Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

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 dommage ou d'une perte de données potentiels et vous indique comment éviter ce problème.

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

Mars 2005

Retour au sommaire

Introduction

Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

Le PowerConnect 3424/3448 et le PowerConnect 3424P/3448P sont des unités évoluées et empilables multicouches. Ils peuvent fonctionner en tant que commutateurs autonomes ou être intégrés à une pile de six unités maximum.

Le *Guide d'utilisation* contient les informations relatives à l'installation, la configuration et la gestion de l'unité.

Description du système

Le PowerConnect 3424/3448 et le PowerConnect 3424P/3448P combinent des qualités de polyvalence avec des besoins minimes en termes de gestion. Les séries 3424 et 3448 englobent les types d'unités suivants :

- PowerConnect 3424
- PowerConnect 3424P
- PowerConnect 3448
- PowerConnect 3448P

PowerConnect 3424

Le PowerConnect 3424 comporte 24 ports à 10/100 Mbps, 2 ports SFP et 2 ports cuivre qui peuvent être utilisés pour la gestion du trafic, si l'unité est utilisée en autonome, ou comme ports d'empilage si l'unité fait partie d'une pile. Le PowerConnect comprend également un port de console RS-232. Il peut être utilisé dans une pile ou en autonome.

PowerConnect 3424P

Le PowerConnect 3424P comporte 24 ports à 10/100 Mbps, 2 ports SFP et 2 ports cuivre qui peuvent être utilisés pour la gestion du trafic, si l'unité est utilisée en autonome, ou comme ports d'empilage si l'unité fait partie d'une pile. Il comprend également un port de console RS-232. Il peut être utilisé dans une pile ou en autonome, et offre également la fonction Power over Ethernet (PoE).

Figure 1-1. PowerConnect 3424 et PowerConnect 3424P

PowerConnect 3448

Le PowerConnect 3448 comporte 48 ports à 10/100 Mbps, 2 ports SFP et 2 ports cuivre qui peuvent être utilisés pour la gestion du trafic, si l'unité est utilisée en autonome, ou comme ports d'empilage si l'unité fait partie d'une pile. Il comprend également un port de console RS-232. Il peut être utilisé dans une pile ou en autonome.

PowerConnect 3448P

Le PowerConnect 3448P comporte 48 ports à 10/100 Mbps, 2 ports SFP et 2 ports cuivre qui peuvent être utilisés pour la gestion du trafic, si l'unité est utilisée en autonome, ou comme ports d'empilage si l'unité fait partie d'une pile. Il comprend également un port de console RS-232, et offre également la fonction Power over Ethernet (PoE).

Figure 1-2. PowerConnect 3448 et PowerConnect 3448P

Présentation de l'empilage

L'empilage d'unités PowerConnect 3424P et 3448P permet la gestion de plusieurs commutateurs à travers un point unique, comme si l'ensemble des membres de la piles constituaient une seule unité. Tous les membres de la pile sont gérés et accessibles via une adresse IP unique. La pile peut-être gérée de différentes façons :

- Via une interface Web
- Via une station de gestion SNMP
- À l'aide de l'interface de ligne de commande (interface CLI)

Les unités PowerConnect 3424/P et PowerConnect 3448/P peuvent être empilées (jusqu'à six unités par pile) ou fonctionner en autonome.

Lors de la configuration de la pile, un commutateur est désigné comme étant l'unité maître. Il est possible de configurer un autre membre de la pile en tant qu'unité maître de secours. Toutes les unités sont configurées comme étant des membres de la pile et associées à un ID unique.

Les logiciels du commutateur sont téléchargés séparément pour chaque membre de la pile. Cependant, toutes les unités de la pile doivent exécuter les mêmes versions de logiciels.

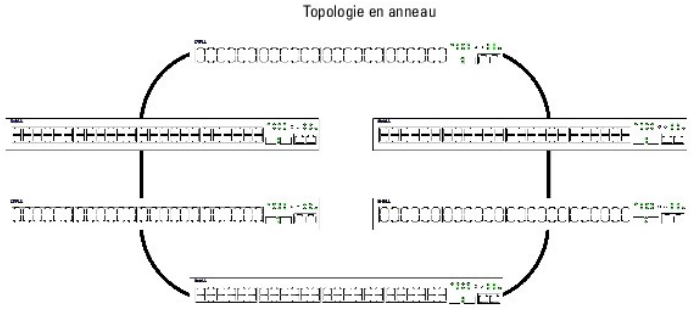
L'unité maître assure la gestion et la configuration de la pile. Elle détecte et reconfigure les ports avec un impact minimal sur son fonctionnement lorsque les événements suivants se produisent :

- Panne d'une unité
- Perte de la liaison entre les unités
- Insertion d'une unité
- Retrait d'une unité

Topologie de la pile

Les unités de la série PowerConnect 3400 fonctionnent dans une topologie en anneau. Une topologie en anneau est une configuration dans laquelle toutes les unités de la pile sont reliées entre elles de manière à former une boucle. Chaque unité reçoit les données et les envoie à l'unité à laquelle elle est reliée. Le paquet progresse ainsi dans la pile jusqu'à sa destination. Le système identifie le chemin optimal pour l'envoi du trafic.

Figure 1-3. Topologie en anneau



La plupart des difficultés liées à la topologie en anneau se produisent lorsqu'une unité tombe en panne ou qu'un lien est interrompu. Dans une pile composée d'unités PowerConnect 3424/P et PowerConnect 3448/P, le système bascule automatiquement vers une topologie permettant la prise de relais, sans

interrompre son fonctionnement. Un message SNMP est généré automatiquement, mais aucune action n'est requise concernant la gestion de la pile. Cependant, le lien ou l'unité défaillant(e) doit être réparés pour préserver l'intégrité de la pile.

Une fois le dépannage effectué, l'unité peut être reconnectée à la pile sans interruption du service, et la topologie en anneau est restaurée.

Topologie de prise de relais

Si une panne se produit dans la pile, celle-ci bascule vers une topologie de prise de relais. Dans cette topologie, les unités forment une chaîne. L'unité maître détermine la destination des paquets. Chaque unité est connectée aux deux unités voisines, à l'exception de celles située en bas et en haut de la pile.

Membres de la pile et ID d'unité

L'ID d'unité est essentiel pour la configuration de la pile. Le mode de fonctionnement de la pile est déterminé au cours du processus d'amorçage. Il est déterminé par l'ID d'unité sélectionné au cours du processus d'initialisation. Par exemple, si l'utilisateur sélectionne le mode autonome, l'unité démarre en tant qu'unité autonome.

Les unités sont livrées avec un ID d'unité autonome par défaut. Si une unité fonctionne en tant qu'unité autonome, tous les voyants d'empilage sont éteints.

Si l'utilisateur sélectionne un ID d'unité différent, l'ID d'origine n'est pas effacé et reste valide, même si l'unité est réinitialisée.

Les ID d'unité 1 et 2 sont réservées aux unités maîtres. Les unités 3 à 6 peuvent être attribuées aux membres de la pile.

Lors de l'amorçage de l'unité maître ou lors de l'insertion ou du retrait d'un membre, l'unité maître lance un processus d'exploration sur la pile.

REMARQUE : si deux unités membres possédant le même ID sont identifiées, la pile continue à fonctionner, mais seule l'unité la plus ancienne est ajoutée à la pile. Un message est envoyé à l'utilisateur pour lui indiquer qu'une unité n'a pas rejoint la pile.

Retrait et remplacement de membres de la pile

Les unités 1 et 2 sont compatibles avec la fonction d'unité maître. Elles peuvent être désignées comme unité maître principale ou unité maître de secours. La désignation de l'unité maître est effectuée au cours du processus de configuration. L'une des unités compatibles avec la fonction d'unité maître est désignée comme unité maître principale et l'autre comme unité maître de secours. Le processus de décision utilisé est le suivant :

- Si une seule unité est compatible avec la fonction d'unité maître, elle est désignée comme maître de la pile.
- Si deux unités sont compatibles avec la fonction d'unité maître et si l'une d'entre elles a été configurée manuellement en tant que maître de la pile, c'est cette dernière qui est désignée comme unité maître principale de la pile.
- Si deux unités sont compatibles avec la fonction d'unité maître et si aucune d'entre elles n'a été configurée manuellement en tant que maître de la pile, c'est la plus ancienne qui est désignée comme unité maître principale de la pile.
- Si deux unités sont compatibles avec la fonction d'unité maître et si elles ont toutes deux été configurées manuellement en tant que maître de la pile, c'est la plus ancienne qui est désignée comme unité maître principale de la pile.
- Si les deux unités compatibles avec la fonction d'unité maître possèdent la même ancienneté, l'unité 1 est désignée comme maître de la pile.

REMARQUE : pour que des unités soient considérées comme ayant la même ancienneté, elles doivent avoir été insérées dans la pile dans un intervalle de 10 minutes.

Par exemple, si l'unité 1 est insérée 5 minutes après l'unité 2, les deux sont considérées comme ayant la même ancienneté. Dans ce cas, l'unité 1 est désignée comme maître alors qu'elle a été insérée dans la pile après l'unité 2.

L'unité maître principale et l'unité maître de secours fonctionnent en mode Warm Standby (prise de relais automatique). Ce mode assure la prise de relais par l'unité maître de secours en cas de panne de l'unité maître principale, ce qui permet à la pile de continuer à fonctionner normalement.

Au cours du mode Warm Standby, seule la configuration statique est synchronisée entre l'unité maître principale et l'unité de secours. Lorsque l'unité maître de la pile est configurée, elle doit synchroniser l'unité maître de secours. La configuration dynamique (adresses MAC obtenues dynamiquement, par exemple) n'est pas sauvegardée.

Chaque port de la pile possède un ID d'unité/type de port et un numéro de port spécifiques faisant partie à la fois des commandes de configuration et des fichiers de configuration. Les fichiers de configuration sont gérés uniquement à partir de l'unité maître de la pile, y compris pour les événements suivants :

- Sauvegarde dans la mémoire FLASH
- Envoi des fichiers de configuration vers un serveur TFTP externe
- Téléchargement des fichiers de configuration depuis un serveur TFTP externe

REMARQUE : la configuration de tous les ports configurés est sauvegardée, même si la pile est réinitialisée et/ou si les ports ne sont plus présents.

Une exploration de la topologie est effectuée à chaque redémarrage, permettant à l'unité maître d'identifier toutes les unités de la pile. Les ID d'unité sont sauvegardés dans l'unité correspondante et identifiées lors du processus d'exploration de la topologie. Si une unité non autonome tente de démarrer sans être associée à une unité maître, son démarrage n'aboutit pas.

Les fichiers de configuration ne sont modifiés qu'à travers une configuration utilisateur explicite. Ils ne sont pas modifiés automatiquement dans les conditions suivantes :

- des unités sont ajoutées ;
- des unités sont retirées ;
- les ID affectés aux unités sont modifiés ;
- les unités basculent entre le mode pile et le mode autonome.

À chaque redémarrage du système, le fichier de configuration de l'unité maître est utilisé pour la configuration de la pile.

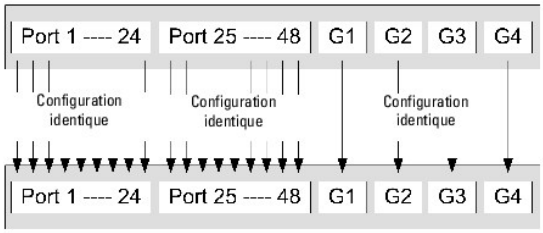
Si un membre est retiré de la pile, puis remplacé par une autre unité possédant le même ID, cette dernière est paramétrée selon la configuration de l'unité d'origine. Seuls les ports physiquement présents sont affichés dans la page d'accueil de PowerConnect OpenManage Switch Administrator et peuvent être configurés par le biais du système de gestion Web. Les ports non présents sont configurés à travers les interfaces CLI ou SNMP.

Échange des membres d'une pile

Si un membre de la pile remplace un autre membre possédant le même ID d'unité, la configuration de l'unité précédente est reportée sur le nouveau membre de la pile. Si la nouvelle unité insérée possède plus ou moins de ports que l'unité précédente, la configuration de ports appropriée est appliquée au nouveau membre. Exemple :

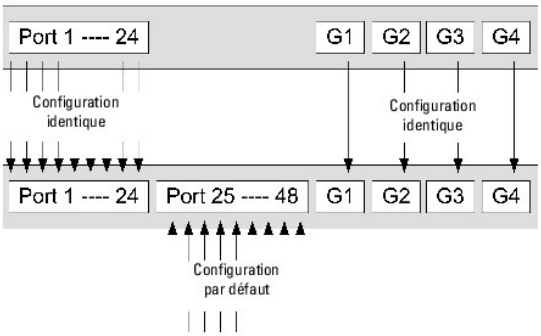
- Si un PowerConnect 3424/P remplace un PowerConnect 3424/P, la configuration des ports demeure inchangée.
- Si un PowerConnect 3448/P remplace un PowerConnect 3448/P, la configuration des ports demeure inchangée.

Figure 1-4. Remplacement d'un PowerConnect 3448/P par un PowerConnect 3448/P



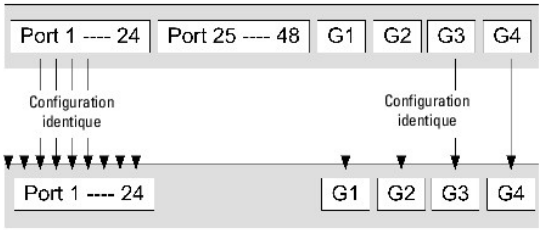
- Si un PowerConnect 3448/P remplace un PowerConnect 3424/P, la configuration des 24 ports FE du 3424/P est appliquée aux 24 premiers ports FE du 3448/P. La configuration des ports GE demeure inchangée. Les ports restants sont paramétrés en fonction de la configuration par défaut définie en usine.

Figure 1-5. Remplacement d'un port du PowerConnect 3448/P par un port du PowerConnect 3424/P



- Si un PowerConnect 3424/P remplace un PowerConnect 3448/P, la configuration des 24 premiers ports FE du 3448/P est appliquée aux 24 ports FE du 3424/P. La configuration des ports GE demeure inchangée.

Figure 1-6. Remplacement d'un port du PowerConnect 3424/P par un port du PowerConnect 3448/P



Basculement entre l'unité maître principale et l'unité maître de secours

L'unité maître de secours remplace l'unité maître principale dans les cas suivants :

- L'unité maître principale tombe en panne ou est retirée de la pile.
- Les interconnexions entre l'unité maître principale et les membres de la pile échouent.
- Un basculement logiciel est effectué via l'interface Web ou CLI.

Le basculement entre l'unité maître et l'unité de secours n'entraîne qu'une interruption de service limitée. Lorsque la panne se produit, les tables dynamiques font l'objet d'une nouvelle exploration. Le fichier de configuration en cours est synchronisé entre l'unité maître et l'unité de secours, puis continue de s'exécuter sur l'unité de secours.

Présentation des fonctions

Cette section décrit les caractéristiques de l'unité. Pour obtenir la liste complète des fonctions mises à jour, consultez la version électronique la plus récente des **Notes de version**.

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 à mettre à jour l'infrastructure du réseau. Elle élimine ainsi la nécessité de devoir placer les périphériques réseau à proximité des prises de courant. La fonction PoE peut être appliquée avec les éléments suivants :

- Téléphones IP
- Points d'accès sans fil
- Passerelles IP

- PDA
- Contrôle à distance audio et vidéo

Pour plus d'informations sur la fonction Power over Ethernet, consultez la section "Gestion de l'alimentation Power over Ethernet".

Blocage HOL

Le blocage HOL (Head of Line) provoque des retards de trafic et une perte de trames dus au fait que le trafic se dispute les mêmes ressources de port de sortie. Les paquets dans les files d'attente du blocage HOL et les paquets en début de file d'attente sont transmis avant les paquets en fin de file d'attente.

Prise en charge du contrôle de flux (IEEE 802.3X)

Le mécanisme de contrôle du flux permet aux périphériques les plus lents de communiquer avec des périphériques fonctionnant à une vitesse supérieure en demandant que ces derniers n'envoient pas de paquets de données. Les transmissions sont temporairement interrompues pour éviter une surcharge de la mémoire tampon.

Pour obtenir des informations sur la configuration du contrôle de flux pour les ports ou les LAG, consultez les sections "Définition de la configuration des ports" ou "Définition des paramètres des LAG".

Prise en charge de la contre-pression

Sur les liaisons semi duplex, le port récepteur empêche les débordements de la mémoire tampon en occupant la liaison pour qu'elle soit indisponible à tout trafic supplémentaire.

Pour obtenir des informations sur la configuration du contrôle de flux pour les ports ou les LAG, consultez les sections "Définition de la configuration des ports" ou "Définition des paramètres des LAG".

Contrôle de câble virtuel (VCT)

Le VCT détecte et rapporte les événements concernant le câblage des liaisons en cuivre, comme des câbles ouverts et des câbles en court-circuit. Pour plus d'informations, consultez la section "Exécution des diagnostics portant sur les câbles".

Support MDI/MDIX

Lorsque la négociation automatique est activée, le périphérique détecte automatiquement le type de câble connecté au port RJ-45 (croisé ou direct).

Le câblage standard des stations terminales est **MDI** (Interface dépendante du média) alors que les concentrateurs et commutateurs utilisent le mode **MDIX** (Interface croisée dépendante du média).

Pour obtenir des informations sur les modes MDI/MDIX pour les ports ou les LAG, consultez les sections "Définition de la configuration des ports" ou "Définition des paramètres des LAG".

Négociation automatique

La négociation automatique permet au périphérique d'informer les autres systèmes de ses modes de fonctionnement. Elle permet d'échanger des informations entre deux périphériques partageant un segment de liaison point à point et de configurer ces périphériques automatiquement de manière à tirer parti de leurs capacités de transmission maximales.

Les unités de la série PowerConnect 3400 améliorent la négociation automatique grâce à une fonction d'annonce des ports, qui permet à l'administrateur système de configurer les vitesses de port annoncées.

Pour plus d'informations sur la négociation automatique, consultez les sections "Définition de la configuration des ports" ou "Définition des paramètres des LAG".

Fonctions prises en charge pour l'adresse MAC

Capacité

Le périphérique prend en charge jusqu'à 8.000 adresses MAC. Certaines adresses MAC spécifiques sont réservées au système.

Entrées MAC statiques

Comme alternative au processus d'apprentissage des adresses MAC à partir des trames entrantes, il est possible de saisir ces adresses manuellement dans la table de pontage. Les entrées définies par l'utilisateur ne sont soumises à aucun délai d'expiration et sont conservées entre chaque réinitialisation ou redémarrage.

Pour plus d'informations, consultez la section "Définition d'adresses statiques".

Apprentissage automatique des adresses MAC

L'unité permet l'apprentissage automatique des adresses MAC à partir des paquets entrants. Ces adresses sont enregistrées dans la table de pontage.

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. Cela permet d'éviter un éventuel débordement de la table de pontage.

Pour obtenir des informations sur la configuration du délai d'expiration des adresses MAC, consultez la section "Affichage des adresses dynamiques".

Commutation VLAN basée sur l'adresse MAC

L'unité effectue toujours un routage basé sur les VLAN. Il n'effectue pas un pontage classique (IEEE802.1D), pour lequel les trames sont transférées uniquement en fonction de leur adresse MAC de destination. Il est cependant possible de configurer une fonctionnalité similaire pour les trames non balisées. Les trames envoyées à une adresse MAC de destination qui n'est associée à aucun port sont acheminées simultanément vers tous les ports du VLAN correspondant.

Support multidiffusion pour les adresses MAC

Le service de multidiffusion est un service de diffusion limitée autorisant des connexions de type "un-vers-plusieurs" et "plusieurs-vers-plusieurs" pour la distribution de l'information. Dans le cas d'un service de multidiffusion de couche 2, une seule trame est envoyée à une adresse de multidiffusion spécifique à partir de laquelle des copies de cette trame sont transmises aux ports appropriés.

Pour plus d'informations, consultez la section "Affectation de paramètres de transfert multidiffusion total".

Fonctions de couche 2

IGMP Snooping (surveillance IGMP)

Le processus appelé "IGMP Snooping" examine le contenu des trames IGMP lorsqu'elles sont transmises par le périphérique depuis un poste de travail vers un routeur multidiffusion situé en amont. À partir de la trame, l'unité identifie les postes de travail configurés pour des sessions de multidiffusion, ainsi que les routeurs multidiffusion qui envoient des trames de multidiffusion.

Pour plus d'informations, consultez la section "Surveillance IGMP".

Mise en miroir des ports

La mise en miroir des ports surveille et met en miroir le trafic réseau en transmettant des copies des paquets entrants et sortants, depuis un port contrôlé jusqu'à un port de contrôle. Les utilisateurs indiquent le port cible qui recevra les copies de tout le trafic qui passe par un port source indiqué.

Pour plus d'informations, consultez la section "Définition de sessions de mise en miroir des ports".

Broadcast Storm Control

Cette fonction permet de limiter le nombre de trames de multidiffusion et de diffusion acceptées et transmises par l'unité.

En cas de transmission de trames de couche 2, les trames de diffusion et de multidiffusion sont acheminées simultanément vers tous les ports du VLAN correspondant. Cela résulte en une occupation de la bande passante et en une surcharge de tous les noeuds connectés aux ports.

Pour plus d'informations, consultez la section "Activation de la fonction Storm Control".

Fonctions des VLAN prises en charge

Prise en charge des VLAN

Les VLAN sont des ensembles de ports de commutation qui ne comprennent qu'un seul domaine de diffusion. Les paquets sont désignés comme appartenant à un VLAN d'après la balise VLAN ou d'après une combinaison port d'entrée/contenu du paquet. Les paquets possédant des attributs en commun peuvent être regroupés dans le même VLAN.

Pour plus d'informations, consultez la section "Configuration des VLAN".

LAN virtuels basés sur les ports

Les VLAN basés sur les ports classent les paquets entrants vers d'autres VLAN en fonction de leur port d'entrée.

Pour plus d'informations, consultez la section "Définition des paramètres des ports de VLAN".

Conformité totale au balisage VLAN 802.1Q

La norme IEEE 802.1Q définit une architecture pour les VLAN en pont, les services offerts dans les VLAN et les protocoles et algorithmes inclus dans la fourniture de ces services.

Support GVRP

Le protocole GVRP (Protocole d'enregistrement VLAN GARP) permet l'élagage du VLAN conformément à la norme IEEE 802.1Q et la création dynamique de VLAN sur des ports de jonction 802.1Q. Lorsque le GVRP est activé, le périphérique enregistre et diffuse l'appartenance au VLAN sur tous les ports qui font partie de la topologie "**Protocole STP**" sous-jacente active.

Pour plus d'informations, consultez la section "Configuration des paramètres GVRP".

VLAN privés

Les ports de VLAN privés sont une fonction de sécurité de couche 2 permettant d'établir une isolation entre différents ports au sein du même domaine de diffusion.

Pour plus d'informations sur les VLAN privés, consultez la section "Configuration des VLAN privés".

Protocole STP

Protocole STP (Spanning Tree)

Le protocole STP du standard 802.1d est une exigence des commutateurs de couche 2 qui permet 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 activent et désactivent de façon sélective le transfert sur les ports.

Pour plus d'informations, consultez la section "Configuration du protocole STP".

Fast Link

Le protocole STP peut nécessiter 30 à 60 secondes pour converger. Pendant ce temps, il détecte les boucles potentielles, ce qui laisse le temps aux modifications d'état de se propager et aux périphériques concernés de répondre. Pour de nombreuses applications, un temps de réponse de 30 à 60 secondes est considéré comme trop long. L'option Fast Link évite ce retard et peut être appliquée dans des topologies de réseau sans boucles de transmission.

Pour plus d'informations sur l'activation du Fast Link pour les ports et les LAG, consultez les sections "Définition des paramètres des ports STP" ou "Définition d'adresses statiques".

Protocole RSTP (Rapide Spanning Tree) conforme à la norme IEEE 802.1w

Le Spanning Tree peut nécessiter 30 à 60 secondes avant que chaque hôte décide si ses ports transmettent activement du trafic. Le protocole RSTP (Rapid Spanning Tree) détecte les utilisations des topologies réseau pour activer la convergence rapide, sans créer pour autant des boucles de transmission.

Pour plus d'informations, consultez la section "Définition de Rapid Spanning Tree (RSTP)".

Protocole MSTP (Multiple Spanning Tree) conforme à la norme IEEE 802.1s

Le mode MSTP permet de mapper les VLAN avec des instances STP. Il fournit différents scénarios d'équilibrage de la charge. Les paquets affectés à différents VLAN sont transmis via des chemins différents dans des régions MSTP. Ces régions sont matérialisées par un ou plusieurs ponts MSTP utilisés pour la transmission des trames. Le mode MSTP permet à l'administrateur d'affecter le trafic du VLAN à des chemins uniques.

Pour plus d'informations, consultez la section "Configuration du protocole STP".

Agrégation des liaisons

Agrégation des liaisons

Un groupe de liaisons agrégées (LAG) peut contenir jusqu'à huit liaisons agrégées, chacune avec huit ports membres. Les avantages sont les suivants :

- Tolérance aux pannes liées à la rupture des liaisons physiques
- Amélioration du débit des connexions
- Meilleure granularité de la bande passante
- Connectivité serveur à large bande passante

Un LAG est composé de ports ayant la même vitesse et réglés en mode duplex intégral.

Pour plus d'informations, consultez la section "Définition des paramètres des LAG".

Agrégation de liaisons et LACP

Le protocole LACP utilise les échanges peer-to-peer à travers les liaisons pour déterminer, sur une base constante, la fonction d'agrégation des différentes liaisons, et fournir en permanence le niveau maximum d'agrégation pouvant être atteint entre deux systèmes donnés. Le protocole LACP détermine, configure, relie et contrôle automatiquement l'association du port avec les agrégateurs à l'intérieur du système.

Pour plus d'informations, consultez la section "Agrégation des ports".

Clients BootP et DHCP

Le protocole DHCP (Protocole de configuration dynamique d'hôtes) autorise la réception de paramètres de configuration supplémentaires à partir d'un serveur réseau, et ce dès le démarrage du système. Le service DHCP est un processus évolutif. Il s'agit d'une extension du protocole BootP.

Pour plus d'informations, consultez la section "Définition des paramètres d'interface IP DHCP".

Fonctions QoS (qualité de service)

Prise en charge de CoS (Class Of Service) 802.1p

La technique de signalisation IEEE 802.1p est une norme OSI de couche 2 relative au marquage et à la gestion des priorités du trafic réseau au niveau de la sous-couche liaison de données/MAC. Le trafic 802.1p est classé puis envoyé vers sa destination. Aucune réservation ou limite de bande passante n'est établie ou obligatoire. La norme 802.1p est un sous-produit de la norme 802.1Q (VLAN). Elle définit huit niveaux de priorité, similaires au champ binaire IP Precedence IP Header (En-tête IP de priorité IP).

Pour plus d'informations, consultez la section "Configuration de la qualité de service".

Fonctions de gestion de l'unité

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 (Protocole de gestion de réseau simple) vers une liste de destinataires d'interruptions.

Pour plus d'informations, consultez la section "Définition des paramètres SNMP".

SNMP version 1 et version 2

Le Protocole SNMP (Simple Network Management Protocol) sur UDP/IP contrôle l'accès au système. Une liste d'entrées de communauté est définie, chaque entrée étant composée d'une chaîne de communauté et de ses privilèges d'accès. Il existe 3 niveaux de sécurité SNMP : lecture seule, lecture-écriture et super. Seul un super utilisateur peut accéder à la table des communautés.

Pour plus d'informations, consultez la section "Définition des paramètres SNMP".

Gestion basée sur le Web

Grâce à la gestion basée sur le Web, le système peut être géré à partir de n'importe quel navigateur Web. Il contient un serveur Web intégré (fonction EWS, Embedded Web Server) hébergeant les pages HTML à travers lesquelles le système peut être contrôlé et configuré. Le système convertit en interne les entrées Web en commandes de configuration, en paramètres variables MIB et en d'autres paramètres de gestion.

Téléchargement et chargement du fichier de configuration

La configuration de l'unité est enregistrée dans un fichier de configuration contenant à la fois les paramètres appliqués au niveau du système et ceux spécifiques aux ports. Le système peut afficher les fichiers de configuration comme un ensemble de commandes CLI, enregistrées et manipulées comme des fichiers texte.

Pour plus d'informations, consultez la section "Gestion des fichiers".

Protocole TFTP (Trivial File Transfer Protocol)

L'unité prend en charge l'image d'amorçage, le logiciel et le chargement/téléchargement de la configuration via le protocole TFTP.

Surveillance à distance

Remote Monitoring (RMON) est une extension du protocole SNMP qui fournit des fonctions complètes de surveillance du trafic réseau (contrairement au SNMP qui permet la gestion et la surveillance des périphériques réseau). RMON 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.

Pour plus d'informations, consultez la section "Affichage des statistiques".

Interface de ligne de commande (CLI)

La syntaxe et la sémantique de l'interface de ligne de commande (CLI) sont autant que possible conformes aux pratiques de l'industrie. La CLI se compose d'éléments obligatoires et d'éléments facultatifs. L'interpréteur de la CLI fournit un système qui complète les commandes et les mots-clés pour aider l'utilisateur et réduire la saisie.

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, examinées et manipulées. Plusieurs mécanismes sont mis en place pour envoyer des notifications d'événements importants en temps réel et conserver un enregistrement de ces événements pour une utilisation future.

Pour plus d'informations, consultez la section "Gestion des journaux".

SNTP

Le protocole SNTP (Simple Network Time Protocol) assure la synchronisation de l'horloge du commutateur Ethernet avec une précision d'une milliseconde. La synchronisation se fait via un serveur réseau SNTP. Les sources horaires sont établies par des stratums. Les stratums définissent la distance par rapport à l'horloge de référence. Plus le stratum est haut (zéro représente le plus haut), plus l'horloge est précise.

Pour plus d'informations, consultez la section "Configuration des paramètres SNTP".

DNS

Le système de noms de domaines (DNS, Domain Name System) convertit les noms de domaines définis par l'utilisateur en adresses IP. À chaque affectation d'un nom de domaine, le service DNS convertit le nom en adresse IP numérique. Par exemple, www.ipexample.com devient 192.87.56.2. Les serveurs DNS gèrent les bases de données de noms de domaines et les adresses IP correspondantes.

Pour plus d'informations, consultez la section "Configuration des systèmes de noms de domaines".

Traceroute

Traceroute permet d'identifier les routes IP sur lesquelles les paquets ont transité au cours du processus de transmission. L'utilitaire CLI Traceroute peut être exécuté en mode User EXEC (EXEC utilisateur) ou en mode Privileged EXEC (EXEC privilégié).

Fonctions de sécurité

SSL

Le protocole SSL (Secure Socket Layer) est un protocole de niveau application qui permet d'effectuer des transactions de données sécurisées à travers une confidentialité, une authentification et une intégrité des données. Il repose sur des certificats et des clés publiques et privées.

Authentification basée sur le port (802.1x)

L'authentification basée sur le port permet d'authentifier des utilisateurs d'un système en fonction du 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 (Service d'authentification distant des utilisateurs entrants), à l'aide du protocole EAP (Extensible Authentication Protocol).

Pour plus d'informations, consultez la section "Configuration de l'authentification basée sur le port".

Prise en charge du verrouillage de port

Le verrouillage de port est une fonction de sécurité supplémentaire qui permet de restreindre l'accès des utilisateurs possédant des adresses MAC spécifiques à un seul port. Ces adresses peuvent être définies manuellement où 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, consultez la section "Configuration du verrouillage de port".

Client RADIUS

RADIUS est un protocole client/serveur. Un serveur RADIUS gère une base de données utilisateur qui contient des informations d'authentification comme le nom de l'utilisateur, le mot de passe et des statistiques.

Pour plus d'informations, consultez la section "Configuration des paramètres RADIUS".

SSH

Secure Shell (SSH) est un protocole qui fournit une connexion distante sécurisée à un périphérique. SSH version 2 est actuellement pris en charge. La fonction de serveur SSH permet à un client SSH d'établir une connexion cryptée et sécurisée avec une unité. La fonction de cette connexion est similaire à celle d'une connexion Telnet entrante. SSH utilise la cryptographie à clé publique RSA pour la connexion et l'authentification des périphériques.

TACACS+

TACACS+ apporte une sécurité centralisée 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.

Pour plus d'informations, consultez la section "Définition des paramètres TACACS+".

Gestion des mots de passe

La gestion des mots de passe permet d'améliorer la sécurité du réseau et de bénéficier d'un contrôle accru 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, consultez la section "Gestion des mots de passe".

Documentation supplémentaire sur l'interface CLI

Le CD de documentation contient un guide de référence pour l'interface CLI, qui présente les commandes CLI utilisées pour la configuration de l'unité. Vous y trouverez la description des commandes, leur syntaxe, les valeurs par défaut, des instructions d'utilisation et des exemples.

