chaque groupe de multidiffusion IP.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **PIM-SM** → **Candidate RP Summary** (Récapitulatif des RP candidats) dans l'arborescence.

Figure 13-32. Page **PIM-SM Candidate RP Summary** (Récapitulatif des RP PIM-SM candidats)



La page **PIM-SM Candidate RP Summary** (Récapitulatif des RP PIM-SM candidats) contient les champs suivants dans un tableau :

Group Address (Adresse de groupe) : adresse de groupe transmise dans les annonces des RP candidats.

Group Mask (Masque de groupe) : masque d'adresse de groupe transmis dans les annonces des RP candidats pour identifier totalement la portée du groupe pris en charge par le routeur, si celui-ci est élu comme point de rendez-vous.

Address (Adresse) : adresse de monodiffusion de l'interface annoncée comme RP candidat.

Affichage du récapitulatif des RP PIM-SM candidats à l'aide de la commande CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 PIM-SM Commands (Commandes PIM-SM)

Configuration des RP statiques

Utilisez la page **Static RP Configuration** (Configuration des RP statiques) pour créer l'adresse IP du RP statique spécifié pour le routeur PIM-SM.

Pour afficher cette page, cliquez sur **IP Multicast** (Multidiffusion IP) → **PIM-SM** → **Static RP Configuration** (Configuration des RP statiques) dans l'arborescence.

Figure 13-33. Page Static RP Configuration (Configuration d'un RP statique)



La page **Static RP Configuration** (Configuration d'un RP statique) contient les champs suivants :

IP Address (Adresse IP) : adresse IP du RP à créer.

Group (Groupe) : adresse de groupe du RP à créer.

Group Mask (Masque de groupe) : masque de groupe IP du RP à créer.

Les configurations existantes apparaissent dans un tableau, en bas de la page.

Configuration d'un RP statique

1. Affichez la page **Static RP Configuration** (Configuration d'un RP statique).
2. Entrez des valeurs dans les champs **IP Address** (Adresse IP), **Group** (Groupe) et **Group Mask** (Masque de groupe) pour configurer le RP statique.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse IP du RP statique spécifié pour le routeur PIM-SM est créée et le périphérique est mis à jour.

Configuration d'un RP statique à l'aide des commandes CLI

Pour plus d'informations sur la commande CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document *CLI Reference Guide* (Guide de référence CLI) :

- 1 PIM-SM Commands (Commandes PIM-SM)

[Retour au sommaire](#)

[Retour au sommaire](#)

Configuration du système Dell™ PowerConnect™

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Démarrage de l'interface de ligne de commande](#)
- [Informations générales sur la configuration](#)
- [Démarrage du commutateur](#)
- [Présentation de la configuration](#)
- [Configuration avancée](#)
- [Téléchargement de logiciels et réamorçage](#)
- [Fonctions du menu d'amorçage](#)
- [Exemple de processus de configuration](#)

Ce chapitre présente la configuration initiale du commutateur. Les thèmes abordés sont les suivants :

- 1 [Démarrage de l'interface de ligne de commande](#)
- 1 [Informations générales sur la configuration](#)
- 1 [Démarrage du commutateur](#)
- 1 [Présentation de la configuration](#)
- 1 [Configuration avancée](#)
- 1 [Téléchargement de logiciels et réamorçage](#)
- 1 [Fonctions du menu d'amorçage](#)
- 1 [Exemple de processus de configuration](#)

Une fois toutes les connexions externes mises en place, connectez un terminal au commutateur pour contrôler le démarrage et les autres procédures.

 **REMARQUE :** Si vous installez une *pile* de commutateurs, connectez le terminal au commutateur maître. Lorsqu'une pile est mise sous tension pour la première fois, l'un des commutateurs est désigné comme maître de la pile. Ce commutateur peut occuper n'importe quel emplacement. Ce commutateur est identifié par l'allumage du voyant Master Switch (Commutateur maître). Si vous le connectez à un autre commutateur, vous ne pourrez pas utiliser l'interface CLI.

Reportez-vous ensuite à la [Figure 5-1](#) pour connaître l'ordre d'installation et les procédures de configuration à suivre. Lors de la configuration initiale, procédez à la configuration standard du commutateur. L'exécution des autres fonctions est décrite ultérieurement dans cette section.

 **AVIS :** Avant de continuer, lisez les notes d'édition concernant ce produit. Vous pouvez les télécharger à partir du site support.dell.com.

Démarrage de l'interface de ligne de commande

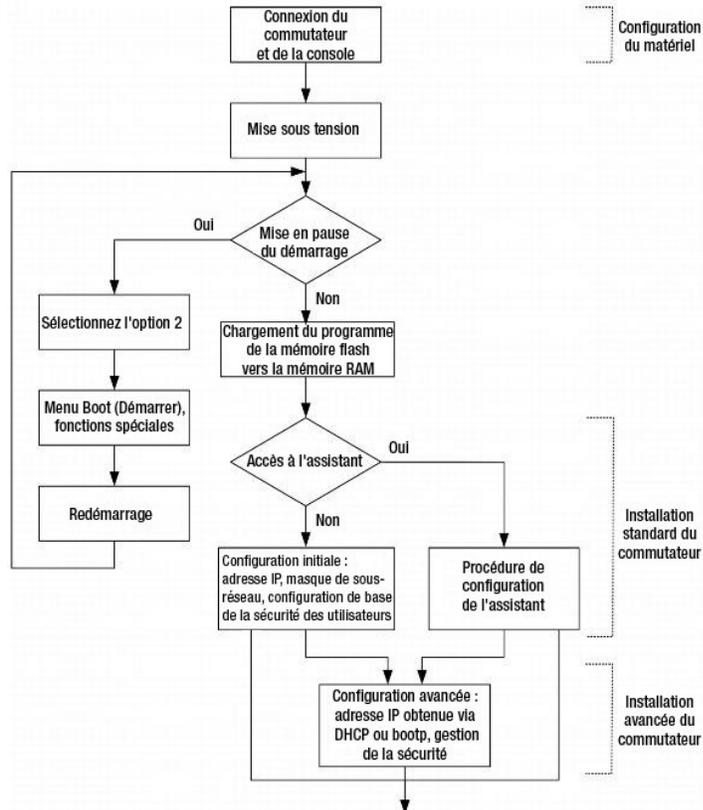
Exécutez la procédure ci-dessous pour démarrer l'interface de ligne de commande.

 **REMARQUE :** Ces opérations doivent être effectuées à partir de la console.

1. Démarrez le commutateur et attendez la fin de la procédure de démarrage. Le message d'accueil de l'utilitaire **Easy Setup Wizard** (Assistant d'installation) s'affiche.
2. Utilisez l'assistant **Easy Setup** pour configurer le commutateur et entrer les commandes permettant d'exécuter les opérations requises.
3. Lorsque vous avez terminé, refermez la session à l'aide de la commande **quit** ou **exit**.

Le commutateur (ou la pile) peut être géré par le biais d'une connexion directe avec le port de la console ou par l'intermédiaire d'une connexion Telnet. Si vous êtes connecté directement au commutateur, vous pouvez y accéder sans compte utilisateur. Toutefois, pour pouvoir accéder au commutateur via Telnet, vous devez définir au moins un compte utilisateur. En outre, pour que les commandes CLI puissent être utilisées en cas d'accès par le biais d'une connexion Telnet, une adresse IP doit être définie pour le commutateur, les autorisations de gestion appropriées doivent être accordées et une station de travail doit être connectée au commutateur.

Figure 5-1.



Organigramme des procédures d'installation et de configuration

Informations générales sur la configuration

Les commutateurs de la série 6200 sont fournis avec des fichiers binaires qui contiennent leur système d'exploitation et des fichiers de configuration ASCII qui définissent les relations entre les commutateurs et leur environnement réseau. La procédure de configuration consiste à modifier les fichiers ASCII de sorte que chaque commutateur soit configuré pour sa topologie de réseau.

Négociation automatique

La négociation automatique permet à un commutateur (ou une pile fonctionnant comme une unité unique) de négocier un mode de fonctionnement et de partager des informations avec un autre commutateur via une liaison point à point. Cette fonctionnalité configure automatiquement les deux commutateurs de manière à tirer le maximum de leurs capacités.

La négociation automatique est entièrement exécutée dans les couches physiques lors de l'initialisation des liens, sans aucune charge supplémentaire imposée aux couches de protocole MAC ou supérieures. La négociation automatique permet aux ports d'exécuter les fonctions suivantes :

- 1 Annonce des capacités
- 1 Accusé de réception et compréhension des modes de fonctionnement communs aux deux commutateurs
- 1 Refus d'utiliser des modes de fonctionnement qui ne sont pas partagés par les deux commutateurs
- 1 Configuration des deux ports sur le mode de fonctionnement commun le plus élevé pris en charge

REMARQUE : Dans la mesure du possible, utilisez la négociation automatique aux deux extrémités de la liaison afin d'éviter tout problème.

Si vous connectez un port du commutateur à la carte réseau (NIC) d'une station de travail ou d'un serveur qui ne prend pas en charge la négociation automatique ou qui n'est pas configuré pour celle-ci, plusieurs opérations supplémentaires sont nécessaires. Le port du commutateur et la carte réseau doivent être configurés manuellement sur la même vitesse et pour le mode duplex. Pour ce faire, vous pouvez utiliser l'interface du navigateur Web ou les commandes CLI.

AVIS : Si la station qui partage la liaison tente de négocier automatiquement avec un port qui a été configuré manuellement en duplex intégral, la négociation automatique aboutit à une tentative de fonctionnement de la station en mode semi-duplex. L'incompatibilité qui en résulte peut conduire à une perte de trame significative. Ce phénomène est inhérent aux normes utilisées par la négociation automatique.

Configuration de la connexion du terminal

Pour que le commutateur puisse être configuré, les paramètres de connexion du terminal suivants doivent être définis :

- | Aucune parité
- | Un bit d'arrêt
- | 8 bits de données
- | Pas de contrôle de flux

Débit

Les débits en bauds peuvent être modifiés manuellement de manière à correspondre aux valeurs suivantes :

- | 2400
- | 4800
- | 9 600 (débit par défaut)
- | 19200
- | 38400
- | 57600
- | 115200

Voici un exemple de configuration pour la modification du débit par défaut à l'aide des commandes CLI :

```
console#configure
console(config)#line console
console(config-line)#speed 115200
```

 **REMARQUE :** N'oubliez pas de définir le débit en bauds dans le logiciel d'émulation de terminal de votre station de travail de sorte qu'il corresponde à la vitesse du commutateur.

Autres conditions requises pour la configuration

Les éléments suivants sont requis pour le téléchargement du logiciel intégré et pour la configuration du commutateur :

- | Terminal ASCII (ou émulation) connecté au port série (câble croisé) situé à l'arrière de l'unité
- | Adresse IP attribuée au commutateur pour le contrôle distant de celui-ci via Telnet, SSH, etc.

Démarrage du commutateur

Lorsque le système est mis sous tension et que le terminal local est déjà connecté, le commutateur effectue un POST (autotest à la mise sous tension). Ce test s'exécute à chaque initialisation du commutateur ; il passe les composants en revue pour vérifier que l'unité est opérationnelle avant que le démarrage ne soit totalement effectif.

Si un problème critique est détecté, l'exécution du programme s'arrête. Si l'autotest à la mise sous tension se déroule sans incident, une image exécutable valide est chargée dans la mémoire vive.

Les messages de l'autotest à la mise sous tension sont affichés sur le terminal et indiquent le succès ou l'échec du test.

Pour démarrer le commutateur, procédez comme suit :

1. Vérifiez que le câble série est connecté au terminal.
2. Connectez le bloc d'alimentation au commutateur.
3. Démarrez le commutateur.

Lors du démarrage, le test commence par calculer la mémoire disponible du commutateur, puis le démarrage se poursuit.

4. Au cours du démarrage, vous pouvez utiliser le menu **Boot** (Amorçage) pour exécuter des procédures spéciales, s'il y a lieu. Pour accéder au menu **Boot** (amorçage), appuyez sur 2 dans les 10 secondes suivant l'affichage du message suivant :

```
Select an option. If no selection in 10 seconds then
operational code will start.
```

1 - Start operational code.

2 - Start Boot Menu.

Select (1, 2):2

Pour plus d'informations sur le menu **Boot** (Amorçage), voir [Fonctions du menu d'amorçage](#). L'exemple suivant présente l'intégralité des informations qui s'affichent lors de l'auto-test de démarrage (POST) :

```
CPU Card ID: 0x508541

volume descriptor ptr (pVolDesc): 0xffefd00

cache block I/O descriptor ptr (cbio): 0xffefde0

auto disk check on mount: NOT ENABLED

max # of simultaneously open files: 22

file descriptors in use: 0

# of different files in use: 0

# of descriptors for deleted files: 0

# of obsolete descriptors: 0

current volume configuration:

- volume label: NO LABEL ; (in boot sector: )

- volume Id: 0x0

- total number of sectors: 60,716

- bytes per sector: 512

- # of sectors per cluster: 4

- # of reserved sectors: 1

- FAT entry size: FAT16

- # of sectors per FAT copy: 60

- # of FAT table copies: 2

- # of hidden sectors: 4

- first cluster is in sector # 136

- Update last access date for open-read-close = FALSE

- directory structure: VFAT

- root dir start sector: 121

- # of sectors per root: 15

- max # of entries in root: 240

FAT handler information:

-----

- allocation group size: 2 clusters

- free space on volume: 15,335,424 bytes

Boot Menu Version: 22 Dec 2006

Select an option. If no selection in 10 seconds then

operational code will start.

1 - Start operational code.

2 - Start Boot Menu.

Select (1, 2):2

Boot Menu Version: 22 Dec 2006
```

```
Options available

1 - Start operational code

2 - Change baud rate

3 - Retrieve event log using XMODEM

4 - Load new operational code using XMODEM

5 - Display operational code vital product data

6 - Run flash diagnostics

7 - Update boot code

8 - Delete backup image

9 - Reset the system

10 - Restore configuration to factory defaults (delete config files)

11 - Activate Backup Image

12 - Password Recovery Procedure

[Boot Menu]
```

Le processus de démarrage dure environ 60 secondes.

Le message d'amorçage automatique qui apparaît à la fin du POST (voir les dernières lignes ci-dessus) indique qu'aucun problème n'a été rencontré. Pour revenir au code opérationnel à partir de l'invite [Boot Menu] ([Menu Démarrer]), appuyez sur 1.

 **REMARQUE :** Les lignes suivantes présentent un exemple de configuration. Les éléments tels que les adresses, les versions et les dates peuvent être différents pour chaque commutateur.

Operational Code Date: Fri May 4 07:44:08 2007

Uncompressing....

50% 100%

|||||

Attaching interface lo0...done

Adding 36263 symbols for standalone.

volume descriptor ptr (pVolDesc): 0xffc0650

cache block I/O descriptor ptr (cbio): 0xffc0730

auto disk check on mount: NOT ENABLED

max # of simultaneously open files: 22

file descriptors in use: 0

of different files in use: 0

of descriptors for deleted files: 0

of obsolete descriptors: 0

current volume configuration:

- volume label: NO LABEL ; (in boot sector:)

- volume Id: 0x0

- total number of sectors: 60,716

- bytes per sector: 512

- # of sectors per cluster: 4

- # of reserved sectors: 1

- FAT entry size: FAT16

- # of sectors per FAT copy: 60

- # of FAT table copies: 2

```

- # of hidden sectors: 4
- first cluster is in sector # 136
- Update last access date for open-read-close = FALSE
- directory structure: VFAT
- root dir start sector: 121
- # of sectors per root: 15
- max # of entries in root: 240

FAT handler information:
-----

- allocation group size: 2 clusters
- free space on volume: 15,337,472 bytes

Timebase: 66.666666 MHz, MEM: 266.666664 MHz, PCI: 66.666666 MHz, CPU: 533.33332
8 MHz

SOC unit 0 attached to PCI device BCM56314_A0
SOC unit 1 attached to PCI device BCM56314_A0
Adding BCM transport pointers
Configuring CPUTRANS TX
Configuring CPUTRANS RX

hpc - No stack ports. Starting in stand-alone mode.

(Unit 1 - Waiting to select management unit)>

<188> JAN 01 00:00:08 0.0.0.0-1 POE[254746256]: broad_poe.c(286) 4 % Unable to set POE Power bank 73

Applying configuration, please wait ...

No Potential unit to configure as Standby when unit 1 joined

<187> JAN 01 00:00:13 192.168.2.1-1 UNITMGR[244207968]: unitmgr.c(4490) 15 % No

Potential unit to configure as Standby when unit 1 joined

....

console>

```

Une fois le démarrage effectué avec succès, une invite s'affiche ; vous pouvez utiliser le terminal local pour commencer à configurer le commutateur. Toutefois, avant de configurer le commutateur, assurez-vous que celui-ci est équipé de la toute dernière version du logiciel. Si tel n'est pas le cas, téléchargez et installez la dernière version du logiciel. Voir [Téléchargement de logiciels et réamorçage](#).

Présentation de la configuration

Avant de configurer le commutateur, demandez les informations suivantes à l'administrateur réseau :

- 1 Masque de sous-réseau IP
- 1 Adresse IP de la passerelle par défaut (routeur suivant) permettant de configurer l'itinéraire par défaut

Il existe deux types de configuration :

- 1 *Initiale* : fonctions de base en matière de configuration et de sécurité.
- 1 *Avancée* : configuration de l'adresse IP dynamique et mise en place de fonctions de sécurité plus évoluées.

 **AVIS** : Une fois la configuration modifiée, elle doit être enregistrée avant le redémarrage. Pour enregistrer la configuration, entrez :

```
console#copy running-config startup-config
```

Assistant Easy Setup

L'assistant **Easy Setup** s'affiche lorsque seule la configuration définie en usine est détectée au démarrage du système, ou lorsque ce dernier n'est pas configuré. Cet assistant est conçu pour vous aider à effectuer certaines étapes initiales de configuration et d'activation des fonctions de sécurité afin de faire

en sorte que le commutateur puisse être géré. Il exige que le compte administrateur initial soit configuré lors de la mise sous tension du commutateur. Le compte administrateur défini par l'assistant dispose du plus haut niveau de privilège (niveau 15).

L'assistant **Easy Setup** vous guide lors de la configuration initiale d'un commutateur récemment installé, de sorte que celui-ci puisse être immédiatement déployé, fonctionnel et totalement gérable via le Web, l'interface de ligne de commande et Dell Network Manager. Une fois la configuration initiale effectuée, vous pouvez accéder au système pour définir des paramètres de configuration avancés.

Par défaut, le commutateur est réglé à la livraison sur l'adresse IP 192.168.2.1 et le masque de sous-réseau 255.255.255.0. Le système est paramétré sur l'ID VLAN de gestion par défaut (1). La mise sous tension initiale doit être effectuée à partir de l'interface série car, sans adresse IP, les autres interfaces de gestion ne sont pas accessibles.

L'assistant effectue les opérations de configuration suivantes sur le commutateur :

- 1 Il met en place le compte utilisateur privilégié initial et le mot de passe correspondant. Cette opération est effectuée pendant la configuration. Ce compte est doté du niveau de privilège le plus élevé (niveau 15).
- 1 Il permet l'ouverture de session via l'interface CLI et l'accès HTTP/HTTPS (paramètre d'authentification local uniquement). Vous pourrez revenir en arrière ultérieurement pour configurer RADIUS ou TACACS+.
- 1 Il permet de définir l'adresse IP pour le VLAN de gestion.
- 1 Il définit la chaîne de communauté SNMP qui doit être utilisée par le gestionnaire SNMP sur une adresse IP donnée. Vous pouvez ignorer cette étape si le commutateur n'est pas géré via SNMP. S'il est configuré, le niveau d'accès par défaut est défini sur l'accès maximum disponible pour l'interface de gestion SNMP. Initialement, seul SNMPv1/2c est activé. SNMPv3 est désactivé jusqu'à ce que vous l'activiez de manière explicite en paramétrant l'ID du moteur, la vue, etc. La chaîne de communauté SNMP peut comporter des espaces. Dans l'assistant, si vous souhaitez insérer des espaces dans la chaîne de communauté, vous devez les placer entre guillemets. Bien qu'autorisée, l'utilisation d'espaces dans la chaîne de communauté est déconseillée. La chaîne de communauté par défaut ne contient pas d'espaces.
- 1 Il permet d'indiquer l'IP du serveur de gestion ou d'autoriser l'accès SNMP à partir de toutes les adresses IP.
- 1 Il définit l'adresse IP de la passerelle par défaut.

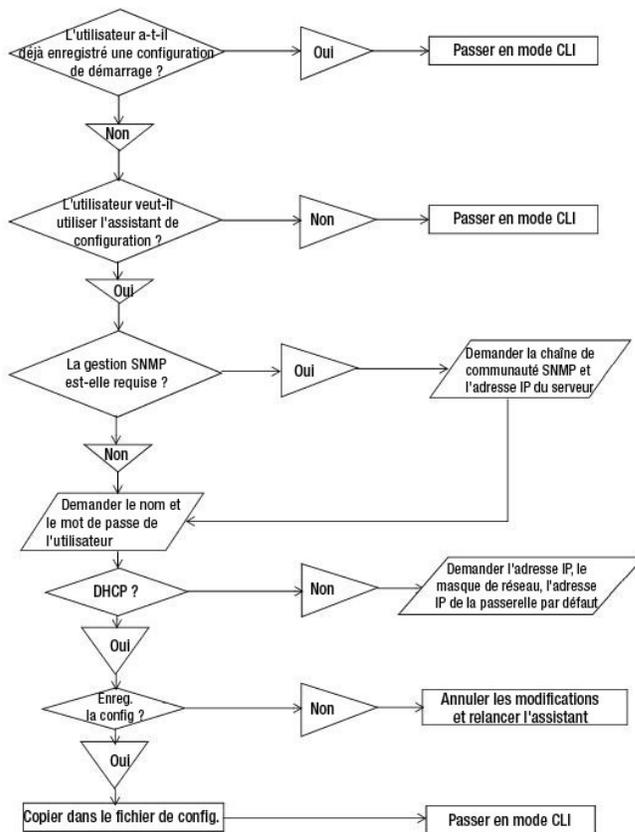
Si vous n'utilisez pas l'assistant dès le départ, la session s'ouvre en mode CLI par défaut. L'assistant de configuration s'affiche à chaque fois que vous vous connectez, jusqu'à ce que vous enregistriez une configuration. Dès lors, l'option de lancement de l'assistant ne s'affiche à nouveau que si vous rétablissez les paramètres d'usine sur le commutateur.

Le commutateur pouvant être mis sous tension sans connexion série, un commutateur non configuré attend pendant 60 secondes que vous répondiez à une invite de configuration. Passé ce délai, le commutateur se met à fonctionner normalement avec la configuration définie en usine. Lors du démarrage suivant, vous aurez de nouveau la possibilité d'exécuter l'assistant de configuration.

Organigramme fonctionnel

L'organigramme ci-dessous illustre les procédures de l'assistant **Easy Setup**.

Figure 5-2. Organigramme de l'assistant d'installation



Exemple de session de l'assistant Easy Setup

Cette section illustre une session de l'assistant **Easy Setup**. Pour une description plus générale, reportez-vous à l'organigramme présenté dans la section précédente. Les valeurs utilisées dans l'exemple ci-dessous sont fournies à titre d'exemple. Demandez à votre administrateur réseau de vous communiquer les valeurs réelles.

- 1 Adresse IP du VLAN de gestion : 192.168.1.1:255.255.255.0.
- 1 Nom d'utilisateur : *admin*, mot de passe : *admin123*.
- 1 Adresse IP du système de gestion du réseau : 192.168.1.10.
- 1 Passerelle par défaut : 192.168.1.100.
- 1 Chaîne de communauté SNMP à utiliser : *Dell_Network_Manager*.