Retour au sommaire

Retour au sommaire

Description du matériel

Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

Ports

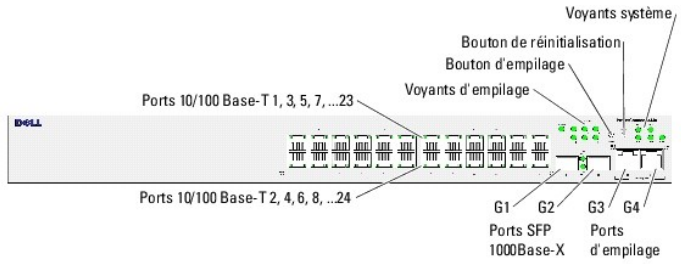
Description des ports du PowerConnect 3424

L'unité PowerConnect 3424 comprend les ports suivants :

- **24 ports Fast Ethernet :** ports RJ-45 10/100Base-T
- **2 ports fibre :** ports SFP 1000Base-X
- **2 ports Gigabit :** ports 1000Base-T
- **Port de console :** port RS-232

La figure suivante montre le panneau avant du PowerConnect 3424.

Figure 2-1. Panneau avant du PowerConnect 3424



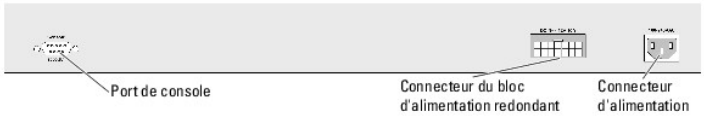
Le panneau avant contient 24 ports RJ-45 numérotés de 1 à 24. La rangée du haut contient les ports portant des numéros impairs (1-23) et la rangée du bas contient les numéros pairs (2-24). Le panneau avant contient également les ports fibre G1 et G2, et les ports cuivre G3 et G4. G3 et G4 peuvent être utilisés comme ports d'empilage si l'unité fait partie d'une pile, ou pour la gestion du trafic si l'unité est utilisée en autonome.

Le panneau avant comprend deux boutons. Le bouton Stack ID (ID de pile) permet de sélectionner les numéros d'unités. Le bouton de réinitialisation permet d'effectuer une réinitialisation manuelle. Il est encastré dans le panneau avant pour éviter son activation accidentelle. Les voyants de l'unité sont tous situés sur le panneau avant.

La figure suivante présente l'arrière du PowerConnect 3424.

Figure 2-2. Panneau arrière du PowerConnect 3424

Le panneau arrière contient un connecteur pour le bloc d'alimentation redondant, un port de console et un connecteur d'alimentation.



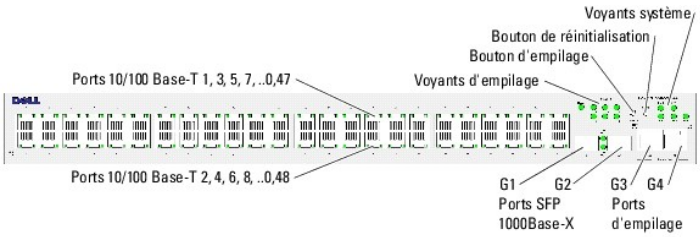
Description des ports du PowerConnect 3448

L'unité PowerConnect 3448 comprend les ports suivants :

- **48 ports Fast Ethernet :** ports RJ-45 désignés en tant que ports 10/100Base-T
- **2 ports fibre :** désignés en tant que ports SFP 1000Base-X
- **2 ports Gigabit :** désignés en tant que ports 1000Base-T
- **Port de console :** port RS-232

La figure suivante montre le panneau avant du PowerConnect 3448.

Figure 2-3. Panneau avant du PowerConnect 3448

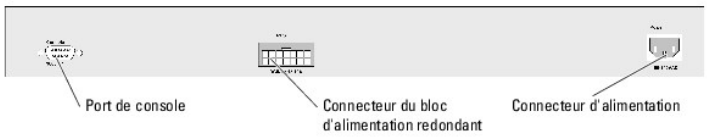


Le panneau avant contient 48 ports RJ-45 numérotés de 1 à 48. La rangée du haut contient les ports portant des numéros impairs (1-47) et la rangée du bas contient les numéros pairs (2-48). Le panneau avant contient également les ports fibre G1 et G2, et les ports cuivre G3 et G4. G3 et G4 peuvent être utilisés comme ports d'empilage si l'unité fait partie d'une pile, ou pour la gestion du trafic si l'unité est utilisée en autonome.

Le panneau avant comprend deux boutons. Le bouton Stack ID (ID de pile) permet de sélectionner les numéros d'unités. Le bouton de réinitialisation permet d'effectuer une réinitialisation manuelle. Il est encastré dans le panneau avant pour éviter son activation accidentelle. Les voyants de l'unité sont tous situés sur le panneau avant.

La figure suivante présente l'arrière du PowerConnect 3448.

Figure 2-4. Panneau arrière du PowerConnect 3448



Le panneau arrière contient un connecteur pour le bloc d'alimentation redondant, un port de console et un connecteur d'alimentation.

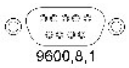
Ports SFP

Les ports SFP (Small Form Factor Plugable) disposent d'une interface série bifilaire prenant en charge les communications via un périphérique logique programmable complexe (Complex Programmable Logic Device, CPLD) désigné comme étant un périphérique 1000Base-SX ou LX.

Port de console RS-232

Un connecteur DB-9 permet de relier un terminal pour le débogage, le téléchargement de logiciels, etc. Le débit par défaut est de 9600 bps et peut être configuré à une valeur comprise entre 2400 bps à 115200 bps.

Figure 2-5. Port de console



Dimensions

Les dimensions des PowerConnect 3424/P et PowerConnect 3448/P sont les suivantes :

Modèle PoE :

- **Largeur :** 440 mm (17,32 pouces)
- **Profondeur :** 387 mm (15,236 pouces)
- **Hauteur** : 43,2 mm (1,7 pouces)

Modèle sans PoE :

- **Largeur :** 440 mm (17,32 pouces)
- **Profondeur :** 257 mm (10,118 pouces)
- **Hauteur** : 43,2 mm (1,7 pouces)

Signification des voyants

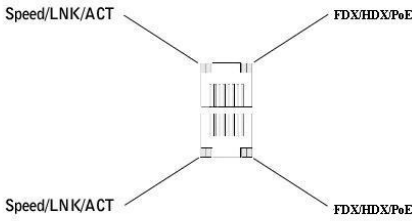
Le panneau avant est doté de voyants indiquant l'état des liaisons, des blocs d'alimentation, des ventilateurs et des diagnostics.

Voyants des ports

Chaque port 10/100/1000 Base-T port et 10/100 Base-T est doté de deux voyants. Le voyant de vitesse est situé à gauche du port tandis que le voyant Link/Duplex/Activity (Lien/Duplex/Activité) se trouve sur le côté droit.

La figure suivante présente les voyants des ports 10/100 Base-T sur les commutateurs PowerConnect 3424 /P et PowerConnect 3448/P.

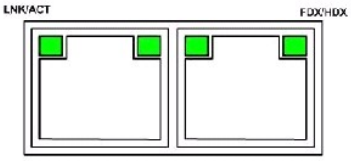
Figure 2-6. Voyants du port cuivre RJ-45 10/100 BaseT



Le port RJ-45 100 Base-T des PowerConnect 3424 /P et 3448/P comprend deux voyants marqués LNK/ACT.

Ces voyants sont représentés dans la figure suivante.

Figure 2-7. Voyants du port RJ-45 1000 BaseT



La signification des voyants du port RJ-45 pour le PowerConnect 3424 et le PowerConnect 3448 est indiquée dans le tableau suivant.

Tableau 2-1. Signification des voyants du port 100BaseT RJ-45 sur les systèmes PowerConnect 3424 et 3448

Voyant	Couleur	Description
Link/Activity/Speed	Vert fixe	Le port fonctionne à 100 Mbps.
	Vert clignotant	Le port transmet ou reçoit des données à 100 Mbps.
	Jaune fixe	Le port fonctionne à 10 Mbps.
	Jaune clignotant	Le port transmet ou reçoit des données à 10 Mbps.
	ÉTEINT	Le port n'est pas actif.
FDX	Vert fixe	Le port fonctionne actuellement en duplex intégral.
	ÉTEINT	Le port fonctionne actuellement en semi duplex.

La signification des voyants du port RJ-45 pour le PowerConnect 3424P et le PowerConnect 3448P est indiquée dans le tableau suivant.

Tableau 2-2. Signification des voyants du port cuivre RJ-45 100BaseT sur les systèmes PowerConnect 3424P et 3448P

Voyant	Couleur	Description
Speed/Link/Act	Vert fixe	Le port est actuellement connecté à 100 Mbps.
	Vert clignotant	Le port est actuellement connecté à 100 Mbps.
	ÉTEINT	Le port fonctionne actuellement à 10 Mbps, ou bien il n'est pas connecté.
PoE	Vert fixe	Le périphérique PoE est détecté et fonctionne avec une charge normale. Pour plus d'informations sur les périphériques PoE, consultez la section "Gestion de l'alimentation Power over Ethernet"
	Orange fixe	Une surcharge ou un court-circuit s'est produit(e) sur le périphérique PoE. Pour plus d'informations sur la fonction Power over Ethernet, consultez la section "Gestion de l'alimentation Power over Ethernet".
	Orange clignotant	La puissance requise par le périphérique PoE est supérieure à la puissance allouée. Pour plus d'informations sur la fonction Power over Ethernet, consultez la section "Gestion de l'alimentation Power over Ethernet".
	ÉTEINT	Aucun périphérique PoE n'a été détecté.

Voyants du port Gigabit

Le tableau suivant décrit les voyants du port Gigabit (port d'empilage).

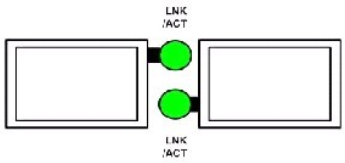
Tableau 2-3. Signification des voyants du port cuivre RJ-45 100BaseT sur les systèmes PowerConnect 3424 et 3448

Voyant	Couleur	Description
Link/Activity/Speed	Vert fixe	Le port fonctionne à 1000 Mbps.
	Vert clignotant	Le port transmet ou reçoit des données à 1000 Mbps.
	Jaune fixe	Le port fonctionne à 10 ou 100 Mbps.
	Jaune clignotant	Le port transmet ou reçoit des données à 10 ou 100 Mbps.
	ÉTEINT	Le port n'est pas actif.
FDX	Vert fixe	Le port fonctionne actuellement en mode duplex intégral.
	ÉTEINT	Le port fonctionne actuellement en mode semi duplex.

Voyants des ports SFP

Les ports SFP sont dotés d'un voyant marqué "LNK/ACT". Sur les PowerConnect 3424/P et 3448/P, ces voyants se trouvent entre les ports et sont de forme ronde. Les figures suivantes présentent les voyants de chaque unité.

Figure 2-8. Voyants des ports SFP



La signification des voyants des ports SFP est indiquée dans le tableau suivant.

Tableau 2-4. Signification des voyants des ports SFP

Voyant	Couleur	Description
Link/Activity	Vert fixe	Une liaison est établie.
	Vert clignotant	Le port est actuellement en train de transmettre ou de recevoir des données.
	ÉTEINT	Aucune liaison n'est active sur le port.

Voyants système

Les voyants système des PowerConnect 3424/P et 3448/P fournissent des informations sur les blocs d'alimentation, les ventilateurs, les conditions thermiques et les diagnostics. Ils sont présentés dans la figure suivante.

Figure 2-9. Voyants système

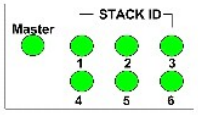
Le tableau ci-après décrit les voyants du système.

Tableau 2-5. Voyants système

Voyant	Couleur	Description
Bloc d'alimentation (PWR)	Vert fixe	Le commutateur est sous tension.
	ÉTEINT	Le commutateur est hors tension.
Bloc d'alimentation redondant (RPS) (modèles : 3424 et 3448)	Vert fixe	Le bloc d'alimentation redondant est en fonctionnement.
	Rouge fixe	Le bloc d'alimentation redondant est en panne.
	ÉTEINT	Le bloc d'alimentation redondant n'est pas branché.
Bloc d'alimentation redondant (RPS) (modèles : 3424P et 3448P)	Vert fixe	Le bloc d'alimentation redondant est en fonctionnement.
	ÉTEINT	Le bloc d'alimentation redondant (RPS) est défectueux ou n'est pas branché.
Diagnostics (DIAG)	Vert clignotant	Le test de diagnostic du système est en cours.
	Vert fixe	Le test de diagnostic du système s'est terminé sans erreur.
	Rouge fixe	Le test de diagnostic du système a échoué.
	ÉTEINT	Le système fonctionne normalement.
Température (TEMP)	Rouge fixe	La température de l'unité est supérieure à la limite maximale autorisée.
	ÉTEINT	La température de l'unité est comprise dans la plage autorisée.
Ventilateur (FAN)	Vert fixe	Tous les ventilateurs de l'unité fonctionnent normalement.
	Rouge fixe	Un ou plusieurs ventilateurs ne fonctionnent pas.

Les voyants d'empilage indiquent la position de l'unité dans la pile. La figure suivante présente les voyants du panneau avant.

Figure 2-10. Voyants d'empilage



Les voyants d'empilage sont numérotés de 1 à 6. Le voyant allumé sur chaque unité indique son ID. Si le voyant 1 ou 2 est allumé, cela signifie que l'unité est soit maître de la pile, soit maître de secours.

Tableau 2-6. Signification des voyants d'empilage

Voyant	Couleur	Description
Tous les voyants d'empilage	ÉTEINT	Le commutateur fonctionne en tant qu'unité autonome.
Voyants d'empilage 1 à 6 (S1-S6)	Vert fixe	Le numéro du voyant indique l'ID de l'unité.
	ÉTEINT	L'unité n'est pas associée à l'ID n.
Voyant de l'unité maître	Vert fixe	L'unité correspondante est définie comme maître de la pile.
	ÉTEINT	L'unité n'est pas définie comme maître de la pile.

Blocs d'alimentation

L'unité est équipée d'un bloc d'alimentation en CA interne et d'un connecteur permettant de relier le PowerConnect 3424/P et le PowerConnect 3448/P à une unité PowerConnect EPS-470, ou dans le cas des PowerConnect 3424 et 3448, à une unité PowerConnect RPS-600. Les PowerConnect 3424/P et 3448/P sont dotés d'un bloc d'alimentation interne (12 Volts).

Le fonctionnement de l'unité avec les deux blocs d'alimentation est régulé au moyen d'un mécanisme de partage de la charge. Les voyants des blocs d'alimentation indiquent leur état.

Les unités PowerConnect 3424/P et 3448/P sont dotés d'un bloc d'alimentation interne de 470 W (12 V/-48 V), avec un total de 370 W par tranche de 24 ports PoE.

Bloc d'alimentation en CA

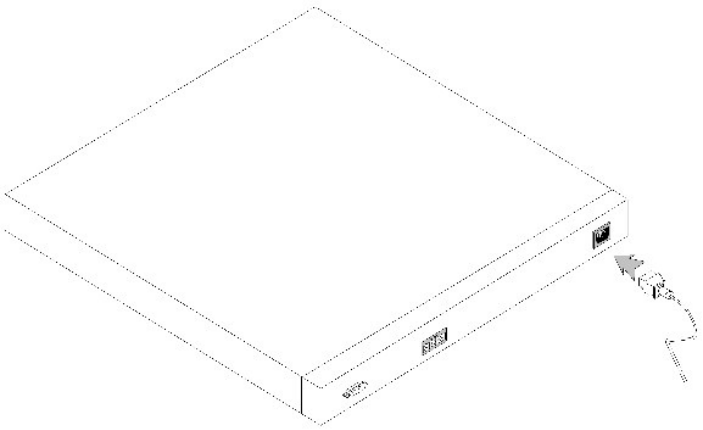
Le bloc d'alimentation en CA fonctionne de 90 à 264 V.c.a (47 à 63 Hz). Il est doté d'un connecteur standard. Le voyant du panneau avant indique si le bloc d'alimentation est connecté.

Bloc d'alimentation en CC

Il est possible de mettre en place une alimentation redondante en connectant les commutateurs PowerConnect 3424 et 3448 à une unité RPS-600 externe. Aucune configuration n'est requise. Le voyant "RPS" du panneau avant indique si l'unité RPS-600 externe est connectée. Voir le tableau 2-5 pour interpréter les voyants du bloc d'alimentation redondant.

Il est possible de mettre en place une alimentation redondante en connectant les commutateurs PowerConnect 3424/P et 3448/P à une unité EPS-470 externe. Aucune configuration n'est requise. Le voyant "RPS" du panneau avant indique si l'unité EPS-470 externe est connectée. Voir le tableau 2-5 pour interpréter les voyants du bloc d'alimentation redondant.

Figure 2-11. Connexion de l'alimentation



Lorsque l'unité est connectée à une source d'alimentation différente, les risques de panne en cas de coupure de courant diminuent.

Bouton Stack ID (ID de pile)

Le panneau avant de l'unité comprend un bouton "Stack ID" qui permet de sélectionner manuellement l'ID de chaque membre de la pile.

L'unité maître et les membres de la pile doivent être sélectionnés dans les 15 secondes qui suivent leur démarrage. Passé ce délai, l'unité est démarrée en autonome. Vous devez alors la redémarrer pour sélectionner un ID d'unité.

L'unité maître est associée à l'ID 1 ou 2. Si à la fois l'unité 1 et l'unité 2 sont présentes, celle qui n'est pas sélectionnée comme maître est définie comme unité maître de secours. Les membres de la pile sont associées aux ID 3 à 6. Par exemple, dans une pile contenant 4 unités, l'unité maître est associée à l'ID 1 ou 2 et l'unité maître de secours est associée à l'ID 1 ou 2, selon la sélection effectuée pour l'unité maître. Le troisième membre de la pile est associé à l'ID 3 et le quatrième à l'ID 4.

REMARQUE : les unités autonomes ne sont pas détectées automatiquement. Si un ID a déjà été sélectionné pour une unité prévue pour fonctionner en autonome, vous devez appuyer plusieurs fois sur le bouton Stack ID de cette unité, jusqu'à ce que tous ses voyants d'empilage soient éteints.

Bouton de réinitialisation

Les commutateurs PowerConnect 3424/P et 3448/P sont dotés d'un bouton de réinitialisation situé sur le panneau avant. Ce bouton permet de procéder à une réinitialisation manuelle. Si l'unité maître est réinitialisée, la pile l'est également. En revanche, la pile n'est pas réinitialisée lorsque vous réinitialisez l'un de ses membres.

Le circuit de réinitialisation du commutateur est activé par la mise sous tension ou en cas de sous-tension.

Système de ventilation

Les commutateurs PowerConnect 3424/P et 3448/P avec fonction PoE sont équipés de cinq ventilateurs intégrés. Les commutateurs PowerConnect 3424 et 3448 (sans fonction PoE) en contiennent deux. Le fonctionnement des ventilateurs peut être vérifié à l'aide du voyant correspondant.

Retour au sommaire

Retour au sommaire

Installation du PowerConnect 3424/P et du PowerConnect 3448/P

Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

Préparation du site

Les PowerConnect 3424/P et 3448/P peuvent être montés dans un rack standard de 19 pouces (48,26 cm), posés sur une table ou fixés sur un mur. Avant de les installer, vérifiez que l'emplacement choisi répond aux conditions suivantes :

- **Alimentation :** l'unité doit être installée à proximité d'une prise électrique facilement accessible de 100-240 V c.a. à 50-60 Hz.
- **Tous modèles :** vérifiez que le bloc d'alimentation redondant (RPS) est correctement installé en vous assurant que les voyants du panneau avant sont allumés.
- **Modèles PoE :** vérifiez que le bloc d'alimentation redondant est installé en vous assurant que les voyants PoE du panneau avant sont allumés.
- **Dégagement :** l'avant de l'unité doit être suffisamment dégagé pour rester accessible à un opérateur. Prévoyez un dégagement pour le câblage, les connexions électriques et la ventilation.
- **Câblage :** les câbles doivent être acheminés de façon à éviter les sources de bruit électrique, telles que les émetteurs radioélectriques, les amplificateurs de diffusion, les lignes électriques et les luminaires pour lampes fluorescentes.
- **Conditions ambiantes :** la température ambiante doit être comprise entre 0 et 50º C (32 et 122º F) avec une humidité relative maximale de 95 % sans condensation.

Déballage

Contenu du carton

Lors du déballage de l'unité, vérifiez que le carton contient les éléments suivants :

- Unité/Commutateur
- Cordon d'alimentation en CA
- Câble inverseur RS-232
- Patins adhésifs en caoutchouc
- Kit de montage pour l'installation en rack ou kit de fixation murale
- CD de documentation
- Guide d'information sur le produit

Déballage de l'unité

REMARQUE : avant de déballer l'unité, examinez le carton d'emballage et signalez immédiatement tout dommage apparent.

1. Placez la boîte sur un plan propre.
2. Ouvrez-la ou retirez sa partie supérieure.
3. Avec précaution, retirez l'unité de sa boîte et posez-la sur une surface propre et stable.
4. Retirez tout le matériel d'emballage.
5. Vérifiez que l'unité et ses accessoires ne sont pas endommagés. Signalez immédiatement tout dommage constaté.

Montage de l'unité

Les instructions de montage ci-après s'appliquent aux unités PowerConnect 3424/P et 3448/P. Le port de console se trouve sur le panneau arrière. Les connecteurs d'alimentation sont également situés sur le panneau arrière. La connexion d'un bloc d'alimentation redondant (RPS) est facultative, mais recommandée. Le connecteur à utiliser pour cette opération se trouve sur le panneau arrière des unités.

Montage en rack

⚠ **PRÉCAUTION : lisez le Guide d'information sur le produit (section "Consignes de sécurité") pour obtenir des informations relatives à la sécurité concernant les périphériques connectés au commutateur ou assurant sa prise en charge.**

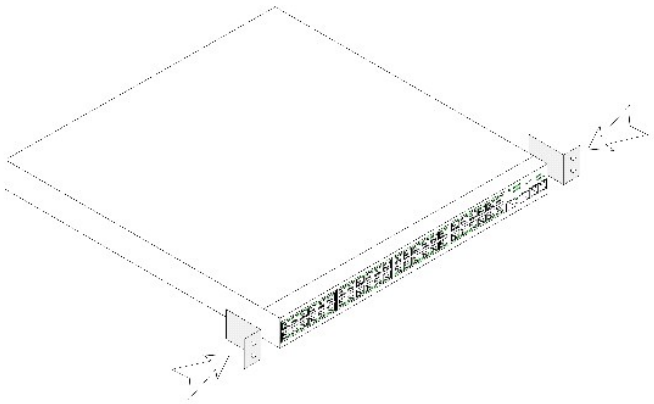
⚠ **PRÉCAUTION : déconnectez tous les câbles avant de monter l'unité dans un rack ou une armoire.**

⚠ **PRÉCAUTION : si vous installez plusieurs unités dans un rack, commencez par les emplacements du bas et procédez en remontant vers le haut du rack.**

1. Placez le support de fixation du rack sur un côté de l'unité, en alignant les orifices de montage des deux éléments.

   L'illustration suivante indique l'emplacement où les supports doivent être placés.

Figure 3-1. Installation des supports pour un montage en rack



2. Insérez les vis fournies dans les orifices et serrez-les à l'aide d'un tournevis.
3. Répétez l'opération de l'autre côté de l'unité.
4. Insérez l'unité dans le rack, en veillant à ce que ses orifices de montage soient bien alignés sur ceux du rack.
5. Fixez ensuite l'unité sur le rack à l'aide des vis appropriées (non fournies). Vous devez fixer les deux vis du bas avant celles du haut. Vérifiez que les orifices de ventilation ne sont pas obstrués.

Installation sur une surface plane

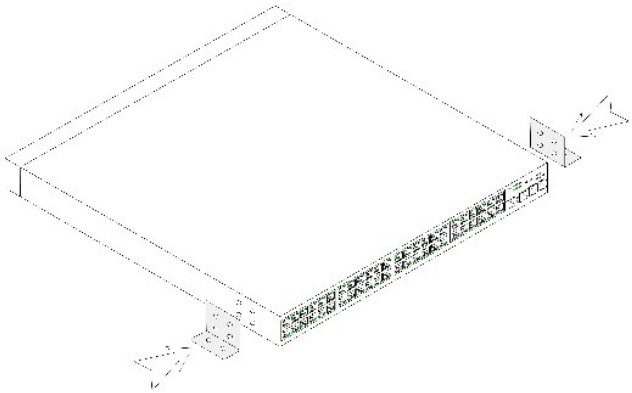
L'unité doit être installée sur une surface plane si elle n'est pas installée dans un rack. Cette surface doit pouvoir supporter le poids de l'unité et de ses câbles.

1. Fixez les patins adhésifs en caoutchouc sur les emplacements marqués, sous le châssis.
2. Posez l'unité sur une surface plane en laissant un espace de 5 cm (2 pouces) de chaque côté et de 13 cm (5 pouces) à l'arrière.
3. Assurez-vous que l'unité est suffisamment ventilée.

Fixation murale

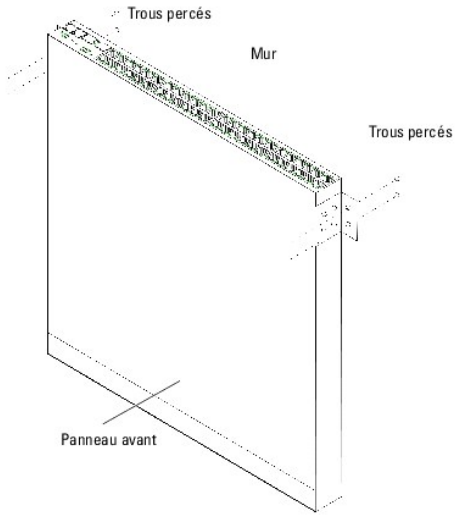
1. Placez le support de fixation murale sur un côté de l'unité, en alignant les orifices de montage des deux éléments. L'illustration suivante indique l'emplacement où les supports doivent être montés.

Figure 3-2. Installation du support pour une fixation murale



2. Insérez les vis fournies dans les orifices et serrez-les à l'aide d'un tournevis.
3. Répétez l'opération de l'autre côté de l'unité.
4. Placez l'unité contre le mur, à l'endroit où elle sera installée.
5. Faites des marques sur le mur pour repérer les emplacements où les vis de fixation devront être placées.
6. Percez le mur aux endroits marqués et placez des chevilles (non fournies) dans les trous.
7. Fixez ensuite l'unité sur le mur à l'aide des vis appropriées (non fournies). Vérifiez que les orifices de ventilation ne sont pas obstrués.

Figure 3-3. Fixation murale de l'unité



Connexion à un terminal

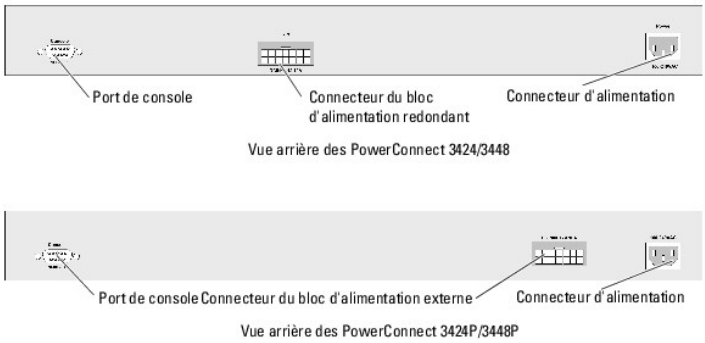
1. Connectez un câble inverseur RS-232 au terminal ASCII ou au connecteur série d'un système de bureau exécutant un logiciel d'émulation de terminal.
2. Branchez le connecteur femelle DB-9 situé à l'autre extrémité du câble sur le connecteur de port série de l'unité.

Connexion de l'unité à un bloc d'alimentation

Branchez le cordon d'alimentation en CA qui vous a été fourni sur le connecteur d'alimentation approprié du panneau arrière.

REMARQUE : à ce stade, vous ne devez pas encore brancher le cordon d'alimentation sur une prise reliée à la terre. Ce branchement est décrit à la section "Démarrage et configuration de l'unité".

Figure 3-4. Connecteur d'alimentation du panneau arrière



Une fois ce branchement effectué, vérifiez que le périphérique est alimenté et fonctionne correctement, en observant les voyants situés sur le panneau avant.

Installation en pile

Généralités

Chaque unité peut fonctionner en autonome ou en tant que membre d'une pile. Chaque pile peut contenir jusqu'à 6 unités ou 192 ports.

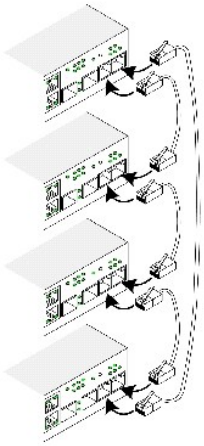
Chaque pile contient une unité maître et des unités membres. Elle peut éventuellement compter une unité maître de secours.

Installation en pile de commutateurs PowerConnect 3400

Chaque pile de commutateurs PowerConnect 3400 contient une seule unité maître et peut contenir une unité maître de secours. Toutes les autres unités sont considérées comme des membres de la pile.

Pour permettre l'empilage, les commutateurs de la série PowerConnect 3400 disposent de ports RJ-45 Ethernet Gigabit (G3 et G4), qui permettent de connecter les unités les unes aux autres sans faire appel à des accessoires supplémentaires. Pour procéder au câblage de la pile, branchez un câble standard de catégorie 5 sur le port G3 de l'unité se trouvant sur le dessus de la pile, puis sur le port G4 de l'unité voisine. Répétez l'opération jusqu'à ce que toutes les unités soient connectées. Connectez ensuite le port G3 de l'unité la plus basse de la pile au port G4 de l'unité la plus haute.

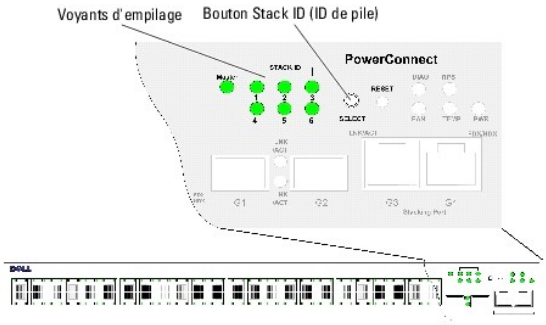
Figure 3-5. Diagramme de câblage de la pile



REMARQUE : dans une configuration d'empilage, les ports G3 et G4 n'apparaissent pas dans l'interface de gestion Web, car ils sont alors indexés de façon différente.

L'identification des unités de la pile est effectuée à l'aide du bouton Stack ID situé sur leur panneau avant.

Figure 3-6. Configuration de la pile et panneau d'identification



Chaque unité de la pile possède un identificateur unique définissant sa position dans la pile et sa fonction. Si l'unité fonctionne en autonome, le voyant d'empilage est éteint. Le fonctionnement en autonome est activé par défaut.

L'ID d'unité est configuré manuellement à l'aide du bouton Stack ID. Il est indiqué par les voyants d'ID de pile. Les ID d'unité 1 et 2 sont réservés à l'unité maître et à l'unité maître de secours. Les ID 3 à 6 sont dédiés aux unités membres.

Procédure de sélection des ID d'unité

La sélection des ID d'unité s'effectue comme suit :

1. Assurez-vous que le port de console de l'unité maître ou autonome est relié à un terminal (ou à un émulateur de terminal) VT100 par un câble inverseur RS-232.
2. Localisez une prise de courant.
3. Mettez-la hors tension.
4. Branchez l'unité sur cette prise.
5. Mettez la prise sous tension.

Lors de la mise sous tension, le voyant correspondant au numéro d'ID configuré précédemment clignote pendant 15 secondes. Pendant ce délai, vous devez sélectionner un ID en appuyant sur le bouton Stack ID, jusqu'à ce que le voyant associé à l'ID voulu s'allume.

6. Procédure de sélection : pour passer d'un numéro de voyant au suivant, continuez à appuyer sur le bouton Stack ID. Si vous appuyez sur le bouton Stack ID lorsque le voyant 6 clignote, l'unité est configurée en mode autonome. Si vous appuyez de nouveau sur le bouton Stack ID, vous revenez à l'ID 1. Les ID 1 et 2 sont réservés aux unités maîtres. Voir "Présentation de l'empilage" Procédure de sélection de l'unité maître.

7. **Fin de la procédure de sélection :** la procédure de sélection prend fin au bout de 15 secondes, lorsque le voyant cesse de clignoter. Le bouton Stack ID devient alors inactif, et l'unité en cours de définition est associée automatiquement au numéro du voyant qui clignotait lorsque le délai imparti a expiré.

REMARQUE : suivez cette procédure pour chaque unité une à la fois, jusqu'à ce que tous les membres de la pile disposent d'un ID et soient mis sous tension. Le fait de procéder unité par unité permet de bénéficier d'un délai suffisant pour sélectionner l'ID d'empilage. Avant de mettre les unités sous tension, vérifiez que le câblage de la pile est complet et conforme au "Diagramme de câblage de la pile".

Démarrage et configuration de l'unité

Une fois toutes les connexions externes mises en place, connectez un terminal à l'unité pour configurer celle-ci. Les procédures de configuration avancées sont décrites à la section "Configuration avancée".

REMARQUE : avant de continuer, lisez les notes d'édition concernant ce produit. Vous pouvez les télécharger à partir du site d'assistance technique de Dell, **support.dell.com**.

REMARQUE : nous vous recommandons de vous procurer la version la plus récente de la documentation, disponible sur le site **support.dell.com**.

Connexion à l'unité

Pour que l'unité puisse être configurée, elle doit être connectée à une console. Si elle fait partie d'une pile, seule l'unité maître doit être connectée à un terminal. La pile fonctionnant comme une seule unité, seule l'unité maître est configurée.

Connexion du terminal à l'unité

L'unité est équipée d'un port de console qui permet de la connecter à un terminal ou à un système exécutant un logiciel d'émulation de terminal, et ce afin de contrôler le fonctionnement de l'unité et de procéder à sa configuration. Le port de console est un connecteur DB-9 configuré en tant que connecteur DTE (data terminal equipment, ou équipement de terminal de données).

Pour utiliser le port de console, vous devez disposer des équipements suivants :

- Terminal compatible VT100 ou système de bureau équipé d'un port série et exécutant un logiciel d'émulation de terminal VT100
- Câble inverseur avec un connecteur femelle DB-9 pour le branchement sur le port de console et un autre connecteur du format approprié pour le branchement sur le terminal

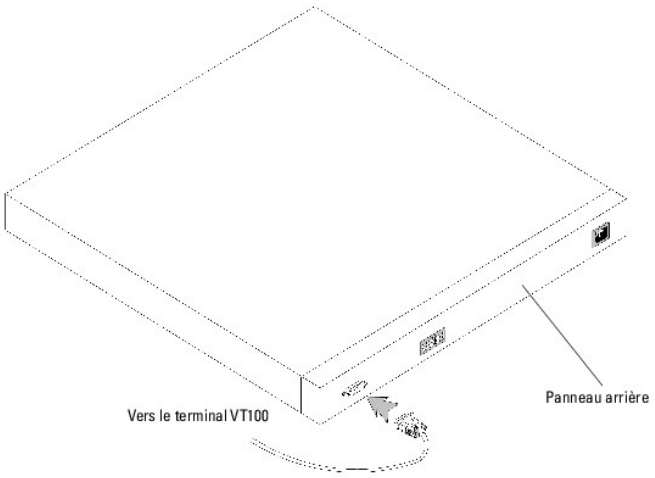
Pour connecter un terminal au port de console :

1. Branchez le câble inverseur RS-232 (fourni) sur le terminal exécutant le logiciel d'émulation VT100.
2. Sélectionnez le port série approprié (1 ou 2) pour la connexion à la console.
3. Paramétrez le débit sur 9600 bauds.
4. Paramétrez le format de données sur 8 bits de données, 1 bit d'arrêt et aucune parité.
5. Définissez le contrôle de flux sur aucun.
6. Sous Propriétés, sélectionnez le mode VT100 pour émulation.
7. Choisissez l'option "Touches de terminal" dans le champ "Les touches de fonction, de direction et Ctrl agissent en tant que". Vérifiez que le paramétrage correspond bien à "Touches de terminal", *et non à* "Touches Windows".

AVIS : si vous utilisez HyperTerminal avec Microsoft® Windows® 2000, assurez-vous que le service pack 2 (ou suivant) de Windows 2000 est installé. Ce service pack permet aux touches fléchées de fonctionner correctement dans l'émulation VT100 d'HyperTerminal. Pour plus d'informations concernant les service packs Windows 2000, visitez le site www.microsoft.com.

8. Branchez la prise femelle du câble inverseur RS-232 directement sur le port de console de l'unité maître/autonome, puis serrez les vis imperdables. Sur le PowerConnect 3400, le port de console se trouve sur le panneau arrière.

Figure 3-7. Connexion au port de console d'un PowerConnect série 3400



REMARQUE : une console peut être connectée au port de console de n'importe quelle unité de la pile, mais les opérations relatives à la gestion de cette dernière peuvent uniquement être effectuées à partir de son unité maître (ID 1 ou 2).

Retour au sommaire

Retour au sommaire

Configuration des PowerConnect 3424/P et 3448/P

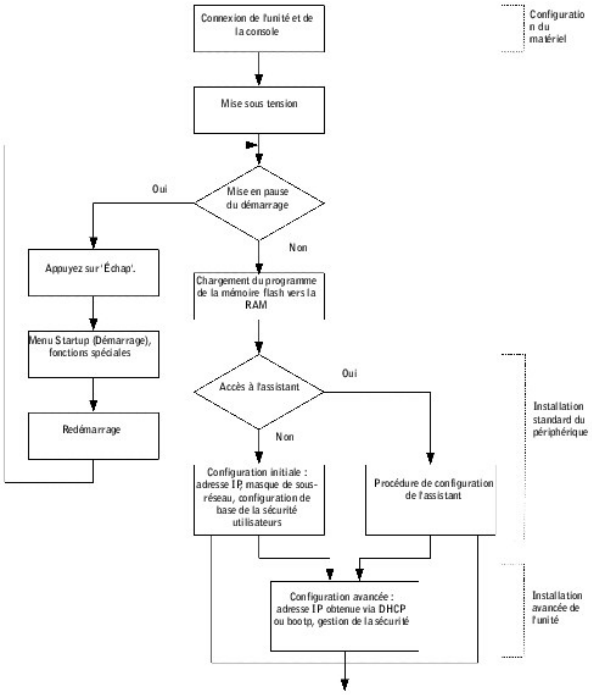
Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

Procédures de configuration

Une fois toutes les connexions externes de l'unité en place, vous devez connecter celle-ci à un terminal de façon à pouvoir contrôler diverses procédures (démarrage, etc.). La figure ci-après indique l'ordre des procédures d'installation et de configuration.

REMARQUE : avant de continuer, lisez les notes d'édition concernant ce produit. Vous pouvez les télécharger à partir du site **support.dell.com**.

Figure 4-1. Déroulement des procédures d'installation et de configuration



Démarrage du commutateur

Lorsque le système est mis sous tension et que le terminal local est déjà connecté, l'unité effectue un POST (auto-test de démarrage). Ce test s'exécute à chaque initialisation de l'unité ; 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'auto-test de démarrage se déroule sans incident, une image exécutable valide est chargée dans la mémoire vive. Les messages de l'auto-test de démarrage sont affichés sur le terminal et indiquent le succès ou l'échec du test.

Le processus de démarrage dure environ 30 secondes.

Configuration initiale

REMARQUE : avant de continuer, lisez les notes d'édition concernant ce produit. Vous pouvez les télécharger à partir du site d'assistance technique de Dell, **support.dell.com**.

REMARQUE : la configuration initiale est basée sur les hypothèses suivantes :

- L'unité PowerConnect n'a jamais été configurée auparavant et se trouve dans le même état que lorsque vous l'avez reçue.
- L'unité PowerConnect a démarré correctement.
- La connexion à une console est établie et l'invite de la console est affichée sur l'écran d'un terminal VT100.

La configuration initiale de l'unité s'effectue à l'aide du port de console. Une fois cette première étape effectuée, l'unité peut être gérée soit à partir de la console connectée, soit à distance, via une interface définie lors de la configuration initiale.

S'il s'agit du premier démarrage de l'unité, ou si le fichier de configuration est vide car l'unité n'a pas encore été configurée, l'utilisateur est invité à lancer l'assistant de configuration. Cet assistant vous guide dans les étapes nécessaires à la configuration initiale de l'unité. Il vous aide également à la faire fonctionner en un minimum de temps.

REMARQUE : demandez les informations suivantes à votre administrateur réseau avant de configurer l'unité :

- Adresse IP à attribuer à l'interface du VLAN 1 utilisée pour la gestion de l'unité. Par défaut, tous les ports sont membres du VLAN 1.
- Masque de sous-réseau IP
- Adresse IP de la passerelle par défaut (routeur suivant) permettant de configurer la route par défaut
- Adresse IP de la chaîne de communauté et du système de gestion SNMP (facultatif)
- Nom d'utilisateur et mot de passe

L'assistant vous guide dans les étapes nécessaires à la configuration initiale du commutateur. Il vous aide également à le faire fonctionner en un minimum de temps. Vous n'êtes cependant pas obligé de l'utiliser : vous pouvez configurer le commutateur manuellement via l'interface CLI.

L'assistant permet de configurer les paramètres suivants :

- Adresse IP de la chaîne de communauté et du système de gestion SNMP (facultatif)
- Nom d'utilisateur et mot de passe
- Adresse IP de l'unité
- Adresse IP de la passerelle par défaut

Le message suivant s'affiche :

```
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.
The system will prompt you with a default answer; by pressing enter, you accept the default.
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.


Would you like to enter the Setup Wizard (you must answer this question within 60 seconds? (Y/N)[Y]Y
You can exit the Setup Wizard at any time by entering [ctrl+Z].
```

Si vous appuyez sur [N], l'assistant disparaît. Si vous ne répondez pas dans un délai de 60 secondes, il disparaît automatiquement et l'invite CLI s'affiche.

Si vous appuyez sur [Y], l'assistant démarre.

REMARQUE : si vous ne répondez pas dans les 60 secondes et si un serveur BootP se trouve sur le réseau, une adresse est obtenue à partir de ce dernier.

REMARQUE : vous pouvez quitter l'assistant à tout moment en appuyant sur [CTRL+Z].

Assistant - Étape 1

Le message suivant s'affiche :

```
The system is not setup for SNMP management by default.
To manage the switch using SNMP (required for Dell Network Manager) you can

   l  Setup the initial SNMP version 2 account now.

   l  Return later and setup additional SNMP v1/v3 accounts.


For more information on setting up SNMP accounts, please see the user documentation.


Would you like to setup the SNMP management interface now? (Y/N)[Y]Y
```

Appuyez sur [N] pour passer à l'étape 2.

Appuyez sur [Y] pour poursuivre l'utilisation de l'assistant. Le message suivant s'affiche :

```
To setup 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 CLI to change this setting, and to add additional management systems. 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: [Dell_Network_Manager]
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]
```

Entrez les informations suivantes :

- Chaîne de communauté SNMP, par exemple : Dell_Network_Manager.
- Adresse IP du système de gestion (A.B.C.D) ou caractères génériques (0.0.0.0) pour pouvoir assurer un contrôle à partir de toute station de gestion.

REMARQUE : les adresses IP et les masques commençant par zéro ne peuvent pas être utilisés.

Appuyez sur **Entrée**.

Assistant - Étape 2

Le message suivant s'affiche :

```
Now we need to setup your initial privilege (Level 15) user account.
This account is used to login to the CLI and Web interface.
You may setup other accounts and change privilege levels later.
For more information on setting up user accounts and changing privilege levels, see the user documentation.
To setup a user account:
Enter the user name<1-20>:[admin]
Please enter the user password:*
Please reenter the user password:*
```

Entrez les informations suivantes :

- Nom d'utilisateur (ex : "admin")
- Mot de passe et confirmation

REMARQUE : si les mots de passe entrés dans les deux champs ne sont pas identiques, une invite demande à l'utilisateur de recommencer.

Appuyez sur **Entrée**.

Assistant - Étape 3

Le message suivant s'affiche :

```
Next, an IP address is setup.

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.To setup an IP address:

Please enter the IP address of the device (A.B.C.D):[1.1.1.1]

Please enter the IP subnet mask (A.B.C.D or nn): [255.255.255.0]
```

Entrez l'adresse IP et le masque de sous-réseau IP (par exemple, respectivement 1.1.1.1 et 255.255.255.0).

Appuyez sur **Entrée**.

Assistant - Étape 4

Le message suivant s'affiche :

```
Finally, setup the default gateway.
Please enter the IP address of the gateway from which this network is reachable (e.g. 192.168.1.1).Default gateway (A.B.C.D):[0.0.0.0]
```

Entrez la passerelle par défaut.

Appuyez sur Entrée. Les informations suivantes s'affichent (selon les paramètres de l'exemple ci-dessus) :

```
This is the configuration information that has been collected:

============================================================

SNMP Interface = Dell_Network_Manager@0.0.0.0
User Account setup = admin
Password = *
Management IP address = 1.1.1.1 255.255.255.0
Default Gateway = 1.1.1.2

============================================================
```

Assistant - Étape 5

Le message suivant s'affiche :

```
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]Y
```

Appuyez sur [N] pour redémarrer l'assistant.

Appuyez sur [Y] pour poursuivre l'utilisation de l'assistant. Le message suivant s'affiche :

```
Configuring SNMP management interface
Configuring user account......
Configuring IP and subnet......

Thank you for using Dell Easy Setup Wizard. You will now enter CLI mode.
```

Assistant - Étape 6

L'invite CLI s'affiche.

Configuration avancée

Cette section fournit des informations relatives à l'allocation dynamique d'adresses IP et à la gestion de la sécurité basée sur le mécanisme AAA (Authentication, Authorization, Accounting). Elle traite des sujets suivants :

- Configuration des adresses IP via DHCP
- Configuration des adresses IP via BOOTP
- Gestion de la sécurité et configuration du mot de passe

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.

Obtention d'une adresse IP à partir d'un serveur DHCP

Lorsque le protocole DHCP est utilisé pour obtenir une adresse IP, l'unité agit en tant que client DHCP. Lorsque l'unité est réinitialisée, la commande DHCP est sauvegardée dans le fichier de configuration, mais pas l'adresse IP. Pour obtenir une adresse IP à partir d'un serveur DHCP, procédez comme suit :

1. 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.
2. Entrez les commandes suivantes pour utiliser le port sélectionné pour la réception de l'adresse IP. Dans l'exemple suivant, les commandes sont basées sur le type de port utilisé pour la configuration.
    - Attribution des adresses IP dynamiques :

```
console# configure

console(config)# interface ethernet 1/e1
```

```
console(config-if)# ip address dhcp hostname powerconnect

console(config-if)# exit

console(config)#
```

- Attribution des adresses IP dynamiques (dans un VLAN) :

```
console# configure

console(config)# interface ethernet vlan 1

console(config-if)# ip address dhcp hostname device

console(config-if)# exit

console(config)#
```

L'interface reçoit automatiquement l'adresse IP.

3. Pour vérifier cette adresse, entrez la commande **show ip interface** à l'invite du système, comme indiqué dans l'exemple suivant.

```
console# show ip interface

IP Address I/F Type



------------- ------ -------

100.1.1.1/24 vlan 1 dynamic
```

REMARQUE : il n'est pas nécessaire de supprimer la configuration de l'unité pour obtenir une adresse IP du serveur DHCP.

REMARQUE : lors de la copie des fichiers de configuration, évitez d'utiliser un fichier de configuration contenant une instruction permettant d'activer DHCP sur une interface correspondant au même serveur DHCP, ou à un serveur possédant une configuration identique. Si vous n'observez pas cette précaution, l'unité extrait le nouveau fichier de configuration et démarre à partir de celui-ci. Ensuite, elle active le DHCP comme indiqué dans ce nouveau fichier de configuration, et le DHCP lui donne alors l'instruction de recharger le même fichier.

REMARQUE : si vous configurez une adresse IP via DHCP, cette adresse est obtenue dynamiquement et la commande ip address dhcp est sauvegardée dans le fichier de configuration. En cas de défaillance de l'unité maître, l'unité de sauvegarde tente de nouveau d'obtenir l'adresse DHCP. Cela peut avoir les conséquences suivantes :

- La même adresse IP est attribuée.
- Une adresse IP différente est attribuée, provoquant une perte de la connectivité avec la station de gestion.
- Si le serveur DHCP n'est pas disponible, l'adresse IP ne peut pas être obtenue, provoquant une perte de la connectivité avec la station de gestion.

Réception d'une adresse IP à partir d'un serveur BOOTP

Le protocole standard BOOTP permet à l'unité de télécharger automatiquement sa configuration IP à partir de n'importe quel serveur BOOTP standard du

réseau. Dans ce cas, l'unité fonctionne en tant que client BOOTP.

Obtention d'une adresse IP à partir d'un serveur BOOTP :

1. Sélectionnez et connectez n'importe quel port à un serveur BOOTP ou à un sous-réseau contenant ce type de serveur, de manière à obtenir l'adresse IP.
2. À l'invite du système, tapez la commande **delete startup configuration** de manière à supprimer la configuration de démarrage de la mémoire flash.

L'unité se réamorce sans configuration et envoie des requêtes BOOTP au bout de 60 secondes. L'unité reçoit automatiquement l'adresse IP.

REMARQUE : lorsque l'unité redémarre, le fait d'entrer des données sur le terminal ASCII ou le clavier annule automatiquement le processus BOOTP et empêche l'obtention de l'adresse IP.

L'exemple suivant présente ce processus :

```
console> enable

console# delete startup-config

Startup file was deleted

console# reload

You haven't saved your changes. Are you sure you want to continue (y/n) [n]?

This command will reset the whole system and disconnect your current session. Do you want to continue (y/n) [n]?

*****************************************************

/* the device reboots */
```

Pour vérifier l'adresse IP, entrez la commande **show ip interface**.

L'unité est maintenant paramétrée avec une adresse IP.

Gestion de la sécurité et configuration du mot de passe

La sécurité du système est traitée via le mécanisme AAA (Authentication, Authorization, Accounting) qui gère les droits d'accès des utilisateurs, les privilèges et les méthodes de gestion. AAA utilise 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 **Startup** (Démarrer). Cette procédure est applicable uniquement sur le terminal local et permet d'accéder une seule fois à l'unité 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 :

- Terminal
- Telnet
- SSH
- HTTP
- HTTPS

REMARQUE : les mots de passe sont définis par l'utilisateur.

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. Bien que les noms d'utilisateur puissent être associés au niveau de privilège 15 sans qu'aucun mot de passe soit défini, il est recommandé de toujours en définir un. Dans le cas contraire, les utilisateurs dotés de privilèges peuvent accéder à l'interface Web avec n'importe quel mot de passe.

REMARQUE : il est possible de sécuriser les mots de passe en utilisant des commandes de gestion permettant, par exemple, de forcer leur expiration. Pour plus d'informations, consultez la section "Gestion de la sécurité et configuration du mot de passe".

Configuration d'un mot de passe initial pour le terminal

Pour configurer un mot de passe initial pour le terminal, 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 george
```

- Lorsque vous vous connectez à une unité pour la première fois via une session de terminal, tapez george à l'invite du mot de passe.
- Lorsque vous modifiez le mode de l'unité à "enable", tapez george à l'invite du mot de passe.

Configuration d'un mot de passe Telnet initial

Pour configurer un mot de passe Telnet initial, tapez 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 bob
```

- Lorsque vous vous connectez à une unité pour la première fois via une session Telnet, tapez bob comme mot de passe.
- Lorsque vous modifiez le mode de l'unité à "enable", tapez bob.

Configuration d'un mot de passe SSH initial

Pour configurer un mot de passe SSH initial, tapez les commandes suivantes :

```
console(config)# aaa authentication login default line

console(config)# aaa authentication enable default line

console(config)# line ssh

console(config-line)# login authentication default

console(config-line)# enable authentication default

console(config-line)# password jones
```

- Lorsque vous vous connectez à une unité pour la première fois via une session SSH, tapez jones comme mot de passe.
- Lorsque vous modifiez le mode de l'unité à "enable", tapez jones.

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 user1 level 15
```

Configuration d'un mot de passe HTTPS initial

Pour configurer un mot de passe HTTPS initial, tapez les commandes suivantes :

```
console(config)# ip https authentication local

console(config)# username admin password user1 level 15
```

Tapez les commandes suivantes une fois lorsque vous configurez une session de terminal, telnet ou SSH pour utiliser une session HTTPS.

REMARQUE : dans le navigateur Web, activez SSL version 2.0 ou suivante pour afficher le contenu de la page.

```
console(config)# crypto certificate generate key_generate
```

```
console(config)# ip https server
```

Lorsque vous activez une session http ou https pour la première fois, entrez le nom d'utilisateur admin et le mot de passe user1.

REMARQUE : les services http et https nécessitent un privilège de niveau 15 et permettent un accès direct aux fonctions de configuration.

Procédures de démarrage

Procédures du menu Startup (Démarrage)

Le menu Startup permet d'effectuer diverses opérations telles que le téléchargement de logiciels, la gestion de la mémoire flash et la récupération de mots de passe. Les procédures de diagnostic sont réservées exclusivement au personnel de maintenance et ne sont donc pas présentées dans ce document.

Vous pouvez accéder au menu Startup lors du démarrage de l'unité, immédiatement après la fin de l'auto-test de démarrage.

Pour accéder au menu Startup :

1. Mettez l'unité sous tension et attendez le message de démarrage automatique.

```
************************************************

********** SYSTEM RESET **********

************************************************

Boot1 Checksum Test.............................PASS

Boot2 Checksum Test.............................PASS

Flash Image Validation Test.....................PASS

BOOT Software Version 1.0.0.05 Built 06-Jan-2005 14:46:49

Carrier board, based on PPC8247

128 MByte SDRAM. I-Cache 16 KB. I-Cache 16 KB. Cache Enabled.

Autoboot in 2 seconds - press RETURN or Esc. to abort and enter prom.
```

2. Lorsque ce message s'affiche, appuyez sur <Entrée> pour accéder au menu Startup. Les procédures du menu de démarrage peuvent être lancées à partir du terminal ASCII ou de Windows HyperTerminal.

```
[1] Download Software
```

```
[2] Erase Flash File


[3] Password Recovery Procedure


[4] Enter Diagnostic Mode


[5] Set Terminal Baud-Rate


[6] Back
```

Les sections qui suivent décrivent les options du menu Startup.

REMARQUE : n'oubliez pas que la sélection des options du menu Startup doit être effectuée dans un délai de 35 secondes (valeur par défaut). Ce délai peut être modifié via l'interface CLI.

REMARQUE : le mode Diagnostics ne peut être utilisé que par le personnel de maintenance **(option[4])**. Il n'est donc pas décrit dans ce guide.

Option [1] - Download software (Téléchargement de logiciels)

Cette procédure est utilisée lorsqu'une nouvelle version d'un programme doit être téléchargée pour remplacer des fichiers altérés ou mettre à niveau les logiciels du système. Pour télécharger des logiciels à partir du menu Startup :

1. À partir du menu Startup, appuyez sur [1]. L'invite suivante s'affiche :

```
Downloading code using XMODEM


****************************************************************


*** Running SW Ver. 1.0.0.30 Date 09-Jan-2005 Time 14:30:02


****************************************************************


HW version is


Base Mac address is  : 00:00:b0:45:54:00


Dram size is: 128M bytes


Dram first block size is: 36864K bytes


Dram first PTR is : 0x1C00000


Flash size is: 16M


Loading running configuration.
```

```
Number of configuration items loaded: 5

Loading startup configuration.

Number of configuration items loaded: 5

Device configuration:

Slot 1 - PowerConnect 3424 HW Rev. 0.0

------------------------------

-- Unit Number 1 Standalone --

------------------------------

BOXP_high_appl_init: dpssIpcInitStandAlone

Tapi Version: v1.3.1.6P_01_03

Core Version: v1.3.1.6P_01_02

01-Jan-2000 01:01:19 %INIT-I-InitCompleted: Initialization task is completed

01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG: FAN# 1 status changed - operational.

01-Jan-2000 01:01:19 %Entity-I-SEND-ENT-CONF-CHANGE-TRAP: entity configuration change trap.

01-Jan-2000 01:01:19 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

01-Jan-2000 01:01:19 %Box-I-PS-STAT-CHNG: PS# 1 status changed - operational.
```

2. Si vous utilisez HyperTerminal, cliquez sur Transfer (Transférer) dans la barre de menus d'HyperTerminal.
3. Dans la zone Filename (Nom de fichier), entrez le chemin d'accès du fichier à télécharger.
4. Vérifiez que le protocole Xmodem est sélectionné dans la zone Protocol (Protocole).
5. Cliquez sur Send (Envoyer). Le logiciel est téléchargé.

REMARQUE : une fois le téléchargement terminé, l'unité redémarre automatiquement.

Option [2] - Erase FLASH File (Supprimer le fichier Flash)

Il arrive que la configuration de l'unité doive être effacée. Tous les paramètres définis via CLI, SNMP ou à l'aide de l'interface Web doivent alors être reconfigurés.

Pour effacer la configuration de l'unité :

1. À partir du menu Startup, appuyez sur [2] dans un délai de 2 secondes pour effacer le fichier flash. Le message suivant s'affiche :

```
Warning! About to erase a Flash file.


Are you sure (Y/N)? y
```

2. Appuyez sur Y. Le message suivant s'affiche :

```
Write Flash file name (Up to 8 characters, Enter for none.):config


File config (if present) will be erased after system initialization


======== Press Enter To Continue ========
```

3. Tapez le nom de fichier flash config. La configuration est effacée et l'unité redémarre.
4. Recommencez la configuration initiale de l'unité.

Option [3] - Password Recovery (Récupération de mot de passe)

Le menu Startup permet également de lancer une procédure de récupération des mots de passe perdus. Cette procédure permet d'accéder à l'unité une seule fois sans mot de passe.

Pour récupérer un mot de passe, uniquement à partir de la console locale :

1. À partir du menu Startup, tapez [3] et appuyez sur <Entrée>. Le mot de passe est supprimé.

   Entrez votre choix ou appuyez sur 'Échap' pour quitter le menu.

```
Current password will be ignored!
```

REMARQUE : pour protéger l'unité contre tout accès non autorisé à la configuration, reconfigurez les mots de passe associés aux fonctions de gestion.

Option [4] - Enter Diagnostic Mode (Accéder au mode diagnostics)

Cette option est réservée au personnel de maintenance.

Option [5] - Set Terminal Baud-Rate (Définir le débit en bauds du terminal)

Pour définir le débit en bauds du terminal, tapez [5] et appuyez sur <Entrée>.

Entrez votre choix ou appuyez sur "Échap" pour quitter le menu.

Définissez le débit en bauds de l'unité à 38400.

Téléchargement de logiciels via le serveur TFTP

Cette section indique comment télécharger l'image système et l'image de démarrage de l'unité via un serveur TFTP. Vous devez avoir configuré le serveur TFTP avant de lancer le téléchargement.

Téléchargement de l'image système

L'unité démarre en décompressant l'image système stockée dans la zone de mémoire flash. Lorsqu'une nouvelle image est téléchargée, elle est enregistrée dans l'autre zone de mémoire réservée à une copie de l'image système.

Au démarrage suivant, l'unité décompresse l'image système en cours et s'exécute à partir de celle-ci, sauf si l'utilisateur a configuré les paramètres de démarrage différemment.

Pour télécharger une image système via le serveur TFTP :

1. Assurez-vous qu'une adresse IP est configurée sur l'un des ports de l'unité et que des requêtes ping peuvent être envoyées au serveur TFTP.
2. Assurez-vous que le fichier à télécharger est enregistré sur le serveur TFTP (fichier arc).
3. Tapez la commande **show version** pour vérifier quelle version du logiciel est actuellement exécutée sur l'unité. Exemple des informations affichées :

```
console# show version

SW version 1.0.0.30 (date 27-Jan-2005 time 13:42:41)

Boot version 1.0.0.05 (date 27-Jan-2005 time 15:12:20)

HW version
```

4. Tapez la commande **show bootvar** pour vérifier l'image système en cours. Exemple des informations affichées :

```
console# show bootvar

Images currently available on the Flash

Image-1 active (selected for next boot)

Image-2 not active

console#
```

5. Entrez la commande **copy tftp:**//{adresse tftp}/{nom du fichier} **image** pour copier une nouvelle image système sur l'unité. Une fois la nouvelle image téléchargée, elle est enregistrée dans une zone allouée à cet effet (image-2 dans l'exemple). Exemple des informations affichées :

```
console# copy tftp://176.215.31.3/file1.ros image

Accessing file `file1' on 176.215.31.3Ö

Loading file1 from 176.215.31.3:

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy took 00:01:11 [hh:mm:ss]
```

Les points d'exclamation indiquent qu'une copie est en cours. Chaque point d'exclamation correspond au transfert réussi de 512 octets. Un point indique un dépassement du délai autorisé pour la copie. Plusieurs points successifs indiquent que la copie a échoué.

6. Sélectionnez l'image à utiliser pour le démarrage suivant en tapant 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.

Exemple des informations affichées :

```
console# boot system image-2

console# show bootvar

Images currently available on the Flash

Image-1 active

Image-2 not active (selected for next boot)
```

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.

7. Entrez la commande **reload**. Le message suivant s'affiche :

```
console# reload

This command will reset the whole system and disconnect your current session. Do you want to continue (y/n)[n]?
```

8. Entrez y. L'unité redémarre.

Téléchargement de l'image de démarrage

Pour mettre à jour l'image de démarrage, vous devez télécharger la nouvelle image à partir du serveur TFTP et la programmer dans la mémoire flash. Cette image est chargée lors de la mise sous tension de l'unité. Les utilisateurs n'ont aucun contrôle sur les copies d'images de démarrage. Pour télécharger une image de démarrage via le serveur TFTP :

1. Assurez-vous qu'une adresse IP est configurée sur l'un des ports de l'unité et que des requêtes ping peuvent être envoyées au serveur TFTP.
2. Assurez-vous que le fichier à télécharger est enregistré sur le serveur TFTP (fichier rfb).
3. Tapez la commande show version pour vérifier quelle version du logiciel est actuellement exécutée sur l'unité. Exemple des informations affichées :

```
console# show version

SW version 1.0.0.30 (date 27-Jan-2005 time 13:42:41)

Boot version 1.0.0.05 (date 27-Jan-2005 time 15:12:20)

HW version
```

4. Entrez la commande **copy tftp://**{adresse tftp}/{nom du fichier} **boot** pour copier l'image de démarrage sur l'unité. Exemple des informations affichées :

```
console# copy tftp://176.215.31.3/332448-10018.rfb boot
```

```
Erasing file..done.


!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!