L'assistant définit les valeurs initiales comme indiqué ci-dessus. Une fois son exécution terminée, le système est configuré de la façon suivante :

- 1 SNMPv1/2c est activé et la chaîne de communauté est définie comme indiqué ci-dessus. SNMPv3 est désactivé.
- 1 Le compte utilisateur *admin* est configuré comme indiqué ci-dessus.
- 1 Un système de gestion du réseau est configuré. À partir de cette station de gestion, vous pouvez accéder aux interfaces SNMP, HTTP et CLI. Vous pouvez également décider d'autoriser toutes les adresses IP à accéder à ces interfaces de gestion en sélectionnant l'adresse IP 0.0.0.0.
- 1 Une adresse IP est configurée pour le VLAN de gestion par défaut (1).
- 1 Une adresse de passerelle par défaut est configurée.

REMARQUE : Dans l'exemple ci-après, les options que l'utilisateur peut sélectionner sont présentées entre crochets, []. Les valeurs par défaut sont présentées entre accolades { }. Si vous appuyez sur <Entrée> sans avoir défini les options, la valeur par défaut est prise en compte. Le texte de l'aide est entre parenthèses.

L'exemple suivant montre une suite d'invites et de réponses affichées dans l'assistant Dell **Easy Setup**. Les valeurs utilisées sont indiquées ci-dessus.

Welcome to Dell Easy Setup Wizard

The setup wizard guides you through the initial switch configuration, and gets you up and running as quickly as possible. You can skip the setup wizard, and enter CLI mode to manually configure the switch. You must respond to the next question to run the setup wizard within 60 seconds, otherwise the system will continue with normal operation using the default system configuration. Note: You can exit the setup wizard at any point by entering [ctrl+z].

Would you like to run the set up wizard (you must answer this question within 60 seconds)? [Y/N] **y**

Step 1:

The system is not set up for SNMP management by default. To manage the switch using SNMP (required for Dell Network Manager) you can:

- o Set up the initial SNMP version 2 account now.
- o Return later and set up other SNMP accounts. (For more information on setting up an SNMP version 1 or 3 account, see the user documentation).

Would you like to set up the SNMP management interface now? [Y/N] **y**

To set up the SNMP management account you must specify the management system IP address and the "community string" or password that the particular management system uses to access the switch. The wizard automatically assigns the highest access level [Privilege Level 15] to this account. You can use Dell Network Manager or other management interfaces to change this setting and to add additional management system later. For more information on adding management systems, see the user documentation.

To add a management station:

Please enter the SNMP community string to be used {public}:

>> **Dell_Network_Manager**<Entrée>

Please enter the IP address of the Management System (A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station {0.0.0.0}:

>> **192.168.1.10**<Entrée>

Step 2:

Now we need to set up your initial privilege (Level 15) user account. This account is used to login to the CLI and Web interface. You may set up other accounts and change privilege levels later. For more information on setting up user accounts and changing privilege levels, see the user documentation.

To set up a user account:

Please enter the user name {admin}: **admin**<Entrée>

Please enter the user password: *********<Entrée>

Please reenter the user password: *********<Entrée>

 **REMARQUE :** Si les mots de passe entrés dans les deux champs ne sont pas identiques, un message invite l'utilisateur à recommencer.

Step 3:

Next, an IP address is set up. The IP address is defined on the default VLAN (VLAN #1), of which all ports are members. This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch. Optionally you may request that the system automatically retrieve an IP address from the network via DHCP (this requires that you have a DHCP server running on the network).

To set up an IP address:

Please enter the IP address of the device (A.B.C.D) or enter "DHCP" (without the quotes) to automatically request an IP address from the network DHCP server (192.168.2.1):

>> **192.168.2.1**<Entrée>

Please enter the IP subnet mask (A.B.C.D or /nn){255.255.255.0}:

>> **255.255.255.0**<Entrée>

 **REMARQUE :** Si vous avez sélectionné DHCP ci-dessus, le système ne vous demande pas de masque de sous-réseau IP car cette information est fournie par le serveur DHCP.

Step 4:

Finally, set up the default gateway. Please enter the IP address of the gateway from which this network is reachable (for example 0.0.0.0): >> **192.168.2.100**<Entrée>

 **REMARQUE :** Si vous avez sélectionné DHCP ci-dessus, le système ne vous demande pas de passerelle par défaut car cette information est fournie par le serveur DHCP.

This is the configuration information that has been collected:

SNMP Interface = "Dell_Network_Manager"@192.168.1.10

User Account set up = admin

Password = *****

Management IP address = 192.168.2.1 255.255.255.0

Default Gateway = 192.168.2.100

Step 5:

If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file. If the information is incorrect, select (N) to discard configuration and restart the wizard: [Y/N] **y**

Thank you for using Dell Easy Set up Wizard. You will now enter CLI mode.

Configuration avancée

Généralités sur l'interface de ligne de commande

En modes User EXEC (EXEC utilisateur) et Privileged EXEC (EXEC privilégié), la commande help affiche les raccourcis clavier disponibles. L'exemple suivant illustre l'affichage du résultat de la commande help :

```
Console>help

HELP:

Special keys:

DEL, BS .... delete previous character

Ctrl-A .... go to beginning of line

Ctrl-E .... go to end of line

Ctrl-F .... go forward one character

Ctrl-B .... go backward one character

Ctrl-D .... delete current character

Ctrl-U, X .. delete to beginning of line

Ctrl-K .... delete to end of line

Ctrl-W .... delete previous word

Ctrl-T .... transpose previous character

Ctrl-P .... go to previous line in history buffer

Ctrl-R .... rewrites or pastes the line

Ctrl-N .... go to next line in history buffer

Ctrl-Y .... print last deleted character

Ctrl-Z .... return to root command prompt

Ctrl-Q .... enables serial flow

Ctrl-S .... disables serial flow

Tab, <SPACE> command-line completion

Exit .... go to next lower command prompt

? .... list choices
```

Aide contextuelle

Utilisez la commande ? pour obtenir une aide contextuelle lors de l'utilisation de l'interface de ligne de commande. Cette commande permet d'afficher la liste des sous-commandes disponibles ou les commandes commençant par une chaîne de caractères indiquée. Entrée sur une ligne vide, la commande ? affiche la liste des commandes associées à ce niveau de l'arborescence de commandes. Le signe ? peut également être intégré à une commande ; la liste des paramètres requis pour cette commande s'affiche alors. Les paramètres déjà indiqués par l'utilisateur ne figurent pas dans la liste ; seuls les paramètres manquants sont répertoriés.

Convention de dénomination des interfaces

Dans une implémentation CLI conforme aux normes de l'industrie, il existe une convention approuvée pour nommer les interfaces. La convention de dénomination des interfaces sur les unités Dell est la suivante :

- 1 **N° d'unité/ID d'interface** : chaque interface est identifiée par un *N° d'unité* suivi du symbole /, suivi de l'*ID d'interface* (voir ci-dessous). Par

exemple, **2/g10** identifie le port gigabit 10 de la deuxième unité d'une pile.

- 1 **N° d'unité** : le numéro d'unité est utilisé uniquement dans le cadre d'une solution dans laquelle plusieurs commutateurs sont empilés pour former une unité virtuelle. Dans ce cas, le *numéro d'unité* est l'identificateur de l'unité physique dans la pile.
- 1 **ID d'interface** : il est constitué du type d'interface suivi du numéro d'interface. Il existe actuellement une liste prédéfinie de *types d'interface* (voir ci-dessous). Si vous devez en définir d'autres, vous devez les faire homologuer auprès de Dell. Par exemple, **2/g10** identifie le port gigabit 10 de la deuxième unité.
- 1 **Types d'interface** : les types d'interface suivants sont définis dans les commutateurs de la série 6200 :
 - o **g** : port Ethernet gigabit (par exemple, **1/g2** représente le port Ethernet gigabit 2).
 - o **xg** : port Ethernet 10 gigabits (par exemple, **1/xg2** représente le port Ethernet 10 gigabits 2).

Guide de référence CLI pour les systèmes PowerConnect 6200

Pour obtenir des informations détaillées sur les commandes CLI disponibles pour les commutateurs de la série 6200, consultez le document *CLI Reference Guide* (Guide de référence CLI).

Cette section présente des informations récapitulatives sur des tâches courantes telles que les suivantes :

- 1 [Modification des paramètres par défaut du port de commutation](#)
- 1 [Obtention d'une adresse IP à partir d'un serveur DHCP](#)
- 1 [Configuration d'un mot de passe de console initial](#)
- 1 [Configuration d'un mot de passe Telnet initial](#)
- 1 [Configuration d'un mot de passe HTTP initial](#)
- 1 [Configuration d'un mot de passe HTTPS initial](#)

Modification des paramètres par défaut du port de commutation

Lors de la configuration/réception d'adresses IP via DHCP et BOOTP, la configuration reçue de la part de ces serveurs inclut l'adresse IP et éventuellement le masque de sous-réseau et la passerelle par défaut.

Lors de la première connexion, l'interface de ligne de commande accède à la racine de la hiérarchie de commandes. Pour changer de niveau, utilisez des commandes telles que **configure** ; l'interface de ligne de commande accède alors à la sous-arborescence *config*. Pour revenir au niveau précédent dans la hiérarchie, utilisez la commande **exit**.

```
SwitchA#configure
SwitchA(config)#exit
SwitchA#
```

Les exemples suivants illustrent les invites système utilisées par les commutateurs de la série 6200 :

- 1 **SwitchA >** : indique que le nom de l'unité est *SwitchA* et que l'interface de ligne de commande se trouve actuellement au niveau supérieur de la hiérarchie de commandes. Elle se trouve également en mode *User EXEC* (EXEC utilisateur).
- 1 **SwitchA#** : le signe # indique que l'interface de ligne de commande se trouve en mode Privileged EXEC (EXEC privilégié) et non User EXEC (EXEC utilisateur).
- 1 **SwitchA(config)#** : indique que l'interface de ligne de commande se trouve en mode *configuration globale* dans la hiérarchie de commandes. Pour accéder à ce mode, entrez **configure** à partir du niveau supérieur.
- 1 **SwitchA(config-if)#** : cette invite indique que l'interface de ligne de commande se trouve actuellement en mode de configuration *interface*. Pour accéder à ce mode, entrez **interface range ethernet**, **interface range port-channel** ou **interface range vlan** à partir du mode *config*. Dans ce cas, aucune interface spécifique n'est référencée ; le système utilise un ensemble générique d'interfaces.
- 1 **SwitchA(config-if-1/g1)#** : indique que l'interface de ligne de commande fonctionne actuellement sur l'interface Ethernet gigabit 1.

Paramètres par défaut des ports de commutation

Le tableau ci-dessous décrit les paramètres par défaut des ports de commutation.

Table 5-1. Paramètres par défaut des ports

Fonction	Paramètre par défaut
Vitesse et mode du port	1000 Mbps, négociation automatique
État de transfert du port	Activé
Prévention des blocages en tête de ligne	Activé
Contrôle de flux	Éteint
Contre-pression	Éteint

Voici un exemple de modification de la vitesse du port sur le port 1/ g1 l'aide des commandes CLI :

```
console(config)#interface ethernet 1/g1
console(config-if-1/g1)#speed 100
```

Obtention d'une adresse IP à partir d'un serveur DHCP

Lorsque le protocole DHCP est utilisé pour obtenir une adresse IP, le commutateur agit en tant que client DHCP.

Pour obtenir une adresse IP à partir d'un serveur DHCP, procédez comme suit :

Sélectionnez et connectez n'importe quel port à un serveur DHCP ou à un sous-réseau possédant un serveur DHCP, de manière à obtenir l'adresse IP.

 **REMARQUE :** Il n'est pas nécessaire de supprimer la configuration du commutateur pour obtenir une adresse IP du serveur DHCP.

1. Entrez les commandes ci-dessous pour utiliser le port sélectionné pour la réception de l'adresse IP.

1 Attribution d'adresses IP dynamiques :

```
console#config
console(config)#ip address dhcp
```

L'interface reçoit automatiquement l'adresse IP.

2. Pour vérifier l'adresse IP, entrez la commande `show ip interface` à l'invite du système, comme indiqué dans l'exemple suivant.

```
console#show ip interface
Management Interface:
IP Address..... 10.240.4.125
Subnet Mask..... 255.255.255.0
Default Gateway..... 10.240.4.1
Burned In MAC Address..... 00:10:18:82:04:35
Network Configuration Protocol Current..... DHCP
Management VLAN ID..... 1
Routing Interfaces:
Netdir Multi
Interface IP Address IP Mask Bcast CastFwd
-----
vlan1      192.168.10.10 255.255.255.0 Disable Disable
vlan2      0.0.0.0 0.0.0.0 Enable Disable
loopback2 0.0.0.0 0.0.0.0 Disable Disable
```

Gestion de la sécurité et configuration du mot de passe

La sécurité du système est contrôlée via le mécanisme AAA (Authentication, Authorization, Accounting) qui gère les droits d'accès des utilisateurs, les privilèges et les méthodes de gestion. AAA fait appel à des bases de données utilisateur à la fois locales et distantes. Le cryptage des données est traité via le mécanisme SSH.

Le système est livré sans mot de passe par défaut. Les mots de passe sont tous définis par l'utilisateur. Si un mot de passe défini par l'utilisateur est perdu, une procédure de récupération du mot de passe peut être lancée à partir du menu **Boot** (Amorçage). Cette procédure est applicable uniquement sur le terminal local et permet d'accéder une seule fois au commutateur sans saisir de mot de passe.

Configuration de mots de passe de sécurité

Vous pouvez configurer des mots de passe de sécurité pour les services suivants :

```
1 Console
1 Telnet
1 SSH
```

- 1 HTTP
- 1 HTTPS

 **REMARQUE :** Lors de la création d'un nom d'utilisateur, la priorité par défaut est 1, ce qui signifie que l'utilisateur peut accéder au système mais pas aux fonctions de configuration. L'accès à la configuration n'est possible que si le niveau de priorité 15 a été défini.

Configuration d'un mot de passe de console initial

Pour configurer un mot de passe de console initial, entrez les commandes suivantes :

```
console(config)#aaa authentication login default line
console(config)#aaa authentication enable default line
console(config)#line console
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password secret123
```

- 1 Lorsque vous vous connectez pour la première fois à un commutateur à partir d'une session de console, entrez `secret123` à l'invite du mot de passe.
- 1 Lorsque vous activez le mode "enable" sur le commutateur, tapez `secret123` à l'invite du mot de passe.

Configuration d'un mot de passe Telnet initial

Pour configurer un mot de passe Telnet initial, entrez les commandes suivantes :

```
console(config)#aaa authentication login default line
console(config)#aaa authentication enable default line
console(config)#line telnet
console(config-line)#login authentication default
console(config-line)#enable authentication default
console(config-line)#password pass1234
```

- 1 Lorsque vous vous connectez à un commutateur pour la première fois via une session Telnet, tapez `pass1234` à l'invite du mot de passe.
- 1 Lorsque vous activez le mode "enable" sur le commutateur, tapez `pass1234` à l'invite du mot de passe.

Configuration d'un mot de passe HTTP initial

Pour configurer un mot de passe HTTP initial, entrez les commandes suivantes :

```
console(config)#ip http authentication local
console(config)#username admin password user1234 level 15
```

Configuration d'un mot de passe HTTPS initial

Pour configurer un mot de passe HTTPS initial, entrez les commandes suivantes :

```
console(config)#ip https authentication local
```

 **REMARQUE :** Vous devez générer un nouveau certificat de cryptographie à chaque fois que vous mettez à niveau le logiciel de contrôle du commutateur.

Entrez les commandes ci-dessous une fois lorsque vous configurez l'utilisation d'une session HTTPS via une console, Telnet ou SSH.

 **REMARQUE :** Dans le navigateur Web, activez SSL version 2.0 ou suivante pour afficher le contenu de la page.

```
console(config)#crypto certificate 1 generate
console(config)#ip https server
```

 **REMARQUE :** Les services http et https nécessitent un privilège de niveau 15 et permettent un accès direct aux fonctions de configuration.

Téléchargement de logiciels et réamorçage

Téléchargement de logiciels via XModem

Cette section présente des instructions permettant de télécharger les logiciels du commutateur (images système et de démarrage) à l'aide de XModem, protocole de transfert de données utilisé pour la mise à jour des fichiers de configuration de sauvegarde.

 **REMARQUE :** Pour effectuer cette opération, vous devez être connecté à l'interface de console série, qui est la seule à permettre le téléchargement via XModem.

Pour télécharger un fichier image de logiciel à l'aide de XModem :

Indiquez le chemin d'accès du fichier source pour lancer le processus de transfert.

L'exemple suivant illustre les informations qui s'affichent :

```
console#copy xmodem image

Mode..... XMODEM

Data Type..... Code

Destination Filename..... image2

Management access will be blocked for the duration of the transfer

Are you sure you want to start? (y/n) y

console#boot system image2
```

Téléchargement des logiciels via le serveur TFTP

Cette section indique comment télécharger l'image système et l'image d'amorçage du commutateur via un serveur TFTP. Le serveur TFTP doit être disponible sur le réseau pour que vous puissiez lancer le téléchargement.

Le commutateur démarre en décompressant l'image système stockée dans la zone de mémoire flash.

 **AVIS :** Vous devez exécuter la commande `boot system` pour activer l'image que vous venez de télécharger.

Au démarrage suivant, le commutateur décompresse l'image système en cours et l'exécute, sauf si l'utilisateur a configuré les paramètres de démarrage différemment.

Pour télécharger une image via le serveur TFTP :

1. Assurez-vous qu'une adresse IP est configurée sur l'un des ports du commutateur et que des requêtes ping peuvent être envoyées au serveur TFTP.
2. Assurez-vous que le fichier à télécharger (.stk) est enregistré sur le serveur TFTP.
3. Entrez la commande `show version` pour vérifier quelle version du logiciel est actuellement exécutée sur le commutateur.

L'exemple suivant illustre les informations qui s'affichent :

```
console>show version

Image Descriptions

image1 : default image

image2 :

Images currently available on Flash

-----

unit image1  image2  current-active next-active

-----

1  0.15.0.0  0.15.0.0  image1      image1
```

4. Entrez la commande `show bootvar` pour vérifier l'image système en cours. L'exemple suivant illustre les informations qui s'affichent :

```
console>show bootvar
```

```

Image Descriptions
image1 : default image
image2 :

Images currently available on Flash

-----
unit image1  image2  current-active  next-active
-----
1  0.15.0.0  0.15.0.0  image1          image1

```

- Entrez la commande **copy tftp://{adresse tftp}/{nom du fichier} image2** pour copier une nouvelle image système sur le commutateur.

Une fois la nouvelle image téléchargée, elle est enregistrée dans une zone allouée à cet effet (image2 dans l'exemple). L'exemple suivant illustre les informations qui s'affichent :

```

console#copy tftp://10.254.24.64/pc62xxr0v34.stk image2
Mode..... TFTP
Set TFTP Server IP..... 10.254.24.64
TFTP Path..... ./
TFTP Filename..... pc62xxr0v34.stk
Data Type..... Code
Destination Filename..... image2

Management access will be blocked for the duration of the transfer

Are you sure you want to start? (y/n) y

```

Les points d'exclamation indiquent qu'une copie est en cours. Un point indique un dépassement du délai autorisé pour la copie. Plusieurs points successifs indiquent que la copie a échoué.

- Sélectionnez l'image à utiliser pour l'amorçage suivant en entrant la commande **boot system**. Entrez ensuite la commande **show bootvar** pour vérifier que la copie indiquée comme paramètre de la commande **boot system** est sélectionnée pour le démarrage suivant.

L'exemple suivant illustre les informations qui s'affichent :

```

console#boot system image2
Activating image image2 ..

console>show bootvar

Image Descriptions
image1 : default image
image2 :

Images currently available on Flash

-----
unit  image1  image2  current-active  next-active
-----
1  0.15.0.0  0.15.0.0  image1          image2

```

Si l'image à utiliser pour le démarrage suivant n'est pas précisée avec la commande **boot system**, le système charge l'image en cours au prochain démarrage (image1 dans l'exemple ci-dessus).

- Entrez la commande **reload**. Le message suivant s'affiche :

```

console#reload

Management switch has unsaved changes.

Are you sure you want to continue? (y/n)

```

- Entrez **y**. Le message suivant s'affiche alors :

```
Configuration Not Saved!  
  
Are you sure you want to reload the stack? (y/n)
```

- Entrez **y** pour redémarrer le commutateur.

Mise à jour du code de démarrage

Utilisez la commande **update bootcode** pour mettre à jour le code de démarrage sur tous les commutateurs. Pour chaque commutateur, le code de démarrage est extrait de l'image en cours et programmé en mémoire flash. Pour mettre à jour le code de démarrage pour un commutateur, spécifiez l'unité dans la commande (voir l'exemple ci-dessous).

Pour afficher le code de démarrage d'un commutateur, redémarrez celui-ci. Les dates de build s'affichent au cours du démarrage.

- Entrez la commande suivante, où 2 correspond au numéro de l'unité :

```
console# update bootcode 2  
  
Updating boot code ...  
  
Boot code update completed successfully.
```

- Entrez la commande **reload**.

```
console#reload  
  
Are you sure you want to reload the stack? (y/n)
```

- Entrez **y** pour redémarrer le commutateur.

Fonctions du menu d'amorçage

Vous pouvez effectuer de nombreuses tâches de configuration à partir du menu **Boot** (Amorçage), qui peut être affiché à la fin de la première partie du POST (auto-test de démarrage).

Pour afficher le menu **Boot** (Amorçage) :

- Au cours du processus de démarrage, appuyez sur **2** dans les 10 secondes qui suivent l'affichage du message suivant :

```
Boot Menu Version: Oct 20 2004  
  
Select an option. If no selection in 10 seconds then  
operational code will start.  
  
1 - Start operational code.  
2 - Start Boot Menu.  
  
Select (1, 2):
```

Le menu **Boot** (Amorçage) s'affiche. Il contient les fonctions de configuration suivantes :

```
1 - Start operational code  
2 - Change baud rate  
3 - Retrieve event log using XMODEM  
4 - Load new operational code using XMODEM  
5 - Display operational code vital product data  
6 - Run flash diagnostics  
7 - Update boot code  
8 - Delete backup image  
9 - Reset the system  
10 - Restore configuration to factory defaults (delete config files)
```

- 11 - Activate Backup Image
- 12 - Password Recovery Procedure

Les sections qui suivent décrivent les options du menu **Boot** (Amorçage).

Démarrage du code opérationnel

Utilisez l'option 1 pour reprendre le chargement du code opérationnel.

Pour relancer le processus de démarrage à partir du menu **Boot** (Amorçage) :

1. Dans le menu **Boot** (Amorçage), sélectionnez 1 et appuyez sur <Entrée>.

L'invite suivante s'affiche :

```
Operational Code Date: Thu Jun 8 12:51:44 2006
Uncompressing....
50% 100%
|||||
1 File: bootos.c Line: 462 Task: fffffe00 EC: 2863311530 (0xaaaaaaaa)
(0 d 0 hrs 0 min 13 sec)
Timebase: 24.750275 MHz, MEM: 99.001100 MHz, PCI: 33.000366 MHz, CPU: 198.002200 MHz
PCI device BCM5675_A0 attached as unit 0.
PCI device BCM5695_B0 attached as unit 1.
PCI device BCM5695_B0 attached as unit 2.
PCI device BCM5673_A1 attached as unit 3.
PCI device BCM5673_A1 attached as unit 4.
Adding BCM transport pointers
Configuring CPUTRANS TX
Configuring CPUTRANS RX
st_state(0) = 0x0
st_state(1) = 0x3
st_state(2) = 0x2
```

Modification du débit en bauds

Utilisez l'option 2 pour modifier le débit en bauds de l'interface série.