Copy: 2739187 bytes copied in 00:01:13 [hh:mm:ss]
```

5. Entrez la commande **reload**. Le message suivant s'affiche :

```
console# reload


This command will reset the whole system and disconnect your current session. Do you want to continue (y/n)[n]?
```

6. Entrez y. L'unité redémarre.

Paramètres par défaut des ports

Parmi les généralités sur la configuration des ports du périphérique, vous trouverez une brève description du mécanisme de négociation automatique et des paramètres par défaut des ports de commutation.

Négociation automatique

La négociation automatique permet la détection automatique de la vitesse, du mode duplex et du contrôle de flux sur tous les ports de commutation 10/100/1000BaseT. Par défaut, elle est activée au niveau de chaque port.

La négociation automatique est un protocole entre deux partenaires de liaison, qui 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 (fonction désactivée par défaut). Les ports communiquent ensuite en utilisant leur dénominateur commun le plus élevé.

Si vous connectez un contrôleur NIC qui ne prend pas en charge la négociation automatique ou n'est pas défini sur négociation automatique, le port de commutation de l'unité et le contrôleur NIC doivent être définis manuellement sur la même vitesse et le mode duplex.

Si la station située de l'autre côté du lien tente de négocier automatiquement avec un port 100BaseT de l'unité qui a été configuré manuellement en duplex intégral, l'auto-négociation aboutit à une tentative de fonctionnement de la station en mode semi duplex.

MDI/MDIX

L'unité prend en charge la détection automatique des câbles directs et croisés sur tous les ports de commutation 10/100/1000BaseT. Cette fonction est activée en même temps que la négociation automatique, dont elle fait partie.

Lorsque la fonction MDI/MDIX (Interface croisée dépendante du média) est activée, la correction automatique des erreurs sur la sélection de câbles est possible, ce qui rend inutile la distinction entre câbles directs et câbles simulateurs de modem. Le câblage standard des stations terminales est MDI (Interface dépendante du média) et le câblage standard des concentrateurs et des commutateurs est MDIX.

Contrôle de flux

L'unité prend en charge le contrôle de flux 802.3x pour les ports configurés en mode duplex intégral. Par défaut, cette fonction est désactivée. Elle peut être activée indépendamment sur chaque port. Le mécanisme de contrôle du flux permet à la partie réceptrice de signaler à la partie émettrice que la transmission doit être interrompue temporairement pour empêcher la surcharge de la mémoire tampon.

Contre-pression

L'unité prend en charge la contre-pression pour les ports configurés en mode semi duplex. Par défaut, cette fonction est désactivée. Elle peut être activée indépendamment sur chaque port. Le mécanisme de contre-pression empêche temporairement la partie émettrice de transmettre du trafic. La partie réceptrice peut occuper une liaison pour la rendre indisponible au trafic.

Paramètres par défaut du port de commutation

Le tableau suivant décrit les paramètres par défaut des ports.

Tableau 4-1. Paramètres par défaut des ports

Fonction	***Paramètre par défaut***
Vitesse et mode du port	Cuivre 10/100BaseT : négociation automatique 100 Mbps, duplex intégral
	Cuivre/SFP 10/100/1000BaseT : négociation automatique 1000 Mbps, duplex intégral
État de transfert du port	Activé
Marquage du port	Pas de marquage
Contrôle de flux	Inactif (désactivé sur le port d'entrée)
Contre-pression	Inactive (désactivée sur le port d'entrée)

Retour au sommaire

Retour au sommaire

Utilisation de Dell OpenManage Switch Administrator

Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

Cette section présente l'interface utilisateur de Dell OpenManage Switch Administrator.

Démarrage de l'application

REMARQUE : l'adresse IP doit être définie avant le démarrage de l'application. Pour plus d'informations, consultez la section "Configuration initiale".

1. Ouvrez un navigateur Web.
2. Tapez l'adresse IP de l'unité dans la barre d'adresse et appuyez sur <Entrée>.
3. Lorsque la fenêtre **Log In** (Ouverture de session) s'affiche, entrez le nom d'utilisateur et le mot de passe appropriés.

REMARQUE : les mots de passe font la distinction entre majuscules et minuscules, et doivent obligatoirement être alphanumériques.

4. Cliquez sur **OK**.

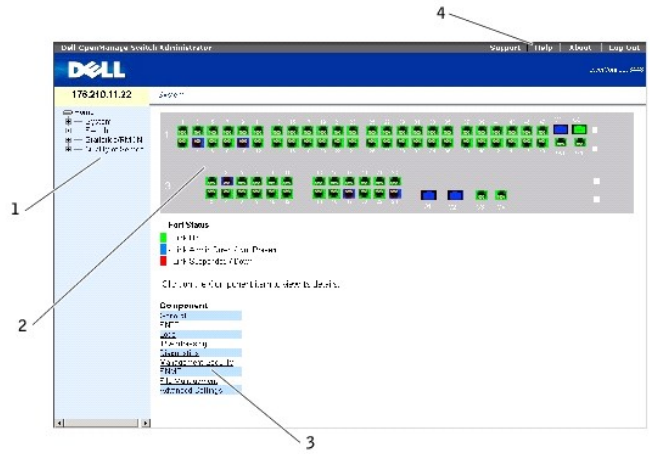
La page d'accueil de **Dell OpenManage™ Switch Administrator** s'affiche.

Présentation de l'interface

La page d'accueil offre différents modes d'affichage :

- Vue Arborescence : affichée dans le volet gauche de la page d'accueil, cette vue fournit une représentation hiérarchisée des différentes fonctionnalités et de leurs composants.
- Vue de l'unité : située dans le volet droit de la page d'accueil, cette vue fournit une représentation graphique de l'unité, une zone d'informations ou un tableau et des instructions de configuration.

Figure 5-1. Composants de Switch Administrator



Le tableau 5-1 répertorie les éléments de l'interface et indique les numéros correspondants.

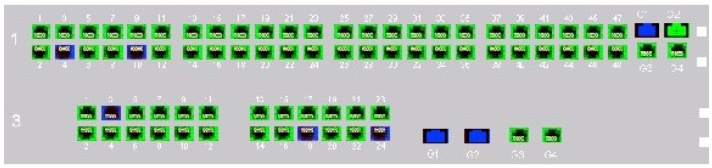
Tableau 5-1. Éléments de l'interface

Composant	Description
1	L'arborescence contient la liste des différentes fonctionnalités de l'unité. Vous pouvez développer ou réduire les branches de l'arborescence de façon à afficher ou à masquer les composants rattachés à une fonctionnalité spécifique. En déplaçant la barre verticale vers la droite, vous pouvez agrandir le volet de l'arborescence pour afficher le nom complet des composants.
2	La vue de l'unité fournit des informations sur les ports, la configuration et l'état en cours, les tableaux et les composants. Selon l'option sélectionnée, la zone située en bas de cette vue affiche soit des informations supplémentaires sur l'unité, soit des boîtes de dialogue de configuration.
3	La liste des composants répertorie les composants de l'unité. Vous pouvez également afficher des composants en développant une fonctionnalité dans l'arborescence.
4	Les boutons d'information permettent d'accéder à des informations sur l'unité et au support Dell. Pour plus d'informations, consultez la section "Boutons d'information".

Représentation de l'unité

La page d'accueil contient une représentation graphique du panneau avant de l'unité.

Figure 5-2. Voyants des ports



La couleur associée à un port permet de déterminer s'il est actif. Les couleurs possibles sont les suivantes :

Tableau 5-2. Voyants des ports et voyants d'empilage du PowerConnect

Composant	Description
Voyants des ports	
Vert	Le port est activé.
Rouge	Une erreur est survenue sur le port.
Bleu	Le port est désactivé.

Rouge	L'unité n'est pas reliée à une pile.

REMARQUE : dans le module OpenManage Switch Administrator, les voyants des ports ne sont pas représentés sur le panneau avant des PowerConnect. L'état des voyants ne peut donc être déterminé qu'en les observant directement sur l'unité. Cependant, les voyants d'empilage reflètent l'état des ports d'empilage. Pour plus d'informations sur les voyants, consultez la section "Signification des voyants".

Utilisation des boutons de Switch Administrator

Cette section présente les boutons de l'interface d'OpenManage Switch Administrator. Ces boutons sont répartis dans les catégories suivantes :

Boutons d'information

Les boutons d'information permettent d'accéder au support et à l'aide en ligne, ainsi qu'à des informations sur les interfaces du programme Switch Administrator.

Tableau 5-3. Boutons d'information

Bouton	Description
Support	Ouvre 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 de l'unité. L'aide est contextuelle. Cela signifie, par exemple, que si la page **IP Addressing** (Adressage IP) est ouverte, la rubrique d'aide relative à la définition de l'adresse 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 (Fermeture de session)	Affiche la fenêtre de fermeture de session.

Boutons de gestion de l'unité

Les boutons de gestion permettent de configurer facilement les informations de l'unité. Il s'agit des boutons suivants :

Tableau 5-4. Boutons de gestion de l'unité

Bouton	Description
Apply Changes (Appliquer les modifications)	Applique les modifications définies à l'unité.
Add (Ajouter)	Ajoute des informations dans des tableaux ou des fenêtres.
Telnet	Ouvre une session Telnet.
Query (Interroger)	Effectue des recherches dans des tables.
Show All (Afficher tout)	Affiche les tables de l'unité.
Left arrow / Right arrow (Flèche gauche/droite)	Fait passer des informations d'une liste à une autre.
Refresh (Actualiser)	Actualise les informations relatives à l'unité.
Reset All Counters (Réinitialiser tous les compteurs)	Réinitialise les compteurs de statistiques.
Print (Imprimer)	Imprime les informations qui figurent dans les pages ou les tables du **système de gestion du réseau**.
Draw (Dessiner)	Crée des graphiques de statistiques en temps réel.

Définitions des champs

Les champs définis par l'utilisateur peuvent contenir de 1 à 159 caractères, sauf indication contraire figurant sur la page Web d'OpenManage Switch Administrator. Tous les caractères peuvent être utilisés, à l'exception des suivants :

1 \

- /
- :
- *
- ?
- <
- >
- |

Accès à l'unité via l'interface CLI

L'unité peut être gérée par le biais d'une connexion directe avec le port du terminal ou par l'intermédiaire d'une connexion Telnet. Dans ce dernier cas, assurez-vous qu'une adresse IP est définie pour l'unité et que la station de travail utilisée pour accéder à l'unité est connectée avant d'utiliser les commandes de l'interface CLI.

Pour plus d'informations sur la configuration d'une adresse IP initiale, consultez la section "Configuration initiale".

REMARQUE : vérifiez que le logiciel a été téléchargé sur l'unité avant d'utiliser l'interface CLI pour ouvrir une connexion distante.

Connexion par l'intermédiaire du terminal

1. Mettez l'unité sous tension et attendez la fin du démarrage.
2. À l'affichage de l'invite `Console>`, tapez `enable` et appuyez sur <Entrée>.
3. Configurez l'unité et entrez les commandes nécessaires à l'exécution des tâches requises.
4. Lorsque vous avez terminé, entrez la commande **exit** du mode Privileged EXEC (EXEC privilégié).

   La session est fermée.

REMARQUE : lorsqu'un utilisateur ouvre une session en mode Privileged EXEC, il est connecté à la place de l'utilisateur en cours.

Connexion Telnet

Le protocole Telnet est un protocole TCP/IP d'émulation de terminal. Les terminaux RS-232 peuvent être reliés à l'unité locale au moyen d'une connexion virtuelle, via un réseau utilisant le protocole TCP/IP. La connexion Telnet constitue une alternative à la connexion à un terminal local lorsqu'une connexion distante s'impose.

L'unité peut gérer jusqu'à quatre sessions Telnet simultanées. Toutes les commandes de l'interface CLI peuvent être utilisées au cours d'une session Telnet.

Pour ouvrir une session Telnet :

1. Sélectionnez Démarrer>Exécuter.

   La fenêtre Exécuter s'affiche.
2. Dans la fenêtre **Exécuter**, tapez `Telnet` *<adresse IP>* dans la zone **Ouvrir**.
3. Cliquez sur **OK.**

   La session Telnet démarre.

Utilisation de l'interface de ligne de commande (CLI)

Cette section contient des informations sur l'utilisation de l'interface CLI.

Présentation des modes de commande

L'interface de ligne de commande comprend différents modes de commande. Un ensemble de commandes spécifiques est associé à chaque mode. Pour afficher la liste des commandes disponibles pour un mode spécifique, il suffit de taper un point d'interrogation (?) à l'invite du terminal.

La commande permettant d'accéder à un autre mode varie selon le mode utilisé.

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 terminal et utilisé pour accéder à des sous-systèmes de configuration tels que l'interface CLI. L'accès au niveau suivant (mode Privileged EXEC) exige la saisie d'un mot de passe (s'il a été configuré).

Le mode Privileged EXEC permet d'accéder à la configuration générale de l'unité. Pour modifier globalement certaines configurations spécifiques, vous devez passer au niveau suivant, appelé "Global Configuration" (Configuration globale). La saisie d'un mot de passe n'est pas obligatoire.

Le mode Global Configuration gère la configuration de l'unité au niveau général.

Le mode Interface Configuration (Configuration de l'interface) permet de configurer l'unité 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" (Configuration de la sous-interface). La saisie d'un mot de passe n'est pas obligatoire.

Mode User EXEC (EXEC utilisateur)

Le mode User EXEC est activé par défaut lorsque vous ouvrez une session sur l'unité. L'invite se compose du nom d'hôte suivi d'un chevron (>). 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 unités distantes, 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 (EXEC privilégié)

Ce mode permet de protéger le système et les paramètres de fonctionnement contre tout accès non autorisé. Les mots de passe s'affichent à l'écran et font la distinction entre majuscules et minuscules.

Pour accéder à ce mode et afficher la liste des commandes disponibles :

1. À l'invite, tapez `enable` et appuyez sur <Entrée>.
2. À l'invite de saisie du mot de passe, entrez le mot de passe et appuyez sur <Entrée>.

L'invite du mode Privileged EXEC se compose du nom d'hôte de l'unité, suivi du symbole #. Exemple :

```
console#
```

Pour afficher la liste des commandes disponibles, tapez ? à l'invite.

Pour revenir du mode Privileged EXEC au mode User EXEC, tapez `disable` et appuyez sur <Entrée>.

L'exemple ci-dessous explique comment accéder au mode Privileged EXEC et revenir au mode User EXEC :

```
console> enable

Enter Password: ******

console#

console# disable

console>
```

Utilisez la commande **exit** pour revenir à un mode précédent (par exemple, pour passer du mode Interface Configuration au mode Global Configuration, ou pour accéder de ce dernier au mode Privileged EXEC).

Mode Global Configuration (Configuration globale)

Les commandes de configuration globale s'appliquent aux fonctionnalités du système, plutôt qu'à un protocole ou à une interface spécifique.

Pour accéder au mode de configuration globale, à l'invite du mode Privileged EXEC, tapez la commande **configure** et appuyez sur <Entrée>. L'invite du mode Global Configuration se compose du nom d'hôte de l'unité suivi de (config) et du symbole dièse (#).

```
console(config)#
```

Pour afficher la liste des commandes disponibles, tapez ? à l'invite.

Pour revenir du mode Global Configuration au mode Privileged EXEC, tapez la commande **exit** ou utilisez le raccourci-clavier <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#
```

Pour obtenir la liste complète des modes de l'interface CLI, consultez le document **Dell™ PowerConnect™ 3424/P and PowerConnect 3448/P CLI Guide** (Guide de référence CLI des systèmes Dell™ PowerConnect™ 3424/P et PowerConnect 3448/P).

Retour au sommaire

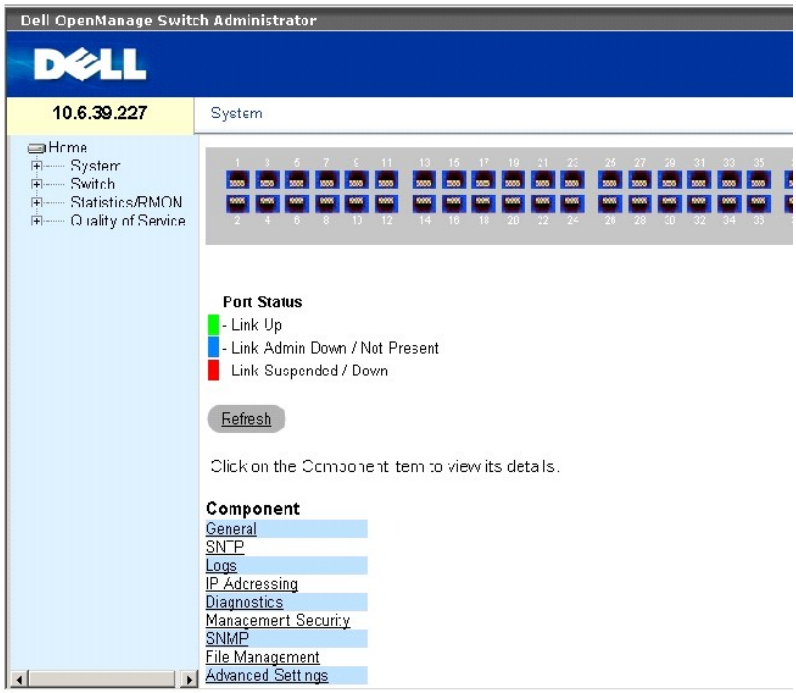
Retour au sommaire

Configuration des informations du système

Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

Cette section fournit des informations sur la définition des paramètres système, et plus particulièrement sur les fonctions de sécurité, sur le téléchargement de logiciels et sur la réinitialisation de l'unité. Pour ouvrir la page **System** (Système), cliquez sur **System** dans l'arborescence.

Figure 6-1. System (Système)



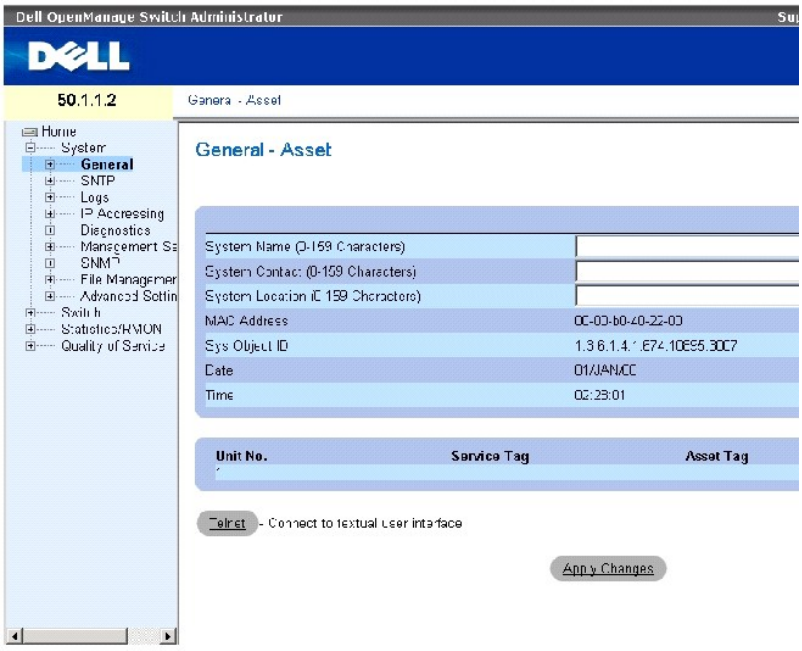
Définition des informations générales relatives au commutateur

La page **General** (Général) contient des liens vers des pages qui permettent aux administrateurs réseau de configurer certains paramètres du commutateur.

Affichage des informations d'inventaire du commutateur

La page Asset (Inventaire) contient les paramètres qui permettent de configurer et d'afficher des informations générales sur l'unité : nom du système, emplacement et contact, adresse MAC du système, ID d'objet du système, date, heure et durée de fonctionnement. Pour ouvrir la page Asset (Inventaire), cliquez sur System (Système) → General (Général) → Asset (Inventaire) dans l'arborescence.

Figure 6-2. Asset (Inventaire)



La page Asset (Inventaire) contient les champs suivants :

System Name (Nom du système - 0 à 159 caractères) : indique le nom attribué à l'unité par l'utilisateur.

System Contact (Contact système - 0 à 159 caractères) : indique le nom de la personne qui fait office de contact pour ce système.

System Location (Emplacement du système - 0 à 159 caractères) : indique l'emplacement sur lequel le système est actuellement exécuté.

MAC Address (Adresse MAC) : indique l'adresse MAC de l'unité.

Sys Object ID (ID objet sys) : identification du fournisseur du sous-système de gestion du réseau dans l'entité.

Date (DD/MMM/YY) (Date, JJ/MMM/AA) : indique la date du jour, au format jour, mois, année. Par exemple, la date 10/OCT/03 correspond au 10 octobre 2003.

Time (HH:MM:SS) (Heure, HH/MM/SS) : indique l'heure, au format heure, minute, seconde. Par exemple, 20:12:21 correspond à vingt heures, douze minutes et vingt-et-une secondes.

Unit No. (N° d'unité) : indique le numéro d'unité pour lequel les informations d'inventaire d'unité sont affichées.

Service Tag (Numéro de service) : indique le numéro de référence à communiquer pour la maintenance de l'unité.

Asset Tag (Numéro d'inventaire - 0 à 16 caractères) : indique la référence attribuée à l'unité par l'utilisateur.

Serial No. (Numéro de série) : indique le numéro de série de l'unité.

Définition des informations système

1. Affichez la page Asset (Inventaire).
2. Complétez les champs correspondants.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres système sont définis et l'unité est mise à jour.

Ouverture d'une session Telnet

1. Affichez la page Asset (Inventaire).
2. Cliquez sur **Telnet**.

Une session Telnet s'affiche alors.

Configuration des informations relatives à l'unité à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher et de compléter les champs de la page Asset (Inventaire).

Tableau 6-1. Commandes d'inventaire CLI

Commande CLI	Description
hostname nom	Définit ou modifie le nom d'hôte de l'unité.
snmp-server contact texte	Définit un contact pour le système.
snmp-server location texte	Précise l'emplacement de l'unité.
clock set hh:mm:ss jour mois année	Définit manuellement l'horloge et la date du système.
show clock [detail]	Affiche l'heure et la date de l'horloge système.
show system id	Affiche le numéro de service.
show system	Affiche les informations système.
asset-tag texte	Définit le numéro d'inventaire attribué à l'unité.
show stack <1-6>	Affiche les informations des piles système.
show system [unit *unité*]	Affiche les informations système.
show system id [unit *unité*]	Affiche les informations d'identification système.

Voici un exemple de définition du nom d'hôte de l'unité, du nom de la personne qui fait office de contact pour ce système, de l'emplacement de l'unité, de l'heure et de la date de l'horloge système à l'aide des commandes CLI :

```
console(config)# hostname dell

dell (config)# snmp-server contact Dell_Tech_Supp

dell (config)# snmp-server location New_York

dell (config)# exit

Console(config)# snmp-server host 10.1.1.1 management 2
```

```
Console# clock set 13:32:00 7 Mar 2002

Console# show clock

15:29:03 Jun 17 2002
```

Voici un exemple d'affichage des informations système d'une unité autonome à l'aide des commandes CLI :

console# **show system id**	
Service tag :	
Serial number : 51	
Asset tag :	
console# **show system**	
System Description:	Ethernet Switch
System Up Time (days,hour:min:sec):	0,00:00:57
System Contact:	
System Name:	CARRIER-1
System Location:	
System MAC Address:	00:00:00:08:12:51
System Object ID:	1.3.6.1.4.1.674.10895.3006
Type:	PowerConnect 3424
Main Power Supply Status:	OK
Fan 1 Status:	NOT OPERATIONAL
Fan 2 Status:	NOT OPERATIONAL
Temperature (Celsius):	30

Temperature Sensor Status:	OK

Voici un exemple d'affichage des informations système d'une pile d'unités à l'aide des commandes CLI :

console# **show system id**

Unit	Serial number	Asset tag	Service tag
1	893658972	mkt-1	89788978
2	893658973	mkt-2	89788979
3	893658974	mkt-3	89788980
4	893658975	mkt-4	89788981
5	893658976	mkt-5	89788982
6	893658977	mkt-6	89788983

console# **show system**

Unit	Type
1	PowerConnect 3424
2	PowerConnect 3424
3	PowerConnect 3428
4	PowerConnect 3424P
5	PowerConnect 3424P
6	PowerConnect 3424P

Unit	Main Power Supply		Redundant Power Supply		
----	----------		----------		
1	OK				
2	OK				
3	OK				
4	OK		OK		
5	OK		OK		
6	OK		OK		
Unit	Fan1	Fan2	Fan3	Fan4	Fan5
----	----	----	----	----	----
1	OK	OK			
2	OK	OK			
3	OK	OK			
4	OK	OK	OK	OK	OK
5	OK	OK	OK	OK	OK
6	OK	OK	OK	OK	OK
Unit	Temperature (Celsius)		Temperature Sensor Status		
----	----------		----------		
1	30		OK		
2	30		OK		
3	30		OK		
4	30		OK		
5	30		OK		

6	30		OK		

Définition des paramètres horaires du système

La page Time Synchronization (Synchronisation horaire) contient des champs permettant de définir les paramètres horaires système pour l'horloge du matériel locale et l'horloge SNTP externe. Si l'heure système est mise à jour à l'aide d'une horloge SNTP externe et que cette horloge tombe en panne, l'heure système de l'horloge du matériel locale est rétablie. L'option Daylight Savings Time (Heure d'été) peut être activée sur l'unité. Voici une liste des passages à l'heure d'été dans certains pays :

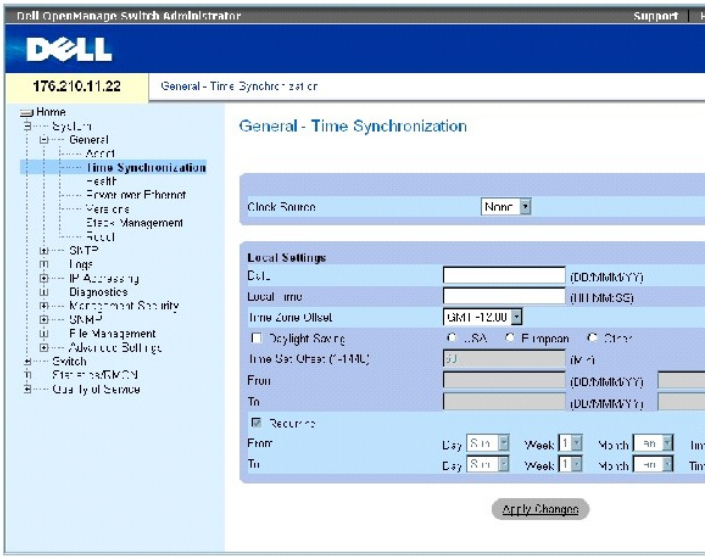
- Albanie : du dernier week-end de mars au dernier week-end d'octobre.
- Australie : de la fin octobre à la fin mars.
- Australie - Tasmanie : du début octobre à la fin mars.
- Arménie : du dernier week-end de mars au dernier week-end d'octobre.
- Autriche : du dernier week-end de mars au dernier week-end d'octobre.
- Bahamas : d'avril à octobre, conformément au passage à l'heure d'été aux États-Unis.
- Biélorussie : du dernier week-end de mars au dernier week-end d'octobre.
- Belgique : du dernier week-end de mars au dernier week-end d'octobre.
- Brésil : du 3ème dimanche d'octobre au 3ème samedi de mars. Pendant cette période, les Brésiliens habitant dans la plupart des régions du sud-est avancent leur montre d'une heure.
- Chili : (Île de Pâques) du 9 mars au 12 octobre. Le premier dimanche de mars ou après le 9 mars.
- Chine : pas de passage à l'heure d'été en Chine.
- Canada : du premier dimanche d'avril au dernier dimanche d'octobre. Le passage à l'heure d'été est généralement fixé par les gouvernements des provinces et des territoires. Des exceptions peuvent s'appliquent dans certaines villes.
- Cuba : du dernier dimanche de mars au dernier dimanche d'octobre.
- Chypre : du dernier week-end de mars au dernier week-end d'octobre.
- Danemark : du dernier week-end de mars au dernier week-end d'octobre.
- Égypte : du dernier vendredi d'avril au dernier jeudi de septembre.
- Estonie : du dernier week-end de mars au dernier week-end d'octobre.
- Finlande : du dernier week-end de mars au dernier week-end d'octobre.
- France : du dernier week-end de mars au dernier week-end d'octobre.
- Allemagne : du dernier week-end de mars au dernier week-end d'octobre.
- Grèce : du dernier week-end de mars au dernier week-end d'octobre.
- Hongrie : du dernier week-end de mars au dernier week-end d'octobre.
- Inde : pas de passage à l'heure d'été en Inde.
- Iran : du 1er Farvardin au 1er Mehr.
- Irak : du 1er avril au 1er octobre.
- Irlande : du dernier week-end de mars au dernier week-end d'octobre.
- Israël : varie selon les années.
- Italie : du dernier week-end de mars au dernier week-end d'octobre.
- Japon : pas de passage à l'heure d'été au Japon.
- Jordanie : du dernier week-end de mars au dernier week-end d'octobre.
- Lettonie : du dernier week-end de mars au dernier week-end d'octobre.
- Liban : du dernier week-end de mars au dernier week-end d'octobre.
- Lituanie : du dernier week-end de mars au dernier week-end d'octobre.
- Luxembourg : du dernier week-end de mars au dernier week-end d'octobre.
- Macédoine : du dernier week-end de mars au dernier week-end d'octobre.
- Mexique : du premier dimanche d'avril à 02:00 au dernier dimanche d'octobre à 02:00.
- Moldavie : du dernier week-end de mars au dernier week-end d'octobre.
- Monténégro : du dernier week-end de mars au dernier week-end d'octobre.
- Pays-Bas : du dernier week-end de mars au dernier week-end d'octobre.
- Nouvelle-Zélande : du premier dimanche d'octobre au premier dimanche avant ou après le 15 mars.
- Norvège : du dernier week-end de mars au dernier week-end d'octobre.
- Paraguay : du 6 avril au 7 septembre.

- Pologne : du dernier week-end de mars au dernier week-end d'octobre.
- Portugal : du dernier week-end de mars au dernier week-end d'octobre.
- Roumanie : du dernier week-end de mars au dernier week-end d'octobre.
- Russie : du dernier week-end de mars au dernier week-end d'octobre.
- Serbie : du dernier week-end de mars au dernier week-end d'octobre.
- Slovaquie : du dernier week-end de mars au dernier week-end d'octobre.
- Afrique du Sud : pas de passage à l'heure d'été en Afrique du Sud.
- Espagne : du dernier week-end de mars au dernier week-end d'octobre.
- Suède : du dernier week-end de mars au dernier week-end d'octobre.
- Suisse : du dernier week-end de mars au dernier week-end d'octobre.
- Syrie : du 31 mars au 30 octobre.
- Taiwan : pas de passage à l'heure d'été à Taiwan.
- Turquie : du dernier week-end de mars au dernier week-end d'octobre.
- Royaume-Uni : du dernier week-end de mars au dernier week-end d'octobre.
- États-Unis : du premier dimanche d'avril à 02:00 au dernier dimanche d'octobre à 02:00.

Pour plus d'informations sur SNTP, voir "Configuration des paramètres SNTP".

Pour ouvrir la page Time Synchronization (Synchronisation horaire), cliquez sur **System** (Système) → **General** (Général) → **Time Synchronization** (Synchronisation horaire) dans l'*arborescence*.

Figure 6-3. Time Synchronization (Synchronisation horaire)



La page Time Synchronization (Synchronisation horaire) contient les champs suivants :

Source de l'horloge

Clock Source (Source de l'horloge) : source utilisée pour régler l'horloge système. Ce champ peut prendre les valeurs suivantes :

SNTP (SNTP) : indique que l'heure système est réglée à l'aide d'un serveur SNTP. Pour plus d'informations, voir "Configuration des paramètres SNTP".

None (Aucune) : indique que l'heure système n'est pas réglée par une source externe.

Paramètres régionaux

Date : définit la date système. Le format de ce champ est JJ/MMM/AA, par exemple, 04/Mai/50.

Local Time (Heure locale) : définit l'heure système. Le format de ce champ est HH/MM/SS, par exemple, 21/15/03.

Time Zone Offset (Décalage horaire) : différence entre l'heure GMT (Greenwich Mean Time) et l'heure locale. Par exemple, le décalage horaire de Paris est GMT +1:00 tandis que l'heure locale de New York est GMT –5:00.

Il existe deux types de passage à l'heure d'été : à une date spécifique d'une année précise, ou à une date récurrente quelle que soit l'année. Pour sélectionner une date spécifique d'une année précise, complétez la zone **Daylight Savings** (Passage à l'heure d'été). Pour sélectionner une date récurrente, complétez la zone **Recurring** (Récurrente).

Daylight Savings (Passage à l'heure d'été) : permet de spécifier la date du passage à l'heure d'été (DST) de l'unité en fonction de sa localisation. Ce champ peut prendre les valeurs suivantes :

USA (États-Unis) : le périphérique passe à l'heure d'été à 2h00 le premier dimanche d'avril, et revient à l'heure standard à 2h00 le dernier dimanche d'octobre.

European (Europe) : le périphérique passe à l'heure d'été à 1:00 le dernier dimanche de mars et revient à l'heure standard à 1:00 le dernier dimanche d'octobre. L'option European (Europe) concerne les membres de l'Union européenne et les autres pays d'Europe qui appliquent ce passage à l'heure d'été.

Other (Autre) : le passage à l'heure d'été est défini par l'utilisateur selon la localisation de l'unité. Si cette option est sélectionnée, les champs **From** (De) et **To** (À) doivent être complétés.

Time Set Offset (1-1440) (Décalage horaire [1-1440]) : pour les pays autres que les États-Unis et les pays européens, le passage à l'heure d'été peut être défini en minutes. La valeur par défaut est de 60 minutes.

From (De) : définit l'heure du passage à l'heure d'été dans les pays autres que les États-Unis et les pays européens, en spécifiant le format JJ/MMM/AA dans un champ et l'heure dans un autre. Par exemple, si le passage à l'heure d'été a lieu le 25 octobre 2007 à 5:00, les deux champs sont définis sous la forme 25/Oct/07 et 05:00. Ces champs peuvent prendre les valeurs suivantes :

Date : date du passage à l'heure d'été. La plage de valeurs possibles pour ce champ est 1-31.

Month (Mois) : mois de l'année du passage à l'heure d'été. La plage de valeurs possibles pour ce champ est Jan-Dec.

Year (Année) : année du passage à l'heure d'été.

Time (Heure) : heure du passage à l'heure d'été. Le format de ce champ est Heure: Minute, par exemple, 05:30.

To (À) : définit l'heure du passage à l'heure d'hiver dans les pays autres que les États-Unis et les pays européens, en spécifiant le format JJ/MMM/AA dans un champ et l'heure dans un autre. Par exemple, si le passage à l'heure d'hiver a lieu le 23 mars 2008 à 12:00, les deux champs sont définis sous la forme 23/Mar/08 et 12:00. Ces champs peuvent prendre les valeurs suivantes :

Date : date du passage à l'heure d'hiver. La plage de valeurs possibles pour ce champ est 1-31.

Month (Mois) : mois de l'année du passage à l'heure d'hiver. La plage de valeurs possibles pour ce champ est Jan-Dec.

Year (Année) : année du passage à l'heure d'hiver.

Time (Heure) : heure du passage à l'heure d'hiver. Le format de ce champ est Heure:Minute, par exemple, 05:30.

Recurring (Récurrent) : définit le passage à l'heure d'été dans les pays autres que les États-Unis ou les pays européens dans lesquels ce passage est constant d'une année sur l'autre. Ce champ peut prendre les valeurs suivantes :

From (De) : définit le passage à l'heure d'été chaque année. Par exemple, le passage à l'heure d'été a lieu localement chaque deuxième dimanche d'avril à 5:00. Ce champ peut prendre les valeurs suivantes :

Day (Jour) : jour de la semaine du passage à l'heure d'été chaque année. La plage de valeurs possibles pour ce champ est Sunday-Saturday (Dimanche-Samedi).

Week (Semaine) : semaine du mois du passage à l'heure d'été chaque année. La plage de valeurs possibles pour ce champ est 1-5.

Month (Mois) : mois de l'année du passage à l'heure d'été chaque année. La plage de valeurs possibles pour ce champ est Jan-Dec.

Time (Heure) : heure du passage à l'heure d'été chaque année. Le format de ce champ est Heure: Minute, par exemple, 02:10.

To (À) : définit le passage récurrent à l'heure d'hiver chaque année. Par exemple, le passage à l'heure d'hiver a lieu localement chaque quatrième vendredi d'octobre à 5:00. Ce champ peut prendre les valeurs suivantes :

Day (Jour) : jour de la semaine du passage à l'heure d'hiver chaque année. La plage de valeurs possibles pour ce champ est Sunday-Saturday (Dimanche-Samedi).

Week (Semaine) : semaine du mois du passage à l'heure d'hiver chaque année. La plage de valeurs possibles pour ce champ est 1-5.

Month (Mois) : mois de l'année du passage à l'heure d'hiver chaque année. La plage de valeurs possibles pour ce champ est Jan-Dec.

Time (Heure) : heure du passage à l'heure d'hiver chaque année. Le format de ce champ est Heure:Minute, par exemple, 05:30.

Sélection d'une source d'horloge

1. Affichez la page Time Synchronization (Synchronisation horaire).
2. Complétez le champ **Clock Source** (Source de l'horloge).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le source de l'horloge est sélectionnée et l'unité est mise à jour.

Définition des paramètres d'horloge régionaux

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

Les paramètres d'horloge régionaux sont appliqués.

Définition des paramètres d'horloge à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page Time Synchronization (Synchronisation horaire).

REMARQUE : les opérations suivantes doivent être effectuées avant de régler l'heure d'été :

1. Configurer l'heure d'été.
2. Définir le fuseau horaire.
3. Régler l'horloge.

Exemple :

```
console(config)# clock summer-time recurring usa
console(config)# clock time zone 2 zone TMZ2
console(config)# clock set 10:00:00 apr 15 2004
```

Tableau 6-2. Commandes CLI de réglage de l'horloge

CLI	Description
clock source sntp	Configure une source externe pour l'horloge système.
clock time zone *décalage en heures* [**minutes** *décalage en minutes*] [**zone** *acronyme*]	Définit le fuseau horaire à des fins d'affichage.
clock summer-time	Configure le système pour un passage automatique à l'heure d'été (Daylight Savings Time).
clock summer-time recurring {**usa** | **eu** | *semaine jour mois hh:mm semaine jour mois hh:mm}* [**offset** *décalage*] [**zone** *acronyme*]	Configure le système pour un passage automatique à l'heure d'été à l'aide des modes USA (États-Unis) et European (Europe).
clock summer-time date *date mois année hh:mm date mois année hh:mm* **[offset** *décalage***] [zone** *acronyme***]**	Configure le système pour un passage automatique à l'heure d'été (Daylight Savings Time) pendant une période donnée (format date/mois/année).

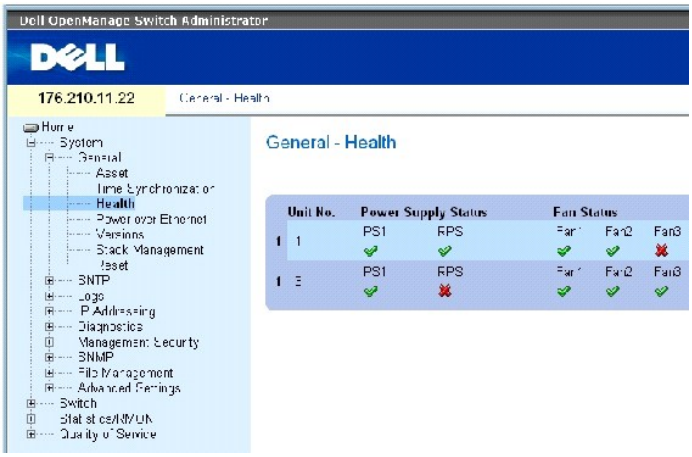
Voici un exemple de commandes CLI :

```
console(config)# clock
timezone -6 zone CST

console(config)# clock
summer-time recurring
first sun apr 2:00 last
sun oct 2:00

console(config)# clock
source sntp

console(config)# interface
ethernet g11

console(config-if)# sntp
client enable

console(config-if)# exit

console(config)# sntp
broadcast client enable
```

Affichage d'informations sur l'intégrité du système

La page System Health (Intégrité du système) fournit des informations matérielles sur les unités physiques, y compris les sources d'alimentation et de ventilation. Pour ouvrir la page System Health (Intégrité du système), cliquez sur **System** (Système) → **General** (Général) → **Health** (Intégrité) dans l'arborescence.

Figure 6-4. System Health (Intégrité du système)



La page System Health (Intégrité du système) contient les champs suivants :

Unit No. (Numéro d'unité) : indique le numéro d'unité pour lequel les informations d'inventaire de l'unité sont affichées.

Power Supply Status (État du bloc d'alimentation) : l'unité est équipée de deux blocs d'alimentation. Dans l'interface, le bloc d'alimentation 1 est désigné par PS1 et le bloc d'alimentation redondant par RPS. Ce champ peut prendre les valeurs suivantes :

: le bloc d'alimentation fonctionne normalement.

: le bloc d'alimentation ne fonctionne pas normalement.

Not Present (Absent) : le bloc d'alimentation est absent.

Fan Status (État du ventilateur) : les unités non-PoE comportent deux ventilateurs et les unités PoE cinq ventilateurs. Chaque ventilateur est désigné sous la forme « ventilateur+numéro du ventilateur » dans l'interface. Ce champ peut prendre les valeurs suivantes :

: le ventilateur fonctionne normalement.

: le ventilateur ne fonctionne pas normalement.

Not Present (Absent) : un ventilateur est absent.

Temperature (Température) : température actuelle de l'unité. La température de l'unité est exprimée en degrés celsius. Le seuil de température de l'unité est compris entre 0 et 40 C (32 et 104 F). Le tableau suivant indique la température en degrés Fahrenheit par incréments de 5.

Tableau 6-3. Tableau de conversion Celsius-Fahrenheit

Celsius	Fahrenheit
0	32
5	41
10	50
15	59
20	68
25	77
30	86
35	95
40	104

Affichage des informations sur l'intégrité du système à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher les champs de la page System Health (Intégrité du système).

Tableau 6-4. Commande CLI d'intégrité du système

Commande CLI	Description
show system [**unit** *unité*]	Affiche les informations système.

Voici un exemple de commandes CLI d'intégrité du système.

```
Console> show system

System Description: Ethernet switch

System Up Time (days,hour:min:sec): 1,22:38:21

System Contact:

System Name: RS1

System Location:

System MAC Address: 00.10.B5.F4.00.01

Sys Object ID: 1.3.6.1.4.1.674.10895.3004

Type: PowerConnect 3424

Temperature Sensors:

Unit    Sensor                Temperature (Celsius)        Status
----    ------                ---------------------        ------
```

1	1		41	OK
1	2		41	OK
2	1		42	OK
2	2		42	OK
Unit	Power Supply	Source	Status	
----	----------	------	------	
1	Main	AC	OK	
2	Secondary	AC	OK	
Unit	Fan	Status		
----	---	------		
1	CPU	OK		
2	CPU	OK		

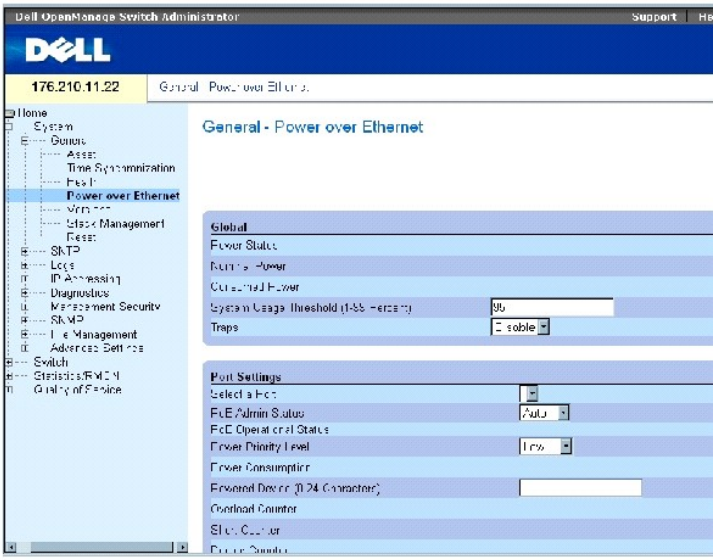
Gestion de l'alimentation Power over Ethernet

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 à mettre à jour l'infrastructure du réseau. Grâce à la norme Power over Ethernet, les périphériques réseau n'ont plus besoin d'être connectés à des sources d'alimentation.

Les unités sont alimentées à partir des blocs d'alimentation PowerConnect, par exemple des téléphones IP. Les périphériques alimentés sont connectés au périphérique PowerConnect via des ports Ethernet. Les périphériques alimentés sont connectés soit via la totalité des 24 ports FE du périphérique PowerConnect 3424P ou la totalité des 48 ports FE du périphérique PowerConnect 3448P.

Pour ouvrir la page Power over Ethernet, cliquez sur **System** (Système) → **General** (Général) → **Power over Ethernet** dans l'arborescence.

Figure 6-5. Power over Ethernet



La page Power over Ethernet contient les sections suivantes :

- Global (Paramètres globaux)
- Port Settings (Paramètres de port)

Global (Paramètres globaux)

La section Power over Ethernet Global Settings (Paramètres globaux Power over Ethernet) contient les champs suivants :

Power Status (État de l'alimentation) : indique l'état de la source d'alimentation en ligne.

On (Activé) : indique que le bloc d'alimentation fonctionne.

Off (Désactivé) : indique que le bloc d'alimentation ne fonctionne pas.

Faulty (Défectueux) : indique que le bloc d'alimentation fonctionne mais qu'une erreur s'est produite. Par exemple, une surcharge ou un court-circuit.

Nominal Power (Puissance nominale) : indique la puissance réelle électrique que le périphérique peut fournir. La valeur de ce champ est exprimée en Watts.

Consumed Power (Puissance consommée) : indique la puissance électrique consommée par le périphérique. La valeur de ce champ est exprimée en Watts.

System Usage Threshold (1-99 Percent) (Seuil d'utilisation du système [1 à 99 %]) : indique le pourcentage d'alimentation consommée avant le déclenchement d'une alarme. La valeur de ce champ est 1 à 99 %. La valeur par défaut est de 95 %.

Traps (Interruptions) : active ou désactive la réception d'interruptions sur le périphérique PoE. Par défaut, cette option est désactivée.

Port Settings (Paramètres de port)

Select a Port (Sélectionner un port) : indique l'interface spécifique pour laquelle des paramètres PoE sont définis et associés à l'interface alimentée connectée

au port sélectionné.

PoE Admin Status (État admin PoE) : indique le mode PoE du périphérique. Ce champ peut prendre les valeurs suivantes :

Auto : active le protocole Device Discovery (Identification de périphérique) et alimente le périphérique via le module PoE. Le protocole Device Discovery permet au périphérique d'identifier les périphériques alimentés connectés aux interfaces et de connaître leur classification. Cette option est sélectionnée par défaut.

Never (Jamais) : désactive le protocole Device Discovery et coupe l'alimentation du périphérique via le module PoE.

PoE Operational Status (État opérationnel PoE) : indique si le port peut fonctionner en mode PoE. Ce champ peut prendre les valeurs suivantes :

On (Activé) : indique que le périphérique alimente l'interface.

Off (Désactivé) : indique que le périphérique alimente l'interface.

Test Fail (Échec du test) : indique que le test du périphérique alimenté a échoué. Par exemple, un port n'a pas pu être activé et ne peut pas être utilisé pour alimenter le périphérique.

Testing (Test) : indique qu'un test est effectué sur le périphérique alimenté. Par exemple, un périphérique est testé pour confirmer qu'il est alimenté à partir du bloc d'alimentation.

Searching (Recherche) : indique que le périphérique PowerConnect recherche un périphérique alimenté. Il s'agit de l'état opérationnel par défaut du mode PoE.

Fault (Panne) : indique que le périphérique PowerConnect a détecté une panne sur le périphérique alimenté. Par exemple, la mémoire du périphérique alimenté est illisible.

Power Priority Level (Niveau de priorité d'alimentation) : Détermine la priorité des ports si l'alimentation est faible. La priorité d'alimentation des ports est utilisée si l'alimentation est faible. La valeur par défaut de ce champ est low (faible). Par exemple, si l'alimentation est utilisée à 99 %, qu'un port 1 affiche une priorité high (élevée) mais que le port 3 affiche une priorité low (faible), l'alimentation du port 1 est prioritaire et le port 3 peut ne pas être alimenté.

Critical (Critique) : attribue le niveau de priorité d'alimentation le plus élevé.

High (Élevé) : attribue le second niveau de priorité d'alimentation le plus élevé.

Low (Faible) : attribue le niveau de priorité d'alimentation le plus faible.

Power Consumption (Consommation électrique) : indique la consommation électrique attribuée au périphérique alimenté connecté à l'interface sélectionnée. Les périphériques sont classés par le périphérique alimenté, et les périphériques PowerConnect utilisent les informations de classification. Les valeurs de ce champ sont exprimées en Watts. Ce champ peut prendre les valeurs suivantes :

0.44 – 12.95 : indique qu'un niveau de consommation électrique de 0,44 à 12,95 Watts est attribué au port.

0.44 – 3.8 : indique qu'un niveau de consommation électrique de 0,44 à 3,8 Watts est attribué au port.

3.84 – 6.49 : indique qu'un niveau de consommation électrique de 3,84 à 6,49 Watts est attribué au port.

6.49 – 12.95 : indique qu'un niveau de consommation électrique de 6,49 à 12,95 Watts est attribué au port.

Power Device (0-24 characters) (Périphérique alimenté [0 à 24 caractères]) : fournit une description définie par l'utilisateur du périphérique alimenté. Ce champ peut contenir jusqu'à 24 caractères.

Overload Counter (Compteur de surcharges) : indique le nombre total de surcharges.

Short Counter (Compteur de courts-circuits) : indique le nombre total de courts-circuits.

Denied Counter (Compteur de refus) : indique le nombre total de refus d'alimentation du périphérique.

Absent Counter (Compteur de coupures) : indique le nombre total de fois où l'alimentation a été coupée car le périphérique n'a pas été détecté.

Invalid Signature Counter (Compteur de signatures incorrectes) : indique le nombre de signatures incorrectes reçues. Les signatures permettent au périphérique alimenté de s'identifier sur le PSE. Elles sont créées lors de la détection, classification ou maintenance du périphérique alimenté.

Définition des paramètres PoE

1. Affichez la page Power over Ethernet.
2. Complétez les champs avec les valeurs appropriées.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres PoE sont définis et l'unité est mise à jour.

Gestion PoE à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher les champs de la page Power over Ethernet.

Tableau 6-5. Paramètres POE

Commande CLI	Description
power inline {auto | never}	Configure le mode d'administration de l'alimentation en ligne d'une interface.
power inline powered-device *type de périphérique alimenté*	Ajoute une description du type de périphérique alimenté.
power inline priority {critical | high | low}	Configure la priorité de l'interface du point de vue de la gestion d'alimentation en ligne.
power inline usage-threshold	Configure le seuil de déclenchement des alarmes
power inline traps enable	Active les interruptions de périphérique PoE
show power inline [interface ethernet]	Affiche les informations de configuration PoE

Voici un exemple de commandes CLI PoE :

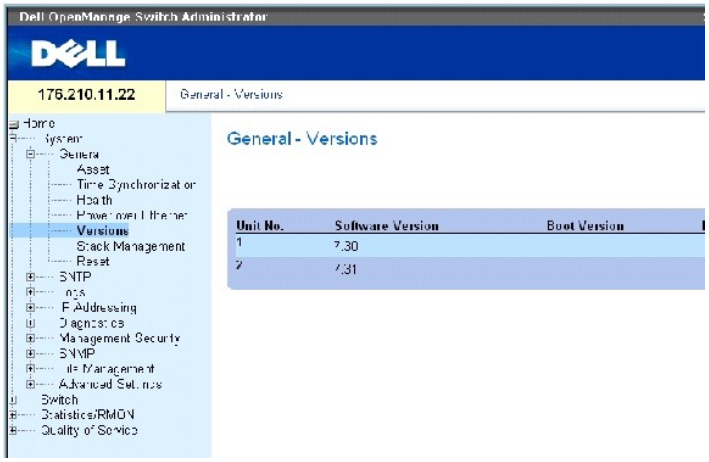
```
Console# show power inline
```

```
Power: On

Nominal Power: 150 Watts

Consumed Power: 120 Watts (80%)

Usage Threshold: 95%

Traps: Enabled

Port  Powered Device     State  Priority  Status  Classification [W]
----  --------------     -----  --------  ------  ------------------
1/e1  IP Phone Model A   Auto   High      On      0.44 - 12.95
2/e1  Wireless AP Model  Auto   Low       On      0.44 - 3.84
3/e1                     Auto   Low       Off     N/A


Console# show power inline ethernet 1/e1

Port  Powered Device     State  Priority  Status  Classification [W]
----  --------------     -----  --------  ------  ------------------
1/1e  IP Phone Model A   Auto   High      On      0.44 - 12.95

Overload Counter: 1

Short Counter: 0

Denied Counter: 0

Absent Counter: 0

Invalid Signature Counter: 0
```

Affichage des informations sur les versions

La page Versions fournit des informations sur les versions des matériels et des logiciels que vous utilisez. Pour ouvrir la page Versions, cliquez sur System (Système) → General (Général) → Versions dans l'arborescence.

Figure 6-6. Versions



La page Versions contient les champs suivants :

Unit No. (Numéro d'unité) : indique le numéro d'unité dont les versions d'unité sont affichées.

Software Version (Version du logiciel) : version actuelle du logiciel exécutée sur l'unité.

Boot Version (Version de démarrage) : version actuelle de démarrage exécutée sur l'unité.

Hardware Version (Version du matériel) : version actuelle du matériel.

Affichage des versions de l'unité à l'aide de l'interface de ligne de commande

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher les champs de la page Versions.

Tableau 6-6. Commandes CLI des versions

Commande CLI	Description
show version	Affiche les informations sur les versions du système.

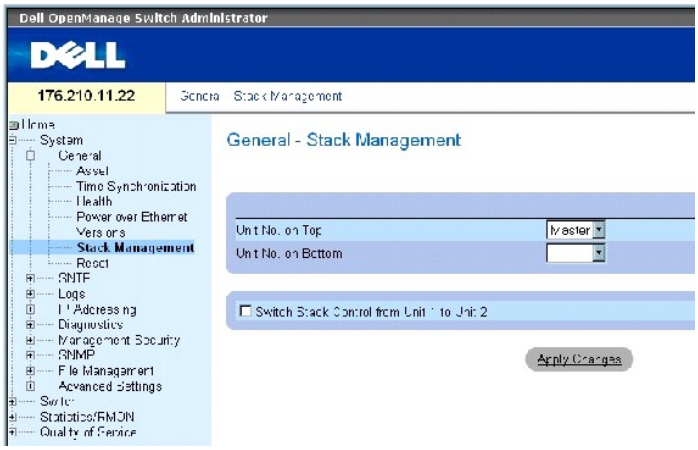
Voici un exemple de commandes CLI :

```
console> show version


SW version 1.0.0.0 (date 23-Jan-2005 time 17:34:19)


Boot version 1.0.0.0 (date 11-Jan-2005 time 11:48:21)


HW version 1.0.0
```

Gestion des membres de la pile

La page Stack Management (Gestion de la pile) permet aux administrateurs réseau de réinitialiser la pile entière ou un périphérique spécifique. Pour ouvrir la page Stack Management (Gestion de la pile), cliquez sur **System** (Système) → **General** (Général) → **Stack Management** (Gestion des piles) dans l'arborescence.

Figure 6-7. Stack Management (Gestion de la pile)



REMARQUE : enregistrez toutes les modifications apportées au fichier de configuration en cours d'exécution avant de réinitialiser la pile. Cela évite de perdre la configuration matérielle existante. Pour plus d'informations sur l'enregistrement des fichiers de configuration, consultez la section "Gestion des fichiers".

Unit No. on Top (Numéro d'unité en haut) : numéro du premier membre de la pile. Ce champ peut prendre les valeurs suivantes : Master (Maître) et 1-6.

Unit No. on Bottom (Numéro d'unité en bas) : numéro du deuxième membre de la pile. Ce champ peut prendre les valeurs suivantes : Master (Maître) et 1-6.

Switch Stack Control from Unit 1 to Unit 2 (Basculement du contrôle de la pile de l'unité 1 vers l'unité 2) : active la commutation de l'unité maître en cours vers l'unité maître de secours.

REMARQUE : la réinitialisation de l'unité maître réinitialise toute la pile.

Basculement entre unités maîtres

1. Affichez la page Stack Management (Gestion de la pile).
2. Cochez la case Switch Stack Control from Unit 1 to Unit 2 (Basculement du contrôle de la pile de l'unité 1 vers l'unité 2).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

   Un message de confirmation s'affiche.
4. Cliquez sur OK.

   Le périphérique est réinitialisé. Une fois le périphérique réinitialisé, un message vous demandant de saisir un nom d'utilisateur et un mot de passe s'affiche.

Configuration de l'ordre d'affichage de la pile

1. Affichez la page Stack Management (Gestion de la pile).
2. Définissez la topologie de la pile en spécifiant les unités supérieures et inférieures. Ces unités doivent être voisines.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'ordre d'affichage est reconfiguré à la page System (Système).

Gestion des piles à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher les champs de la page Stack Management (Gestion de la pile).

Tableau 6-7. Commandes CLI de gestion des piles

Commande CLI	Description
reload	Recharge le système d'exploitation.
stack reload	Recharge les membres de la pile.
stack master	Force la sélection de l'unité maître de la pile.

Voici un exemple de commandes CLI :

```
console# reload


Are you sure you want to erase running configuration (y/n) [n]
```

Réinitialisation de l'unité

La page Reset (Réinitialiser) permet de réinitialiser l'unité à partir d'un site distant. Pour ouvrir la page Reset (Réinitialiser), cliquez sur System (Système) → General (Général) → Reset (Réinitialiser) dans l'arborescence.

La page Reset (Réinitialiser) contient les champs suivants :

Reset Unit No. (Réinitialiser l'unité n°) : réinitialise le membre de la pile sélectionné.

REMARQUE : enregistrez toutes les modifications apportées au fichier de configuration de démarrage avant de réinitialiser la pile. Cela évite de perdre la configuration matérielle existante. Pour plus d'informations sur l'enregistrement des fichiers de configuration, consultez la section "Gestion des fichiers".

Réinitialisation de l'unité

1. Affichez la page Reset (Réinitialiser).
2. Sélectionnez une unité dans le champ **Reset Unit Number** (Réinitialiser l'unité n°).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

   Un message de confirmation s'affiche.
4. Cliquez sur **OK**.

   Le périphérique est réinitialisé. La réinitialisation effectuée, l'utilisateur est invité à saisir un nom et un mot de passe.
5. Entrez un nom d'utilisateur et un mot de passe pour vous reconnecter à l'interface Web.

Réinitialisation de l'unité à l'aide de l'interface de ligne de commande

Le tableau suivant récapitule les commandes CLI équivalentes permettant de réinitialiser le périphérique via l'interface de ligne de commande :

Tableau 6-8. Commande CLI de réinitialisation

Commande CLI	Description
reload	Recharge le système d'exploitation.

Voici un exemple de commandes CLI :

```
console >reload



This command will reset
the whole system and
disconnect your current
session. Do you want to
continue (y/n)[n]?
```

Configuration des paramètres SNTP

Le commutateur prend en charge le commutateur Simple Network Time Protocol (SNTP). SNTP assure la synchronisation de l'horloge système du réseau avec une précision de l'ordre du millième de seconde. Cette synchronisation est effectuée par un serveur réseau SNTP. SNTP fonctionne uniquement comme client et ne fournit aucun service d'horloge à d'autres systèmes.

Le commutateur peut interroger les types de serveurs suivants pour connaître l'heure du serveur :

- Unicast (Monodiffusion)
- Anycast (Multidiffusion)
- Broadcast (Diffusion)

Les sources d'heure sont définies par des stratums. Les stratums définissent la précision de l'horloge de référence. Plus le stratum est élevé (zéro étant la valeur la plus élevée), plus l'horloge est précise. Le commutateur reçoit l'heure à partir du stratum 1 et supérieur. Voici un exemple de stratums :

- **Stratum 0** : indique qu'une horloge de temps réel est utilisée comme source, par exemple, un système GPS.
- **Stratum 1** : indique qu'un serveur relié directement à une source d'heure Stratum 0 est utilisé. Les serveurs d'heure Stratum 1 proposent des protocoles d'heure réseau primaires.
- **Stratum 2** : indique que la source d'heure est définie à distance du serveur Stratum 1 via un réseau. Par exemple, un serveur Stratum 2 reçoit l'heure via une liaison réseau, via NTP, à partir d'un serveur Stratum 1.

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 :

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

L'unité peut interroger les types de serveurs suivants pour connaître l'heure du serveur : Unicast (Monodiffusion), Anycast (Multidiffusion) et Broadcast (Diffusion).

L'interrogation d'informations Unicast 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 temps T1-T4 servent à définir l'heure du serveur. Il s'agit de la méthode la plus sûre pour synchroniser l'heure du périphérique. Si cette méthode est sélectionnée, les informations SNTP sont acceptées uniquement si elles proviennent des serveurs SNTP définis sur le périphérique à l'aide des instructions de la page SNTP Servers (Serveurs SNTP).

L'interrogation d'informations Anycast (Multidiffusion) est utilisée lorsque l'adresse IP du serveur est inconnue. Si cette méthode est sélectionnée, tous les serveurs SNTP sur le réseau peuvent envoyer des informations de synchronisation. Le périphérique est synchronisé lorsqu'il demande de façon proactive des informations de synchronisation. La meilleure réponse (stratum le plus bas) provenant des 3 premiers serveurs SNTP à une requête d'informations de

synchronisation sert à définir la valeur de temps. Les niveaux d'heure T3 et T4 servent à déterminer l'heure du serveur.

Pour obtenir des informations afin de synchroniser l'heure du périphérique time, préférez la méthode d'interrogation Anycast (Multidiffusion) à la méthode d'interrogation Broadcast (Diffusion). Cependant, cette méthode offre moins de sécurité car elle accepte les paquets SNTP provenant de serveurs SNTP qui ne sont pas configurés sur le périphérique.

L'interrogation d'informations Broadcat (Diffusion) est utilisée lorsque l'adresse IP du serveur est inconnue. Lorsqu'un message Broadcast est envoyé à partir d'un serveur SNTP, le SNTP écoute le message. Si l'interrogation Broadcast (Diffusion) est activée, toutes les informations de synchronisation sont acceptées, même si elles n'ont pas été demandées par le périphérique. Il s'agit de la méthode la moins sûre.

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

- Les informations provenant de serveurs définis sur le périphérique sont extraites en priorité. Si la méthode d'interrogation Unicast est désactivée ou si aucun serveur n'est défini sur le périphérique, ce dernier accepte les informations de temps provenant de n'importe quel serveur SNTP qui répond.
- Si plusieurs périphériques Unicast répondent, les informations de synchronisation sont extraites en priorité du périphérique affichant le stratum le plus bas.
- Si les serveurs affichent le même stratum, le périphérique accepte les informations de synchronisation provenant du serveur SNTP qui a répondu le premier.

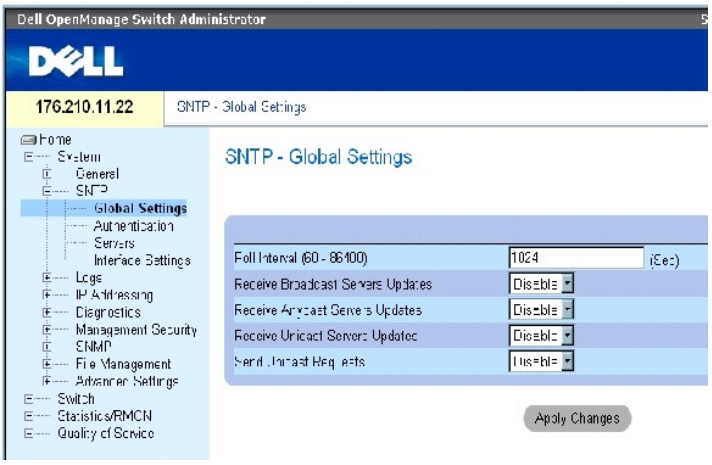
L'authentification MD5 (Message Digest 5) protège les liens de synchronisation entre le périphérique et les serveurs SNTP. MD5 est un algorithme qui crée un hachage 128 bits. MD5 est une variante de MD4 offrant plus de la sécurité. MD5 vérifie l'intégrité de la communication et en authentifie l'origine.

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

Définition des paramètres globaux SNTP

La page SNTP Global Settings (Paramètres globaux SNTP) fournit des informations sur la définition globale des paramètres SNTP. Pour ouvrir la page SNTP Global Settings (Paramètres globaux SNTP), cliquez sur **System** (Système) → **SNTP** → **Global Settings** (Paramètres globaux) dans l'arborescence.

Figure 6-8. SNTP Global Settings (Paramètres globaux SNTP)



La page SNTP Global Settings (Paramètres globaux SNTP) contient les champs suivants :

Poll Interval (60-86400) (Intervalle d'interrogation [60-86400]) : définit l'intervalle d'interrogation (en secondes) du serveur SNTP pour obtenir des informations Unicast. Par défaut, l'intervalle d'interrogation est de 1024 secondes.

Receive Broadcast Servers Updates (Recevoir des mises à jour des serveurs Broadcast) : écoute les serveurs SNTP pour obtenir des informations sur l'heure du serveur Broadcast sur les interfaces sélectionnées.

Receive Anycast Servers Updates (Recevoir des mises à jour des serveurs Anycast) : interroge le serveur SNTP pour obtenir des informations sur l'heure du serveur Anycast. Si les deux options **Receive Anycast Servers Update** (Recevoir des mises à jour des serveurs Broadcast) et **Receive Broadcast Servers Update** (Recevoir des mises à jour des serveurs Broadcast) sont activées, l'heure système est définie selon les informations de l'heure du serveur Anycast.

Receive Unicast Servers Updates (Recevoir des mises à jour des serveurs Unicast) : interroge le serveur SNTP pour obtenir des informations sur l'heure du serveur Unicast. Si les trois options **Receive Broadcast Servers Updates** (Recevoir des mises à jour des serveurs Broadcast), **Receive Anycast Servers Updates** (Recevoir des mises à jour des serveurs Anycast) et **Receive Unicast Servers Updates** (Recevoir des mises à jour des serveurs Unicast) sont activées, l'heure système est définie selon les informations d'heure du serveur Unicast.

Send Unicast Requests (Envoyer des requêtes Unicast) : envoie les informations sur l'heure du serveur SNTP Unicast au serveur SNTP.

Sélection d'une source d'horloge

1. Affichez la page Time Synchronization (Synchronisation horaire).
2. Complétez le champ **Clock Source** (Source de l'horloge).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le source de l'horloge est sélectionnée et l'unité est mise à jour.

Définition des paramètres d'horloge régionaux

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

Les paramètres d'horloge régionaux sont appliqués.

Définition des paramètres globaux SNTP à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher les champs de la page **SNTP Global Settings.**

Tableau 6-9. Commandes CLI des paramètres globaux SNTP

Commande CLI	Description
sntp broadcast client enable	Active les clients SNTP Broadcast
sntp anycast client enable	Active les clients SNTP Anycast
sntp unicast client enable	Active les clients SNTP Unicast prédéfinis

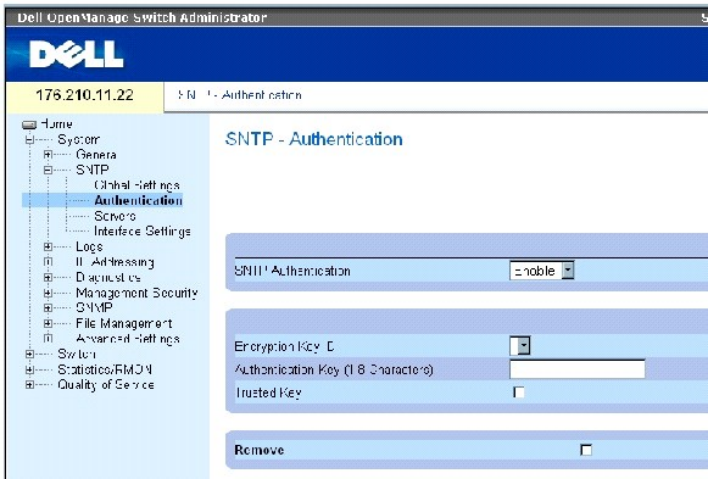
Voici un exemple de commandes CLI :

```
console(config)# sntp
anycast client enable
```

Définition des méthodes d'authentification SNTP

La page SNTP Authentication (Authentification SNTP) active l'authentification SNTP entre le périphérique et un serveur SNTP. La méthode d'authentification du serveur SNTP est également sélectionnée à la page SNTP Authentication (Authentification SNTP). Cliquez sur **System** (Système) → **SNTP** → **Authentication** (Authentification) dans l'arborescence pour ouvrir la page SNTP Authentication (Authentification SNTP).