Pour modifier le débit en bauds à partir du menu **Boot** (Amorçage) :

1. Dans le menu **Boot** (Amorçage), sélectionnez 2 et appuyez sur <Entrée>.

L'invite suivante s'affiche :

```
[Boot Menu]2
Select baud rate:
1 - 1200
2 - 2400
3 - 4800
4 - 9600
5 - 19200
6 - 38400
```

7 - 57600
8 - 115200
0 - no change

 **REMARQUE** : Le débit sélectionné entre en vigueur immédiatement.

2. Le processus de démarrage reprend.

Extraction du journal des événements à l'aide de XMODEM

Utilisez l'option 3 pour extraire le journal des événements et le télécharger sur votre terminal ASCII.

Pour extraire le journal des événements à partir du menu **Boot** (Amorçage) :

1. Dans le menu **Boot** (Amorçage), sélectionnez 3 et appuyez sur <Entrée>.

L'invite suivante s'affiche :

```
[Boot Menu] 3  
  
Sending event log, start XMODEM receive....  
  
File ascillog.bin Ready to SEND in binary mode  
  
Estimated File Size 169K, 1345 Sectors, 172032 Bytes  
  
Estimated transmission time 3 minutes 20 seconds  
  
Send several Control-X characters to cancel before transfer starts.
```

2. Le processus de démarrage reprend.

Chargement d'un nouveau code opérationnel à l'aide de XMODEM

Utilisez l'option 4 lorsqu'une nouvelle version d'un logiciel doit être téléchargée pour remplacer des fichiers altérés ou mettre à niveau ou à jour les logiciels du système.

Pour télécharger des logiciels à partir du menu **Boot** (Amorçage) :

1. Dans le menu **Boot** (Amorçage), sélectionnez 4 et appuyez sur <Entrée>.

L'invite suivante s'affiche :

```
[Boot Menu] 4  
  
Ready to receive the file with XMODEM/CRC....  
  
Ready to RECEIVE File xcode.bin in binary mode  
  
Send several Control-X characters to cancel before transfer starts.
```

2. Si vous utilisez HyperTerminal, cliquez sur **Transfer (Transférer)** dans la barre de menus d'**HyperTerminal**.

3. Dans le menu **Transfer (Transférer)**, sélectionnez **Send File (Envoyer un fichier)**.

La fenêtre **Send File (Envoyer un fichier)** s'affiche.

4. Entrez le chemin d'accès du fichier à télécharger.
5. Assurez-vous que le protocole Xmodem est sélectionné.

6. Cliquez sur **Send (Envoyer)**.

Le logiciel est téléchargé. Cette opération prend plusieurs minutes. L'application d'émulation de terminal (HyperTerminal, par exemple), peut afficher la progression du processus de téléchargement.

Affichage des données produit vitales du code opérationnel

Utilisez l'option 5 pour afficher les informations relatives à l'image d'amorçage.

Pour afficher les informations sur l'image d'amorçage à partir du menu **Boot** (Amorçage) :

1. Dans le menu **Boot** (Amorçage), sélectionnez 5 et appuyez sur <Entrée>.

L'invite suivante s'affiche :

```
[Boot Menu] 5

The following image is in the Flash File System:

File Name.....image1

CRC.....0xb017 (45079)

Target Device.....0x00508541

Size.....0x8ec50c (9356556)

Number of Components.....2

Operational Code Size.....0x7ec048 (8306760)

Operational Code Offset.....0x74 (116)

Operational Code FLASH flag.....1

Operational Code CRC.....0x9B4D

Boot Code Version.....1

Boot Code Size.....0x100000 (1048576)

Boot Code Offset.....0x7ec0bc (8306876)

Boot Code FLASH flag.....0

Boot Code CRC.....0x1CB8

VPD - rel 0 ver 31 maint_lvl 0

Timestamp - Thu Jun 8 12:51:44 2006

File - pc62xxr0v31.stk
```

2. Le processus de démarrage reprend.

Exécution des diagnostics de la mémoire flash

Utilisez l'option 6 pour exécuter les diagnostics de la mémoire flash. Avant l'exécution de la commande, une question Y/N vous invite à confirmer votre choix.

Pour lancer un test complet de la mémoire flash à partir du menu **Boot** (Amorçage) :

1. Dans le menu **Boot** (Amorçage), sélectionnez 6 et appuyez sur <Entrée>.

L'invite suivante s'affiche :

```
[Boot Menu] 6

Do you wish to run flash diagnostics? (Boot code region will not be tested.) (y/n): y

Input number of diagnostic iterations -> 1

Testing 2 x 28F128J3 base: 0xfe000000

Iterations remaining = 1

Erasing sector 0

Verify sector 0 erased

Writing sector 0

Erasing sector 1
```

```
Verify sector 1 erased
Writing sector 1
Erasing sector 2
Verify sector 2 erased
Writing sector 2
Erasing sector 3
Verify sector 3 erased
Writing sector 3
Erasing sector 4
Verify sector 4 erased
Writing sector 4
Erasing sector 5
Verify sector 5 erased
Writing sector 5
Erasing sector 6
Verify sector 6 erased
Writing sector 6
```

 **REMARQUE :** Ce processus continue de s'exécuter jusqu'à ce que tous les secteurs aient été effacés, vérifiés et écrits.

```
Flash Diagnostics passed
[Boot Menu]
```

2. Le processus de démarrage reprend.

Mise à jour du code de démarrage

Utilisez l'option 7 pour mettre à jour le code de démarrage en mémoire flash. Cette option ne peut être sélectionnée qu'après le chargement d'un nouveau code de démarrage à l'aide de l'option 4 du menu Boot (Amorçage). Avant l'exécution de la commande, une question Y/N vous invite à confirmer votre choix.

Pour télécharger des logiciels à partir du menu **Boot** (Amorçage) :

1. Dans le menu **Boot** (Amorçage), sélectionnez 7 et appuyez sur <Entrée>.

L'invite suivante s'affiche :

```
Do you wish to update Boot Code? (y/n) y
Erasing Boot Flash....Done.
Wrote 0x10000 bytes.
Wrote 0x10000 bytes.
Wrote 0x30000 bytes.
Wrote 0x40000 bytes.
Wrote 0x50000 bytes.
Wrote 0x60000 bytes.
Boot code updated
```

2. Le processus de démarrage reprend.

Suppression de l'image de sauvegarde

Utilisez l'option 8 pour supprimer l'image de sauvegarde de la mémoire flash. Avant l'exécution de la commande, une question Y/N vous invite à confirmer votre choix.

Pour supprimer l'image de sauvegarde à partir du menu **Boot** (Amorçage) :

1. Dans le menu **Boot** (Amorçage), sélectionnez 8 et appuyez sur <Entrée>.

L'invite suivante s'affiche :

```
Are you SURE you want to delete backup image : image2 ? (y/n):y
```

```
Backup image deleted...
```

```
[Boot Menu]
```

2. Le processus de démarrage reprend.

Réinitialisation du système

Utilisez l'option 9 pour effacer toute la mémoire flash et rétablir le paramétrage système par défaut. Avant l'exécution de la commande, une question Y/N vous invite à confirmer votre choix.

Pour réinitialiser le système à partir du menu **Boot** (Amorçage) :

1. Dans le menu **Boot** (Amorçage), sélectionnez 9 et appuyez sur <Entrée>.

L'invite suivante s'affiche :

```
[Boot Menu] 9
```

```
Are you SURE you want to reset the system? (y/n):y
```

2. Le processus d'amorçage démarre.

Restauration de la configuration par défaut définie en usine (suppression des fichiers de configuration)

Utilisez l'option 10 pour charger la configuration système par défaut et démarrer sans utiliser la configuration de démarrage en cours. Lorsque vous sélectionnez l'option 10 du menu **Boot** (Amorçage), les valeurs système par défaut sont rétablies. Pour lancer la séquence de démarrage, sélectionnez ensuite l'option 1 du menu **Boot** (Amorçage).

Pour télécharger des logiciels à partir du menu **Boot** (Amorçage) :

1. Dans le menu **Boot** (Amorçage), sélectionnez 10 et appuyez sur <Entrée>.

L'invite suivante s'affiche :

```
Are you SURE you want to delete the configuration? (y/n):y
```

2. Le processus de démarrage reprend.

Activation de l'image de sauvegarde

Utilisez l'option 11 pour activer l'image de sauvegarde. L'image active est sauvegardée lorsque vous sélectionnez cette option.

Pour activer l'image de sauvegarde :

1. Dans le menu **Boot** (Amorçage), sélectionnez 11 et appuyez sur <Entrée>.

Le message suivant s'affiche :

```
Backup image - image2 activated.
```

2. Le processus de démarrage reprend.

Procédure de récupération du mot de passe

Utilisez l'option 12 en cas de perte d'un mot de passe. Cette option permet au commutateur de démarrer une fois sans que l'utilisateur soit invité à indiquer le

mot de passe de la console. Dans ce mode, le mot de passe *enable* n'est pas demandé.

Pour récupérer un mot de passe (pour le terminal local uniquement) :

1. Dans le menu **Boot** (Amorçage), sélectionnez **12** et appuyez sur <Entrée>.

Le mot de passe est supprimé.

2. Le processus de démarrage reprend.
3. Pour protéger le commutateur contre tout accès non autorisé, reconfigurez les mots de passe associés aux fonctions de gestion.

Exemple de processus de configuration

Cette section décrit les opérations de base permettant d'établir une connexion de gestion de réseau à distance avec le commutateur. Les différentes configurations disponibles sur le commutateur et les commandes correspondantes ne sont pas abordées.

Cette section indique également la procédure permettant d'accéder au commutateur pour la première fois à l'aide de la configuration et des définitions par défaut. Si une configuration précédente pose problème, le fichier de configuration de démarrage (qui correspond à la configuration du commutateur une fois celui-ci allumé) doit être supprimé. Vous devez ensuite redémarrer le commutateur. Voir [Paramètres par défaut du périphérique](#).

Éléments requis pour la configuration du commutateur

Les composants suivants sont requis pour cet exemple :

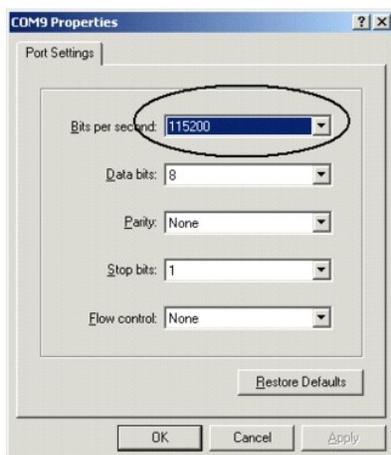
1. Commutateur PowerConnect série 6200
1. Station de travail avec les éléments suivants installés :
 - o Carte réseau
 - o Application de terminal ASCII (par exemple Microsoft® Windows® HyperTerminal ou Procomm Plus™ Terminal)
 - o Navigateur
1. Câble F2F null modem
1. Câble(s) à paires torsadées non blindées (UTP) de catégorie 5, croisé(s) ou droit(s)

Connexion initiale

1. Connectez le commutateur à la station de travail en utilisant le port RS-232.
2. Définissez les paramètres ci-dessous pour le terminal ASCII et sélectionnez le port COM approprié.

Cet exemple d'écran utilise HyperTerminal.

Figure 5-3. Fenêtre des propriétés de HyperTerminal



REMARQUE : Par défaut, un nouveau commutateur se voit attribuer un débit de 9600 bauds. Le débit du commutateur concerné peut donc être différent. Si le terminal ne s'affiche pas lorsque vous utilisez le débit par défaut, essayez-en un autre.

3. Connectez la station de travail au commutateur à l'aide d'un câble F2F null modem.

 **REMARQUE :** Si vous configurez une *pile*, connectez la station de travail au commutateur maître.

4. Branchez le cordon d'alimentation du commutateur et mettez celui-ci sous tension. Le démarrage du système commence. Lorsque les informations ci-dessous s'affichent, vous pouvez exécuter des procédures spéciales, si nécessaire, en sélectionnant 2 pour accéder au menu **Boot** (Amorçage).

```
Select an option. If no selection in 10 seconds then operational code will start.
```

```
1 - Start operational code.
```

```
2 - Start Boot Menu.
```

```
Select (1, 2):2
```

Si vous n'accédez pas au menu **Boot** (Amorçage), le système décompresse le code en mémoire RAM. Le code démarre à partir de la RAM et la liste des numéros de port disponibles ainsi que leur état (disponible ou non disponible) s'affiche.

 **REMARQUE :** L'écran suivant est un exemple de configuration. Les éléments tels que les adresses, les versions et les dates peuvent être différents pour chaque commutateur.

```
current volume configuration:
- volume label: NO LABEL ; (in boot sector: )
- volume Id: 0x0
- total number of sectors: 60,716
- bytes per sector: 512
- # of sectors per cluster: 4
- # of reserved sectors: 1
- FAT entry size: FAT16
- # of sectors per FAT copy: 60
- # of FAT table copies: 2
- # of hidden sectors: 4
- first cluster is in sector # 136
- Update last access date for open-read-close = FALSE
- directory structure: VFAT
- root dir start sector: 121
- # of sectors per root: 15
- max # of entries in root: 240
FAT handler information:
-----
- allocation group size: 2 clusters
- free space on volume: 21,348,352 bytes
Boot Menu Version: 27 Apr 2006
Select an option. If no selection in 10 seconds then
operational code will start.
1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):1
Operational Code Date: Wed May 17 10:54:19 2006
Uncompressing.....
```

```

50% 100%
|||||
volume descriptor ptr (pVolDesc): 0xfd7e6c0
cache block I/O descriptor ptr (cbio): 0xfd7fe40
auto disk check on mount: NOT ENABLED
max # of simultaneously open files: 22
file descriptors in use: 0
# of different files in use: 0
# of descriptors for deleted files: 0
# of obsolete descriptors: 0
current volume configuration:
- volume label: NO LABEL ; (in boot sector: )
- volume Id: 0x0
- total number of sectors: 60,716
- bytes per sector: 512
- # of sectors per cluster: 4
- # of reserved sectors: 1
- FAT entry size: FAT16
- # of sectors per FAT copy: 60
- # of FAT table copies: 2
- # of hidden sectors: 4
- first cluster is in sector # 136
- Update last access date for open-read-close = FALSE
- directory structure: VFAT
- root dir start sector: 121
- # of sectors per root: 15
- max # of entries in root: 240
FAT handler information:
-----
- allocation group size: 2 clusters
- free space on volume: 21,350,400 bytes
File: unitmgr.c, Line: 3419, Error 0 (0x0)
Timebase: 66.666666 MHz, MEM: 266.666664 MHz, PCI: 66.666666 MHz, CPU: 533.333328 MHz
SOC unit 0 attached to PCI device BCM56304_B0
SOC unit 1 attached to PCI device BCM56304_B0
Adding BCM transport pointers
Configuring CPUTRANS TX
Configuring CPUTRANS RX
hpc - No stack ports. Starting in stand-alone mode.
(Unit 1 - Waiting to select management unit)>

```

Paramètres par défaut du périphérique

Pour revenir aux paramètres par défaut, utilisez la commande `delete startup-config` à l'invite du mode privilégié (#) et redémarrez l'unité. Le périphérique redémarre avec les paramètres par défaut.

```
console>
console>enable
console# delete startup-config
Startup file was deleted
console#reload
Management switch has unsaved changes.
Are you sure you want to continue? (y/n) y
Configuration Not Saved!
Are you sure you want to reload the stack? (y/n) y
Reloading all switches..
```

Activation de la gestion à distance

1. Entrez la commande **enable** sur la console pour accéder au mode d'affichage Privileged EXEC (EXEC privilégié) :

```
console>enable
console#
```

2. Connectez la station de gestion au commutateur via l'un des ports Ethernet, ou par l'intermédiaire d'un réseau connecté au commutateur. Pour ce faire, utilisez un câble de catégorie 5.

Cet exemple utilise le port **1/g1**.

3. Sur le terminal ASCII, vérifiez que l'état de l'interface a été modifié en "up" (active) et que l'état STP affiche "forwarding" (transmission) au bout de 30 secondes, comme illustré ci-dessous.

```
console#
01-Jan-2000 01:43:03 %LINK-I-Up: Vlan 1
01-Jan-2000 01:43:03 %LINK-I-Up: 1/g1
01-Jan-2000 01:43:34 %STP-I-PORTSTATUS: Port 1/g1: STP status Forwarding
```

4. Entrez la commande **config** sur la console pour accéder au mode de l'écran de configuration, comme indiqué ci-après.

```
console#config
```

5. Utilisez la commande suivante pour définir l'adresse IP sur DHCP :

```
console(config)#ip address dhcp
```

6. Utilisez la commande suivante pour définir la passerelle par défaut :

```
console(config)#ip default-gateway 10.254.24.162
```

7. Si la station de gestion fait partie d'un réseau distant et n'est pas connectée directement à l'interface, configurez un itinéraire statique.

L'adresse IP configurée doit appartenir au même sous-réseau que l'une des interfaces IP du commutateur. Dans cet exemple, l'adresse statique est 192.168.20.100.

```
console(config)#ip route 192.168.10.10 255.255.255.0 192.168.20.1 200
```

8. A partir du commutateur, exécutez la commande ping sur la station de gestion pour vérifier que la connexion a été établie.

Avant d'exécuter la commande ping sur la station de gestion, attendez 30 secondes pour que le port passe en mode de transmission STP. Dans cet exemple, l'adresse IP de la station de gestion est 50.1.1.2.

```
console>ping 50.1.1.2
64 bytes from 50.1.1.2: icmp_seq=1. time=0 ms
```

```

64 bytes from 50.1.1.2: icmp_seq=2. time=0 ms
64 bytes from 50.1.1.2: icmp_seq=3. time=0 ms
64 bytes from 50.1.1.2: icmp_seq=4. time=0 ms
----50.1.1.2 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0

```

9. Définissez un nom et un mot de passe pour accorder à un utilisateur distant l'accès au commutateur avec le niveau de privilège 15 (HTTP et HTTPS).

Dans cet exemple, le nom d'utilisateur est **Dell**, le mot de passe **Dell1234** et le niveau de privilège 15. Les niveaux de privilège vont de 1 à 15, 15 étant le niveau le plus élevé. Le niveau 15 est le seul à permettre l'accès à l'interface Web.

```

console#config

console(config)#username Dell password Dell1234 level 15

console(config)#ip http authentication local

console(config)#ip https authentication local

console(config)#crypto certificate generate key_generate

Generating RSA private key, 1024 bit long modulus

console(config)#ip https server

```

10. Définissez un nom et un mot de passe pour accorder l'accès à un utilisateur local (via une console, une session Telnet ou un serveur Web, par exemple).

Dans cet exemple, le nom d'utilisateur est **Dell**, le mot de passe **Dell1234** et le niveau de privilège 15.

```

console(config)#username Dell password Dell1234 level 15

console(config)#aaa authentication login default line

console(config)#aaa authentication enable default line

console(config)#line console

console(config-line)#login authentication default

console(config-line)#enable authentication default

console(config-line)#password tommy123

console(config-line)#exit

console(config)#line telnet

console(config-line)#login authentication default

console(config-line)#enable authentication default

console(config-line)#password bobby123

console(config-line)#exit

console(config)# line ssh

console(config-line)#login authentication default

console(config-line)#enable authentication default

console(config-line)#password jones123

console(config-line)#exit

```

11. Enregistrez le fichier **running-config** dans le fichier **startup-config**.

Vous vous assurez ainsi que la configuration définie restera inchangée si le commutateur est redémarré.

```

console(config)#exit

console#copy running-config startup-config

```

Le commutateur est désormais configuré ; il peut être géré via différentes options telles que Telnet, l'interface du navigateur Web, etc.

Configuration de l'accès de gestion sécurisé (HTTPS)

Lors de la gestion sécurisée du commutateur via le navigateur Web standard, le protocole de sécurité SSL (Secure Socket Layer) est utilisé.

Pour gérer le commutateur en toute sécurité à partir du navigateur Web standard, procédez comme suit :

1. Pour configurer le commutateur de manière à autoriser l'accès du serveur HTTPS et pour créer une clé de sécurité, utilisez les commandes **ip https server** et **crypto certificate 1 generate** :

```
console#configure

console(config)#crypto certificate 1 generate

Generating RSA private key, 1024 bit long modulus

console(config)#ip https server

console(config)#
```

2. Configurez la station de gestion comme pour une connexion HTTP normale.
3. Connectez-vous au commutateur via HTTPS en entrant l'adresse `https://adresse IP du périphérique` dans la fenêtre du navigateur (vous devez obligatoirement taper `https`).

La fenêtre **Security Alert** (Alerte de sécurité) s'affiche.

4. Cliquez sur **Yes** pour accepter la certification de sécurité (en l'absence d'authentification par un tiers).

La fenêtre **Login Screen** (Écran de connexion) s'affiche.

5. Entrez le nom et le mot de passe utilisateur appropriés.

La fenêtre de Dell OpenManage™ Switch Administrator s'affiche.

[Retour au sommaire](#)

[Retour au sommaire](#)

Obtention d'aide

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Demande d'assistance](#)
- [Service Dell de formation et de certification pour les entreprises](#)
- [Incidents liés à votre commande](#)
- [Informations sur les produits](#)
- [Renvoi d'articles pour une réparation sous garantie ou un remboursement](#)
- [Avant d'appeler](#)
- [Contacter Dell](#)

Demande d'assistance

Si un incident se produit, vous pouvez procéder aux opérations suivantes pour établir un diagnostic et appliquer des procédures de dépannage :

1. Complétez la [liste de vérification des diagnostics](#).
2. Pour vous aider lors des procédures d'installation et de dépannage, utilisez toute la gamme de services en ligne proposés par Dell sur le site [support.dell.com](#). Voir [Services en ligne](#) pour obtenir une liste plus complète des services de support Dell accessibles en ligne.
3. Si les étapes précédentes n'ont pas résolu l'incident, voir [Contacter Dell](#).

 **REMARQUE :** Passez votre appel à partir d'un téléphone qui se trouve près du système pour que le support technique puisse vous guider dans l'accomplissement des opérations nécessaires.

 **REMARQUE :** Il se peut que le système de code de service express Dell ne soit pas disponible dans votre pays.

Lorsque le système téléphonique automatisé de Dell vous le demande, entrez votre code de service express pour acheminer directement votre appel vers le personnel de support compétent. Si vous ne disposez pas d'un code de service express, ouvrez le dossier **Dell Accessories** (Accessoires Dell), double-cliquez sur l'icône **Express Service Code** (Code de service express) et suivez les indications.

Pour obtenir des instructions sur l'utilisation du support Dell, voir [Service de support](#).

 **REMARQUE :** Une partie des services suivants n'est disponible que dans certains pays. Contactez votre représentant Dell local pour plus d'informations.