Figure 6-9. SNTP Authentication (Authentification SNTP)



La page SNTP Authentication (Authentification SNTP) contient les champs suivants :

SNTP Authentication (Authentification SNTP) : si cette option est sélectionnée, active l'authentification d'une session SNTP entre le périphérique et un serveur SNTP.

Encryption Key ID (ID de clé de chiffrement) : identifie la clé permettant d'authentifier le serveur SNTP et le périphérique. La valeur maximale de ce champ est 4294967295.

Authentication Key (1-8 Characters) (Clé d'authentification [1 à 8 caractères]) : clé utilisée pour l'authentification.

Trusted Key (Clé de confiance) : Indique la clé de chiffrement utilisée (Unicast) pour authentifier le serveur SNTP.

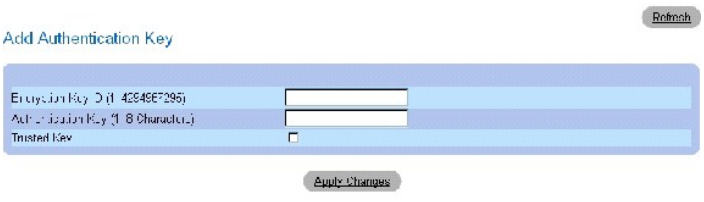
Remove (Supprimer) : supprime les clés d'authentification sélectionnées.

Ajout d'une clé d'authentification SNTP

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

La page suivante s'affiche.

Figure 6-10. Add Authentication Key (Ajouter une clé d'authentification)



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

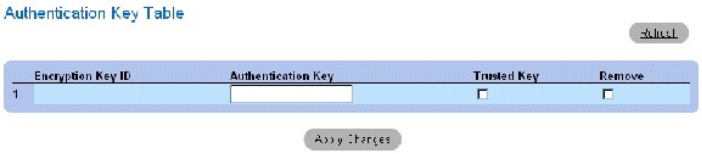
La clé d'authentification SNMP est ajoutée et l'unité est mise à jour.

Affichage de la table des clés d'authentification

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

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

Figure 6-11. Authentication Key Table (Table des clés d'authentification)



Suppression de la clé d'authentification

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

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

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

L'entrée est supprimée et l'unité est mise à jour.

Définition des paramètres d'authentification SNTP à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page SNTP Authentication (Authentification SNTP).

Tableau 6-10. Commandes CLI d'authentification SNTP

Commande CLI	Description
sntp authenticate	Définit l'authentification du trafic Simple Network Time Protocol (SNTP) provenant des serveurs.
sntp trusted key	Authentifie l'identité d'un système selon lequel le protocole SNTP sera synchronisé.
sntp authentication-key *numéro* **md5** *valeur*	Définit une clé d'authentification pour le protocole SNTP.

Voici un exemple de commandes CLI :

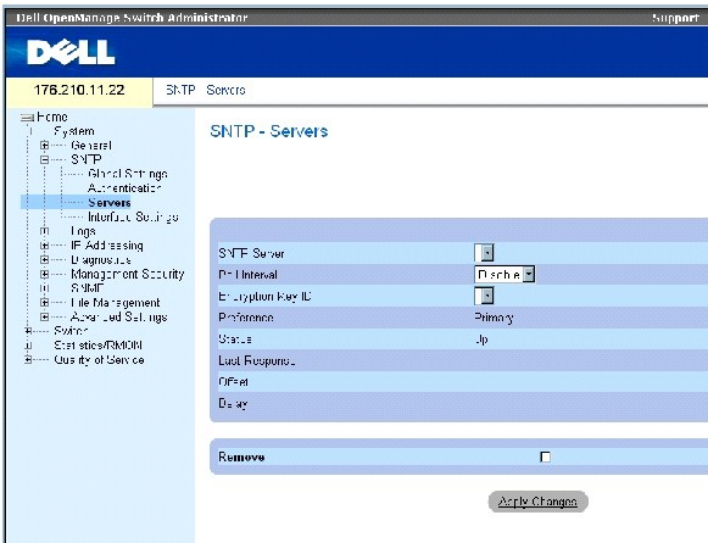
```
console(config)# sntp
authentication-key 8 md5
Calked


console(config)# sntp
trusted-key 8


Console(config)# sntp
```

```
authenticate
```

Définition des serveurs SNTP

Vous pouvez activer des serveurs SNTP ou en ajouter de nouveaux dans la page SNTP Servers (Serveurs SNTP). Pour ouvrir la page SNTP Servers (Serveurs SNTP), cliquez sur **System** (Système) → **SNTP** → **Servers** (Serveurs) dans l'arborescence.

Figure 6-12. SNTP Servers (Serveurs SNTP)



La page SNTP Servers (Serveurs SNTP) contient les champs suivants :

SNTP Server (Serveur SNTP) : sélectionnez l'adresse IP d'un serveur SNTP défini par l'utilisateur. Vous pouvez définir jusqu'à huit serveurs SNTP.

Poll Interval (Intervalle d'interrogation) : si cette option est sélectionnée, interroge le serveur SNTP sélectionné pour obtenir les informations sur l'heure système.

Encryption Key ID (ID de clé de chiffrement) : identifie la clé utilisée pour la communication entre le serveur SNTP et le périphérique. La plage est comprise entre 1 et 4294967295.

Preference (Préférence) : serveur SNTP qui fournit les informations sur l'heure système SNTP. Ce champ peut prendre les valeurs suivantes :

Primary (Primaire) : serveur primaire qui fournit des informations SNTP.

Secondary (Secondaire) : serveur de secours qui fournit des informations SNTP.

Status (État) : état de fonctionnement du serveur SNTP. Ce champ peut prendre les valeurs suivantes :

Up (Actif) : le serveur SNTP fonctionne correctement.

Down (Inactif) : indique qu'un serveur SNTP est actuellement indisponible. Par exemple, le serveur SNTP n'est pas connecté ou est inactif.

In progress (En cours) : le serveur SNTP envoie ou reçoit des informations SNTP.

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

Last Response (Dernière réponse) : dernière réponse reçue du serveur SNTP.

Offset (Décalage) : différence horaire entre l'horloge locale du périphérique et l'heure du serveur SNTP.

Delay (Retard) : temps nécessaire pour atteindre le serveur SNTP.

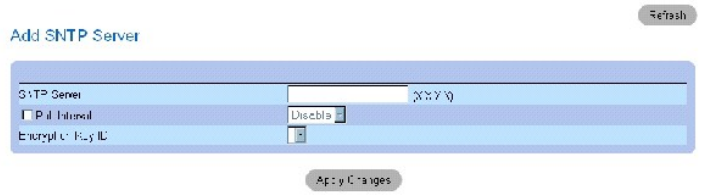
Remove (Supprimer) : supprime un serveur SNTP spécifique de la liste **SNTP Servers** (Serveurs SNTP).

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 6-13. Add SNTP Server (Ajouter un serveur SNTP)



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

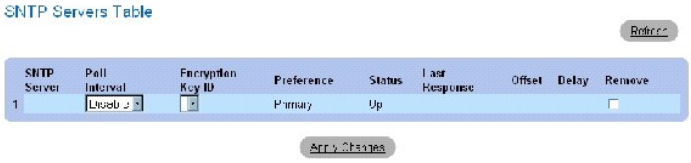
Le serveur SNTP est ajouté et l'unité est mise à jour.

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 6-14. SNTP Servers Table (Table des serveurs SNTP)



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. Sélectionnez un serveur SNTP.
4. Complétez les champs correspondants.
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 l'unité est mise à jour.

Définition des paramètres des serveurs SNTP à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page **SNTP Server** (Serveur SNTP).

Tableau 6-11. Commandes CLI du serveur SNTP

Commande CLI	Description
sntp server adresse IP|nom d'hôte [poll] [key ID clé]	Configure le périphérique pour qu'il utilise le protocole SNTP afin de demander ou d'accepter le trafic SNTP provenant d'un serveur.

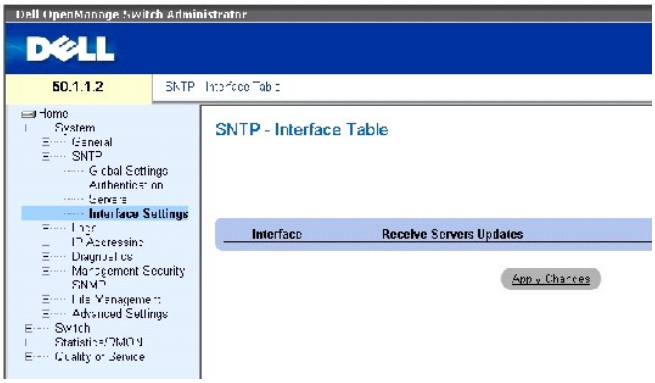
Voici un exemple de commandes CLI :

```
Console(config)# sntp
server 100.1.1.1 poll key
10
```

Définition d'interfaces SNTP

La page SNTP Interface Settings (Paramètres d'interface SNTP) contient les informations d'interface SNTP. Pour ouvrir la page SNTP Interface Settings (Paramètres d'interface SNTP), cliquez sur System (Système) → **SNTP**→ Interface Settings (Paramètres d'interface).

Figure 6-15. SNTP Interface Settings (Paramètres d'interface SNTP)



La page SNTP Interface Settings (Paramètres d'interface SNTP) contient les champs suivants :

Unit No. (Numéro d'unité) : indique le membre de la pile pour lequel l'interface SNTP est activée.

Interface : contient une liste d'interfaces sur lesquelles le protocole SNTP peut être activé.

Receive Servers Updates (Recevoir des mises à jour des serveurs) : active ou désactive le protocole SNTP sur l'interface spécifique.

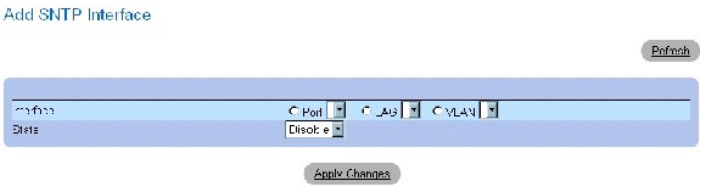
Remove (Supprimer) : supprime SNTP d'une interface spécifique.

Ajout d'une interface SNTP

1. Affichez la page SNTP Interface Settings (Paramètres d'interface SNTP).
2. Cliquez sur Add (Ajouter).

La page **Add SNTP Interface** (Ajouter une interface SNTP) s'affiche.

Figure 6-16. Add SNTP Interface (Ajouter une interface SNTP)



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

L'interface SNTP est ajoutée et l'unité est mise à jour.

Définition des paramètres d'interface SNTP à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page SNTP Interface Settings (Paramètres d'interface SNTP).

REMARQUE : une adresse IP doit être spécifiée dans l'interface afin de la définir comme interface Anycast ou Broadcast.

Tableau 6-12. Commandes CLI des paramètres d'interface SNTP

Commande CLI	Description
sntp client enable	Active le client Simple Network Time Protocol (SNTP) sur une interface.
show sntp configuration	Affiche la configuration Simple Network Time Protocol (SNTP).

Voici un exemple de commandes CLI permettant d'afficher des interfaces SNTP :

```
console# show sntp configuration
Polling interval: 7200 seconds.

MD5 Authentication keys: 8, 9
Authentication is required for synchronization.
Trusted Keys: 8,9

Unicast Clients Polling: Enabled.
Server                          Polling     Encryption Key
-----------                     --------    ---------------
176.1.1.8                       Enabled     9
176.1.8.179                     Disabled    Disabled

Broadcast Clients: Enabled
Broadcast Clients Poll: Enabled
Broadcast Interfaces:1/e1, 1/e3
```

Gestion des journaux

La page **Logs** (Journaux) contient des liens vers différentes pages de journalisation. Pour ouvrir la page **Logs** (Journaux), cliquez sur System (Système) → Logs (Journaux) dans l'arborescence.

Définition des paramètres globaux de journalisation

Les journaux système permettent d'afficher les événements de l'unité en temps réel et de les enregistrer en vue d'une utilisation ultérieure. Les journaux système enregistrent et gèrent les événements, et consignent les erreurs ou les messages informatifs.

Les messages relatifs aux événements se présentent sous un format unique, conforme au protocole des journaux système recommandé pour tous les rapports d'erreurs. Par exemple, un code de sévérité ainsi qu'une notation mnémonique permettant d'identifier l'application source du message, sont associés aux messages de rapport sur les unités locales et Syslog. Cela permet de filtrer les messages en fonction de leur urgence ou de leur pertinence. La distribution des messages de journalisation vers différentes destinations telles que le tampon de journalisation, le fichier de journalisation ou le serveur Syslog est gérée par les paramètres de configuration Syslog. Les utilisateurs peuvent définir jusqu'à huit serveurs Syslog.

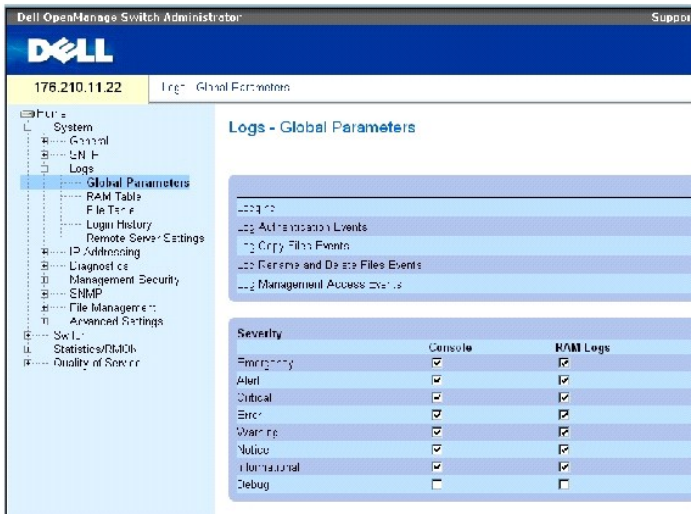
Le tableau ci-après récapitule les différents niveaux de sévérité des journaux :

Tableau 6-13. Niveaux de sévérité des journaux

Type de sévérité	Niveau de sévérité	Description
Urgence	0	Le système ne fonctionne pas.
Alerte	1	Le système exige une intervention immédiate.
Critique	2	L'état du système est critique.
Erreur	3	Une erreur système est survenue.
Avertissement	4	Un avertissement a été émis par le système.
Mise en garde	5	Le système fonctionne correctement, mais une mise en garde a été émise.
Informations	6	Fournit des informations sur l'unité.
Débogage	7	Fournit des informations détaillées sur le journal. En cas d'erreur de débogage, contactez le support technique en ligne de Dell.

La page Global Log Parameters (Paramètres globaux de journalisation) contient des champs permettant de définir les événements et les journaux dans lesquels ces événements sont enregistrés. Elle contient des champs permettant d'activer les journaux de façon globale et de définir des paramètres de journalisation. Les messages de journalisation sont classés par ordre décroissant de sévérité. Pour ouvrir la page Global Log Parameters (Paramètres globaux de journalisation), cliquez sur System (Système) → Logs (Journaux) → Global Parameters (Paramètres globaux) dans l'arborescence.

Figure 6-17. Global Log Parameters (Paramètres globaux de journalisation)



La page Global Log Parameters (Paramètres globaux de journalisation) contient les paramètres suivants :

Logging (Journalisation) : active la journalisation générale pour les journaux en mémoire cache, dans un fichier et sur serveur. Les journaux de la console sont activés par défaut.

Log Authentication Events (Journalisation des événements d'authentification) : active la création de journaux lorsque des utilisateurs sont authentifiés.

Log Copy Files Events (Journalisation des événements de copie de fichiers) : active la création de journaux lorsque des fichiers sont copiés.

Log Rename and Delete Files Events (Journalisation des événements d'attribution de nom et de suppression de fichiers) : active la création de journaux lorsque des fichiers de configuration sont renommés ou supprimés.

Log Management Access Events (Journalisation des événements de gestion d'accès) : active la création de journaux lorsqu'une méthode de gestion définit l'accès à l'unité. Par exemple, un journal est créé chaque fois que vous accédez à l'unité à l'aide de la méthode SSH.

Severity (Sévérité) : il existe différents niveaux de sévérité de journalisation des événements :

Emergency (Urgence) : niveau d'avertissement le plus élevé. Si l'unité est en panne ou ne fonctionne pas correctement, un message d'urgence est consigné à l'emplacement de journalisation spécifié.

Alert (Alerte) : niveau d'avertissement élevé, au second rang sur l'échelle de sévérité. Un journal d'alerte est enregistré en cas de dysfonctionnement grave de l'unité, par exemple lors d'une tentative de téléchargement d'un fichier de configuration qui n'existe pas.

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

Error (Erreur) : une erreur d'unité est survenue ; par exemple lorsqu'une opération de copie a échoué.

Warning (Avertissement) : niveau d'avertissement le plus faible. Par exemple, l'unité fonctionne mais le lien du port est actuellement désactivé.

Notice (Remarque) : fournit des informations importantes sur l'unité.

Informational (Informations) : fournit des informations sur l'unité. Par exemple, un port est actuellement activé.

Debug (Débogage) : fournit des messages de débogage.

REMARQUE : lorsqu'un niveau de sévérité est sélectionné, toutes les options qui lui sont associées le sont automatiquement.

La page **Global Log Parameters** (Paramètres globaux de journalisation) contient également des cases à cocher qui correspondent à un système de journalisation distinct :

Console : niveau de sévérité minimum à partir duquel les journaux sont envoyés à la console.

RAM Logs (Journaux RAM) : niveau de sévérité minimum à partir duquel les journaux sont envoyés dans le fichier journal stocké en RAM (cache).

Log File (Fichier journal) : niveau de sévérité minimum à partir duquel les journaux sont envoyés dans le fichier journal stocké en mémoire FLASH.

Activation des journaux :

1. Affichez la page **Global Log Parameters** (Paramètres globaux de journalisation).
2. Sélectionnez **Enable (Activer)** dans la liste déroulante **Logging** (Journalisation).
3. Sélectionnez le type de journal et la sévérité à l'aide des cases à cocher **Global Log Parameters** (Paramètres globaux de journalisation).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de journalisation sont enregistrés et l'unité est mise à jour.

Activation des journaux à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant d'afficher les champs de la page **Global Log Parameters** (Paramètres globaux de journalisation).

Tableau 6-14. Commandes CLI des paramètres globaux de journalisation

Commande CLI	Description
logging on	Active la journalisation des messages d'erreur.
logging {adresse IP | nom d'hôte} [port port] [severity niveau] [facility lieu] [description texte]	Consigne les messages sur un serveur syslog. Pour connaître la liste des niveaux de sévérité, consultez la section "Niveaux de sévérité des journaux".
logging console niveau	Limite les messages consignés sur la console en fonction de leur sévérité.
logging buffered niveau	Limite les messages syslog affichés à partir d'un tampon interne (RAM) en fonction de leur sévérité.
logging file niveau	Limite les messages syslog envoyés au fichier de journalisation en fonction de leur sévérité.
clear logging	Efface les journaux.
clear logging file	Efface les messages du fichier de journalisation.

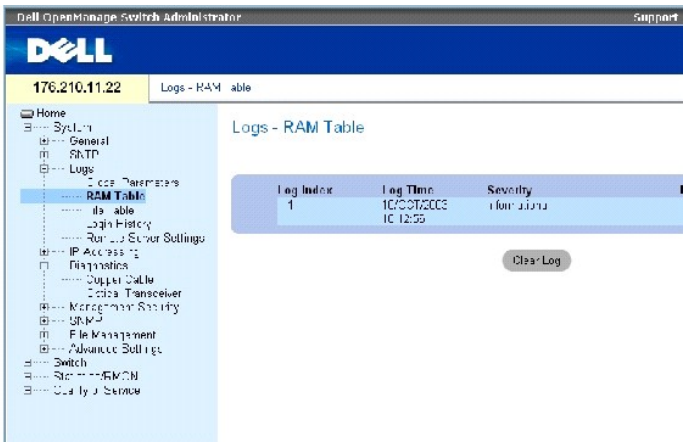
Voici un exemple de commandes CLI :

```
console(config)# logging
on

console(config)# logging
console errors

console(config)# logging
buffered debugging

console(config)# logging
file alerts

console(config)# end

console# clear logging
file

Clear Logging File [y/n]y
```

Affichage de la table des journaux en RAM

La page RAM Log Table (Table des journaux en RAM) fournit des informations sur les entrées de journaux stockées en RAM. Elle indique notamment l'heure de création du journal, sa sévérité ou encore sa description. Pour ouvrir la page RAM Log Table (Table des journaux en RAM), cliquez sur System (Système) → Logs (Journaux) → RAM Table (Table RAM) dans l'arborescence.

Figure 6-18. RAM Log Table (Table des journaux en RAM)



La page RAM Log Table (Table des journaux en RAM) contient les champs suivants :

Log Index (Index du journal) : numéro du journal dans la **table des journaux en RAM**.

Log Time (Heure du journal) : indique l'heure à laquelle le journal a été créé dans la **table des journaux en RAM**.

Severity (Sévérité) : indique la sévérité du journal.

Description : description de l'entrée de journal.

Suppression d'informations de journalisation

1. Affichez la page RAM Log Table (Table des journaux en RAM).
2. Cliquez sur Clear Log (Effacer le journal).

Les informations de journalisation sont supprimées de la **table des journaux en RAM** et l'unité est mise à jour.

Affichage et effacement de la table des journaux en RAM à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher et effacer les champs de la page RAM Log Table (Table des journaux en RAM).

Tableau 6-15. Commandes CLI de la table des journaux en RAM

Commande CLI	Description
show logging	Affiche l'état de la journalisation et les messages syslog stockés dans la mémoire tampon interne.
clear logging	Efface les journaux.

Voici un exemple de commandes CLI :

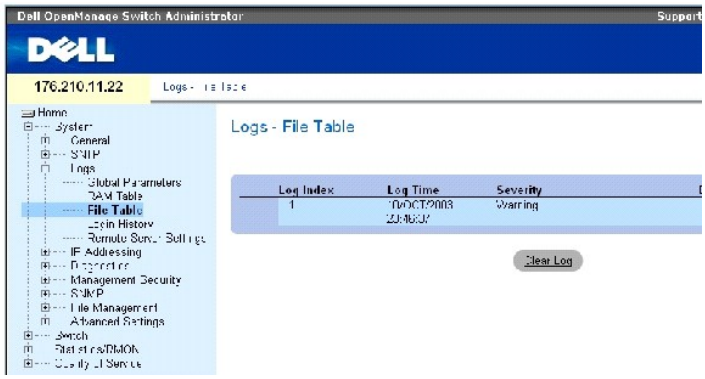
```
console# show logging

Logging is enabled.
```

```
Console Logging: Level
info. Console Messages: 0
Dropped.



Buffer Logging: Level
info. Buffer Messages: 26
Logged, 26 Displayed, 200
Max.



File Logging: Level error.
File Messages: 157 Logged,
26 Dropped.



1 messages were not logged



01-Jan-2000 01:03:42 :%
INIT-I-Startup: Cold
Startup



01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e14



01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e13



01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e12



01-Jan-2000 01:01:36 :%
LINK-W-Down: 1/e15



01-Jan-2000 01:01:32 :%
INIT-I-InitCompleted:
Initialization task is
completed




console# clear logging



Clear Logging Buffer
[y/n]?
```

Affichage de la table des fichiers journaux

La page Log File Table (Table des fichiers journaux) fournit des informations sur les entrées de journaux enregistrées dans le fichier journal stocké en mémoire FLASH. Elle indique notamment l'heure de création du journal, sa sévérité et donne une description du message de journalisation. Pour ouvrir la page Log File Table (Table des fichiers journaux), cliquez sur System (Système) → Logs (Journaux) → File Table (Table des fichiers) dans l'arborescence.

Figure 6-19. Log File Table (Table des fichiers journaux)



La page Log File Table (Table des fichiers journaux) contient les champs suivants :

Log Index (Index du journal) : numéro du journal dans la **table des fichiers journaux**.

Log Time (Heure du journal) : indique l'heure à laquelle le journal a été créé dans la **table des fichiers journaux**.

Severity (Sévérité) : indique la sévérité du journal.

Description : texte du journal.

Affichage de la table des fichiers journaux à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher et de compléter les champs de la page Log File Table (Table des fichiers journaux).

Tableau 6-16. Commandes CLI de la table des fichiers journaux

Commande CLI	Description
show logging file	Affiche l'état de la journalisation et les messages syslog stockés dans le fichier de journalisation.
clear logging file	Efface les messages du fichier de journalisation.

Voici un exemple de commandes CLI :

```
console# show logging
file


Logging is enabled.


Console Logging:
Level info. Console
Messages: 0 Dropped.


Buffer Logging: Level
info. Buffer
Messages: 62 Logged,
62 Displayed, 200
Max.
```

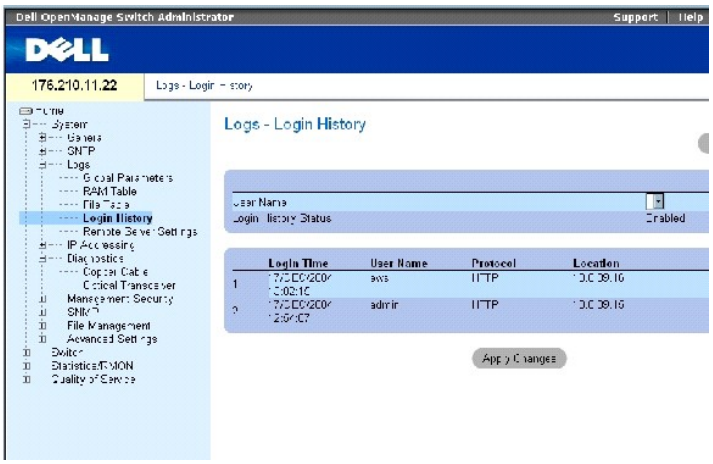
```
File Logging: Level
debug. File Messages:
11 Logged, 51
Dropped.



SysLog server
12.1.1.2 Logging:
warning. Messages: 14
Dropped.



SysLog server 1.1.1.1
Logging: info.
Messages: 0 Dropped.



01-Jan-2000
01:12:01 :%COPY-W-
TRAP: The copy
operation was
completed
successfully



01-Jan-2000
01:11:49 :%LINK-I-Up:
1/e11



01-Jan-2000
01:11:46 :%LINK-I-Up:
1/e12



01-Jan-2000
01:11:42 :%LINK-W-
Down: 1/e13



01-Jan-2000
01:11:35 :%LINK-I-Up:
1/e14
```

Affichage de l'historique des connexions du périphérique

La page Login History (Historique des connexions) fournit des informations permettant d'afficher et de gérer l'utilisation du périphérique, y compris le temps de connexion de l'utilisateur et le protocole utilisé pour se connecter au périphérique.

Pour ouvrir la page Login History (Historique des connexions), cliquez sur System (Système) → Logs (Journaux) → Login History (Historique des connexions) dans l'arborescence.

Figure 6-20. Login History (Historique des connexions)



La page Login History (Historique des connexions) contient les champs suivants :

User Name (Nom d'utilisateur) : affiche une liste de noms définis par l'utilisateur.

Login History Status (État de l'historique des connexions) : indique si les journaux d'historique des mots de passe sont activés sur le périphérique.

Login Time (Temps de connexion) : indique le temps de connexion au périphérique de l'utilisateur sélectionné.

User Name (Nom d'utilisateur) : identifie l'utilisateur connecté au périphérique.

Protocol (Protocole) : indique le protocole utilisé pour connecter l'utilisateur au périphérique.

Location (Emplacement) : indique l'adresse IP de la station qui accède au périphérique.

Affichage de l'historique des connexions

1. Affichez la page Login History (Historique des connexions).
2. Sélectionnez un utilisateur dans le champ **User Name** (Nom d'utilisateur).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les informations de connexion relatives à l'utilisateur sélectionné s'affichent.

Affichage de l'historique des connexions au périphérique à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher et de compléter les champs de la page Login History (Historique des connexions).

Tableau 6-17. Commandes CLI de l'historique des connexions au périphérique

Commande CLI	Description
show users login-history	Affiche les informations sur l'historique de gestion des mots de passe.

Voici un exemple de commandes CLI :

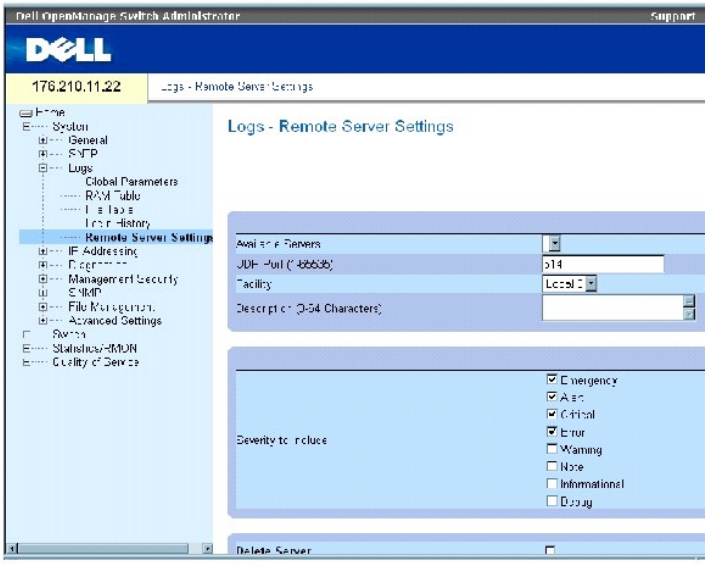
console# **show users login-history**

Login Time	Username	Protocol	Location
----------	--------	--------	----------
Jan 1. 2005 23:58:17	Anna	HTTP	172.16.1.8
Jan 1. 2005 07:59:23	Errol	HTTP	172.16.0.8
Jan 1. 2005 08:23:48	Amy	Serial	
Jan 1. 2005 08:29:29	Alan	SSH	172.16.0.8
Jan 1. 2005 08:42:31	Bob	HTTP	172.16.0.1
Jan 1. 2005 08:49:52	Cindy	Telnet	172.16.1.7

Modification des définitions des serveurs de journalisation à distance

La page Remote Log Server Settings (Paramètres des serveurs de journalisation à distance) contient des champs permettant d'afficher et de configurer les serveurs de journalisation disponibles. Elle vous donne en outre la possibilité de définir de nouveaux serveurs de journalisation et d'envoyer les niveaux de sévérité des journaux à chaque serveur. Pour ouvrir la page Remote Log Server Settings (Paramètres des serveurs de journalisation à distance), cliquez sur System (Système) → Logs (Journaux) → Remote Server Settings (Paramètres des serveurs à distance) dans l'arborescence.

Figure 6-21. Remote Log Server Settings (Paramètres des serveurs de journalisation à distance)



La page Remote Log Server Settings (Paramètres des serveurs de journalisation à distance) contient les champs suivants :

Available Servers (Serveurs disponibles) : dresse la liste des serveurs auxquels les journaux peuvent être envoyés.

UDP Port (1-65535) (Port UDP [1-65535]) : port UDP sur lequel les journaux sont envoyés pour le serveur sélectionné. Les valeurs possibles vont de 1 à 65535. La valeur 514 est utilisée par défaut.

Facility (Voie de transmission) : spécifie une application définie par l'utilisateur à partir de laquelle les journaux système sont envoyés au serveur à distance. Une seule voie de transmission peut être affectée à un serveur unique. Si un second niveau de voie de transmission est affecté, il remplace le premier niveau. Toutes les applications définies pour une unité utilisent la même voie de transmission sur un serveur. La valeur par défaut est de Local 7. Les valeurs possibles sont :

Local 0 - Local 7

Description (0-64 Characters) (Description [0 à 64 caractères]) : description définie par l'utilisateur pour le serveur.

Delete Server (Supprimer le serveur) : supprime le serveur sélectionné de la liste des serveurs disponibles.

La page Remote Log Server Settings (Paramètres des serveurs de journalisation à distance) affiche également une liste des niveaux de sévérité. Ces niveaux de sévérité sont identiques à ceux indiqués à la page Global Log Parameters (Paramètres globaux de journalisation).

Envoi de journaux à un serveur :

1. Affichez la page Remote Log Server Settings (Paramètres des serveurs de journalisation à distance).
2. Sélectionnez un serveur dans la liste déroulante **Available Servers** (Serveurs disponibles).
3. Complétez les champs avec les valeurs appropriées.
4. Définissez la sévérité du journal à l'aide des cases à cocher **Severity to Include** (Sévérité à inclure).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

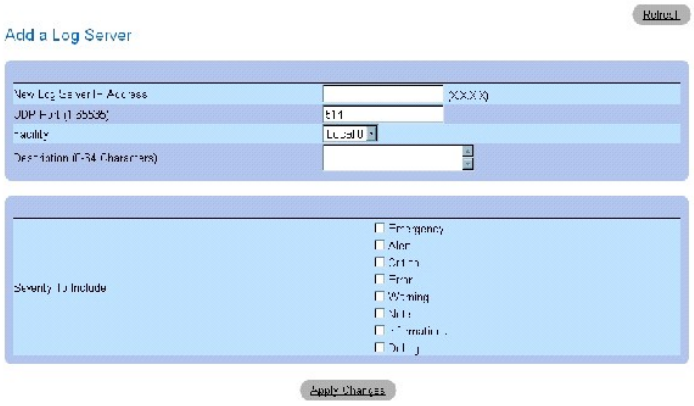
Les paramètres de journalisation sont enregistrés et l'unité est mise à jour.