Services en ligne

Des informations sur les produits et services Dell sont disponibles sur les sites Web suivants :

[www.dell.com](#)
[www.dell.com/ap](#) (région Asie/Pacifique uniquement)
[www.dell.com/jp](#) (Japon uniquement)
[www.euro.dell.com](#) (Europe uniquement)
[www.dell.com/la](#) (pays d'Amérique Latine et Caraïbes)
[www.dell.ca](#) (Canada uniquement)

Vous pouvez accéder au support Dell via les sites Web et adresses e-mail suivants :

- 1 Sites Web du support Dell
[support.dell.com](#)
[support.jp.dell.com](#) (Japon uniquement)
[support.euro.dell.com](#) (Europe uniquement)
- 1 Adresses e-mail du support Dell
mobile_support@us.dell.com
support@us.dell.com
la-techsupport@dell.com (pays d'Amérique Latine et Caraïbes uniquement)
apsupport@dell.com (région Asie/Pacifique uniquement)
- 1 Adresses e-mail du service Marketing et ventes de Dell

apmarketing@dell.com (région Asie/Pacifique uniquement)

sales_canada@dell.com (Canada uniquement)

- 1 Protocole de transfert de fichiers (FTP) anonyme

ftp.dell.com

Connectez-vous en tant que user: `anonymous` et indiquez votre adresse e-mail comme mot de passe.

Service d'état des commandes automatisé

Pour vérifier l'état de vos commandes de produits Dell, vous pouvez vous rendre sur le site Web support.dell.com ou appeler le service automatisé de suivi des commandes. Un message préenregistré vous invite à entrer les informations concernant votre commande afin de la localiser et de vous informer. Pour connaître le numéro de téléphone à appeler pour votre région, voir [Contacter Dell](#).

Gold Premier Enterprise

Le service de support Dell est disponible 24 heures sur 24, 7 jours sur 7, pour répondre à vos questions concernant le matériel Dell. Notre équipe de support technique utilise des diagnostics assistés par ordinateur pour répondre plus rapidement et plus efficacement à vos questions.

Pour contacter le service de support technique de Dell, consultez la section [Avant d'appeler](#) puis reportez-vous aux informations de contact de votre région.

Service Dell de formation et de certification pour les entreprises

Des formations et certifications Dell Enterprise sont disponibles. Pour plus d'informations, consultez le site www.dell.com/training. Ce service n'est disponible que dans certains pays.

Incidents liés à votre commande

Si vous avez un problème avec votre commande (pièces manquantes ou inadaptées, problème de facturation), contactez le service clientèle de Dell. Gardez votre facture ou votre fiche d'expédition à portée de main lorsque vous appelez. Pour connaître le numéro de téléphone à appeler pour votre région, voir [Contacter Dell](#).

Informations sur les produits

Si vous avez besoin d'informations à propos d'autres produits disponibles chez Dell, ou si vous désirez passer une commande, consultez le site Web de Dell à l'adresse www.dell.com. Pour trouver le numéro de téléphone approprié pour votre pays ou pour parler à un spécialiste des ventes, voir [Contacter Dell](#).

Renvoi d'articles pour une réparation sous garantie ou un remboursement

Préparez comme indiqué ci-après tous les articles à renvoyer, que ce soit pour une réparation ou un remboursement :

1. Appelez Dell pour obtenir un numéro d'autorisation de renvoi du matériel et écrivez-le lisiblement et bien en vue sur l'extérieur de la boîte.
Pour connaître le numéro de téléphone à appeler pour votre région, voir [Contacter Dell](#).
2. Joignez une copie de votre facture et une lettre décrivant la raison du renvoi.
3. Joignez une copie de la [liste de vérification des diagnostics](#) indiquant les tests que vous avez effectués et les messages d'erreur éventuellement générés par Dell Diagnostics.
4. Joignez tous les accessoires associés aux éléments renvoyés (câbles d'alimentation, médias [disquettes et CD], guides) s'il s'agit d'une demande de remboursement.
5. Renvoyez l'équipement dans son emballage d'origine (ou un équivalent).

Les frais d'expédition sont à votre charge. Vous devez également assurer les produits retournés et assumer les risques de pertes en cours d'expédition. Les envois contre remboursement ne sont pas acceptés.

Les retours ne comportant pas les éléments décrits ci-dessus seront refusés au quai de réception de Dell et vous seront renvoyés.

Avant d'appeler

 **REMARQUE :** Ayez votre code de service express à portée de main quand vous appelez. Le code permet au système d'assistance téléphonique automatisé de Dell de diriger votre appel plus efficacement.

N'oubliez pas de compléter la [liste de vérification des diagnostics](#). Si possible, allumez votre ordinateur avant de contacter Dell pour obtenir une assistance et utilisez un téléphone qui se trouve à proximité de l'ordinateur. Il peut vous être demandé de taper certaines commandes au clavier, de donner des informations détaillées sur le fonctionnement de l'ordinateur ou d'essayer d'autres méthodes de dépannage qui ne sont possibles que sur le système informatique même. Veillez à vous munir de la documentation de l'ordinateur.

 **PRÉCAUTION :** Avant de travailler à l'intérieur de l'ordinateur, appliquez les consignes de sécurité décrites dans le document *Product Information Guide* (Guide d'information sur le produit).

Liste de vérification des diagnostics
Nom :
Date :
Adresse :
Numéro de téléphone :
Numéro de service (code à barres situé à l'arrière de l'ordinateur ou en dessous) :
Code de service express :
Numéro d'autorisation de renvoi de matériel (fourni par un technicien de support de Dell) :
Système d'exploitation et version :
Périphériques :
Cartes d'extension :
Êtes-vous connecté à un réseau ? Oui Non
Réseau, version et carte réseau :
Programmes et versions :
Consultez la documentation du système d'exploitation pour déterminer le contenu des fichiers de démarrage du système. Si l'ordinateur est relié à une imprimante, imprimez chaque fichier. Sinon, notez le contenu de ces fichiers avant d'appeler Dell.
Message d'erreur, code sonore ou code de diagnostic :
Description de l'incident et procédures de dépannage effectuées :

Contactez Dell

Aux États-Unis, appelez le 800-WWW.DELL (800.999.3355).

 **REMARQUE :** Si vous ne disposez pas d'une connexion Internet active, vous pouvez utiliser les coordonnées figurant sur votre preuve d'achat, votre bordereau de livraison, votre facture ou encore sur le catalogue des produits Dell.

Dell fournit plusieurs options de service et de support en ligne et par téléphone. Leur disponibilité variant d'un pays à l'autre, il est possible que certains services ne soient pas proposés dans votre région. Pour contacter Dell pour des questions ayant trait aux ventes, au support technique ou au service clientèle :

1. Rendez-vous sur le site support.dell.com.
2. Sélectionnez l'option appropriée dans le menu déroulant **Choose A Country/Region** (Choisissez un pays ou une région) situé au bas de la page.
3. Cliquez sur **Contact Us** (Nous contacter) sur la gauche de la page.
4. Sélectionnez le lien correspondant au service ou au support requis.
5. Choisissez la méthode de contact qui vous convient.

[Retour au sommaire](#)

[Retour au sommaire](#)

Utilisation de Dell™ OpenManage™ Switch Administrator

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Définition de l'adresse IP du commutateur](#)
 - [Démarrage de l'application](#)
 - [Présentation de l'interface](#)
 - [Utilisation des boutons de Switch Administrator](#)
 - [Définition des champs](#)
 - [Accès au commutateur via l'interface CLI](#)
 - [Utilisation de l'interface CLI](#)
-

Définition de l'adresse IP du commutateur

Pour définir l'adresse IP du commutateur, vous pouvez utiliser DHCP ou affecter une adresse statique. Pour démarrer l'interface CLI, voir [Accès au commutateur via l'interface CLI](#).

Définition de l'adresse IP via DHCP

1. Tapez `enable` à l'invite `console>` et appuyez sur <Entrée>.
2. Lorsque l'invite s'affiche, tapez `config` et appuyez sur <Entrée>.
3. Tapez `ip address dhcp` et appuyez sur <Entrée>.
4. Tapez `exit`.
5. Tapez `show ip interface management` à l'invite `console#`.

Définition d'une adresse statique

1. Tapez `enable` à l'invite `console>` et appuyez sur <Entrée>.
 2. Lorsque l'invite s'affiche, tapez `config` et appuyez sur <Entrée>.
 3. Tapez `ip address none`.
 4. Par exemple, pour configurer l'adresse IP 10.256.24.64 et lui associer le masque de sous-réseau 255.255.248.0 et la passerelle 10.256.24.1, entrez :

```
ip address 10.256.24.64 255.255.248.0
ip default-gateway 10.256.24.1
```
 5. Tapez `exit`.
 6. Tapez `show ip interface management`.
-

Démarrage de l'application

1. Ouvrez un navigateur Web.
2. Tapez l'adresse IP du commutateur (définie via l'interface CLI) dans la barre d'adresse et appuyez sur <Entrée>.

Pour savoir comment définir l'adresse IP d'un commutateur, voir [Présentation de la configuration](#).
3. Lorsque la fenêtre **Login** (Ouverture de session) s'affiche, entrez un nom d'utilisateur et un mot de passe.

 **REMARQUE** : Le commutateur n'est associé à aucun mot de passe par défaut. Vous pouvez configurer le commutateur sans entrer de mot de passe lorsque vous vous connectez à l'interface CLI par l'intermédiaire du port de console. Les mots de passe sont sensibles à la casse et doivent contenir des caractères alphanumériques. Pour plus d'informations sur la récupération des mots de passe oubliés, voir [Procédure de récupération du mot de passe](#).

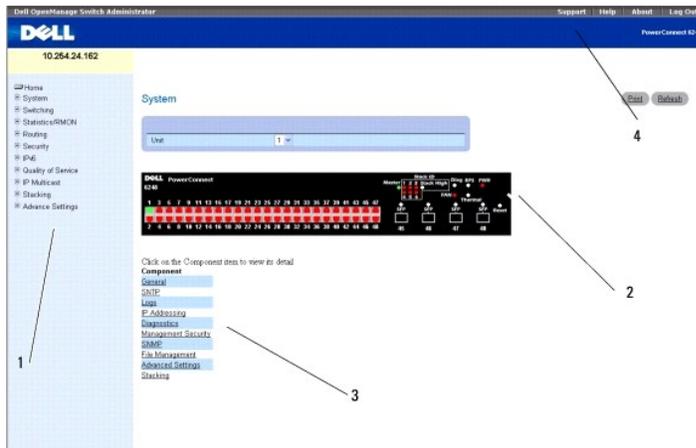
4. Cliquez sur **OK**.
5. La page d'accueil de **Dell OpenManage Switch Administrator** s'affiche.

Présentation de l'interface

La page d'accueil (voir la [Figure 3-1](#)) offre les modes d'affichage suivants :

- 1 **Vue en arborescence** : affichée dans le volet gauche de la page d'accueil, cette vue fournit une représentation hiérarchisée des différentes fonctionnalités et de leurs composants.
- 1 **Vue du périphérique** : située dans le volet droit de la page d'accueil, cette vue contient une représentation graphique du périphérique, une zone d'informations et/ou un tableau et/ou des instructions de configuration.

Figure 3-1. Composants de Switch Administrator



Le [Tableau 3-1](#) répertorie les composants de l'interface et indique les numéros correspondants.

Tableau 3-1. Composants de l'interface

Composant	Nom
1	La vue en arborescence présente la liste des différentes fonctionnalités du périphérique. Vous pouvez développer ou réduire les branches de l'arborescence de façon à afficher ou à masquer les composants rattachés à un élément spécifique. En déplaçant la barre verticale vers la droite, vous pouvez agrandir le volet pour afficher le nom complet des composants.
2	La vue du périphérique fournit des informations sur les ports, la configuration et l'état en cours, les tableaux et les composants. La couleur associée à un port permet de déterminer s'il est actif : le vert indique que le port est activé, le rouge qu'une erreur s'est produite et le bleu que la liaison est désactivée. REMARQUE : L'état des voyants n'apparaît pas dans la vue du périphérique. Vous ne pouvez déterminer cet état qu'en observant les voyants sur le commutateur. Pour plus d'informations, voir Comportement des voyants . Selon l'option sélectionnée, la zone située au bas de la vue du périphérique affiche des informations supplémentaires sur le périphérique et/ou des boîtes de dialogue de configuration.
3	Cette liste répertorie les composants du périphérique. Vous pouvez également afficher les composants en développant la branche correspondante de l'arborescence.
4	Les boutons d'information permettent d'accéder à des informations sur le commutateur et au support Dell. Pour plus d'informations, voir Boutons d'information .

Utilisation des boutons de Switch Administrator

Boutons d'information

Tableau 3-2. Boutons d'information

--	--

Bouton	Description
Support	Affiche la page support.dell.com .
Help (Aide)	Permet d'accéder à l'aide en ligne, qui contient des informations utiles pour la configuration et la gestion du commutateur. L'aide est contextuelle. Par exemple, si la page IP Addressing (Adressage IP) est ouverte, la rubrique d'aide relative à la définition des adresses IP s'affiche lorsque vous cliquez sur Help (Aide).
About (À propos de)	Affiche le numéro d'édition et de version du programme, ainsi que les informations de copyright de Dell.
Log Out (Déconnexion)	Ferme la session de l'application.

Boutons de gestion du périphérique

Tableau 3-3. Boutons de gestion du périphérique

Bouton	Description
Apply Changes (Appliquer les modifications)	Permet de valider les modifications apportées au périphérique.
Add (Ajouter)	Permet d'ajouter des informations dans des tables ou des boîtes de dialogue.
Telnet	Ouvre une session Telnet.
Query (Interrogation)	Permet d'interroger les tables.
Show All (Afficher tout)	Affiche les tables de configuration du périphérique.
Flèches vers la gauche et vers la droite	Permet de déplacer les informations d'une liste à l'autre.
Refresh (Rafraîchir)	Actualise les informations relatives au périphérique.
Reset All Counters (Réinitialiser tous les compteurs)	Réinitialise les compteurs de statistiques.
Print (Imprimer)	Imprime la page Network Management System (Système de gestion du réseau) et/ou les informations contenues dans les tables.
Draw (Créer le graphique)	Permet de créer instantanément des diagrammes de statistiques.

Cases à cocher

Tableau 3-4. Cases à cocher

Type de case à cocher	Description
Add (Ajouter)	Lien hypertexte pointant vers une page de configuration.
Remove (Supprimer)	Supprime l'élément sélectionné.
General selection (Sélection globale)	Permet d'activer un élément de configuration (régler la sensibilité des fichiers journaux, sélectionner des critères de correspondance pour diffserv, sélectionner les paramètres des règles ACL, etc.).

Définition des champs

Les champs définis par l'utilisateur peuvent contenir de 1 à 159 caractères, sauf indication contraire figurant dans la page Web de Dell OpenManage Switch Administrator.

Tous les caractères peuvent être utilisés, à l'exception des suivants :

- 1 \
- 1 /
- 1 :
- 1 *
- 1 ?
- 1 <
- 1 >
- 1 |

Accès au commutateur via l'interface CLI

Le commutateur peut être géré au moyen d'une connexion directe avec le port de console ou par l'intermédiaire d'une connexion Telnet.

 **REMARQUE :** Si vous utilisez une pile de commutateurs, assurez-vous que le câble d'interface série est branché sur le commutateur maître de la pile.

L'utilisation de l'interface CLI est similaire à l'entrée de commandes sous Linux. Si vous utilisez une connexion Telnet, avant d'utiliser les commandes CLI, assurez-vous qu'une adresse IP est définie pour le périphérique et que la station de travail utilisée pour accéder au périphérique est connectée à ce dernier.

Pour plus d'informations sur la configuration d'une adresse IP initiale, voir [Présentation de la configuration](#).

Connexion de la console

1. Mettez le commutateur (ou la pile de commutateurs) sous tension et attendez la fin du démarrage.

 **REMARQUE :** Si vous installez une *pile* de commutateurs, connectez le terminal au commutateur maître. Ce commutateur est identifié par l'allumage du voyant Master Switch (Commutateur maître). Lorsqu'une pile est mise sous tension pour la première fois, l'un des commutateurs est désigné comme maître de la pile. Ce commutateur peut occuper n'importe quel emplacement. Si vous connectez le terminal à un commutateur subordonné, vous ne pourrez pas utiliser l'interface CLI.

2. Si votre administrateur n'a activé aucune méthode d'authentification à la connexion, l'invite `console>` s'affiche au démarrage du commutateur. Sinon, l'invite de connexion `User:` s'affiche.

 **REMARQUE :** Les étapes suivantes supposent que le compte administrateur et le mot de passe associé sont configurés sur le système.

3. À l'invite, tapez `admin` et appuyez sur `<Entrée>`.

L'invite `Password:` s'affiche ensuite.

4. Entrez le mot de passe. Les caractères sont remplacés par des astérisques (*).

L'invite `console#` s'affiche.

5. Configurez le périphérique et entrez les commandes nécessaires pour effectuer les tâches requises.
6. Lorsque vous avez terminé, refermez la session à l'aide de la commande `quit` ou `exit`.

Connexion Telnet

Telnet est un protocole TCP/IP d'émulation de terminal. Les terminaux ASCII peuvent être reliés au périphérique local au moyen d'une connexion virtuelle, via un réseau utilisant le protocole TCP/IP. Telnet est une version alternative d'un terminal de connexion local qui requiert une connexion à distance.

Le commutateur prend en charge jusqu'à quatre sessions Telnet simultanées. Les sessions Telnet reconnaissent toutes les commandes CLI.

Utilisation de l'interface CLI

Présentation des modes de commande

L'interface CLI comprend plusieurs modes de commandes. Chacun de ces modes dispose d'un jeu de commandes spécifique. Pour afficher la liste des commandes disponibles pour un mode spécifique, il suffit de taper un point d'interrogation (?) à l'invite de la console.

Une commande spécifique permet de basculer d'un mode à l'autre.

Lors de l'initialisation de la session CLI, le mode User EXEC (EXEC utilisateur) est activé par défaut. Ce mode ne comprend qu'un sous-ensemble restreint de commandes. Il est réservé aux tâches n'ayant pas d'incidence sur la configuration du commutateur et permet d'accéder à des sous-systèmes de configuration. Le mode Privileged EXEC peut nécessiter un mot de passe (si le mot de passe d'activation est configuré). Pour plus d'informations, voir [Gestion de la sécurité et configuration du mot de passe](#).

Le mode Privileged EXEC permet d'accéder à la configuration générale du périphérique. Pour modifier certaines configurations spécifiques, vous devez passer au niveau suivant, appelé "Global Configuration". Aucun mot de passe n'est requis.

Le mode Global Configuration gère la configuration du périphérique au niveau global.

Le mode Interface Configuration permet de configurer le périphérique au niveau de l'interface physique. Les commandes de ce mode faisant appel à des sous-commandes sont accessibles à un autre niveau appelé "Subinterface Configuration".

Mode User EXEC

L'invite du mode User EXEC se compose du nom d'hôte suivi du symbole <. Exemple :

```
console>
```

 **REMARQUE :** À moins qu'il n'ait été modifié lors de la configuration initiale, le nom d'hôte par défaut est console.

Les commandes accessibles dans ce mode permettent d'établir une connexion avec des périphériques distants, de modifier provisoirement les paramètres des terminaux, d'effectuer des tests de base et de répertorier des informations système.

Pour afficher la liste des commandes disponibles, tapez ? à l'invite.

Mode Privileged EXEC

Ce mode permet de protéger le système et les paramètres de fonctionnement contre tout accès non autorisé. Les mots de passe sont sensibles à la casse. À l'écran, les caractères sont remplacés par des astérisques (*).

Pour accéder à ce mode et afficher la liste des commandes disponibles, procédez comme suit :

1. À l'invite, tapez `enable` et appuyez sur <Entrée>.
2. Le cas échéant, entrez le mot de passe et appuyez sur <Entrée>.

L'invite du mode Privileged EXEC se compose du nom d'hôte du périphérique suivi du symbole #. Exemple :

```
console#
```

3. Pour afficher la liste des commandes disponibles, tapez ? à l'invite.
4. Pour retourner au mode User EXEC, tapez `exit` ou appuyez simultanément sur les touches <Ctrl><Z>.

L'exemple ci-dessous indique comment accéder au mode Privileged EXEC et revenir au mode User EXEC :

```
console>enable  
Enter Password: *****  
console#  
console#exit  
console>
```

Utilisez la commande `exit` pour revenir à un mode précédent (par exemple, pour passer du mode Interface Configuration au mode Global Configuration).

Mode Global Configuration

Les commandes de ce mode s'appliquent aux fonctions du système plutôt qu'à un protocole ou une interface spécifique.

Pour accéder à ce mode, procédez comme suit :

1. À l'invite du mode Privileged EXEC, tapez `configure` et appuyez sur <Entrée>. L'invite du mode Global Configuration se compose du nom d'hôte du périphérique, suivi de (config) et du symbole dièse (#).

```
console(config)#
```

2. Pour afficher la liste des commandes disponibles, tapez ? à l'invite.
3. Pour revenir au mode Privileged EXEC, tapez `exit` ou appuyez simultanément sur les touches <Ctrl><Z>.

L'exemple ci-dessous explique comment accéder au mode *Global Configuration* et revenir au mode *Privileged EXEC* :

```
console#  
console#configure  
console(config)#exit  
console#
```

Mode Interface Configuration

Les commandes de ce mode permettent de modifier certains paramètres d'interface IP spécifiques (groupe de pontage, description, etc.). Les modes disponibles sont les suivants :

- 1 **VLAN** : contient les commandes permettant de créer et de configurer un réseau VLAN dans sa globalité (exemple : création d'un VLAN et définition de son adresse IP).
 - 1 **Port Channel (Canaux)** : contient les commandes permettant de configurer les groupes de liaisons agrégées (LAG).
 - 1 **Ethernet** : contient les commandes permettant de gérer la configuration des ports Ethernet.
 - 1 **Loopback (Boucle de rappel)** : contient les commandes permettant de gérer la configuration de l'interface des boucles de rappel.
 - 1 **Tunnel** : contient les commandes permettant de gérer la configuration de l'interface des tunnels.
-

[Retour au sommaire](#)

[Retour au sommaire](#)

Présentation du matériel

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Présentation des ports](#)
- [Autres caractéristiques](#)
- [Comportement des voyants](#)

Cette section contient des informations sur les caractéristiques du périphérique et sur la configuration matérielle des modules. Les thèmes abordés sont les suivants :

- I [Panneau avant d'un système Dell™ PowerConnect™ série 6200](#)
- I [Panneau arrière d'un commutateur Dell PowerConnect série 6200](#)
- I [Port de console \(RS-232\)](#)
- I [Dimensions](#)
- I [Blocs d'alimentation](#)
- I [Système de ventilation](#)
- I [Emplage](#)
- I [Comportement des voyants](#)

Présentation des ports

Panneau avant d'un système Dell™ PowerConnect™ série 6200

Le panneau avant du PowerConnect 6224 est équipé de 24 ports RJ-45 10/100/1000 Base-T et de quatre ports combo SFP qui disposent d'un mode de détection automatique du débit, du contrôle de flux et du mode duplex. Les émetteurs-récepteurs SFP sont vendus séparément. Le panneau avant du PowerConnect 6248 est équipé de 48 ports RJ-45 10/100/1000 Base-T et de quatre ports combo SFP.

Figure 2-1. PowerConnect 6224 équipé de 24 ports 10/100/1000 Base-T

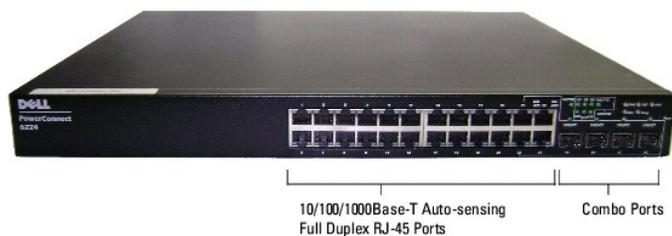


Figure 2-2. PowerConnect 6248 équipé de 48 ports 10/100/1000 Base-T



Figure 2-3. PowerConnect 6224F équipé de 24 ports SFP

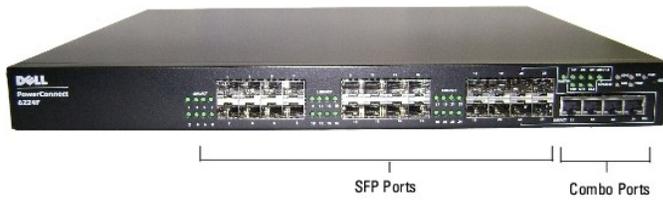


Figure 2-4. PowerConnect 6224P équipé de 24 ports 10/100/1000 Base-T



Figure 2-5. PowerConnect 6248P équipé de 48 ports 10/100/1000 Base-T



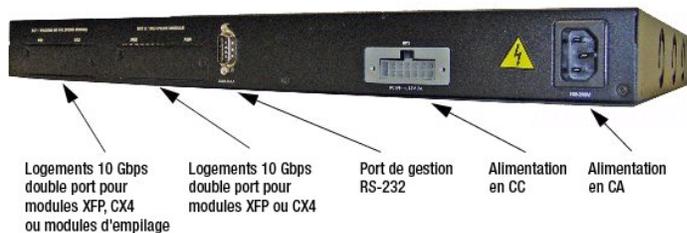
- 1 Le commutateur détecte automatiquement le type de câble branché sur les ports RJ-45 (directs ou croisés).
- 1 Les ports SFP prennent en charge les modules SX et LX.
- 1 Les ports RJ-45 prennent en charge les modes semi duplex et duplex intégral à 10/100/1000 Mbps.
- 1 Le bouton de réinitialisation se trouve sur le panneau avant.

Panneau arrière d'un commutateur Dell PowerConnect série 6200

Chaque commutateur PowerConnect de la série 6200 comprend un port de maintenance RS-232, situé sur le panneau arrière. Ce port série peut être utilisé pour gérer l'intégralité d'une pile de commutateurs.

Deux ports d'extension à 10 Gbps se trouvent également sur le panneau arrière du commutateur. Le logement de droite peut accueillir un module XFP comprenant deux ports 10 GbE ou un module CX4. Celui de gauche peut accueillir un module XFP comprenant deux ports 10 GbE, un module CX4 ou un module d'empilage.

Figure 2-6. Panneau arrière d'un PowerConnect série 6200



Port de console (RS-232)

Le port de console RS-232 est utilisé uniquement pour la gestion via une interface série. Il fournit une connexion directe avec le commutateur et est utilisé pour accéder à l'interface CLI à partir d'un terminal de console connecté à un port EIA/TIA-232.

Le port de console prend en charge les données asynchrones dont le format est le suivant : 8 bits de données, 1 bit d'arrêt, aucun bit de parité et aucun contrôle de flux. Le débit par défaut est de 9600 bps.

REMARQUE : Si vous installez une *pile* de commutateurs, vous devez terminer son montage et son câblage avant de la mettre sous tension et de la configurer. Lorsqu'une pile est mise sous tension pour la première fois, l'un des commutateurs est désigné comme maître de la pile. Ce commutateur peut occuper n'importe quel emplacement. Le voyant du commutateur maître (situé en haut à gauche du panneau avant de la baie) s'allume alors. Connectez le terminal au commutateur maître. Si vous le connectez à un autre commutateur, vous ne pourrez pas utiliser l'interface CLI.

Autres caractéristiques

Dimensions

Les dimensions des commutateurs PowerConnect de la série 6200 sont les suivantes :

- 1 En mm : 440 x 460 x 44 (Largeur x Profondeur x Hauteur)
- 1 En pouces : 17,32 x 18,11 x 1,73 (Largeur x Profondeur x Hauteur)

Blocs d'alimentation

Les commutateurs de la série 6200 sont équipés d'un bloc d'alimentation interne qui peut être branché sur une source d'alimentation standard en CA. Pour les périphériques non PoE, vous pouvez également rattacher un bloc d'alimentation en CC redondant tel que le PowerConnect RPS-600. Pour les périphériques PoE, vous pouvez rattacher un PowerConnect EPS-470. Vous pouvez vérifier le fonctionnement des blocs d'alimentation en observant les voyants. Pour plus d'informations, voir [Voyants du système](#).

Système de ventilation

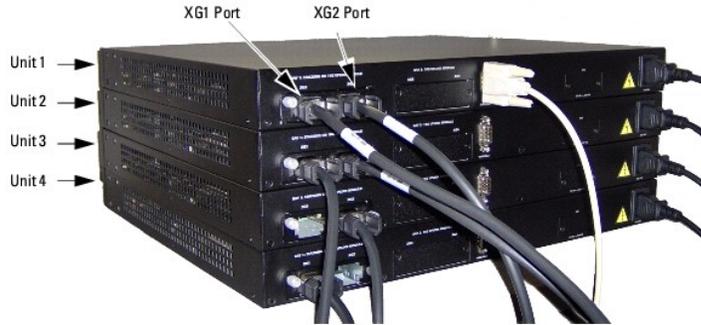
Le PowerConnect 6224 comprend trois ventilateurs. Le PowerConnect 6248 en contient quatre. Vous pouvez vérifier le fonctionnement des ventilateurs en observant les voyants. Pour plus d'informations, voir [Voyants du système](#).

Empilage

Une pile peut contenir jusqu'à 12 commutateurs PowerConnect 6224 et/ou 6248, ce qui représente un maximum de 576 ports frontaux. Pour créer une pile, connectez des commutateurs adjacents en utilisant les ports situés à l'arrière de chaque commutateur, du côté gauche. Voir la [Figure 2-7](#).

1. Utilisez un câble d'empilage court pour relier l'un des ports du commutateur situé en haut de la pile au commutateur situé juste en dessous. Installez un module d'empilage (acheté séparément) dans la "Baie 1" située à l'arrière de chaque commutateur de la pile.
2. Au besoin, utilisez un câble d'empilage long (3 mètres, non fourni) pour connecter les commutateurs. Répétez l'opération jusqu'à ce que toutes les unités soient connectées.
3. Utilisez le câble restant pour relier le port inutilisé du commutateur situé en bas de la pile à celui du commutateur situé en haut de la pile.

Figure 2-7. Connexion d'une pile de commutateurs



Dans la [Figure 2-7](#), les connexions physiques entre les commutateurs sont les suivantes :

- 1 Les unités 1 et 2 sont connectées via les ports XG1 de chaque commutateur.
- 1 Les unités 2 et 3 sont connectées via les ports XG2 de chaque commutateur.
- 1 Les unités 1 et 4 sont connectées via le port XG2 de l'unité 1 et le port XG1 de l'unité 4.

Unité de secours

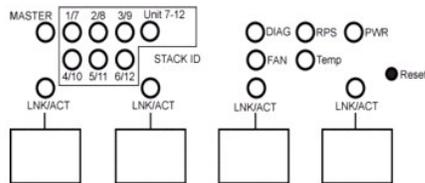
La fonction d'empilage permet d'utiliser une unité de secours prévue pour prendre le relais en cas de panne de l'unité maître de la pile. Dès qu'une panne de l'unité maître de la pile est détectée, l'unité de secours initialise la carte de contrôle et active la configuration en cours sur toutes les autres unités de la pile. Cette unité de secours gère une copie synchronisée de la configuration en cours pour la pile. Pendant la prise de relais, tous les ports sont désactivés puis réactivés. Cela permet d'éviter la création de boucles et de faire en sorte que les logiciels correspondant à la nouvelle unité maître se trouvent dans un état cohérent.

L'unité de secours de la pile est pré-configurée, mais vous pouvez utiliser l'interface CLI pour sélectionner un autre membre. Pour plus d'informations, reportez-vous au document *CLI Reference Guide* (Guide de référence CLI).

Comportement des voyants

Le panneau avant est équipé de voyants indiquant l'état des liaisons, des blocs d'alimentation, des ventilateurs, des diagnostics du système et de la pile.

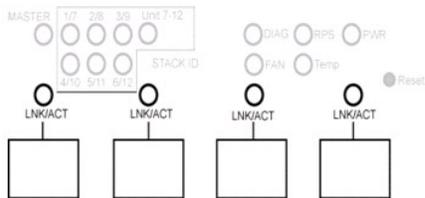
Figure 2-8. Voyants du panneau avant



Voyants des ports SFP

La [Figure 2-9](#) présente les voyants qui se trouvent au-dessus de chaque port SFP.

Figure 2-9. Voyants des ports SFP



Le [Tableau 2-1](#) indique comment interpréter le comportement des voyants des ports SFP.

Tableau 2-1. Comportement des voyants des ports SFP

--	--	--

Voyant	Couleur	Définition
LNK/ACT	Vert fixe	Le port est actuellement connecté.
	Vert clignotant	Le port est en train d'envoyer ou de recevoir des données sur le réseau.
	Éteint	Aucune liaison n'est active sur le port.

Voyants des ports des modules XFP

Les connecteurs XFP sont utilisables lorsque vous installez un module XFP dans le panneau arrière. Le [Tableau 2-2](#) indique comment interpréter le comportement des voyants des ports XFP.

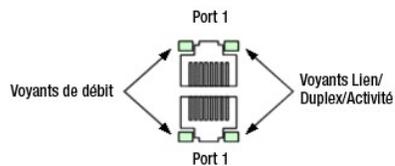
Tableau 2-2. Comportement des voyants des ports XFP

Voyant	Couleur	Définition
XFP	Vert	Le port est actuellement connecté.
	Vert clignotant	Le port est en train d'envoyer ou de recevoir des données sur le réseau.
	Éteint	Aucune liaison n'est active sur le port.

Voyants des ports 10/100/1000 Base-T

Chaque port 10/100/1000 Base-T est équipé de deux voyants. Ces voyants sont représentés dans la figure suivante.

Figure 2-10. Voyants des ports 10/100/1000 Base-T



Le [Tableau 2-3](#) indique comment interpréter le comportement des voyants des ports 10/100/1000 Base-T pour les systèmes PowerConnect 6224, 6248 et 6224F.

Tableau 2-3. Comportement des voyants des ports 10/100/1000 Base-T (systèmes 6224, 6248 et 6224F)

Voyant	Couleur	Définition
Vitesse	Vert	Le port fonctionne à 1000 Mbps.
	Orange	Le port fonctionne à 10/100 Mbps.
	Fixe	La liaison est présente mais inactive.
	Clignotant	La liaison est présente et active.
	Éteint	Pas de liaison.
Liaison	Vert	Mode duplex intégral.
	Éteint	Mode semi duplex.

Le [Tableau 2-4](#) indique comment interpréter le comportement des voyants des ports 10/100/1000 Base-T pour les systèmes PowerConnect 6224P et 6248P.

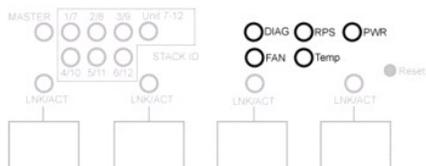
Tableau 2-4. Comportement des voyants des ports 10/100/1000 Base-T (systèmes 6224P et 6248P)

Voyant	Couleur	Définition
Speed/Link/Act	Vert fixe	Le port fonctionne à 1000 Mbps.
	Vert clignotant	Le port fonctionne à 10/100 Mbps.
	Éteint	Pas de liaison.
FDX	Vert fixe	Le périphérique PoE alimenté est détecté et fonctionne avec une charge normale.
	Vert clignotant	Le port fonctionne en mode transitionnel. Le périphérique PoE alimenté est en cours de détection, ou bien il est défectueux.
	Orange fixe	Une surcharge ou un court-circuit s'est produit(e) sur le périphérique alimenté.
	Orange clignotant	La puissance requise par le périphérique PoE est supérieure à la puissance allouée.
	Éteint	Aucun périphérique PoE n'a été détecté.

Voyants du système

Les voyants système situés à droite du panneau avant fournissent des informations sur les blocs d'alimentation, les ventilateurs, les conditions thermiques et les diagnostics. Ils sont représentés [Figure 2-11](#).

Figure 2-11. Voyants du système



Le [Tableau 2-5](#) indique comment interpréter le comportement des voyants du système.

Tableau 2-5. Comportement des voyants du système

Voyant	Couleur	Définition
DIAG	Vert clignotant	Un test de diagnostic est en cours.
	Vert	Le test de diagnostic s'est déroulé correctement.
	Rouge	Le test de diagnostic a échoué.
RPS	Vert	Un bloc d'alimentation redondant (RPS) est installé et fonctionne correctement.
	Rouge	Un bloc d'alimentation redondant (RPS) est installé, mais il est en panne.
	Éteint	Aucun bloc d'alimentation redondant (RPS) n'est installé.
PWR	Vert	Le bloc d'alimentation fonctionne correctement.
	Rouge	Le bloc d'alimentation est en panne.
FAN	Vert	Les ventilateurs fonctionnent correctement.
	Rouge	Un ventilateur (ou plusieurs) est en panne.
Temp	Vert	La température du système est inférieure au seuil autorisé.
	Rouge	La température du système dépasse le seuil maximal autorisé.

Voyants d'empilage

Les voyants d'empilage situés à droite du panneau avant fournissent des informations sur l'emplacement du commutateur dans la pile et son état. Ils sont représentés [Figure 2-12](#). Le [Tableau 2-6](#) indique comment interpréter le comportement des voyants d'empilage.

Figure 2-12. Voyants d'empilage

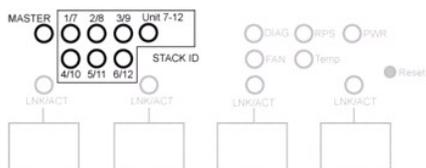


Tableau 2-6. Comportement des voyants d'empilage

Voyant	Couleur	Définition
Aucun voyant allumé		L'unité fonctionne en tant que commutateur autonome.
MASTER	Vert	L'unité est le commutateur maître de la pile.
	Éteint	L'unité n'est pas le commutateur maître de la pile.
Unité 7-12	Vert	L'ID de pile du commutateur est compris entre 7 et 12.
	Éteint	L'ID de pile du commutateur est compris entre 1 et 6.
1/7	Vert	L'unité est le premier ou le septième commutateur de la pile.
	Éteint	L'unité n'est ni le premier, ni le septième commutateur de la pile.

2/8	Vert	L'unité est le deuxième ou le huitième commutateur de la pile.
	Éteint	L'unité n'est ni le deuxième, ni le huitième commutateur de la pile.
3/9	Vert	L'unité est le troisième ou le neuvième commutateur de la pile.
	Éteint	L'unité n'est ni le troisième, ni le neuvième commutateur de la pile.
4/10	Vert	L'unité est le quatrième ou le dixième commutateur de la pile.
	Éteint	L'unité n'est ni le quatrième, ni le dixième commutateur de la pile.
5/11	Vert	L'unité est le cinquième ou le onzième commutateur de la pile.
	Éteint	L'unité n'est ni le cinquième, ni le onzième commutateur de la pile.
6/12	Vert	L'unité est le sixième ou le douzième commutateur de la pile.
	Éteint	L'unité n'est ni le sixième, ni le douzième commutateur de la pile.

[Retour au sommaire](#)

[Retour au sommaire](#)

Introduction

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Caractéristiques](#)
- [Documentation CLI](#)

🔔 **AVIS** : Avant de continuer, lisez les notes d'édition concernant ce produit. Vous pouvez les télécharger à partir du site support.dell.com.

Derniers nés de la famille de commutateurs Dell PowerConnect, les systèmes Dell™ PowerConnect™ de la série 6200 sont des commutateurs de couche 2 et 3 pouvant fonctionner en autonome ou être intégrés à une pile. Ils présentent les caractéristiques suivantes :

- 1 Châssis 1U montable en rack.
- 1 Prise en charge de toutes les fonctionnalités requises par un commutateur multi-couches pour les communications de données : commutation de couche 2, routage IPv4 et IPv6, multidiffusion IP, qualité de service (QoS), sécurité et fonctions de gestion du système.
- 1 Haute disponibilité via l'utilisation de commutateurs subordonnés enfichables à chaud.

Caractéristiques

Cette section décrit les caractéristiques du commutateur pouvant être configurées par l'utilisateur. Pour obtenir la liste de toutes les fonctions, reportez-vous à la version électronique la plus récente des notes d'édition.

Fonctions basées sur les ports

Prise en charge des trames Jumbo

Les trames Jumbo permettent de réduire le nombre de trames requises pour transférer une certaine quantité de données. Elles permettent ainsi de réduire les risques de surcharge, ainsi que les temps de traitement et le nombre d'interruptions.

Détection MDI/MDIX automatique

Le commutateur prend en charge la détection automatique des câbles croisés et directs.

Le câblage standard des stations terminales est MDI (Media-Dependent Interface, interface dépendante du média), alors que celui des concentrateurs et commutateurs est MDIX (Media-Dependent Interface with Crossover, interface croisée dépendante du média).

Pour plus d'informations sur la configuration du mode MDI/MDIX pour les ports ou les LAG, voir [Configuration des ports](#) ou [Configuration des LAG](#).

Négociation automatique

La négociation automatique permet au commutateur de déclarer son mode de fonctionnement auprès des autres systèmes. Elle permet d'échanger des informations entre deux commutateurs partageant un segment de liaison point à point, et de configurer ces commutateurs automatiquement de manière à tirer parti de leurs capacités de transmission maximales.

Les commutateurs de la série PowerConnect 6200 optimisent la négociation automatique grâce à une fonction d'annonce qui permet à l'administrateur système de configurer les vitesses de port déclarées.

Pour plus d'informations sur la négociation automatique, voir [Configuration des ports](#) ou [Configuration des LAG](#).

Prise en charge du contrôle de flux (IEEE 802.3x)

Le mécanisme de contrôle du flux permet aux commutateurs présentant une vitesse de fonctionnement peu élevée de demander aux commutateurs plus rapides de ne pas envoyer de paquets de données. Les transmissions sont temporairement interrompues pour éviter toute saturation de la mémoire tampon.

Pour plus d'informations sur la configuration du contrôle de flux pour les ports ou les LAG, voir [Configuration des ports](#) ou [Configuration des LAG](#).

Prévention des blocages HOL

La prévention des blocages en tête de ligne (HOL, Head of Line) empêche les retards et les pertes de trames qui se produisent lorsque plusieurs éléments du trafic tentent d'utiliser les ressources du même port de sortie. Le blocage HOL met les paquets en file d'attente. Les paquets placés au début de la file d'attente sont transmis avant ceux qui se trouvent à la fin.

Prise en charge de la contre-pression

Sur une liaison semi duplex, un récepteur peut empêcher la saturation de la mémoire tampon en occupant la liaison pour qu'elle soit indisponible à tout trafic supplémentaire.

ASF (Alternate Store and Forward)

La fonction ASF (Alternate Store and Forward) réduit le délai de latence observé lors du traitement des paquets de grande taille. Lorsqu'elle est activée, l'unité de gestion de mémoire (MMU) peut transmettre un paquet au port de sortie avant qu'il n'ait été entièrement reçu dans la mémoire CBP (Cell Buffer Pool, pool de mémoires tampons de cellules). La fonction ASF peut être configurée à l'aide de l'interface de ligne de commande. Pour plus d'informations concernant la configuration de cette fonction, reportez-vous au document CLI Reference Guide (Guide de référence CLI).

Fonctions liées aux adresses MAC

Prise en charge des adresses MAC

Le commutateur prend en charge un maximum de 8000 adresses MAC, dont deux sont réservées à l'utilisation du système.

Apprentissage automatique des adresses MAC

Le commutateur permet l'apprentissage automatique des adresses MAC à partir des paquets entrants.

Expiration automatique des adresses MAC

Les adresses MAC n'ayant fait l'objet d'aucun trafic réseau pendant un certain temps sont considérées comme obsolètes, ce qui permet d'éviter que la table de pontage n'arrive à saturation.

Pour plus d'informations sur la définition du délai d'expiration des adresses MAC, voir [Table des adresses dynamiques](#).

Entrées MAC statiques

Les adresses MAC définies par l'utilisateur sont enregistrées dans la table de pontage avec les adresses apprises automatiquement.

Pour plus d'informations sur la définition d'une adresse MAC statique, voir [Table des adresses statiques](#).

Commutation VLAN basée sur les adresses MAC

Les paquets provenant d'une adresse source inconnue sont envoyés au CPU et ajoutés à la table du matériel. Les paquets qui seront ensuite envoyés à cette adresse ou en proviendront seront ainsi transmis plus efficacement.

Prise en charge de la transmission multidiffusion pour les adresses MAC

La multidiffusion est un service de diffusion limité autorisant des connexions de type "un-vers-plusieurs" et "plusieurs-vers-plusieurs". Dans le cas d'un service de multidiffusion de couche 2, une seule trame envoyée à une adresse de multidiffusion spécifique est reçue. Des copies de la trame à transmettre à chaque port requis sont ensuite créées.

Pour plus d'informations sur la configuration de la prise en charge de la multidiffusion pour les adresses MAC, voir [Prise en charge de la transmission multidiffusion](#).

Fonctions de couche 2

Contrôle IGMP

Le processus appelé "IGMP Snooping" examine le contenu des trames IGMP lorsqu'elles sont transmises par le commutateur depuis une station vers un routeur multidiffusion situé en amont. Ce processus permet au commutateur d'identifier les stations concernées par les sessions de multidiffusion, ainsi que les routeurs qui envoient des trames de multidiffusion.

Mise en miroir des ports

La fonction de mise en miroir des ports permet de surveiller et de dupliquer le trafic réseau. Elle transmet des copies des paquets entrants et sortants, depuis un maximum de quatre ports source jusqu'à un port de contrôle.

Broadcast Storm Control

Lorsque des trames de couche 2 sont transmises, les trames de diffusion, de monodiffusion inconnue et de multidiffusion sont acheminées vers tous les ports du VLAN (réseau local virtuel) approprié. Cela résulte en une saturation de la bande passante et en une surcharge de tous les nœuds connectés aux ports. La fonction Storm Control permet de limiter le nombre de trames de diffusion, de monodiffusion inconnue et de multidiffusion qui sont acceptées et transmises par le commutateur.

Fonctions prises en charge pour les VLAN

Prise en charge des VLAN

Les VLAN sont des ensembles de ports de commutation qui ne comprennent qu'un seul domaine de diffusion. L'appartenance d'un paquet à un VLAN est déterminée par la balise VLAN ou en fonction du port d'entrée et du contenu du paquet. Les paquets possédant des attributs en commun peuvent être regroupés dans le même VLAN.

Pour plus d'informations sur la configuration des VLAN, voir [Configuration des VLAN](#).

VLAN basés sur les ports

Dans un VLAN basé sur les ports, les paquets entrants sont associés à un VLAN en fonction de leur port d'entrée.

Pour plus d'informations sur la configuration des VLAN, voir [Configuration des VLAN](#).

VLAN basés sur le protocole IEEE 802.1v

Les règles de classification des VLAN sont définies au niveau de l'identification du protocole de la couche de liaison de données (couche 2). Les VLAN basés sur le protocole permettent d'isoler le trafic de couche 2 afin de reporter le traitement du trafic lié aux protocoles de couche 3.

Pour plus d'informations sur la définition de VLAN basés sur les protocoles, voir [Groupe de protocoles](#).

Conformité avec la norme 802.1Q pour le balisage des VLAN

La norme IEEE 802.1Q définit une architecture pour les VLAN en pont, les services offerts par les VLAN et les protocoles et algorithmes impliqués par ces services.

Prise en charge du protocole GVRP

Le protocole GVRP (GARP VLAN Registration Protocol) permet d'élaguer les VLAN conformément à la norme IEEE 802.1Q. Il permet également la création dynamique de VLAN sur des ports de jonction 802.1Q. Lorsque le protocole GVRP est activé, le commutateur enregistre et diffuse les informations d'appartenance au VLAN sur tous les ports faisant partie de la topologie STP (Spanning Tree Protocol) active.