Définition d'un nouveau serveur :

1. Affichez la page Remote Log Server Settings (Paramètres des serveurs de journalisation à distance).
2. Cliquez sur **Add** (Ajouter).

La page Add a Log Server (Ajouter un serveur de journalisation) s'affiche.

Figure 6-22. Add a Log Server (Ajouter un serveur de journalisation)



La page Add a Log Server (Ajouter un serveur de journalisation) contient le champ supplémentaire suivant :

New Log Server IP Address (Adresse IP du nouveau serveur de journalisation) : indique l'adresse IP du nouveau serveur de journalisation.

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

Le serveur est défini et ajouté à la liste des **serveurs disponibles**.

Affichage de la Log Servers Table (Table des serveurs de journalisation) distante :

1. Affichez la page Remote Log Server Settings (Paramètres des serveurs de journalisation à distance).
2. Cliquez sur **Show All** (Afficher tout).

La page Log Servers Table (Table des serveurs de journalisation) s'affiche.

Figure 6-23. Log Servers Table (Table des serveurs de journalisation)

Suppression d'un serveur de journalisation de la page Log Servers Table (Table des serveurs de journalisation) :

1. Affichez la page Remote Log Server Settings (Paramètres des serveurs de journalisation à distance).
2. Cliquez sur **Show All** (Afficher tout).

La page Log Servers Table (Table des serveurs de journalisation) s'affiche.

3. Sélectionnez une entrée de la page Log Servers Table (Table des serveurs de journalisation).
4. Cochez la case **Remove** (Supprimer) associée au(x) serveur(s) à supprimer.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est supprimée de la page Log Servers Table (Table des serveurs de journalisation) et l'unité est mise à jour.

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

Le tableau suivant récapitule les commandes CLI équivalentes pour l'utilisation des serveurs de journalisation à distance.

Tableau 6-18. Commandes CLI des serveurs de journalisation à distance

Commande CLI	Description
logging *(adresse IP* **|** *nom d'hôte}* **(port** *port*) (**severity** *niveau*) (**facility** *voie de transmission*) (**description** *texte*)	Consigne les messages sur un serveur à distance.
no logging	Supprime un serveur syslog.
show logging	Affiche l'état de la journalisation et les messages syslog.

Voici un exemple de commandes CLI :

```
console> enable

console# configure

console(config) # logging
10.1.1.1 severity critical

console(config)# end

console# show logging

Logging is enabled.

Console Logging: Level
debug. Console Messages: 5
Dropped.

Buffer Logging: Level
debug. Buffer Messages: 16
Logged, 16 Displayed, 200
Max.

File Logging: Level error.
File Messages: 0 Logged,
209 Dropped.

SysLog server 31.1.1.2
Logging: error. Messages:
22 Dropped.

SysLog server 5.2.2.2
Logging: info. Messages: 0
Dropped.

SysLog server 10.2.2.2
Logging: critical.
Messages: 21 Dropped.

SysLog server 10.1.1.1
Logging: critical.
Messages: 0 Dropped.

1 messages were not logged

03-Mar-2004 12:02:03 :%
LINK-I-Up: 1/e11

03-Mar-2004 12:02:01 :%
LINK-W-Down: 1/e12
```

```
03-Mar-2004 12:02:01 :%
LINK-I-Up: 1/e13
```

Définition de l'adressage IP

La page IP Addressing (Adressage IP) contient des liens permettant d'associer des adresses IP aux interfaces et aux passerelles par défaut et de définir des paramètres ARP et DHCP pour les interfaces. Pour ouvrir la page IP Addressing (Adressage IP), cliquez sur System (Système) → IP Addressing (Adressage IP) dans l'arborescence.

Définition de passerelles par défaut

La page **Default Gateway** (Passerelle par défaut) contient des champs permettant d'affecter des passerelles aux unités. Les paquets sont transférés à l'adresse IP par défaut lors de l'envoi de trames à un réseau distant. L'adresse IP configurée doit appartenir au même sous-réseau d'adresses IP que l'une des interfaces IP. Pour ouvrir la page **Default Gateway** (Passerelle par défaut), cliquez sur System (Système) → IP Addressing (Adressage IP) → Default Gateway (Passerelle par défaut) dans l'arborescence.

La page **Default Gateway** (Passerelle par défaut) contient les champs suivants :

User Defined (Défini par l'utilisateur) : adresse IP de la passerelle de l'unité.

Active : indique que la passerelle est active.

Remove User Defined (Supprimer une passerelle définie par l'utilisateur) : supprime la passerelle de l'unité de la liste **Default Gateway** (Passerelle par défaut).

Sélection d'une passerelle de l'unité :

1. Affichez la page **Default Gateway** (Passerelle par défaut).
2. Sélectionnez une adresse IP dans la liste déroulante **Default Gateway** (Passerelle par défaut).
3. Cochez la case Active .
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La passerelle par défaut de l'unité est sélectionnée et l'unité est mise à jour.

Suppression d'une passerelle d'unité par défaut :

1. Affichez la page **Default Gateway** (Passerelle par défaut).
2. Cochez la case **Remove** (Supprimer) pour supprimer des passerelles par défaut.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est supprimée de la table des passerelles par défaut et l'unité est mise à jour.

Définition d'une passerelle de l'unité à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes pour compléter les champs de la page **Default Gateway** (Passerelle par défaut).

Tableau 6-19. Commandes CLI de la passerelle par défaut

Commande CLI	Description

ip default-gateway adresse_IP	Définit une passerelle par défaut.
no ip default-gateway	Supprime une passerelle par défaut.

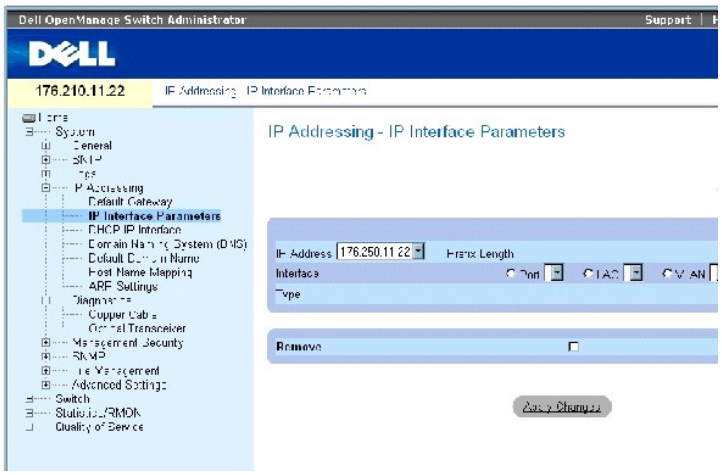
Voici un exemple de commandes CLI :

```
console(config)# ip
default-gateway
196.210.10.1



console(config)# no ip
default-gateway
```

Définition d'interfaces IP

La page IP Interfaces Parameters (Paramètres d'interface IP) contient des champs permettant d'affecter des paramètres IP aux interfaces. Pour ouvrir la page IP Interfaces Parameters (Paramètres d'interface IP), cliquez sur **System** (Système) → **IP Addressing** (Adressage IP) → **IP Interface Parameters** (Paramètres d'interface IP) dans l'arborescence.

Figure 6-24. IP Interfaces Parameters (Paramètres d'interface IP)



La page IP Interfaces Parameters (Paramètres d'interface IP) contient les paramètres suivants :

IP Address (Adresse IP) : adresse d'interface IP.

Prefix Length (Longueur du préfixe) : nombre de bits du préfixe de l'adresse IP source, ou le masque de sous-réseau de l'adresse IP source.

Source Interface (Interface source) : type d'interface pour lequel l'adresse IP est définie. Sélectionnez **Port**, **LAG** ou **VLAN**.

Type : indique si l'adresse IP a été configurée de façon statique ou non.

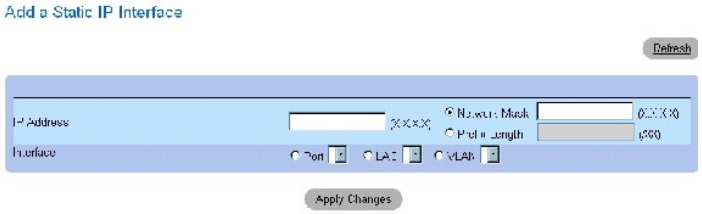
Remove (Supprimer) : supprime l'interface du menu déroulant **IP Address** (Adresse IP).

Ajout d'une interface IP

1. Affichez la page IP Interfaces Parameters (Paramètres d'interface IP).
2. Cliquez sur **Add** (Ajouter).

La page Add a Static IP Interface (Ajouter une interface IP statique) s'affiche.

Figure 6-25. Add a Static IP Interface (Ajouter une interface IP statique)



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

3. Remplissez les champs se trouvant sur cette page.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle adresse IP est ajoutée à l'interface et l'unité est mise à jour.

Modification des paramètres de l'adresse IP

1. Affichez la page IP Interfaces Parameters (Paramètres d'interface IP).
2. Sélectionnez une adresse IP dans le menu déroulant **IP Address** (Adresse IP).
3. Modifiez le type d'interface.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont modifiés et l'unité est mise à jour.

Suppression d'adresses IP

1. Affichez la page IP Interfaces Parameters (Paramètres d'interface IP).
2. Cliquez sur **Show All** (Afficher tout).

La page **IP Interface Parameters Table** (Table des paramètres d'interface IP) s'affiche.

Figure 6-26. IP Interface Parameters Table (Table des paramètres d'interface IP)

3. Sélectionnez une adresse IP, puis cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse IP sélectionnée est supprimée et l'unité est mise à jour.

Définition d'adresses IP à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page IP Interfaces Parameters (Paramètres d'interface IP).

Tableau 6-20. Commandes CLI des paramètres d'interface IP

Commande CLI	Description
ip address adresse_ip {masque | longueur_préfixe}	Définit une adresse IP.
no ip address [adresse-ip]	Supprime une adresse IP.
show ip interface [ethernet numéro_interface | vlan id_vlan | port-channel numéro]	Affiche l'état d'utilisabilité des interfaces IP.

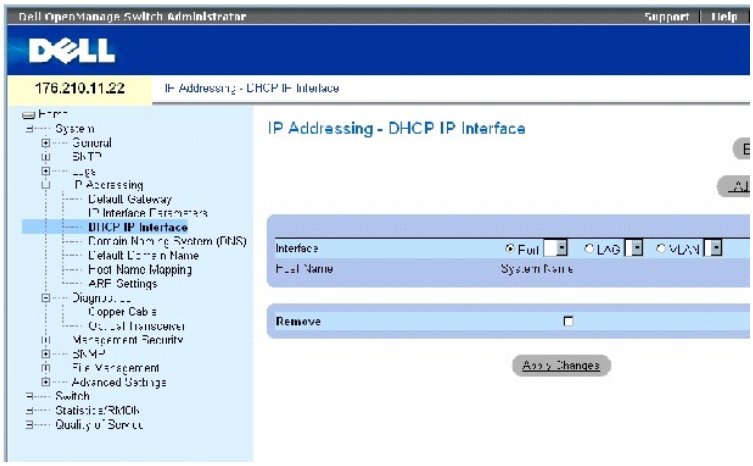
Voici un exemple de commandes CLI :

```
console(config)# interface
vlan 1

console(config-if)# ip
address 92.168.1.123
255.255.255.0

console(config-if)# no ip
address 92.168.1.123

console(config-if)# end

console# show ip interface
vlan 1

Gateway IP Address
Activity status

---------------------- ----
--------------

192.168.1.1 Active

IP address Interface Type

------------------- ------
------ ------------------

192.168.1.123/24 VLAN 1
Static
```

Définition des paramètres d'interface IP DHCP

La page DHCP IP Interface (Interface IP DHCP) contient des paramètres qui permettent de définir les clients DHCP connectés à l'unité. Pour ouvrir la page **DHCP IP Interface** (Interface IP DHCP)**,** cliquez sur **System** (Système) → **IP Addressing** (Adressage IP) → **DHCP IP Interface** (Interface IP DHCP) dans l'arborescence.

Figure 6-27. DHCP IP Interface (Interface IP DHCP)



La page DHCP IP Interface (Interface IP DHCP)contient les champs suivants :

Interface : interface spécifique connectée à l'unité. Activez la case d'option **Port**, **LAG** ou **VLAN** et sélectionnez l'interface connectée à l'unité.

Host Name (Nom d'hôte) : nom du système hôte.

Remove (Supprimer) : supprime les clients DHCP.

Ajout de clients DHCP

1. Affichez la page DHCP IP Interface (Interface IP DHCP).
2. Cliquez sur **Add** (Ajouter).

   La page **Add DHCP IP Interface** (Ajouter des interfaces IP FHCP) s'affiche.
3. Remplissez les champs se trouvant sur cette page.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

   L'interface DHCP est ajoutée et l'unité est mise à jour.

Modification d'une interface IP DHCP

1. Affichez la page DHCP IP Interface (Interface IP DHCP).
2. Complétez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

   L'entrée est modifiée et l'unité est mise à jour.

Suppression d'une interface IP DHCP

1. Affichez la page DHCP IP Interface (Interface IP DHCP).
2. Cliquez sur **Show All** (Afficher tout).

   La page **DHCP Client Table** (Table des clients DHCP) s'affiche.
3. Sélectionnez une entrée de client DHCP.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

   L'entrée sélectionnée est supprimée et l'unité est mise à jour.

Définition des interfaces IP DHCP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des clients DHCP.

Tableau 6-21. Commandes CLI de l'interface IP DHCP

Commande CLI	Description
ip address dhcp [**hostname** *nom_hôte*]	Pour obtenir une adresse IP sur une interface Ethernet à partir du protocole DHCP (Dynamic Host Configuration Protocol).

Voici un exemple de commandes CLI :

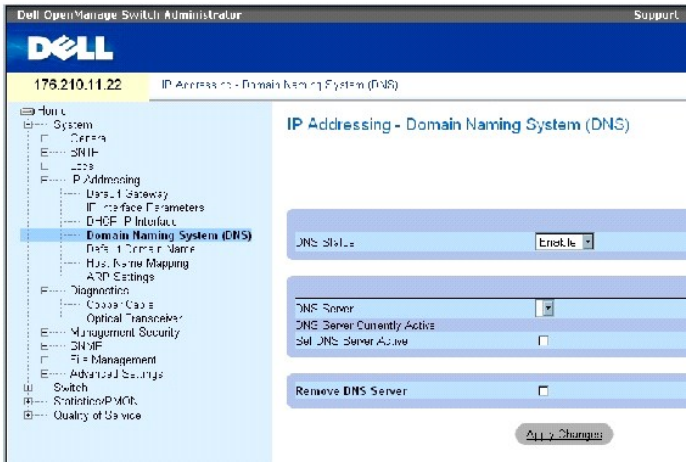
```
console(config)# interface
ethernet 1/e11

console(config-if)# ip
address dhcp
```

Configuration des systèmes de noms de domaines

Le système de noms de domaines (DNS, Domain Name System) convertit les noms de domaines définis par l'utilisateur en adresses IP. À chaque affectation d'un nom de domaine, le service DNS convertit le nom en adresse IP numérique. Par exemple, www.ipexample.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 Naming System (DNS) contient des champs qui permettent d'activer des serveurs DNS spécifiques. Pour ouvrir la page Domain Naming System (DNS), cliquez sur **System** (Système) → **IP Addressing** (Adressage IP) → **Domain Naming System (DNS)** (Système de noms de domaines [DNS]) dans l'arborescence.

Figure 6-28. Domain Naming System (DNS)



La page Domain Naming System (DNS) contient les champs suivants :

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

DNS Server (Serveur DNS) : contient une liste de serveurs DNS. Les serveurs DNS sont ajoutés à la page **Add DNS Server** (Ajouter un serveur DNS).

DNS Server Currently Active (Serveur DNS actif) : serveur DNS actif.

Set DNS Server Active (Définir le serveur DNS actif) : active le serveur DNS sélectionné.

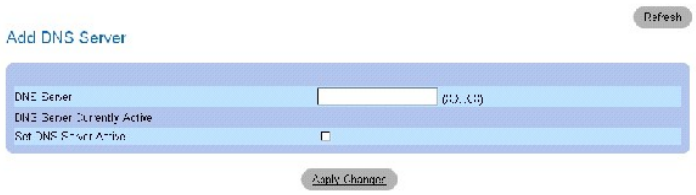
Remove DNS Server (Supprimer le serveur DNS) : supprime le serveur DNS sélectionné.

Ajout d'un serveur DNS

1. Affichez la page Domain Naming System (DNS).
2. Cliquez sur **Add** (Ajouter).

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

Figure 6-29. Add DNS Server (Ajouter un serveur DNS)



DNS Server (Serveur DNS) : adresse IP du serveur DNS.

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

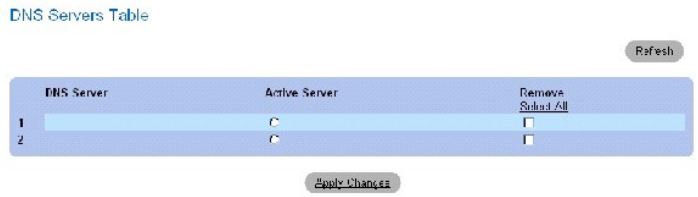
Le nouveau serveur DNS est défini et l'unité est mise à jour.

Affichage de la table des serveurs DNS

1. Affichez la page Domain Naming System (DNS).
2. Cliquez sur **Show All** (Afficher tout).

La page **DNS Server Table** (Table des serveurs DNS) s'affiche.

Figure 6-30. DNS Server Table (Table des serveurs DNS)



Suppression de serveurs DNS

1. Affichez la page Domain Naming System (DNS).
2. Cliquez sur **Show All** (Afficher tout).

La page **DNS Server Table** (Table des serveurs DNS) s'affiche.

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

Le serveur DNS sélectionné est supprimé et l'unité est mise à jour.

Configuration des serveurs DNS à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI permettant la configuration des serveurs DNS.

Tableau 6-22. Commandes CLI du serveur DNS

Commande CLI	Description
ip name-server *adresse_serveur*	Définit les noms de serveurs disponibles. Vous pouvez définir jusqu'à huit noms de serveurs.
no ip name-server *adresse_serveur*	Supprime un nom de serveur.
ip domain-name *nom*	Définit un nom de domaine par défaut utilisé par le logiciel pour compléter les noms d'hôtes non qualifiés.
clear host {nom | *}	Supprime les entrées du cache nom-adresse hôte.
show hosts [*nom*]	Affiche le nom de domaine par défaut, la liste des noms de serveurs hôtes, la liste statique et la liste mise en cache des noms d'hôtes et des adresses.
ip domain-lookup	Active le système DNS pour la conversion des noms d'hôtes en adresses IP.

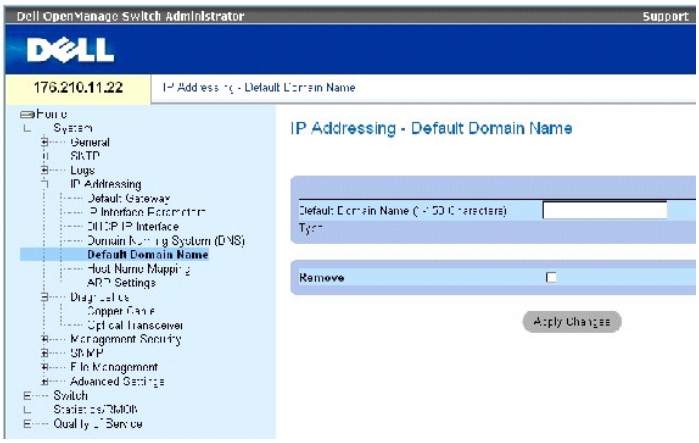
Voici un exemple de commandes CLI :

```
console(config)# ip name-
server 176.16.1.18
```

Définition des domaines par défaut

La page Default Domain Name (Nom de domaine par défaut) fournit des informations permettant de définir les noms de domaines DNS par défaut. Pour ouvrir la page Default Domain Name (Nom de domaine par défaut), cliquez sur **System** (Système) → **IP Addressing** (Adressage IP) → **Default Domain Name** (Nom de domaine par défaut).

Figure 6-31. Default Domain Name (Nom de domaine par défaut)



La page Default Domain Name (Nom de domaine par défaut) contient les champs suivants :

Default Domain Name (1-158 characters) (Nom de domaine par défaut [1 à 158 caractères]) : contient un 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.

Type : type de l'adresse IP. Ce champ peut prendre les valeurs suivantes :

Dynamic (Dynamique) : l'adresse IP est créée de façon dynamique.

Static (Statique) : l'adresse IP est statique.

Remove (Supprimer) : supprime le nom de domaine par défaut.

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

Le tableau suivant récapitule les commandes CLI permettant la configuration des noms de domaines DNS.

Tableau 6-23. Commandes CLI des noms de domaines DNS

Commande CLI	Description
ip domain-name *nom*	Définit un nom de domaine par défaut utilisé par le logiciel pour compléter les noms d'hôtes non qualifiés.
no ip domain-name	Désactive l'utilisation du système de noms de domaines (DNS).
show hosts [*nom***]**	Affiche le nom de domaine par défaut, la liste des noms de serveurs hôtes, la liste statique et la liste mise en cache des noms d'hôtes et des adresses.

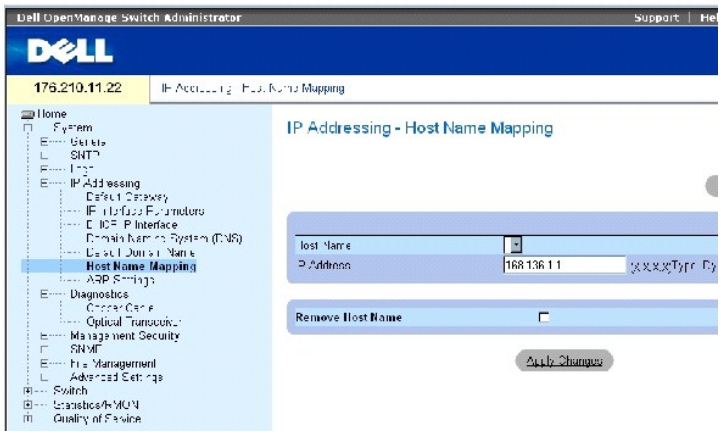
Voici un exemple de commandes CLI :

```
console(config)# ip
domain-name dell.com
```

Adressage d'hôte de domaine

La page Host Name Mapping (Adressage de nom d'hôte) fournit des paramètres permettant d'affecter des adresses IP à des noms d'hôtes statiques. Sur cette page, vous pouvez affecter une adresse IP par hôte. Pour ouvrir la page **Host Name Mapping** (Adressage de nom d'hôte), *cliquez sur* **System** (Système) → **IP Addressing** (Adressage IP) → **Host Name Mapping** (Adressage de nom d'hôte) dans l'arborescence.

Figure 6-32. Host Name Mapping (Adressage de nom d'hôte)



La page Host Name Mapping (Adressage de nom d'hôte) contient les champs suivants :

Host Name (Nom d'utilisateur) : dresse une liste des noms d'hôtes. Les noms d'hôtes sont définis à la page **Add Host Name Mapping** (Ajouter un adressage de noms d'hôtes). Chaque hôte fournit une adresse IP.

IP Address (X.X.X.X) (Adresse IP [X.X.X.X]) : fournit une adresse IP affectée au nom d'hôte spécifié.

Type : le type d'adresse IP. Ce champ peut prendre les valeurs suivantes :

Dynamic (Dynamique) : l'adresse IP est créée de façon dynamique.

Static (Statique) : l'adresse IP est statique.

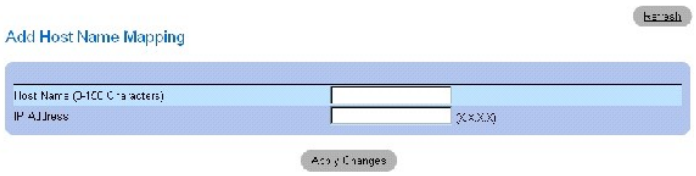
Remove Host Name (Supprimer un nom d'hôte) : supprime l'adressage de l'hôte DNS.

Ajout de noms d'hôtes de domaines

1. Affichez la page Host Name Mapping (Adressage de nom d'hôte).
2. Cliquez sur **Add** (Ajouter).

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

Figure 6-33. Add Host Name Mapping (Ajouter un adressage de nom d'hôte)



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

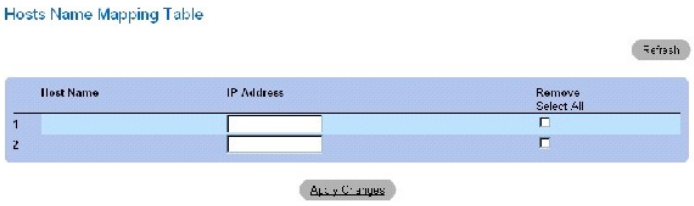
L'adresse IP est affectée au nom d'hôte et l'unité est mise à jour.

Affichage de la table d'adressage de nom d'hôte

1. Affichez la page Host Name Mapping (Adressage de nom d'hôte).
2. Cliquez sur **Show All** (Afficher tout).

La page **Hosts Name Mapping Table** (Table d'adressage de nom d'hôte) s'affiche.

Figure 6-34. Hosts Name Mapping Table (Table d'adressage de nom d'hôte)



Suppression d'un nom d'hôte d'un adressage IP

1. Affichez la page Host Name Mapping (Adressage de nom d'hôte).
2. Cliquez sur **Show All** (Afficher tout).
3. La page **Hosts Name Mapping Table** (Table d'adressage de nom d'hôte) s'affiche.
4. Sélectionnez une entrée dans la table d'adressage de nom d'hôte.
5. Cochez la case **Remove** (Supprimer).
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est supprimée de la **table d'adressage de noms d'hôtes** et l'unité est mise à jour.

Adressage IP de noms d'hôtes de domaines à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'adressage de noms d'hôtes de domaines à des adresses IP.

Tableau 6-24. Commandes CLI des noms d'hôtes de domaines

Commande CLI	Description
ip host *nom*	Définit l'adressage statique nom d'hôte-adresse dans le cache hôte

adresse	
no ip host nom	Supprime l'adressage nom-adresse.
clear host {nom | *}	Supprime les entrées du cache nom-adresse hôte.
show hosts [nom]	Affiche le nom de domaine par défaut, la liste des noms de serveurs hôtes, la liste statique et la liste mise en cache des noms d'hôtes et des adresses.

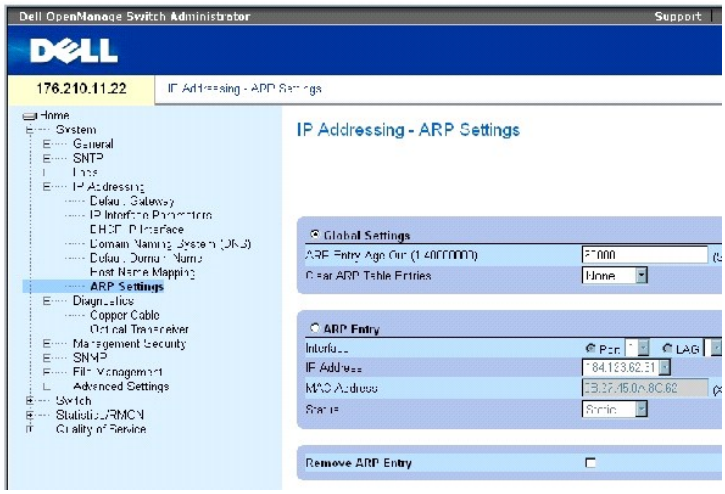
Voici un exemple de commandes CLI :

```
console(config)# ip host
accounting.abc.com
176.10.23.1
```

Définition des paramètres ARP

Le protocole Address Resolution Protocol (Protocole de résolution d'adresse, ARP) convertit les adresses IP en adresses physiques et associe l'adresse IP à une adresse MAC. Le protocole ARP permet à un hôte de communiquer avec d'autres hôtes uniquement lorsque l'adresse IP de ses voisins est connue. Pour ouvrir la page ARP Settings (Paramètres ARP), cliquez sur System (Système) → IP Addressing (Adressage IP) → ARP dans l'arborescence.

Figure 6-35. ARP Settings (Paramètres ARP)



La page ARP Settings (Paramètres ARP)contient les champs suivants :

Global Settings (Paramètres globaux) : sélectionnez cette option pour activer les champs des paramètres globaux ARP.

ARP Entry Age Out (1-40000000) (Délai d'expiration de l'entrée ARP [1 à 40000000]) : indique, pour toutes les unités, le délai (en secondes) qui s'écoule entre les requêtes ARP concernant une entrée de la table ARP. Ce délai écoulé, l'entrée est supprimée de la table. La plage est comprise entre 1 et 40000000. La valeur par défaut est de 60000 secondes.

Clear ARP Table Entries (Effacer les entrées de la table ARP) : le type d'entrées ARP à effacer sur toutes les unités. Les valeurs possibles sont :

None (Aucune) : les entrées ARP ne sont pas effacées.

All (Toutes) : toutes les entrées ARP sont effacées.

Dynamic (Dynamiques) : seules les entrées ARP dynamiques sont effacées.

Static (Statiques) : seules les entrées ARP statiques sont effacées.

ARP Entry (Entrée ARP) : sélectionnez cette option pour activer les champs des paramètres ARP sur une seule unité Ethernet.

Interface : numéro d'interface du port, LAG ou VLAN connecté à l'unité.

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.

Status (État) : état de l'entrée de la table ARP. Les valeurs admises pour ce champ sont les suivantes :

Dynamic (Dynamique) : l'entrée ARP est apprise de façon dynamique.

Static (Statique) : l'entrée ARP est statique.

Remove ARP Entry (Supprimer l'entrée ARP) : supprime une entrée ARP.

Ajout d'une entrée statique dans la table ARP

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

La page **Add ARP Entry** (Ajouter une entrée ARP) s'affiche.

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

L'entrée est supprimée de la **table ARP** et l'unité est mise à jour.

Affichage de la table ARP

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

La page **ARP Table** (Table ARP) s'affiche.

Suppression d'une entrée de la table ARP

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

La page **ARP Table** (Table ARP) s'affiche.

3. Sélectionnez une entrée dans la table.

4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée sélectionnée est supprimée de la **table ARP** et l'unité est mise à jour.

Configuration du protocole ARP à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page ARP Settings (Paramètres ARP).

Tableau 6-25. Commandes CLI des paramètres ARP

Commande CLI	Description
arp adr_ip adr_mat {ethernet numéro_interface | vlan id_vlan | port-channel numéro}	Ajoute une entrée permanente dans le cache ARP.
arp timeout seconds	Indique la durée pendant laquelle une entrée est conservée dans le cache ARP.
clear arp-cache	Supprime toutes les entrées dynamiques du cache ARP
show arp	Affiche les entrées de la table ARP.
no arp	Supprime une entrée de la table ARP.

Voici un exemple de commandes CLI :

```
console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc

console(config)# arp timeout 12000

console(config)# exit

console# show arp

ARP timeout: 12000 Seconds
```

Interface	IP address	HW address	Status
---------	----------	----------	------
1/e11	10.7.1.102	00:10:B5:04:DB:4B	Dynamic
1/e12	10.7.1.135	00:50:22:00:2A:A4	Static

Exécution des diagnostics portant sur les câbles

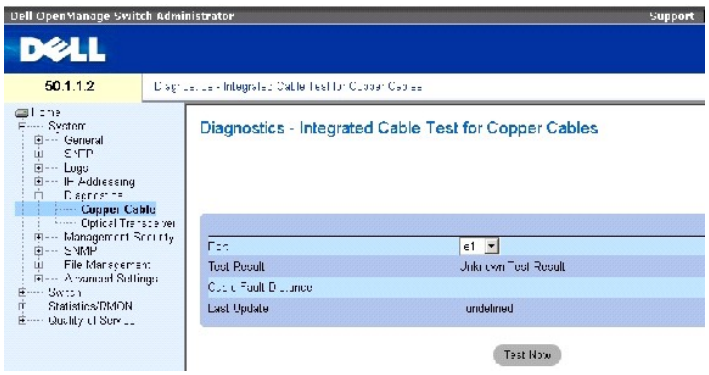
La page **Diagnostics** contient des liens vers des pages permettant d'effectuer des tests virtuels sur les câbles de cuivre. Pour ouvrir la page **Diagnostics**, cliquez sur **System** (Système) → **Diagnostics** dans l'arborescence.