Pour plus d'informations sur la configuration du protocole GVRP, voir [Paramètres GVRP](#).

Ports protégés (Private VLAN Edge)

Un port d'extrémité PVE (Private VLAN Edge) est une fonction de sécurité de couche 2 applicable aux ports faisant partie d'un même VLAN. Il s'agit d'une extension des VLAN standard. Le trafic provenant des ports protégés par cette fonction est transmis uniquement aux ports situés en amont et ne peut pas être envoyé aux autres ports du VLAN.

VLAN basés sur les sous-réseaux

Cette fonction permet d'utiliser l'adresse IP source des paquets entrants non balisés pour les affecter à un VLAN et à une classe de trafic.

Pour plus d'informations sur la configuration de VLAN basés sur des sous-réseaux, voir [Liaison de sous-réseaux IP et de VLAN](#).

VLAN basés sur les adresses MAC

Cette fonction permet d'utiliser l'adresse MAC source des paquets entrants non balisés pour les affecter à un VLAN et à une classe de trafic.

Pour plus d'informations sur la configuration de VLAN basés sur les adresses MAC, voir [Liaison d'adresses MAC et de VLAN](#).

Fonctions du protocole STP

Protocole STP appliqué aux commutateurs

Le protocole STP (Spanning Tree Protocol) 802.1d est une exigence standard des commutateurs de couche 2 permettant aux ponts d'empêcher et de résoudre automatiquement les boucles de transmission L2. Les commutateurs échangent des messages de configuration à l'aide de trames spécialement formatées et procèdent à un transfert sélectif sur les ports.

Pour plus d'informations sur la configuration du protocole Spanning Tree, voir [Configuration du protocole Spanning Tree](#).

Protocole RSTP IEEE 802.1w

Le protocole Rapid Spanning Tree (RSTP) détecte et sélectionne les topologies de réseau offrant une meilleure convergence sans pour autant créer de boucles de transfert.

Pour plus d'informations sur la configuration du protocole Rapid Spanning Tree, voir [Rapid Spanning Tree \(RSTP\)](#).

Protocole MSTP

Le protocole MSTP (Multiple Spanning Tree Protocol) permet de mapper les VLAN avec des instances de Spanning Tree. Il fournit un scénario permettant de temporiser les fonctions d'équilibrage de la charge. Les paquets affectés à différents VLAN sont transmis via des chemins différents dans les régions MSTP. Le terme "régions" désigne un ou plusieurs ponts MSTP interconnectés et présentant des paramètres MSTP identiques. L'administrateur peut affecter le trafic du VLAN à des chemins uniques.

Pour plus d'informations sur la configuration du protocole Multiple Spanning Tree, voir [Paramètres MSTP](#).

Protection de la racine STP

Cette fonction permet d'empêcher toute modification imprévue de la racine d'une instance STP. En effet, même si la priorité d'un pont est définie sur zéro, un autre pont associé à une adresse MAC inférieure peut également définir sa priorité sur zéro et devenir prioritaire de la racine.

Fonction Bridge Protocol Data Unit Guard

Cette fonction permet de désactiver un port si un nouveau commutateur tente d'accéder à la topologie STP existante. Cela empêche toute modification de la topologie STP par des périphériques ne faisant pas partie de l'arborescence d'origine.

Fonctions d'agrégation des liaisons

Agrégation des liaisons

Il est possible de combiner jusqu'à huit ports pour former un groupe d'agrégation de liaisons (LAG). Cette fonction offre une protection contre l'interruption des liaisons physiques. Elle permet également d'optimiser la bande passante et d'améliorer sa granularité.

Un LAG est composé de ports ayant la même vitesse et réglés en mode duplex intégral.

Pour plus d'informations sur la configuration des LAG, voir [Configuration des LAG](#).

Agrégation de liaisons et LACP

Le protocole LACP (Link Aggregate Control Protocol) utilise les échanges entre des systèmes pairs pour déterminer les possibilités d'agrégation des différentes liaisons, et ce de façon constante. Il fournit ainsi en permanence le niveau maximum d'agrégation pouvant être atteint entre deux systèmes donnés. Il détermine, configure, relie et contrôle automatiquement l'association des ports avec les agrégateurs du système.

Pour plus d'informations sur le protocole LACP, voir [Paramètres LACP](#).

Fonctions de support pour le téléphone IP et les points d'accès

Configuration de la fonction PoE (Power Over Ethernet)

Le PowerConnect 6200 prend en charge la configuration PoE pour les seuils de tension, les interruptions SNMP et la prise en charge des périphériques PoE de génération antérieure.

Pour plus d'informations sur la configuration de la fonction PoE, voir [Configuration de la fonction Power Over Ethernet](#).

Fonction LLDP-MED

La fonction LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) est une extension de la norme LLDP appliquée à différentes fonctionnalités : configuration des réseaux, implémentation de stratégies, détection de périphériques, gestion de la fonction PoE et gestion de l'inventaire.

Pour plus d'informations sur la configuration de LLDP-MED, voir [Configuration de LLDP-MED](#).

VLAN voix

La fonction de VLAN voix permet aux ports de commutation de transmettre le trafic correspondant aux données vocales en fonction d'une priorité prédéfinie. Le niveau de priorité permet de séparer le trafic lié aux données entrant sur le port de celui lié à la voix.

Pour plus d'informations sur la configuration de LLDP-MED, voir [Configuration des ports d'un VLAN voix](#).

Fonctions de routage IPv4

Protocole ARP (Address Resolution Protocol)

Les commutateurs PowerConnect 6200 utilisent le protocole ARP pour associer une adresse MAC de couche 2 avec une adresse IPv4 de couche 3. De plus, l'administrateur peut ajouter des entrées statiques dans la table ARP.

OSPF (Open Shortest Path First)

Le protocole de routage OSPF (Open Shortest Path First, "Ouvrir d'abord la voie la plus courte") définit deux types de zones : les zones OSPF standard et les zones d'extrémité (stub). Les informations sur les itinéraires OSPF internes et externes peuvent être transmises via la zone OSPF standard. Cette dernière prend en charge le trafic de transit et les liaisons virtuelles. Les zones d'extrémité (stub), quant à elles, ne peuvent pas recevoir d'informations sur les itinéraires externes. Elles permettent en revanche de limiter la taille de la base de données des zones pour les routeurs dont les ressources sont limitées.

Agent de relais BOOTP/DHCP

Le protocole BootP permet à un périphérique de demander et de recevoir des données et des paramètres de configuration à partir d'un serveur. Le protocole DHCP est une extension de BootP qui permet à des paramètres de configuration supplémentaires d'être reçus à partir d'un serveur réseau dès le démarrage du système. En outre, le service DHCP fonctionne de façon permanente alors que BootP cesse de fonctionner dès l'obtention de l'adresse IP. Ainsi, même si l'adresse IP affectée au système dispose d'une période de validité restreinte, elle peut être renouvelée immédiatement.

Protocole RIP (Routing Information Protocol)

Le protocole de routage utilisé dans un système Internet autonome est appelé IGP (Interior Gateway Protocol). Le protocole RIP est une version d'IGP conçue pour fonctionner sur des réseaux de taille modérée.

Protocole VRRP (Virtual Router Redundancy Protocol)

Le protocole VRRP (Virtual Routing Redundancy Protocol) est utilisé pour fournir des routeurs redondants aux hôtes du réseau. Les systèmes hôtes n'ont pas besoin de détecter la présence des autres routeurs et ne nécessitent aucune reconfiguration.

Fonctions de routage IPv6

Protocole DHCPv6

Le protocole DHCPv6 fait appel au concept de serveur "stateless" (sans état). Ce protocole n'est pas utilisé pour affecter des adresses IP aux clients, mais uniquement pour fournir d'autres informations sur le réseau (liées au DNS, au protocole NTP [Network Time Protocol] et/ou au protocole SIP [Session Initiation Protocol], par exemple).

OSPFv3

OSPFv3 fournit un protocole de routage pour les réseaux en IPv6. Il s'agit d'un nouveau composant de routage basé sur la version 2 d'OSPF. En IPv6 avec support double pile, vous pouvez configurer et utiliser à la fois les composants OSPF et OSPFv3.

Itinéraires IPv6

Les protocoles IP4 et IPv6 peuvent coexister sur un même réseau. Le routeur de ce dernier doit donc être en mesure de transmettre les deux types de trafic. Pour cette raison, les connecteurs PowerConnect 6200 gèrent deux tables de routage (rto et rto6) capables de transmettre des données via le même ensemble d'interfaces. Les interfaces IPv6 sont gérées de la même manière que les interfaces IPv4.

Fonctions QoS (qualité de service)

Prise en charge de la qualité de service

Pour être en mesure de traiter le trafic réseau imprévu et optimiser les performances, vous pouvez appliquer la fonction de qualité de service (QoS) à l'ensemble du réseau. Celle-ci permet de s'assurer que le trafic sera traité en fonction de priorités basées sur des critères spécifiques. Le commutateur prend en charge deux types de fonctions QoS : les services différenciés et la classe de service.

Services différenciés (DiffServ)

La fonction QoS prend en charge les services différenciés (DiffServ). Ces derniers permettent d'organiser le trafic en différents flux et de les traiter en fonction des actions définies pour chaque saut individuel.

Classe de service (CoS)

Cette fonction permet de définir directement certains aspects relatifs à la fonction de mise en file d'attente du commutateur. Le comportement QoS voulu peut ainsi être associé à différents types de trafic réseau lorsque les fonctions plus complexes offertes par les services DiffServ ne sont pas requises.

Fonctions de multidiffusion IPv4

Protocole DVMRP (Distance Vector Multicast Routing Protocol)

Le protocole DVMRP (Distance Vector Multicast Routing Protocol) échange des paquets de sonde avec tous les routeurs compatibles afin d'établir des liaisons bidirectionnelles entre voisins et de créer une table de voisinage. Il échange également des paquets de rapport afin de créer une table de topologie monodiffusion utilisée pour la construction de la table de routage multidiffusion. Cette table est ensuite utilisée pour la transmission des paquets multidiffusion.

Protocole IGMP (Internet Group Management Protocol)

Le protocole IGMP (Internet Group Management Protocol) permet à des systèmes en IPv4 (hôtes et routeurs) de déclarer les groupes de multidiffusion IP auxquels ils appartiennent aux routeurs multidiffusion avoisinants. Les commutateurs PowerConnect 6200 agissent en tant que routeurs multidiffusions en collectant les informations d'appartenance nécessaires pour le routage multidiffusion actif.

Protocole PIM-DM (Protocol Independent Multicast-Dense Mode)

Le protocole PIM (Protocol Independent Multicast) est un protocole permettant un routage multidiffusion interdomaines et évolutif via Internet, indépendamment des mécanismes fournis par tout protocole de routage monodiffusion spécifique. Le protocole PIM-DM utilise une table de routage monodiffusion existante ainsi qu'un mécanisme de jointure/élagage/greffage pour créer une arborescence. Il crée des arborescences de distribution basés sur le plus court chemin jusqu'à la source, via la fonction RPF (Reverse Path Forwarding).

Protocole PIM-SM (Protocol Independent Multicast-Sparse Mode)

Le protocole PIM-SM permet d'optimiser l'acheminement du trafic multidiffusion vers des groupes de multidiffusion dont la taille peut aller jusqu'à celle de réseaux étendus (WAN), mais disposant d'une bande passante limitée. Par défaut, ce protocole utilise des arborescences partagées ; il implémente des arborescences basées sur la source pour une plus grande efficacité. Le basculement d'une arborescence à l'autre se fait en fonction du seuil défini pour le débit des données.

Fonctions de gestion du commutateur

Alarmes et journaux d'interruption SNMP

Le système enregistre les événements avec des codes de gravité et des horodatages. Les événements sont envoyés en tant qu'interruptions SNMP vers une liste de destinataires d'interruptions.

Pour plus d'informations sur les interruptions et les alarmes SNMP, voir [Définition des paramètres globaux SNMP](#).

Gestion basée sur le Web

Vous pouvez gérer le système via n'importe quel navigateur Web. Le commutateur contient un serveur Web intégré prenant en charge les pages HTML à travers lesquelles le système peut être contrôlé et configuré.

Téléchargement de fichiers de configuration

Le fichier de configuration du commutateur contient à la fois les paramètres appliqués au niveau du système et ceux spécifiques aux ports. Il est possible d'afficher les fichiers de configuration à l'aide des commandes de l'interface de ligne de commande (CLI).

Pour plus d'informations sur le téléchargement des fichiers de configuration, voir [Téléchargement de fichiers](#).

Téléchargement de logiciels

Le téléchargement de logiciels permet de stocker des images de sauvegarde du micrologiciel. Pour plus d'informations sur le téléchargement de logiciels, voir [Téléchargement de logiciels et réamorçage](#).

Protocole TFTP (Trivial File Transfer Protocol)

Les commutateurs de la série PowerConnect 6200 prennent en charge le chargement/téléchargement des images d'amorçage, du micrologiciel et des fichiers de configuration via le protocole TFTP (Trivial File Transfer Protocol).

RMON (Remote Monitoring)

RMON ou "Remote Monitoring" (surveillance à distance) est une base de données MIB standard qui définit les statistiques actuelles et archivées de couche MAC et les objets de contrôle, permettant ainsi de capturer les informations en temps réel sur l'ensemble du réseau.

Protocole SNMP (Simple Network Management Protocol) versions 1, 2 et 3

Le système peut être intégralement géré au moyen de variables d'une base de données d'informations de gestion (MIB, Management Information Base) dont les valeurs combinées représentent tous les aspects de l'état du système. Le protocole SNMP (Simple Network Management Protocol) contrôle ces valeurs et les modifie si nécessaire. Le protocole de transport SNMP v1/v2c/v3 via UDP/IP est pris en charge.

Interface de ligne de commande

La syntaxe et la sémantique de l'interface de ligne de commande (CLI) sont autant que possible conformes aux pratiques de l'industrie. Cette interface se compose d'éléments obligatoires et facultatifs. L'aide contextuelle en ligne indique le format et les valeurs admises pour les commandes en cours. L'interpréteur CLI fournit un mécanisme permettant de compléter les commandes et les mots-clés.

Protocole Syslog

Syslog est un protocole qui permet aux notifications d'événements d'être envoyées vers un ensemble de serveurs distants, où elles peuvent être enregistrées, contrôlées et traitées.

Pour plus d'informations sur le protocole Syslog, voir [Gestion des journaux](#).

Protocole SNTP

Le protocole SNTP (Simple Network Time Protocol) synchronise l'horloge du périphérique réseau avec une précision d'un millième de seconde. Cette synchronisation est effectuée par un serveur réseau SNTP.

Pour plus d'informations sur le protocole SNTP, voir [Configuration des paramètres SNTP](#).

Fonctions de sécurité

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) permettent de s'assurer que seuls les utilisateurs autorisés ont accès à des ressources spécifiques. Les demandes d'accès

émanant d'utilisateurs non autorisés sont refusées. Ces listes sont utilisées pour définir le contrôle de flux du trafic, limiter le contenu des mises à jour de routage, définir les types de trafic à transmettre ou à bloquer et sécuriser le réseau.

Pour plus d'informations sur les listes de contrôle d'accès, voir les sections [Configuration des ACL IP](#) et [Configuration des ACL MAC](#).

Authentification basée sur les ports (802.1x)

L'authentification basée sur les ports permet d'authentifier les utilisateurs port par port, via un serveur externe. Seuls les utilisateurs du système authentifiés et approuvés peuvent transmettre et recevoir des données. Les ports sont authentifiés via le serveur RADIUS (Remote Authentication Dial In User Service), à l'aide du protocole EAP (Extensible Authentication Protocol). Les éléments suivants sont également pris en charge : PEAP, EAP-TTL, EAP-TTLS et EAP-TLS.

Prise en charge du verrouillage des ports

Avec cette fonction, l'accès à un port verrouillé est réservé aux utilisateurs disposant d'adresses MAC spécifiques. Ces adresses peuvent être définies manuellement ou identifiées au cours du processus d'apprentissage des adresses MAC. Lorsqu'une trame est repérée sur un port verrouillé et que l'adresse MAC source de la trame n'est pas liée à ce port, le mécanisme de protection est déclenché.

Pour plus d'informations, voir [Verrouillage des ports](#).

Gestion des mots de passe

La gestion des mots de passe permet d'améliorer la sécurité du réseau et de bénéficier d'un contrôle amélioré des mots de passe. Les mots de passe pour l'accès à SSH, Telnet, HTTP, HTTPS et SNMP sont associés à des fonctions de sécurité.

Pour plus d'informations, voir [Gestion des mots de passe](#).

TACACS+

TACACS+ fournit des fonctions de sécurité centralisées pour la vérification des utilisateurs qui accèdent au périphérique. TACACS+ permet de disposer d'un système de gestion centralisée des utilisateurs tout en continuant à utiliser le mécanisme RADIUS et les autres processus d'authentification.

Client RADIUS

RADIUS est un protocole client/serveur dans lequel le serveur gère une base de données utilisateurs contenant des informations d'authentification : noms d'utilisateur, mots de passe, informations de comptabilité, etc.

Protocole SSH/SSL

Secure Shell (SSH) est un protocole qui fournit une connexion distante sécurisée à un périphérique. Cette connexion offre des fonctionnalités similaires à celles d'une connexion Telnet entrante.

Le protocole Secure Sockets Layer (SSL) permet de créer une connexion cryptée entre deux stations. Une fois établie, cette connexion ne présente virtuellement aucune différence par rapport à une connexion non sécurisée.

Documentation CLI

Vous trouverez également des informations concernant les systèmes Dell PowerConnect de la série 6200 dans le document *CLI Reference Guide* (Guide de référence CLI). Cette documentation contient des informations sur les commandes CLI permettant de configurer et de gérer des commutateurs et des piles. Vous y trouverez des descriptions détaillées des commandes CLI et de leur syntaxe, ainsi que des listes de valeurs par défaut et des exemples.

[Retour au sommaire](#)

[Retour au sommaire](#)

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

Modèles PC6224, PC6248, PC6224P, PC6248P et PC6224F



REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre ordinateur.



AVIS : Un AVIS vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.



PRÉCAUTION : Une PRÉCAUTION indique un risque potentiel d'endommagement du matériel, de blessure corporelle ou de mort.

Les informations contenues dans ce document peuvent être modifiées sans préavis.

© 2007 Dell Inc. Tous droits réservés.

La reproduction de ce document de quelque manière que ce soit sans l'autorisation écrite de Dell Inc. est strictement interdite.

Marques utilisées dans ce document : *Dell, Dell OpenManage, le logo DELL, Inspiron, Dell Precision, Dimension, OptiPlex, PowerConnect, PowerApp, PowerVault, Axim, DellNet et Latitude* sont des marques de Dell Inc. ; *Microsoft, Windows et Windows Vista* sont des marques ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays ; *Procomm Plus* est une marque de Symantec Corporation ou de ses filiales aux États-Unis et dans d'autres pays.

Tous les autres noms de marques et marques commerciales utilisés dans ce document se rapportent aux sociétés propriétaires de ces marques et de ces noms ou à leurs produits. Dell Inc. décline tout intérêt dans l'utilisation des marques déposées et des noms de marques ne lui appartenant pas.

Modèles PC6224, PC6248, PC6224P, PC6248P et PC6224F

Septembre 2007 Rév. A00

[Retour au sommaire](#)

[Retour au sommaire](#)

Affichage de statistiques/RMON

Dell™ PowerConnect™ série 6200 - Guide d'utilisation

- [Vues sous forme de tables](#)
- [RMON](#)
- [Diagrammes](#)

La fonction Remote Monitoring (RMON) permet à l'administrateur réseau de contrôler à distance les performances et l'état du réseau. Quatre groupes définis par la norme RMON sont pris en charge : statistiques, historique, alertes et événements.

Cette section présente les options RMON disponibles dans la page **Statistics/RMON** (Statistiques/RMON). Ces options permettent, entre autres, d'afficher des statistiques sous forme de tables, de visualiser et de modifier des statistiques RMON, et d'afficher des graphiques présentant les statistiques sur les ports et les groupes d'agrégation de liaisons (LAG). La page **Statistics/RMON** (Statistiques/RMON) permet d'accéder à ces options, via les fonctions suivantes :

- 1 [Vues sous forme de tables](#)
- 1 [RMON](#)
- 1 [Diagrammes](#)

REMARQUE : Toutes les pages de statistiques/RMON ne peuvent pas être affichées à l'aide des commandes CLI.

Vues sous forme de tables

La page **Table Views** (Vues sous forme de tables) contient des liens vers des pages Web qui permettent d'afficher les statistiques sous forme de tables. Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Table Views** (Vues sous forme de tables) dans l'arborescence. Cette page permet d'accéder aux fonctionnalités suivantes :

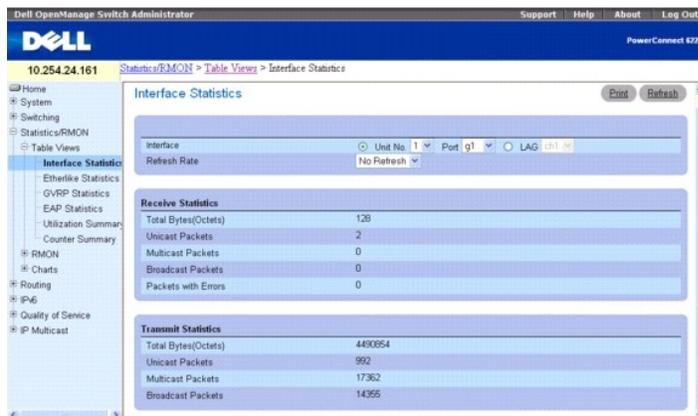
- 1 [Statistiques sur les interfaces](#)
- 1 [Statistiques Etherlike](#)
- 1 [Statistiques GVRP](#)
- 1 [Statistiques EAP](#)
- 1 [Récapitulatif de l'utilisation](#)
- 1 [Récapitulatif des compteurs](#)

Statistiques sur les interfaces

La page **Interface Statistics** (Statistiques sur les interfaces) permet d'afficher des statistiques sur les paquets reçus et transmis (les champs relatifs à ces deux types de paquets sont les mêmes).

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Table Views** (Vues sous forme de tables) → **Interface Statistics** (Statistiques sur les interfaces) dans l'arborescence.

Figure 9-1. Page Interface Statistics (Statistiques sur les interfaces)



Cette page contient les champs suivants :

Interface : identifie l'interface physique (unité, port) ou le LAG correspondant aux statistiques à afficher.

Refresh Rate (Taux de rafraîchissement) : indique l'intervalle entre deux rafraîchissements des statistiques. Les valeurs possibles sont No Refresh (Aucun rafraîchissement), 15, 30 ou 60 secondes. La valeur par défaut est No Refresh (Aucun rafraîchissement).

Section Received Statistics (Statistiques de réception)

Total Bytes - Octets (Nombre total d'octets) : indique le nombre total d'octets reçus sur l'interface sélectionnée.

Unicast Packets (Paquets monodiffusion) : nombre total de paquets monodiffusion reçus sur l'interface sélectionnée.

Multicast Packets (Paquets multidiffusion) : nombre total de paquets multidiffusion reçus sur l'interface sélectionnée.

Broadcast Packets (Paquets de diffusion) : nombre total de paquets de diffusion reçus sur l'interface sélectionnée.

Packets with Errors (Paquets avec erreurs) : indique le nombre total de paquets contenant des erreurs reçus sur l'interface sélectionnée.

Transmit Statistics (Statistiques de transmission)

Total Bytes - Octets (Nombre total d'octets) : indique le nombre total d'octets transmis sur l'interface sélectionnée.

Unicast Packets (Paquets monodiffusion) : nombre total de paquets monodiffusion transmis sur l'interface sélectionnée.

Multicast Packets (Paquets multidiffusion) : nombre total de paquets multidiffusion transmis sur l'interface sélectionnée.

Broadcast Packets (Paquets de diffusion) : nombre total de paquets de diffusion transmis sur l'interface sélectionnée.

Affichage de statistiques sur les interfaces

1. Affichez la page **Interface Statistics** (Statistiques sur les interfaces).
2. Sélectionnez une interface.

Les statistiques concernant cette interface s'affichent.

Affichage de statistiques sur les interfaces à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 Ethernet Configuration Commands (Commandes de configuration Ethernet)

Statistiques Etherlike

La page **Etherlike Statistics** (Statistiques Etherlike) permet d'afficher des statistiques sur les interfaces.

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Table Views** (Vues sous forme de tables) → **Etherlike Statistics** (Statistiques Etherlike) dans l'arborescence.

Figure 9-2. Page Etherlike Statistics (Statistiques Etherlike)



Cette page contient les champs suivants :

Interface : identifie l'interface physique (unité, port) ou le LAG correspondant aux statistiques à afficher.

Refresh Rate (Taux de rafraîchissement) : indique l'intervalle entre deux rafraîchissements des statistiques. Les valeurs possibles sont No Refresh (Aucun rafraîchissement), 15, 30 ou 60 secondes. La valeur par défaut est No Refresh (Aucun rafraîchissement).

Frame Check Sequence (FCS) Errors (Erreurs de séquence de contrôle de trame) : nombre d'erreurs de séquence de contrôle de trame reçues sur l'interface sélectionnée.

Signal Collision Frames (Collisions de trames) : indique le nombre d'erreurs reçues sur l'interface sélectionnée et liées à des collisions de trames.

Late Collisions (Collisions tardives) : indique le nombre de collisions tardives reçues sur l'interface sélectionnée.

Excessive Collisions (Collisions excessives) : indique le nombre de collisions excessives reçues sur l'interface sélectionnée.

Internal MAC Transmit Errors (Erreurs de transmission MAC internes) : indique le nombre d'erreurs de transmission MAC internes reçues sur l'interface sélectionnée.

Oversize Packets (Paquets trop longs) : indique le nombre total de paquets reçus dont le format était valide mais dont la longueur dépassait 1518 octets (sans les bits de synchronisation des trames mais avec les octets de contrôle FCS).

Internal MAC Receive Errors (Erreurs de réception MAC internes) : indique le nombre d'erreurs de réception MAC internes reçues sur l'interface sélectionnée.

Received Pause Frames (Trames de pause reçues) : indique le nombre de trames de pause reçues sur l'interface sélectionnée.

Transmitted Pause Frames (Trames de pause reçues) : indique le nombre de trames de pause transmises sur l'interface sélectionnée.

Affichage de statistiques Etherlike pour une interface

1. Affichez la page **Etherlike Statistics** (Statistiques Etherlike).
2. Sélectionnez une interface.

Les statistiques concernant cette interface s'affichent.

Statistiques GVRP

La page **GVRP Statistics** (Statistiques GVRP) permet d'afficher les statistiques concernant le protocole GVRP pour le commutateur.

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Table Views** (Vues sous forme de tables) → **GVRP Statistics** (Statistiques GVRP) dans l'arborescence.

Figure 9-3. Page GVRP Statistics (Statistiques GVRP)

GVRP Statistics Table Attribute (Counters)		Received	Transmitted
Join Empty		0	0
Empty		0	0
Leave Empty		0	0
Join In		0	0
Leave In		0	0
Leave All		0	0

Error Statistics		Received
Invalid Protocol ID		0
Invalid Attribute Type		0
Invalid Attribute Value		0

Cette page contient les champs suivants :

Interface : identifie l'interface physique (unité, port) ou le LAG correspondant aux statistiques à afficher.

Refresh Rate (Taux de rafraîchissement) : indique l'intervalle entre deux rafraîchissements des statistiques. Les valeurs possibles sont No Refresh (Aucun rafraîchissement), 15, 30 ou 60 secondes. La valeur par défaut est No Refresh (Aucun rafraîchissement).

Section GVRP Statistics Table Attribute (Counters) - Received and Transmitted (Attribut de la table de statistiques GVRP [Compteurs] - Réceptions et transmissions)

Join Empty : affiche les statistiques "Join Empty" relatives au protocole GVRP pour le commutateur.

Empty : affiche les statistiques "Empty" relatives au protocole GRVP pour le commutateur.

Leave Empty : affiche les statistiques "Leave Empty" relatives au protocole GRVP pour le commutateur.

Join In : affiche les statistiques "Join In" relatives au protocole GRVP pour le commutateur.

Leave In : affiche les statistiques "Leave In" relatives au protocole GRVP pour le commutateur.

Leave All : affiche les statistiques "Leave All" relatives au protocole GRVP pour le commutateur.

Error Statistics - Received (Statistiques d'erreurs - Réceptions)

Invalid Protocol ID (ID de protocole incorrect) : affiche les statistiques relatives aux ID de protocole GVRP incorrects pour le commutateur.

Invalid Attribute Type (Type d'attribut incorrect) : affiche les statistiques relatives aux types d'attributs incorrects pour le protocole GVRP.

Invalid Attribute Value (Valeur d'attribut incorrecte) : affiche les statistiques relatives aux valeurs d'attributs incorrectes pour le protocole GVRP.

Invalid Attribute Length (Longueur d'attribut incorrecte) : affiche les statistiques relatives aux longueurs d'attributs incorrectes pour le protocole GVRP.

Invalid Events (Événements non valides) : indique les statistiques relatives aux événements GVRP non valides pour le commutateur.

Affichage de statistiques GVRP pour une interface

1. Affichez la page **GVRP Statistics** (Statistiques GVRP).
2. Sélectionnez une interface dans le champ approprié.

Les statistiques GVRP concernant cette interface s'affichent.

Affichage de statistiques GVRP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 GVRP Commands (Commandes GVRP)

Statistiques EAP

La page **EAP Statistics** (Statistiques EAP) contient des informations sur les paquets EAP reçus sur un port spécifique. Pour plus d'informations sur EAP, voir [Authentification basée sur les ports](#).

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Table Views** (Vues sous forme de tables) → **EAP Statistics** (Statistiques EAP) dans l'arborescence.

Figure 9-4. Page EAP Statistics (Statistiques EAP)

Interface	Unit No.	Port
	1	g1
Refresh Rate	No Refresh	
Frames Received	0	
Frames Transmitted	0	
Start Frames Received	0	
Log off Frames Received	0	
Response ID Frames Received	0	
Response Frames Received	0	
Request Frames Transmitted	0	
Request ID Frames Transmitted	0	
Invalid Frames Received	0	
Length Error Frames Received	0	
Last Frames Version	0	
Last Frames Source	0000.0000.0000	

Interface : indique l'interface sur laquelle les données nécessaires aux statistiques sont collectées.

Refresh Rate (Taux de rafraîchissement) : indique l'intervalle entre deux rafraîchissements des statistiques. Les valeurs possibles sont No Refresh (Aucun rafraîchissement), 15, 30 ou 60 secondes. La valeur par défaut est No Refresh (Aucun rafraîchissement).

Frames Received (Trames reçues) : indique le nombre de trames EAPOL valides reçues sur le port.

Frames Transmitted (Trames transmises) : indique le nombre de trames EAPOL transmises par le port.

Start Frames Received (Trames de début reçues) : indique le nombre de trames EAPOL de début reçues sur le port.

Log off Frames Received (Trames de déconnexion reçues) : indique le nombre de trames EAPOL de déconnexion reçues sur le port.

Respond ID Frames Received (Trames "Respond ID" reçues) : indique le nombre de trames EAPOL "Respond ID" reçues sur le port.

Respond Frames Received (Trames "Respond" reçues) : indique le nombre de trames EAPOL "Respond" valides reçues sur le port.

Request ID Frames Received (Trames "Request ID" reçues) : indique le nombre de trames EAP "Request ID" reçues sur le port.

Request Frames Transmitted (Trames "Request" transmises) : indique le nombre de trames EAP "Request" transmises par le port.

Request ID Frames Transmitted (Trames "Request ID" transmises) : indique le nombre de trames EAP "Request ID" transmises par le port.

Invalid Frames Received (Trames non valides reçues) : indique le nombre de trames EAPOL non reconnues ayant été reçues sur le port.

Length Error Frames Received (Trames de longueur incorrecte reçues) : indique le nombre de trames EAPOL de longueur incorrecte reçues sur le port.

Last Frames Version (Version des dernières trames) : indique le numéro de version du protocole associé à la dernière trame EAPOL reçue.

Last Frames Source (Source de la dernière trame) : indique l'adresse MAC source associée à la dernière trame EAPOL reçue.

Affichage de statistiques EAP pour une interface

1. Affichez la page **EAP Statistics** (Statistiques EAP).
2. Sélectionnez une interface dans le champ approprié.

Les statistiques EAP concernant cette interface s'affichent.

Affichage de statistiques EAP à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. 802.1X Commands (Commandes 802.1x)

Récapitulatif de l'utilisation

La page **Utilization Summary** (Récapitulatif de l'utilisation) permet d'afficher des statistiques sur l'utilisation des interfaces.

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Table Views** (Vues sous forme de tables) → **Utilization Summary** (Récapitulatif de l'utilisation) dans l'arborescence.

Figure 9-5. Page **Utilization Summary** (Récapitulatif de l'utilisation)

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area is titled "Utilization Summary" and includes a "Unit" dropdown menu set to "1" and a "Refresh Rate" dropdown menu set to "No Refresh". Below these are two tables. The first table shows interface utilization for three interfaces: 1/g1 (Up, 0% utilization, 0% unicast received, 0% non-unicast received, 0% error packets received), 1/g2 (Down, 0% utilization, 0% unicast received, 0% non-unicast received, 0% error packets received), and 1/g3 (Up, 0% utilization, 0% unicast received, 0% non-unicast received, 0% error packets received). The second table shows Global System L200 statistics for eight channels (ch1 to ch8), all of which are Down with 0% utilization, 0% unicast received, 0% non-unicast received, and 0% error packets received.

Interface	Interface Status	Interface Utilization %	Unicast Received %	Non Unicast Packets Received %	Error Packets Received %
1 1/g1	Up	0	0	0	0
2 1/g2	Down	0	0	0	0
3 1/g3	Up	0	0	0	0

Global System L200	Interface Status	Interface Utilization %	Unicast Received %	Non Unicast Packets Received %	Error Packets Received %
1 ch1	Down	0	0	0	0
2 ch2	Down	0	0	0	0
3 ch3	Down	0	0	0	0
4 ch4	Down	0	0	0	0
5 ch5	Down	0	0	0	0
6 ch6	Down	0	0	0	0
7 ch7	Down	0	0	0	0
8 ch8	Down	0	0	0	0

Cette page contient les champs suivants :

Unit (Unité) : indique l'unité correspondant aux statistiques affichées.

Refresh Rate (Taux de rafraîchissement) : indique l'intervalle entre deux rafraîchissements des statistiques. Les valeurs possibles sont No Refresh (Aucun rafraîchissement), 15, 30 ou 60 secondes. La valeur par défaut est No Refresh (Aucun rafraîchissement).

Interface : indique l'interface correspondant aux statistiques affichées.

Interface Status (État de l'interface) : indique l'état de l'interface.

Interface Utilization % (% d'utilisation de l'interface) : indique le pourcentage d'utilisation de l'interface réseau, basé sur le mode duplex. Les valeurs admises sont comprises entre 0 et 200%. La valeur maximale (200%) pour une connexion en mode duplex intégral indique que 100% de la bande passante des connexions entrantes et sortantes est utilisé par le trafic qui transite par l'interface. La valeur maximale pour une connexion en mode semi duplex est de 100 %.

Unicast Received % (% de paquets monodiffusion reçus) : indique le pourcentage de paquets monodiffusion reçus sur l'interface.

Non Unicast Packets Received % (% de paquets non-monodiffusion reçus) : indique le pourcentage de paquets non-monodiffusion reçus sur l'interface.

Error Packets Received % (% de paquets avec erreurs reçus) : indique le pourcentage de paquets contenant des erreurs ayant été reçus sur l'interface.

Affichage de statistiques concernant l'utilisation des interfaces à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 RMON Commands (Commandes RMON)

Récapitulatif des compteurs

La page **Counter Summary** (Récapitulatif des compteurs) permet d'afficher des statistiques sur l'utilisation des interfaces sous forme numérique et non sous forme de pourcentages.

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Table Views** (Vues sous forme de tables) → **Counter Summary** (Récapitulatif des compteurs) dans l'arborescence.

Figure 9-6. Page Counter Summary (Récapitulatif des compteurs)

Interface	Interface Status	Received Unicast Packets	Transmit Unicast Packets	Received Non Unicast Packets	Transmit Non Unicast Packets	Received Errors	Transmit Errors
1 1/g1	Up	6639523	6339	365902	133900	0	0
2 1/g2	Down	0	0	0	0	0	0
3 1/g3	Down	0	0	0	0	0	0

Global System LAGs	Status	Received Unicast Packets	Transmit Unicast Packets	Received Non Unicast Packets	Transmit Non Unicast Packets	Received Errors	Transmit Errors
1 ch1	Down	0	0	0	0	0	0
2 ch2	Down	0	0	0	0	0	0
3 ch3	Down	0	0	0	0	0	0
4 ch4	Down	0	0	0	0	0	0
5 ch5	Down	0	0	0	0	0	0
6 ch6	Down	0	0	0	0	0	0
7 ch7	Down	0	0	0	0	0	0
8 ch8	Down	0	0	0	0	0	0

Cette page contient les champs suivants :

Unit (Unité) : indique l'unité correspondant aux statistiques affichées.

Refresh Rate (Taux de rafraîchissement) : indique l'intervalle entre deux rafraîchissements des statistiques. Les valeurs possibles sont No Refresh (Aucun rafraîchissement), 15, 30 ou 60 secondes. La valeur par défaut est No Refresh (Aucun rafraîchissement).

Interface : indique l'interface correspondant aux statistiques affichées.

Interface Status (État de l'interface) : indique l'état de l'interface.

Received Unicast Packets (Paquets monodiffusion reçus) : indique le nombre de paquets monodiffusion reçus sur l'interface.

Transmit Unicast Packets (Paquets monodiffusion transmis) : indique le nombre de paquets monodiffusion transmis à partir de l'interface.

Received Non Unicast Packets (Paquets non-monodiffusion reçus) : indique le nombre de paquets non-monodiffusion reçus sur l'interface.

Transmit Non Unicast Packets (Paquets non-monodiffusion transmis) : indique le nombre de paquets non-monodiffusion transmis à partir de l'interface.

Received Errors (Erreurs reçues) : indique le nombre d'erreurs reçues sur l'interface.

Transmit Errors (Erreurs transmises) : indique le nombre d'erreurs transmises à partir de l'interface.

Définition du taux de rafraîchissement

1. Affichez la page **Counter Summary** (Récapitulatif des compteurs).
2. Sélectionnez le taux de rafraîchissement voulu dans le menu déroulant **Refresh Rate**.

Les statistiques sur les interfaces affichées seront actualisées en fonction de la fréquence sélectionnée.

Affichage de statistiques numériques sur l'utilisation des ports à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

1. RMON Commands (Commandes RMON)

RMON

La fonction Remote Monitoring (RMON) permet à l'administrateur réseau de contrôler à distance les performances et l'état du réseau.

Pour afficher la page **RMON**, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **RMON** dans l'arborescence. Cette page contient des liens vers les fonctionnalités suivantes :

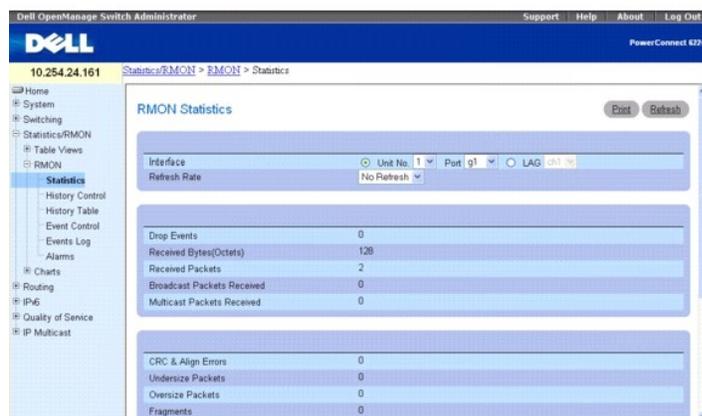
1. [Statistiques RMON](#)
1. [Statistiques de contrôle de l'historique RMON](#)
1. [Table d'historique RMON](#)
1. [Contrôle des événements RMON](#)
1. [Journal des événements RMON](#)
1. [Alarmes RMON](#)

Statistiques RMON

La page **RMON Statistics** (Statistiques RMON) permet d'afficher des informations sur l'utilisation du commutateur : statistiques de traitement des paquets, erreurs, etc.

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **RMON** → **Statistics** (Statistiques) dans l'arborescence.

Figure 9-7. Page RMON Statistics (Statistiques RMON)



Cette page contient les champs suivants :

Interface : indique si les statistiques affichées concernent une unité ou un LAG, et quel LAG/unité est affiché.

Refresh Rate (Taux de rafraîchissement) : indique l'intervalle entre deux rafraîchissements des statistiques. Les valeurs possibles sont No Refresh (Aucun rafraîchissement), 15, 30 ou 60 secondes. La valeur par défaut est No Refresh (Aucun rafraîchissement).

Drop Events (Événements rejetés) : indique le nombre d'événements ayant été rejetés sur l'interface depuis la dernière actualisation du commutateur.

Received Bytes (Octets) (Octets reçus) : indique le nombre d'octets reçus sur l'interface depuis la dernière actualisation du commutateur. Ce nombre inclut les paquets incorrects et les octets de contrôle de trames (FCS), mais pas les bits de synchronisation des trames.

Received Packets (Paquets reçus) : indique le nombre de paquets reçus sur l'interface depuis la dernière actualisation du commutateur, y compris les paquets non valides et les paquets de multidiffusion et de diffusion.

Broadcast Packets Received (Paquets de diffusion reçus) : indique le nombre de paquets de diffusion valides reçus sur l'interface depuis la dernière actualisation du commutateur. Ce nombre n'inclut pas les paquets multidiffusion.

Multicast Packets Received (Paquets multidiffusion reçus) : indique le nombre de paquets multidiffusion valides reçus sur l'interface depuis la dernière actualisation du commutateur.

CRC & Align Errors (Erreurs de CRC et d'alignement) : indique le nombre d'erreurs de CRC et d'alignement qui se sont produites sur l'interface depuis la dernière actualisation du commutateur.

Undersize Packets (Paquets de longueur insuffisante) : indique le nombre de paquets de moins de 64 octets ayant été reçus sur l'interface depuis la dernière actualisation du commutateur.

Oversize Packets (Paquets de longueur excessive) : indique le nombre de paquets de plus de 1518 octets ayant été reçus sur l'interface depuis la dernière actualisation du commutateur.

Fragments : indique le nombre de fragments (paquets de moins de 64 octets, sans les bits de synchronisation des trames mais avec les octets de contrôle FCS) ayant été reçus sur l'interface depuis la dernière actualisation du commutateur.

Jabbers (Jabotages) : indique le nombre de paquets de plus de 1518 octets et possédant un FCS qui ont été reçus pendant la session d'échantillonnage.

Collisions : indique le nombre de collisions ayant été reçues sur l'interface depuis la dernière actualisation du commutateur.

Frames of 64 Bytes (Trames de 64 octets) : indique le nombre de trames de 64 octets ayant été reçues sur l'interface depuis la dernière actualisation du commutateur.

Frames of 65 to 127 Bytes (Trames de 65 à 127 octets) : indique le nombre de trames de 65 à 127 octets ayant été reçues sur l'interface depuis la dernière actualisation du commutateur.

Frames of 128 to 255 Bytes (Trames de 128 à 255 octets) : indique le nombre de trames de 128 à 255 octets ayant été reçues sur l'interface depuis la dernière actualisation du commutateur.

Frames of 256 to 511 Bytes (Trames de 256 à 511 octets) : indique le nombre de trames de 256 à 511 octets ayant été reçues sur l'interface depuis la dernière actualisation du commutateur.

Frames of 512 to 1023 Bytes (Trames de 512 à 1023 octets) : indique le nombre de trames de 512 à 1023 octets ayant été reçues sur l'interface depuis la dernière actualisation du commutateur.

Frames of 1024 to 1518 Bytes (Trames de 1024 à 1518 octets) : indique le nombre de trames de 1024 à 1518 octets ayant été reçues sur l'interface depuis la dernière actualisation du commutateur.

Affichage de statistiques sur les interfaces

1. Affichez la page **RMON Statistics Group** (Groupe de statistiques RMON).
2. Sélectionnez une interface dans le champ approprié.

Les statistiques concernant cette interface s'affichent.

Affichage de statistiques RMON à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 RMON Commands (Commandes RMON)

Statistiques de contrôle de l'historique RMON

La page **RMON History Control** (Contrôle de l'historique RMON) permet de conserver un historique des statistiques sur chaque port. Pour chaque interface (port physique ou canal d'un port), il est possible de définir le nombre de jetons existants, ainsi que l'intervalle entre chaque cliché de jeton.

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **RMON** → **History Control** (Contrôle de l'historique) dans l'arborescence.

Figure 9-8. Page RMON History Control (Contrôle de l'historique RMON)



Cette page contient les champs suivants :

History Entry (Entrée de l'historique) : permet de sélectionner le numéro d'entrée de la table de contrôle de l'historique RMON.

Source Interface (Interface source) : indique l'interface à partir de laquelle les échantillons de l'historique ont été collectés.

Owner (0-20 characters) (Propriétaire, 0-20 caractères) : indique la station ou l'utilisateur RMON qui a demandé les informations RMON.

Max No. of Samples to Keep (1-65535) (Nombre maximum d'échantillons à conserver, 1-65535) : indique le nombre de jetons d'historique correspondant à cette interface.

Current No. of Samples in List (Nombre actuel d'échantillons dans la liste) : indique le nombre d'échantillons existants.

Sampling Interval (1-3600) (Intervalle d'échantillonnage, 1-3600) : indique la fréquence à laquelle des échantillons sont collectés sur les ports. Les valeurs admises vont de 1 à 3600 secondes. La valeur par défaut est de 1800 secondes (30 minutes).

Remove (Supprimer) : si cette option est cochée, l'entrée correspondante est supprimée de la **table de contrôle de l'historique**.

Ajout d'une entrée dans le contrôle de l'historique

1. Affichez la page **RMON History Control** (Contrôle de l'historique RMON).
2. Cliquez sur **Add** (Ajouter).

La page **Add History Entry** (Ajouter une entrée à l'historique) s'affiche.

Figure 9-9. Page Add History Entry (Ajouter une entrée à l'historique)



3. Complétez les champs de cette page et cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est ajoutée à la **table de contrôle de l'historique RMON**.

Affichage de la table de contrôle de l'historique RMON

1. Affichez la page **RMON History Control** (Contrôle de l'historique RMON).
2. Cliquez sur **Show All** (Afficher tout).

La **table de contrôle de l'historique RMON** s'affiche.

Figure 9-10. Page RMON History Control Table (Table de contrôle de l'historique RMON)

History Control Table Print Refresh

History Entry No.	Source Interface	Sampling Interval	Current Number of Samples	Owner	Remove
1	1/g1	1000	10		<input type="checkbox"/>

Apply Changes Back

Suppression d'une entrée de la table de contrôle de l'historique

1. Affichez la page **RMON History Control** (Contrôle de l'historique RMON).
2. Cochez la case **Remove** (Supprimer) située sur la ligne correspondant à l'entrée d'historique à supprimer.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est supprimée et le périphérique est mis à jour.

Affichage de statistiques d'historique RMON à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 RMON Commands (Commandes RMON)

Table d'historique RMON

La page RMON History Table (Table d'historique RMON) permet d'afficher des échantillons de statistiques réseau relatifs à une interface spécifique. Chaque entrée représente l'ensemble des valeurs de compteur compilées lors d'une session d'échantillonnage.

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **RMON** → **History Table** (Table d'historique) dans l'arborescence.

Figure 9-11. Page RMON History Table (Table d'historique RMON)

The screenshot shows the Dell OpenManage Switch Administrator interface. The main content area displays the 'RMON History Table' with a 'Print' and 'Refresh' button. Below the table, there is a detailed table of statistics.

Sample Drop No.	Events	Received Bytes (Octets)	Received Packets	Broadcast Packets	Multicast Packets	CRC Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Utilization
1	0	49595	210	42	13	0	0	0	0	0	0	0

Cette page contient les champs suivants :

History Entry No. (Numéro d'entrée de l'historique) : permet de sélectionner le numéro de l'entrée à afficher dans la **table d'historique RMON**.

Owner (Propriétaire) : indique le nom du propriétaire du groupe de statistiques RMON, le cas échéant.

Source Interface (Interface source) : indique l'interface ou le LAG correspondant aux statistiques collectées.

Max No. of Samples to Keep (Nombre maximal d'échantillons à conserver) : définit la longueur de la liste correspondant à chaque entrée dans la table d'historique.

Sampling Interval (Intervalle d'échantillonnage) : définit le délai (en secondes) écoulé entre deux échantillons successifs.

Sample No. (Numéro d'échantillon) : indique l'échantillon auquel se rapportent les informations affichées dans la table.

Drop Events (Événements rejetés) : indique le nombre total d'événements concernant des paquets rejetés par le port en raison d'une insuffisance de ressources. Ce nombre ne correspond pas nécessairement au nombre de paquets rejetés. Il s'agit simplement du nombre de fois où cette condition précise a été détectée.

Received Bytes (Octets) (Nombre d'octets reçus) : indique le nombre total d'octets de données (paquets non valides compris) reçus sur le réseau, sans les bits de synchronisation des trames mais avec les octets de contrôle FCS.

Received Packets (Paquets reçus) : indique le nombre total de paquets reçus durant l'intervalle d'échantillonnage, y compris les paquets non valides et les paquets multidiffusion et de diffusion.

Broadcast Packets (Paquets de diffusion) : indique le nombre total de paquets valides reçus qui ont été dirigés vers l'adresse de diffusion. Ce nombre n'inclut pas les paquets multidiffusion.

Multicast Packets (Paquets multidiffusion) : indique le nombre total de paquets valides reçus qui ont été dirigés vers l'adresse de multidiffusion. Ce nombre n'inclut pas les paquets dirigés vers l'adresse de diffusion.

CRC Align Errors (Erreurs de CRC et d'alignement) : indique le nombre total de paquets reçus dont la taille se situe entre 64 et 1518 octets (sans les bits de synchronisation des trames mais avec les octets de contrôle FCS), et possédant un FCS incorrect avec un nombre d'octets entier (erreur de FCS) ou non entier (erreur d'alignement).

Undersize Packets (Paquets de longueur insuffisante) : indique le nombre total de paquets reçus dont le format était valide mais dont la longueur était inférieure à 64 octets (sans les bits de synchronisation des trames mais avec les octets de contrôle FCS).

Oversize Packets (Paquets trop longs) : indique le nombre total de paquets reçus dont le format était valide mais dont la longueur dépassait 1518 octets (sans les bits de synchronisation des trames mais avec les octets de contrôle FCS).

Fragments : indique le nombre total de paquets reçus de moins de 64 octets (sans les bits de synchronisation des trames mais avec les octets de contrôle FCS) et possédant un FCS incorrect avec un nombre d'octets entier (erreur de FCS) ou non entier (erreur d'alignement).

Jabbers (Jabotages) : indique le nombre total de paquets reçus de plus de 1518 octets (sans les bits de synchronisation des trames mais avec les octets de contrôle FCS) et possédant un FCS incorrect avec un nombre d'octets entier (erreur de FCS) ou non entier (erreur d'alignement).

Collisions : indique une évaluation optimale du nombre total de collisions détectées sur ce segment Ethernet.

Utilization (Utilisation) : évalue l'utilisation réseau de la couche physique principale constatée sur une interface lors de la session d'échantillonnage. Cette valeur est représentée par un pourcentage.

Affichage de statistiques sur une entrée spécifique de l'historique

1. Affichez la page **RMON History Table** (Table d'historique RMON).
2. Sélectionnez une entrée dans le champ **History Entry No.** (Numéro d'entrée de l'historique).

Les statistiques correspondantes s'affichent.

Affichage du contrôle de l'historique RMON à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 RMON Commands (Commandes RMON)

Contrôle des événements RMON

La page **RMON Events Control** (Contrôle des événements RMON) permet de définir des événements RMON. Ceux-ci sont utilisés par les alarmes RMON pour déclencher certaines actions lorsque le seuil maximal autorisé pour un compteur RMON est dépassé. Les informations sur les événements peuvent être consignées dans un journal et/ou envoyées sous forme d'interruptions vers un récepteur d'interruptions.

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **RMON** → **Event Control** (Contrôle des événements) dans l'arborescence.

Figure 9-12. Page RMON Event Control (Contrôle des événements RMON)

Event Entry	1
Community	public
Description	general access
Event Type	Log and Trap
Time	96079
Owner	

Cette page contient les champs suivants :

Event Entry (Événement) : permet de sélectionner un événement.

Community (Communauté) : indique la communauté à laquelle l'événement est associé.

Description : indique la description de l'événement définie par l'utilisateur.

Event Type (Type d'événement) : permet de sélectionner un événement. Ce champ peut prendre les valeurs suivantes :

Log (Journal) : indique que l'événement est une entrée de journal.

Trap (Interruption) : indique que l'événement est une interruption.

Log and Trap (Journalisation et Interruption) : indique que l'événement est à la fois une entrée de journal et une interruption.

None (Aucun) : aucun événement.

Time (Heure) : indique l'heure à laquelle l'événement s'est produit.

Owner (Propriétaire) : identifie le commutateur ou l'utilisateur qui a défini l'événement.

Remove (Supprimer) : si cette option est cochée, l'événement correspondant est supprimé de la table des événements.

Ajout d'un événement RMON

1. Affichez la page **RMON Event Control** (Contrôle des événements RMON).
2. Cliquez sur **Add** (Ajouter).

La page **Add an Event Entry** (Ajouter un événement) s'affiche.

Figure 9-13. Page Add an Event Entry (Ajouter un événement)

Event Entry	2
Community	
Description	
Event Type	None
Owner	

3. Complétez les champs de cette page.
 4. Cliquez sur **Apply Changes** (Appliquer les modifications).
- L'entrée est ajoutée à la **table des événements RMON** et le périphérique est mis à jour.

Modification d'un événement RMON

1. Affichez la page **RMON Event Control** (Contrôle des événements RMON).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Event Control Table** (Table de contrôle des événements).
3. Cochez la case **Edit** (Modifier) associée à l'événement à modifier.
4. Modifiez les champs de cette page selon vos besoins.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est modifiée et le périphérique est mis à jour.

Affichage de la table de contrôle des événements RMON

1. Affichez la page **RMON Event Control** (Contrôle des événements RMON).
2. Cliquez sur **Show All** (Afficher tout).

La **table de contrôle des événements** s'affiche.

Figure 9-14. Page Event Control Table (Table de contrôle des événements)



Suppression d'événements RMON

1. Affichez la page **RMON Event Control** (Contrôle des événements RMON).
2. Sélectionnez l'événement à supprimer dans le menu déroulant **Event Entry** (Événement) et cochez l'option **Remove** (Supprimer).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est supprimée et le périphérique est mis à jour.

Définition des événements du commutateur à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

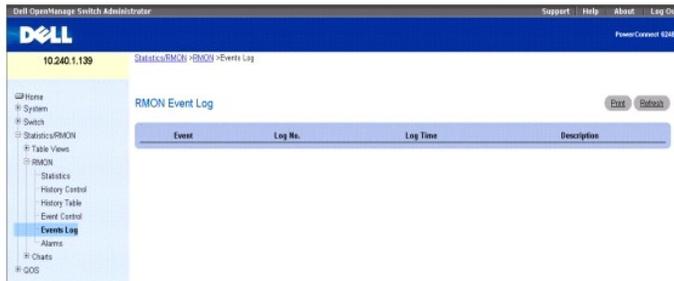
- 1 RMON Commands (Commandes RMON)

Journal des événements RMON

La page **RMON Event Log** (Journal des événements RMON) permet d'afficher la liste des événements RMON.

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **RMON** → **Events Log** (Journal des événements) dans l'arborescence.

Figure 9-15. Page RMON Event Log (Journal des événements RMON)



Cette page contient les champs suivants :

Event (Événement) : affiche le numéro de l'entrée dans le journal des événements RMON.

Log No. (Numéro de consignation) : indique le numéro de consignation.

Log Time (Heure de consignation) : indique l'heure à laquelle l'entrée a été consignée dans le journal.

Description : affiche une description de l'entrée consignée.

Définition des événements du commutateur à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

- 1 RMON Commands (Commandes RMON)

Alarmes RMON

La page **RMON Alarms** (Alarmes RMON) permet de définir des alarmes réseau. Les alarmes sont déclenchées lorsque certains seuils définis pour les compteurs RMON sont dépassés. Elles provoquent la création d'un événement. Ces événements peuvent être configurés comme faisant partie du groupe d'événements RMON. Pour plus d'informations sur les événements, voir [Journal des événements RMON](#).

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **RMON** → **Alarms** (Alarmes) dans l'arborescence.

Figure 9-16. Page RMON Alarms (Alarmes RMON)



Cette page contient les champs suivants :

Alarm Entry (Alarme) : permet de sélectionner une alarme spécifique dans le menu déroulant.

OID (ID d'objet) : indique l'identificateur de l'objet.

Counter Value (Valeur du compteur) : indique le nombre d'événements sélectionnés ayant été recensés.

Sample Type (Type d'échantillon) : indique la méthode d'échantillonnage utilisée pour la variable sélectionnée et compare sa valeur aux seuils. Les valeurs possibles sont les suivantes :

Delta (Différence) : soustrait la valeur du dernier échantillon de la valeur en cours. La différence entre ces valeurs est comparée au seuil.

Absolute (Valeur absolue) : compare les valeurs directement avec les seuils à la fin de l'intervalle d'échantillonnage. Il s'agit de la valeur par défaut. Il s'agit du comportement par défaut.

Rising Threshold (0-2147483647) (Seuil en hausse, 0 à 2147483647) : indique la valeur de hausse du compteur qui déclenche l'alarme de seuil en hausse. Le seuil en hausse est représenté dans la partie supérieure des histogrammes. Une couleur spécifique est associée à chaque variable contrôlée. La valeur par défaut est de 100.

Rising Event (Événement déclenché en cas de hausse) : définit le mécanisme de signalement des alarmes (journalisation, interruption ou les deux). Si la journalisation est sélectionnée, aucun mécanisme d'enregistrement n'est activé sur le commutateur ni dans le système de gestion. Toutefois, si le commutateur n'est pas en cours de réinitialisation, l'événement est conservé dans la table des journaux du commutateur. Si l'option sélectionnée est Trap (Interruption), une interruption SNMP est générée et signalée au moyen du mécanisme correspondant. L'interruption peut être enregistrée à l'aide de ce même mécanisme.

Falling Threshold (0-2147483647) (Seuil en baisse, 0 à 2147483647) : indique la valeur de baisse du compteur qui déclenche l'alarme de seuil en baisse. Le seuil en baisse est représenté dans la partie supérieure des histogrammes. Une couleur spécifique est associée à chaque variable contrôlée. La valeur par défaut est de 20.

Falling Event (Événement déclenché en cas de baisse) : définit le mécanisme de signalement des alarmes (journalisation, interruption ou les deux). Si la journalisation est sélectionnée, aucun mécanisme d'enregistrement n'est activé sur le commutateur ni dans le système de gestion. Toutefois, si le commutateur n'est pas en cours de réinitialisation, l'événement est conservé dans la table des journaux du commutateur. Si l'option sélectionnée est Trap (Interruption), une interruption SNMP est générée et signalée au moyen du mécanisme correspondant. L'interruption peut être enregistrée à l'aide de ce même mécanisme.

Startup Alarms (Alarmes de démarrage) : définit le type d'événement. Les options possibles sont les suivantes : rising (en hausse), rising-falling (en hausse/baisse) et falling (en baisse).

Interval (0-2147483647) (Intervalle, 0 à 2147483647) : affiche l'intervalle entre deux alarmes. La valeur par défaut est de 100.

Owner (Propriétaire) : indique le commutateur ou l'utilisateur ayant défini l'alarme.

Remove (Supprimer) : si cette option est cochée, l'alarme RMON correspondante est supprimée.

Ajout d'une entrée dans la table des alarmes

1. Affichez la page **RMON Alarms** (Alarmes RMON).
2. Cliquez sur **Add** (Ajouter).

La page **Add an Alarm Entry** (Ajouter une alarme) s'affiche.

Figure 9-17. Page Add an Alarm Entry (Ajouter une alarme)

Add an Alarm Entry End Refresh

Alarm Entry	1
OID	
Sample Type	Absolute
Rising Threshold (0 to 2147483647)	
Rising Event	
Falling Threshold (0 to 2147483647)	
Falling Event	
Startup Alarms	Rising
Interval (0 to 2147483647)	(Sec)
Owner	

Apply Changes Back

3. Complétez les champs de cette page selon vos besoins.
 4. Cliquez sur **Apply Changes** (Appliquer les modifications).
- L'alarme RMON est ajoutée et le périphérique est mis à jour.

Affichage de la table des alarmes

1. Affichez la page **RMON Alarms** (Alarmes RMON).
 2. Cliquez sur **Show All** (Afficher tout).
- La partie gauche de la **table des alarmes RMON** s'affiche.

Figure 9-18. Page RMON Alarms Table (Table des alarmes RMON)

RMON Alarms Table End Refresh

Alarm Entry	OID	Counter Value	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event
1		0	Absolute	10	1	20	2

Apply Changes Back

3. Cliquez sur la flèche vers la droite située au bas de l'écran pour afficher la partie droite de la table.

Suppression d'une entrée de la table des alarmes

1. Affichez la page **RMON Alarms** (Alarmes RMON).
 2. Sélectionnez une entrée dans le menu déroulant **Alarm Entry**.
 3. Cochez la case **Remove** (Supprimer) puis cliquez sur **Apply Changes** (Appliquer les modifications).
- L'entrée est supprimée et le périphérique est mis à jour.

Suppression de plusieurs entrées de la table des alarmes

1. Affichez la page **RMON Alarms** (Alarmes RMON).
 2. Cliquez sur **Show All** (Afficher tout).
- La **table des alarmes RMON** s'affiche.
3. Cochez la case **Remove** (Supprimer) en regard de chaque alarme à supprimer.
 4. Cliquez sur **Apply Changes** (Appliquer les modifications).
- Les entrées sont supprimées et le périphérique est mis à jour.

Définition des alarmes du commutateur à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous au chapitre suivant du document CLI Reference Guide (Guide de référence CLI) :

Diagrammes

La page **Chart** (Graphiques) contient des liens vers des pages Web qui permettent de visualiser les statistiques sous forme de graphiques. Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Charts** (Diagrammes) dans l'arborescence. Cette page contient des liens vers les fonctionnalités suivantes :

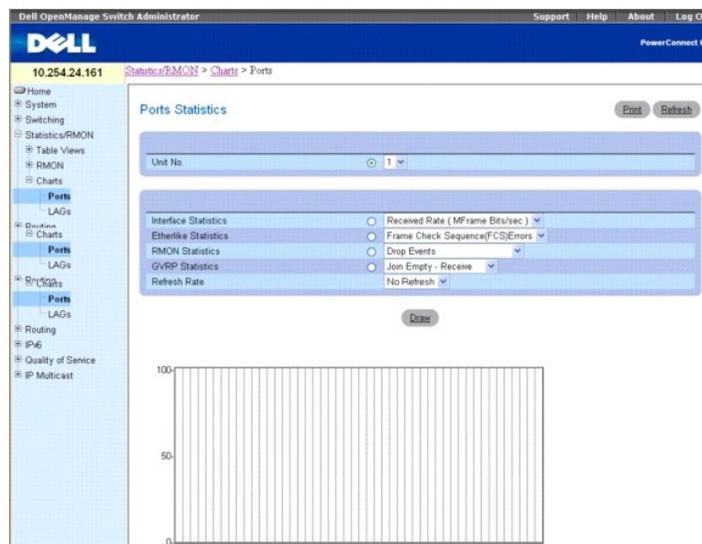
- 1 [Statistiques sur les ports](#)
- 1 [Statistiques sur les LAG](#)

Statistiques sur les ports

La page **Ports Statistics** (Statistiques sur les ports) permet d'afficher les statistiques relatives aux ports sous forme de graphique.

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Charts** (Diagrammes) → **Ports** dans l'arborescence.

Figure 9-19. Page Ports Statistics (Statistiques sur les ports)



Cette page contient les champs suivants :

Unit No. (Numéro d'unité) : permet de sélectionner le port à afficher.

Interface Statistics (Statistiques sur les interfaces) : cette option permet de sélectionner les statistiques sur les interfaces et d'utiliser le menu déroulant pour choisir le type de statistiques à représenter sous forme de graphique. La valeur par défaut est Received Rate (MFrame Bits/sec) (Vitesse de réception, MFrame Bits/s).

Etherlike Statistics (Statistiques Etherlike) : cette option permet de sélectionner les statistiques Etherlike et d'utiliser le menu déroulant pour choisir le type de statistiques à représenter sous forme de graphique. La valeur par défaut est Frame Check Sequence (FCS) Errors (Erreurs de séquence de contrôle de trame [FCS]).

RMON Statistics (Statistiques RMON) : cette option permet de sélectionner les statistiques RMON et d'utiliser le menu déroulant pour choisir le type de statistiques à représenter sous forme de graphique. La valeur par défaut est Drop Events (Événements rejetés).

GVRP Statistics (Statistiques GVRP) : cette option permet de sélectionner les statistiques GVRP et d'utiliser le menu déroulant pour choisir le type de statistiques à représenter sous forme de graphique. La valeur par défaut est Join Empty - Receive (Join Empty - Réception).

Refresh Rate (Taux de rafraîchissement) : indique l'intervalle entre deux rafraîchissements des statistiques. Les valeurs possibles sont No Refresh (Aucun rafraîchissement), 15, 30 ou 60 secondes. La valeur par défaut est No Refresh (Aucun rafraîchissement).

Affichage de statistiques sur les ports

1. Affichez la page **Ports Statistics** (Statistiques sur les ports).
2. Sélectionnez le port pour lequel vous souhaitez afficher un graphique de statistiques.
3. Cliquez sur le bouton radio associé aux statistiques voulues.

- Sélectionnez le type de statistiques dans le menu déroulant associé.
- Sélectionnez un intervalle de rafraîchissement dans le menu **Refresh Rate**.
- Cliquez sur **Draw** (Créer le graphique).

Les statistiques sélectionnées sont présentées sous forme de graphique.

Affichage de statistiques sur les ports à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous aux chapitres suivants du document CLI Reference Guide (Guide de référence CLI) :

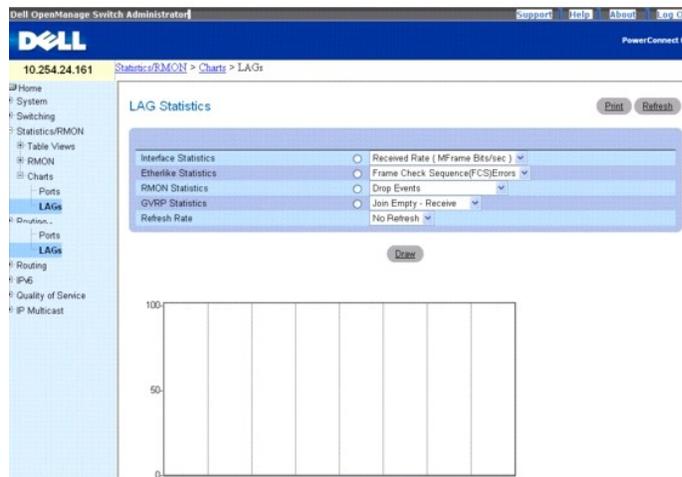
- 1 System Management Commands (Commandes de gestion du système)
- 1 RMON Commands (Commandes RMON)
- 1 GVRP Commands (Commandes GVRP)

Statistiques sur les LAG

La page **LAG Statistics** (Statistiques sur les LAG) permet d'afficher les statistiques relatives aux LAG sous forme de graphique.

Pour afficher cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Charts** (Diagrammes) → **LAGs** dans l'arborescence.

Figure 9-20. Page LAG Statistics (Statistiques sur les LAG)



Cette page contient les champs suivants :

Interface Statistics (Statistiques sur les interfaces) : cette option permet de sélectionner les statistiques sur les interfaces et d'utiliser le menu déroulant pour choisir le type de statistiques à représenter sous forme de graphique. La valeur par défaut est Received Rate (Vitesse de réception).

Etherlike Statistics (Statistiques Etherlike) : cette option permet de sélectionner les statistiques Etherlike et d'utiliser le menu déroulant pour choisir le type de statistiques à représenter sous forme de graphique. La valeur par défaut est Frame Check Sequence Errors (Erreurs de séquence de contrôle de trame).

RMON Statistics (Statistiques RMON) : cette option permet de sélectionner les statistiques RMON et d'utiliser le menu déroulant pour choisir le type de statistiques à représenter sous forme de graphique. La valeur par défaut est Drop Events (Événements rejetés).

GVRP Statistics (Statistiques GVRP) : cette option permet de sélectionner les statistiques GVRP et d'utiliser le menu déroulant pour choisir le type de statistiques à représenter sous forme de graphique. La valeur par défaut est Join Empty - Receive (Join Empty - Réception).

Refresh Rate (Taux de rafraîchissement) : indique l'intervalle entre deux rafraîchissements des statistiques. Les valeurs possibles sont No Refresh (Aucun rafraîchissement), 15, 30 ou 60 secondes. La valeur par défaut est de 15 secondes.

Affichage de statistiques sur les LAG

- Affichez la page **LAG Statistics** (Statistiques sur les LAG).
- Cliquez sur le bouton radio associé aux statistiques voulues.

3. Sélectionnez le type de statistiques dans le menu déroulant associé.
4. Sélectionnez un intervalle de rafraîchissement dans le menu **Refresh Rate**.
5. Cliquez sur **Draw** (Créer le graphique).

Les statistiques sélectionnées sont présentées sous forme de graphique.

Affichage de statistiques sur les LAG à l'aide des commandes CLI

Pour plus d'informations sur les commandes CLI permettant d'exécuter cette fonction, reportez-vous aux chapitres suivants du document CLI Reference Guide (Guide de référence CLI) :

- | System Management Commands (Commandes de gestion du système)
- | RMON Commands (Commandes RMON)
- | GVRP Commands (Commandes GVRP)

[Retour au sommaire](#)