Affichage des diagnostics portant sur les câbles de cuivre

La page Integrated Cable|Test for Copper Cables (Câble intégré|Test pour câbles de cuivre) contient des champs permettant d'effectuer des tests sur des câbles en cuivre. Ces tests permettent d'obtenir des informations sur l'emplacement et le type des problèmes liés aux câbles, ainsi que sur le dernier test de ce type effectué. Ces tests utilisent la technologie Time Domain Reflectometry (TDR) pour vérifier la qualité et les caractéristiques d'un câble de cuivre connecté à un port. Les tests sont possibles sur des câbles d'une longueur maximum de 120 mètres. Pour qu'ils puissent être effectués, les ports doivent être à l'état bas (sauf pour le test "Approximated Cable Length", Longueur approximative du câble).

Pour ouvrir la page Integrated Cable|Test for Copper Cables (Câble intégré|Test pour câbles de cuivre), cliquez sur **System** (Système) → **Diagnostics** → **Copper Cable** (Câble de cuivre) dans l'arborescence.

Figure 6-36. Integrated Cable|Test for Copper Cables (Câble intégré|Test pour câbles de cuivre)



La page Integrated Cable|Test for Copper Cables (Câble intégré|Test pour câbles de cuivre) contient les champs suivants :

Port : port auquel le câble est connecté.

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

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

Open Cable (Câble ouvert) : une seule extrémité du câble est connectée.

Short Cable (Court-circuit) : le câble a fait l'objet d'un court-circuit.

OK : le test est positif.

Cable Fault Distance (Emplacement de la panne) : distance à partir du port où le problème est survenu sur le câble.

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

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

Test d'un câble

1. Vérifiez que les deux extrémités du câble de cuivre sont connectées à une unité.
2. Affichez la page Integrated Cable|Test for Copper Cables (Câble intégré|Test pour câbles de cuivre).
3. Sélectionnez une interface à tester.

4. Cliquez sur **Test Now** (Lancer le test).

Le câble de cuivre est testé et les résultats s'affichent à la page Integrated Cable|Test for Copper Cables (Câble intégré|Test pour câbles de cuivre).

Affichage de la table des résultats du test du câble

1. Affichez la page Integrated Cable|Test for Copper Cables (Câble intégré|Test pour câbles de cuivre).
2. Cliquez sur **Show All** (Afficher tout).

La page Integrated Cable Test Results Table (Table des résultats du test intégré du câble) s'affiche.

REMARQUE : cet écran affiche les résultats des tests qui viennent d'être effectués, mais il -n'applique pas le test à tous les ports.

Outre les champs de la page Integrated Cable|Test for Copper Cables (Câble intégré|Test pour câbles de cuivre), la **table des résultats du test intégré du câble** contient le champ suivant :

Unit No. (Numéro de l'unité) : numéro de l'unité pour laquelle le câble s'affiche.

Exécution des tests du câble de cuivre à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant d'exécuter les tests du câble de cuivre.

Tableau 6-26. Commandes CLI du test du câble de cuivre

Commande CLI	Description
test copper-port tdr *interface*	Exécuter les tests VCT.
show copper-port tdr *interface*	Affiche les résultats des derniers tests VCT effectués sur les ports.
show copper-port cable-length *interface*	Affiche la longueur estimée du câble de cuivre connecté à un port.

Voici un exemple de commandes CLI :

```
console> enable

Console# test copper-port tdr 1/e3

Cable is open at 100 meters.

Console# show copper-port cable-length

Port    Length (meters)
----    ---------------
```

1/e3	110-140
1/e4	Fiber

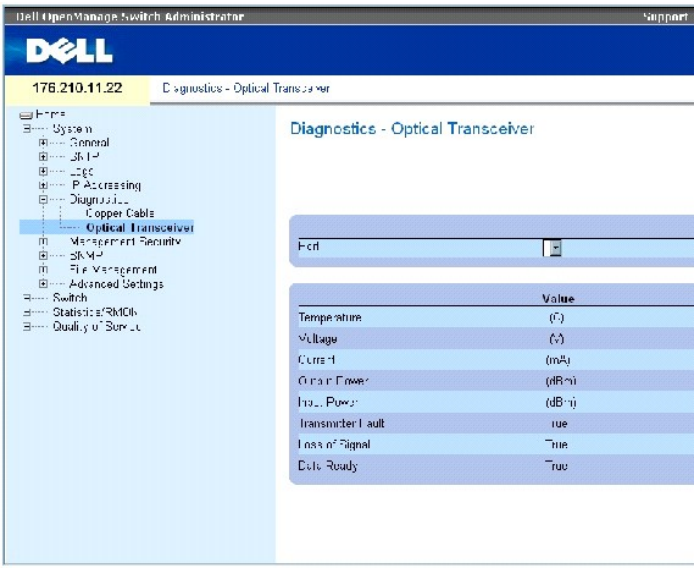
REMARQUE : la longueur de câble obtenue par le test intégré de contrôle des câbles (Integrated Cable Tester, ICT) est une approximation. Les résultats sont classés de la manière suivante : jusqu'à 50 mètres, de 50 à 80 mètres, de 80 à 100 mètres, de 110 à 120 mètres et plus de 120 mètres. La marge d'erreur peut atteindre 20 mètres et la mesure de la longueur du câble ne s'applique pas aux connexions 10 Mbps.

Affichage des diagnostics des émetteurs-récepteurs optiques

Utilisez la page Optical Transceiver (Émetteur-récepteur optique) pour tester les câbles à fibre optique. Pour ouvrir la page Optical Transceiver (Émetteur-récepteur optique), cliquez sur **System** (Système) → **Diagnostics** → **Optical Transceiver** (Émetteur-récepteur optique) dans l'arborescence.

REMARQUE : vous pouvez effectuer des diagnostics des émetteurs-récepteurs optiques uniquement lorsque le lien est présent.

Figure 6-37. Optical Transceiver (Émetteur-récepteur optique)



La page Optical Transceiver (Émetteur-récepteur optique) contient les champs suivants :

Port : 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) : puissance de sortie de l'émission.

Input Power (Puissance d'entrée) : puissance d'entrée de la réception.

Transmitter Fault (Défaillance du 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 (Prêt pour données) : le transmetteur optique est sous tension et les données sont prêtes.

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

1. Affichez la page Optical Transceiver (Émetteur-récepteur optique).
2. Cliquez sur **Show All** (Afficher tout).

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

Outre les champs de la page Optical Transceiver (Émetteur-récepteur optique), la **table des résultats des diagnostics des émetteurs-récepteurs optiques** contient le champ suivant :

Unit No. (Numéro de l'unité) : numéro de l'unité pour laquelle le câble s'affiche.

- **N/A** : Not Available (Non disponible), N/S - Not Supported (Non pris en charge), W – Warning (Avertissement), E – Error (Erreur)

REMARQUE : les émetteurs-transmetteurs Finisar ne prennent pas en charge les tests des diagnostics d'erreur d'émetteur.

REMARQUE : la fonction d'analyse de fibre optique fonctionne uniquement sur les SFP prenant en charge le standard de diagnostic numérique SFF--872.

Exécution des tests du câble à fibre optique à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant d'exécuter les tests du câble à fibre optique.

Tableau 6-27. Commandes CLI du test du câble à fibre optique

Commande CLI	Description
show fiber-ports optical- transceiver [*interface*] [*détail*]	Affiche les diagnostics de l'émetteur-récepteur optique.

Voici un exemple de commandes CLI :

```
Console# show fiber-ports optical-transceiver detailed
```

Port	Temp [C]	Voltage	Current [Volt]	Output [mA]	Input [mWatt]	POWER TX [mWatt]	LOS Fault
----	----	------	-----	------	------	------	-----
1/e1	48	5.15	50	1.789	1.789	No	No
1/e2	43	5.15	10	1.789	1.789	No	No

Gestion de la sécurité du commutateur

La page **Management Security** (Sécurité de gestion) donne accès à différentes pages de sécurisation qui permettent de définir des paramètres de sécurité pour les ports, les méthodes de gestion d'unité, les utilisateurs et le serveur. Pour ouvrir la page **Management Security** (Sécurité de gestion), cliquez sur System (Système) → Management Security (Sécurité de gestion) dans l'arborescence.

Définition de profils d'accès

La page Access Profiles (Profils d'accès) contient des champs permettant de définir des profils et des règles d'accès à l'unité. L'accès aux fonctions de gestion peut être limité à des groupes d'utilisateurs définis par des interfaces d'entrée et une adresse ou des sous-réseaux IP source.

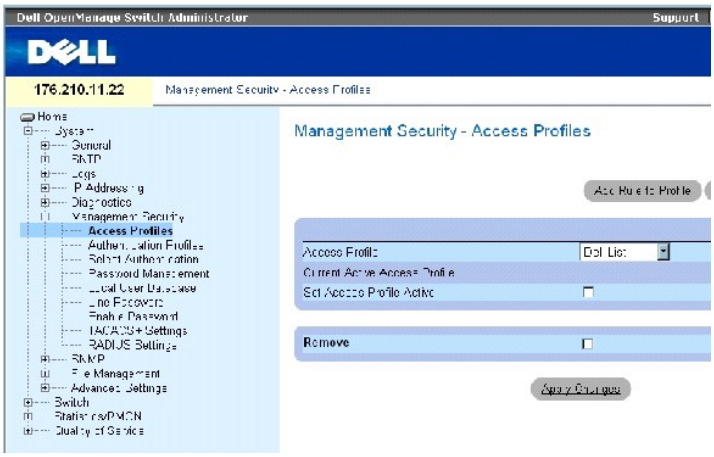
L'accès de gestion peut être défini séparément pour chaque méthode d'accès de gestion, y compris Web (HTTP), Secure Web (HTTPS), Telnet et Secure Telnet.

L'accès aux différentes méthodes de gestion peut différer selon les groupes d'utilisateurs. Par exemple, un groupe d'utilisateurs 1 peut accéder à l'unité uniquement via une session HTTPS tandis qu'un groupe d'utilisateurs 2 peut accéder à l'unité via des sessions HTTPS et Telnet.

Les listes d'accès de gestion contiennent jusqu'à 256 règles qui déterminent quels utilisateurs peuvent gérer l'unité et selon quelles méthodes. Il est également possible d'interdire à des utilisateurs l'accès à l'unité.

La page **Access Profiles** (Profils d'accès) contient des champs permettant de configurer des listes de gestion et de les appliquer à des interfaces spécifiques. Pour ouvrir la page **Access Profiles** (Profils d'accès), cliquez sur **System** (Système) → **Management Security** (Sécurité de gestion) → **Access Profiles** (Profils d'accès) dans l'arborescence.

Figure 6-38. Access Profiles (Profils d'accès)



La page **Access Profiles** (Profils d'accès) contient les champs suivants :

Access Profile (Profil d'accès) : listes de profils d'accès définis par l'utilisateur. La liste des profils d'accès affiche une valeur par défaut **Console Only** (Console uniquement). Lorsque ce profil d'accès est sélectionné, la gestion active de l'unité est effectuée uniquement à l'aide de la console.

Current Active Access Profile (Profil d'accès actif) : profil d'accès actif.

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

Remove (Supprimer) : supprime un profil d'accès de la liste **Access Profile Name** (Nom du profil d'accès).

Activation d'un profil

1. Affichez la page Access Profiles (Profils d'accès).
2. Sélectionnez un profil d'accès dans le champ **Access Profile** (Profil d'accès).
3. Cochez la case **Set Access Profile Active** (Définir le profil d'accès actif).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le profil d'accès est activé.

Ajout d'un profil d'accès

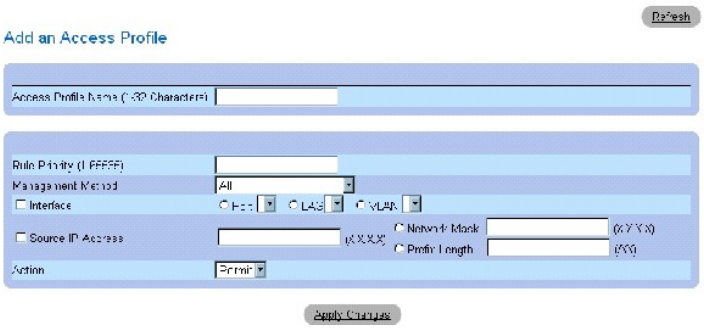
Les règles sont des filtres qui permettent de déterminer la priorité d'une règle, la méthode de gestion de l'unité, le type d'interface, l'adresse IP source et le masque de réseau, ainsi que l'action d'accès de gestion de l'unité. Les utilisateurs peuvent se voir autoriser ou refuser un accès de gestion. La priorité définit l'ordre dans lequel les règles sont appliquées.

Définition des règles d'un profil d'accès :

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

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

Figure 6-39. Add an Access Profile (Ajouter un profil d'accès)



La page Add an Access Profile (Ajouter un profil d'accès) contient les champs supplémentaires suivants :

Access Profile Name (1-32 Characters) (Nom du profil d'accès [1 à 32 caractères]) : nom du profil d'accès défini par l'utilisateur. Le nom du profil d'accès peut contenir jusqu'à 32 caractères.

Rule Priority (1-65535) (Priorité de la règle [1-65535]) : priorité de la règle. Lorsque le paquet est associé à une règle, les groupes d'utilisateurs se voient autoriser ou refuser l'accès de gestion de l'unité. La priorité de la règle est définie à l'aide de ce champ. L'ordre des règles est important car les paquets sont en effet associés avec la première règle qui répond aux critères. Les propriétés de la règle s'affichent à la page **Profile Rules Table** (Table des règles de profil).

Management Method (Méthode de gestion) : méthode de gestion pour laquelle le profil d'accès est défini. Les utilisateurs avec ce profil d'accès se voient refuser ou autoriser l'accès à l'unité à l'aide de la méthode de gestion sélectionnée (ligne).

Interface : interface à laquelle la règle s'applique. Il s'agit d'un champ facultatif. Cette règle peut être appliquée à un port, LAG ou VLAN en cochant la case, puis en sélectionnant l'option et l'interface correspondantes.

REMARQUE : l'association d'un profil d'accès à une interface interdit tout accès via d'autres interfaces. Si un profil d'accès n'est associé à aucune interface, l'unité est accessible à partir de toutes les interfaces.

Source IP Address (X.X.X.X) (Adresse IP source [X.X.X.X]) : adresse IP source à laquelle la règle s'applique. Ce champ facultatif indique que la règle s'applique à un sous-réseau.

Network Mask (X.X.X.X) (Masque de sous-réseau [X.X.X.X]) : masque de sous-réseau IP.

Prefix Length (/XX) (Longueur du préfixe [/XX)] : nombre de bits du préfixe de l'adresse IP source, ou masque de sous-réseau de l'adresse IP source.

Action : autorise ou interdit l'accès de gestion à l'interface définie.

3. Complétez le champ **Access Profile Name** (Nom du profil d'accès).
4. Complétez les champs correspondants.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau profil d'accès est ajouté et l'unité est mise à jour.

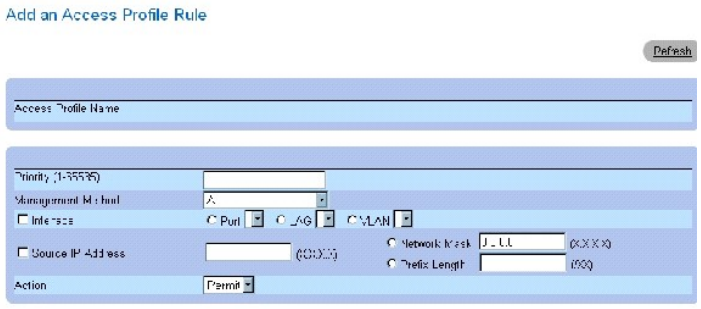
Ajout de règles à un profil d'accès

REMARQUE : vous ne pouvez associer le trafic à des profils d'accès que si la première règle a été définie.

1. Affichez la page **Access Profile** (Profil d'accès).
2. Cliquez sur **Add Rule to Profile** (Ajouter une règle au profil).

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

Figure 6-40. Add an Access Profile Rule (Ajouter une règle à un profil d'accès)



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

La règle est ajoutée au profil d'accès et l'unité est mise à jour.

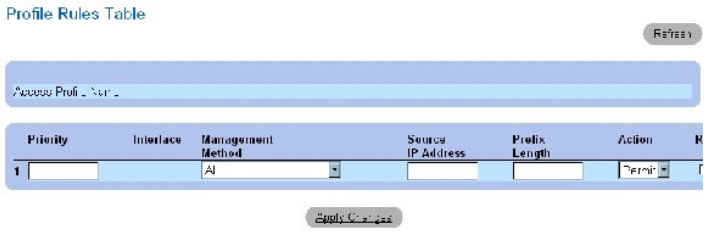
Affichage de la table des règles de profil

REMARQUE : l'ordre selon lequel les règles s'affichent dans la table des règles de profil est important. Les paquets sont en effet associés à la première règle qui répond aux critères.

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

La page **Profile Rules Table** (Table des règles de profil) s'affiche.

Figure 6-41. Profile Rules Table (Table des règles de profil)



Suppression d'une règle

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

La page **Profile Rules Table** (Table des règles de profil) s'affiche.

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

La règle sélectionnée est supprimée et l'unité est mise à jour.

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

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page Access Profiles (Profils d'accès).

Tableau 6-28. Commandes CLI des profils d'accès

Commande CLI	Description
management access-list nom	Définit une liste d'accès de gestion, et crée le contexte de la liste d'accès pour la configuration.
permit [ethernet numéro_interface | vlan id_vlan | port-channel numéro] [service service]	Définit des conditions d'autorisation de port pour la liste d'accès de gestion.
permit ip-source adresse_ip [mask masque | longueur_préfixe] [ethernet numéro_interface | vlan id_vlan | port-channel numéro] [service service]	Définit des conditions d'autorisation de port pour la liste d'accès de gestion et la méthode de gestion sélectionnée.
deny [ethernet numéro_interface | vlan id_vlan | port-channel numéro] [service service]	Définit des conditions de refus de port pour la liste d'accès de gestion et la méthode de gestion sélectionnée.
deny ip-source adresse_ip [mask masque | longueur_préfixe] [ethernet numéro_interface | vlan id_vlan | port-channel numéro] [service service]	Définit des conditions de refus de port pour la liste d'accès de gestion et la méthode de gestion sélectionnée.
management access-class {console-only | nom}	Définit la liste d'accès utilisée pour les connexions de gestion actives.
show management access-list [nom]	Affiche les listes d'accès de gestion actives.
show management access-class	Affiche des informations sur la classe d'accès de gestion.

Voici un exemple de commandes CLI :

```
console(config)#
management access-list
mlist
```

```
console(config-macl)#
permit ethernet 1/e1



console(config-macl)#
permit ethernet 1/e2



console(config-macl)# deny
ethernet 1/e3



console(config-macl)# deny
ethernet 1/e4



console(config-macl)# exit



console(config)#
management access-class
mlist



console(config)# exit



console# show management
access-list



mlist



-----



permit ethernet 1/e1



permit ethernet 1/e2



deny ethernet 1/e3



deny ethernet 1/e4



! (Note: all other access
implicitly denied)



Console# show management
access-class



Management access-class is
enabled, using access list
mlist
```

Définition de profils d'authentification

La page Authentication Profiles (Profils d'authentification) contient des champs permettant de sélectionner la méthode d'authentification des utilisateurs sur

l'unité. L'authentification des utilisateurs est effectuée :

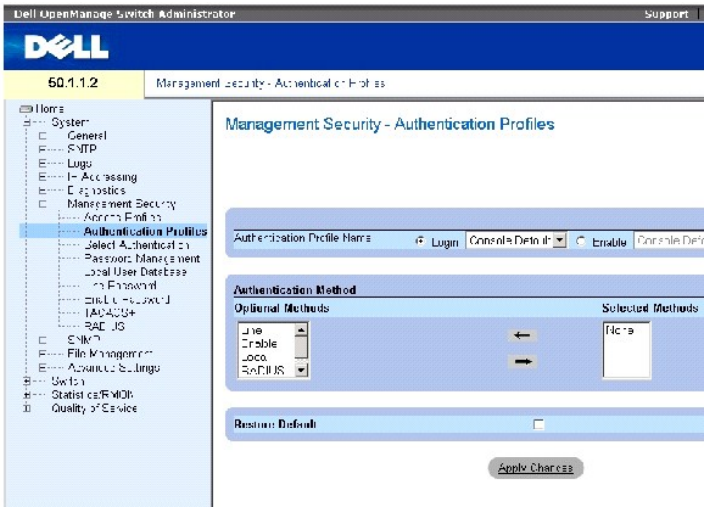
- Localement
- Par le biais d'un serveur externe

Vous pouvez également sélectionner None (Aucune) pour désactiver l'authentification des utilisateurs.

L'authentification des utilisateurs est effectuée dans l'ordre de sélection des méthodes. Si les options Local et RADIUS sont toutes deux sélectionnées, par exemple, l'utilisateur est tout d'abord authentifié localement. Si la base de données d'utilisateurs locale est vide, l'utilisateur est ensuite authentifié via le serveur RADIUS. Le processus d'authentification prend fin en cas d'erreur avec la première méthode.

En cas d'erreur lors du processus d'authentification, la méthode sélectionnée suivante est utilisée. Pour ouvrir la page Authentication Profiles (Profils d'authentification), cliquez sur System (Système) → Management Security (Sécurité de gestion) → Authentication Profiles (Profils d'authentification) dans l'arborescence.

Figure 6-42. Authentication Profiles (Profils d'authentification)



La page Authentication Profiles (Profils d'authentification) contient les champs suivants :

Authentication Profile Name (Nom du profil d'authentification) : listes des profils d'authentification définies par l'utilisateur, auxquelles les profils sont ajoutés. Les valeurs par défaut sont **Network Default** (Valeur par défaut pour le réseau) et **Console Default** (Valeurs par défaut pour la console).

- Login (Nom d'utilisateur) : indique la liste des profils d'authentification définis par l'utilisateur pour les mots de passe login.
- Enable (Activer) : indique la liste des profils d'authentification définie par l'utilisateur pour les mots de passe Enable.

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

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

Local (Locale) : l'authentification des utilisateurs s'effectue au niveau de l'unité. L'unité vérifie le nom d'utilisateur et le mot de passe pour procéder à l'authentification.

RADIUS : l'authentification des utilisateurs s'effectue au niveau du serveur RADIUS. Pour plus d'informations, voir "Configuration des paramètres RADIUS".

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

Enable (Activer) : le mot de passe Enable est utilisé pour l'authentification.

TACACS+ : l'authentification des utilisateurs s'effectue au niveau du serveur TACACS+.

Restore Default (Restaurer les valeurs par défaut) : restaure la méthode par défaut d'authentification des utilisateurs sur l'unité. S'applique uniquement au profil par défaut.

Remove (Supprimer) : supprime le profil sélectionné. Les profils actifs ne peuvent pas être supprimés. S'applique uniquement aux profils définis par l'utilisateur.

Sélection d'un profil d'authentification

1. Affichez la page Authentication Profiles (Profils d'authentification).
2. Sélectionnez un profil dans le champ **Authentication Profile Name** (Nom du profil d'authentification).
3. Sélectionnez la méthode d'authentification à l'aide des flèches de navigation. L'authentification est effectuée dans l'ordre d'affichage des méthodes.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

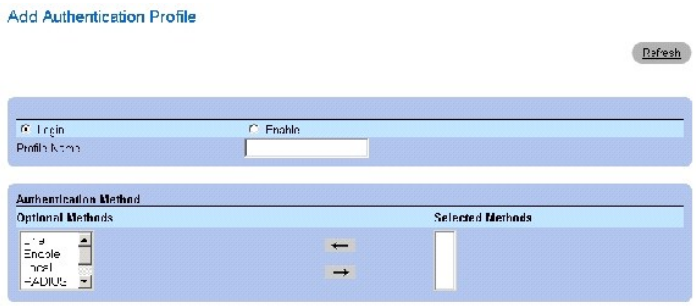
Le profil d'authentification des utilisateurs est mis à jour sur l'unité.

Ajout d'un profil d'authentification

1. Affichez la page Authentication Profiles (Profils d'authentification).
2. Cliquez sur Add (Ajouter).

La page **Add Authentication Profile** (Ajout d'un profil d'authentification) s'affiche.

Figure 6-43. Add Authentication Profile (Ajout d'un profil d'authentification)



3. Configurez le profil.

REMARQUE : n'insérez aucun espace dans le nom du nouveau profil.

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

Le profil d'authentification est mis à jour sur l'unité.

Affichage de la table des profils d'authentification

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

La page **Authentication Profiles Table** (Table des profils d'authentification) s'affiche.

Suppression d'un profil d'authentification

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

La page **Authentication Profiles Table** (Table des profils d'authentification) s'affiche.

3. Sélectionnez un profil d'authentification.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le profil d'authentification sélectionné est supprimé.

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

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page Authentication Profiles (Profils d'authentification).

Tableau 6-29. Commandes CLI relatives aux profils d'authentification

Commande CLI	Description
aaa authentication login {default | nom_liste} méthode1 [méthode2.]	Configure l'authentification des connexions.
no aaa authentication login {default | nom_liste}	Supprime un profil d'authentification des connexions.

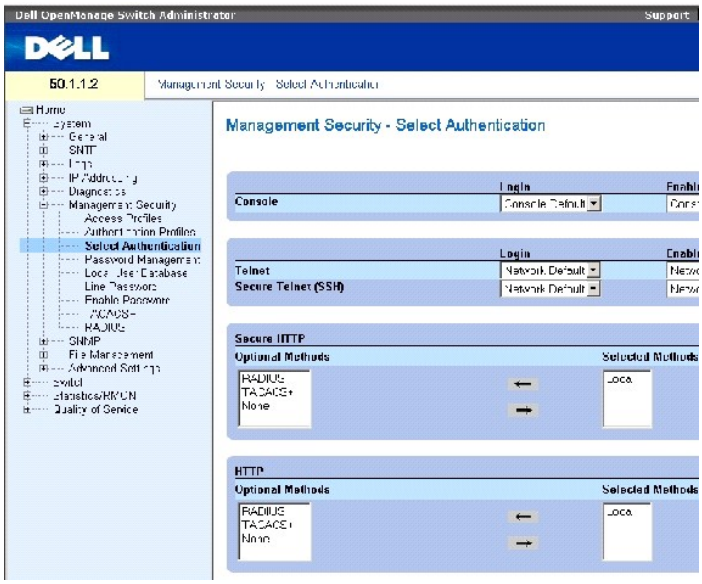
Voici un exemple de commandes CLI :

```
console(config)# aaa
authentication login
default radius local
enable none



console(config)# no aaa
authentication login
default
```

Sélection des profils d'authentification

Après avoir été 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 au moyen de la liste de méthodes d'authentification 1, et les utilisateurs Telnet à l'aide de la liste de méthodes d'authentification 2. Pour ouvrir la page Select Authentication (Sélectionner une authentification), cliquez sur System (Système) → Management Security (Sécurité de gestion) → Select Authentication (Sélectionner une authentification) dans l'arborescence.

Figure 6-44. Select Authentication (Sélectionner une authentification)



La page Select Authentication (Sélectionner une authentification) contient les champs suivants :

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

Login (Connexion) : indique les profils d'authentification à utiliser pour la connexion à l'interface de la console.

Enable (Activer) : spécifie les profils d'authentification à utiliser pour les utilisateurs qui activent le mode Privileged EXEC à partir de l'interface de la console.

Telnet : profils d'authentification utilisés pour authentifier les utilisateurs Telnet.

Secure Telnet (SSH) (Telnet sécurisé [SSH]) : profils utilisés pour authentifier les utilisateurs Secure Shell (SSH). SSH permet aux clients de se connecter à distance de façon sécurisée et chiffrée à l'unité.

HTTP / **Secure HTTP** (HTTP et HTTP sécurisé) : méthode d'authentification utilisée pour l'accès HTTP et HTTP sécurisé, respectivement. Les valeurs admises pour ce champ sont les suivantes :

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

Local (Locale) : l'authentification s'effectue au niveau local.

RADIUS : l'authentification s'effectue au niveau du serveur RADIUS.

TACACS+ : l'authentification s'effectue au niveau du serveur TACACS+.

Application d'une liste 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).

Une liste d'authentification est attribuée aux sessions de console.

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).

Une liste d'authentification est attribuée aux sessions Telnet.

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

Un profil d'authentification est attribué aux sessions Telnet sécurisées (SSH).

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

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

Une séquence d'authentification est attribuée aux sessions HTTP.

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

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

Une séquence d'authentification est attribuée aux sessions HTTP sécurisées.

Attribution de profils ou de séquences d'authentification des accès à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page Select Authentication (Sélectionner une authentification).

Tableau 6-30. Commandes CLI de sélection d'une authentification

Commande CLI	Description
enable authentication [default | nom_liste]	Indique la liste de méthodes d'authentification lors de l'accès à un niveau de droits d'accès élevé à partir d'une console ou d'une session Telnet ou SSH à distance.
login authentication [default | nom_liste]	Indique la liste de méthodes d'authentification des connexions pour une console ou une session Telnet ou SSH à distance.
ip http authentication méthode1 [méthode2.]	Indique les méthodes d'authentification pour les serveurs HTTP.
ip https authentication méthode1 [méthode2.]	Indique les méthodes d'authentification pour les serveurs HTTPS.
show authentication methods	Affiche des informations sur les méthodes d'authentification.

Voici un exemple de commandes CLI :

```
console(config-line)# enable
authentication default
```

```
console(config-line)# login
authentication default
```

```
console(config-line)# exit
```

```
console(config)# ip http
authentication radius local
```

```
console(config)# ip https
authentication radius local
```

```
console(config)# exit
```

```
console# show authentication methods
```

```
Login Authentication Method Lists

---------------------------------
```

Console_Default	: None	
Network_Default	: Local	

```
Enable Authentication Method Lists

---------------------------------
```

Console_Default	: Enable None	
Network_Default	: Enable	
Line	Login Method List	Enable Method List
----	----------	----------
Console	Default	Default
Telnet	Default	Default

SSH	Default	Default
http	: Local	
https	: Local	
dot1x	:	

Gestion des mots de passe

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

- Définition de la longueur minimum du mot de passe
- Expiration du mot de passe
- Rejet d'un mot de passe fréquemment utilisé
- Exclusion des utilisateurs après plusieurs tentatives de connexion infructueuses

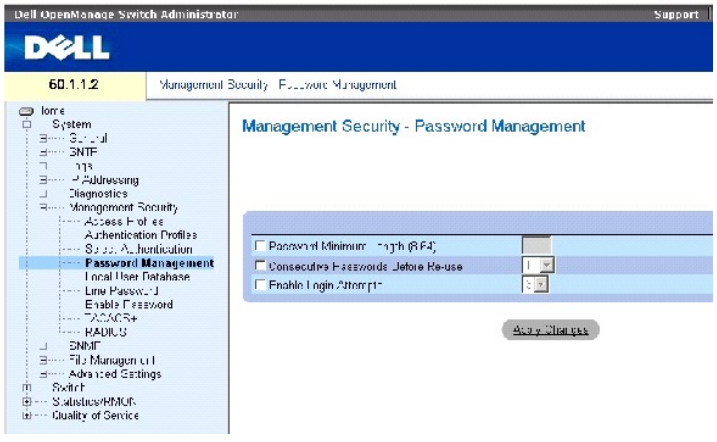
L'expiration du mot de passe commence dès l'activation de la gestion des mots de passe. Les mots de passe expirent après un délai ou une date défini(e) par l'utilisateur. Dix jours avant l'expiration du mot de passe, l'unité affiche un message d'avertissement.

Après expiration du mot de passe, les utilisateurs disposent de trois connexions supplémentaires. Au cours des trois dernières connexions, un message d'avertissement demande à l'utilisateur de modifier immédiatement son mot de passe. S'ils ne modifient pas leur mot de passe, les utilisateurs sont exclus du système et ne peuvent se connecter qu'à partir de la console. Les avertissements relatifs aux mots de passe sont consignés dans le fichier Syslog.

Si un niveau de privilège est redéfini, l'utilisateur doit l'être également. Cependant, le mot de passe expire toujours selon le délai défini initialement par l'utilisateur.

Pour ouvrir la page Password Management (Gestion des mots de passe), cliquez sur System (Système) → Management Security (Sécurité de gestion) → Password Management (Gestion des mots de passe) dans l'arborescence.

Figure 6-45. Password Management (Gestion des mots de passe)



La page Password Management (Gestion des mots de passe)contient les champs suivants :

Password Minimum Length (8-64) (Longueur minimum du mot de passe) : indique la longueur minimum du mot de passe. Par exemple, l'administrateur peut indiquer que tous les mots de passe doivent contenir au moins 10 caractères.

Consecutive Passwords Before Re-use (Mots de passe consécutifs avant réutilisation) : indique le nombre de fois où un mot de passe doit avoir été modifié pour que l'utilisateur puisse définir un mot de passe déjà utilisé auparavant. Les valeurs possibles vont de 1 à 10.

REMARQUE : un message invite l'utilisateur à modifier son mot de passe avant qu'il n'expire. Cependant, les utilisateurs Web ne reçoivent pas ce message.

Enable Login Attempts (Activer le décompte des tentatives de connexion) : empêche l'utilisateur de se connecter à l'unité lorsque le nombre d'utilisations d'un mot de passe erroné dépasse une certaine valeur. Par exemple, si ce champ est activé et configuré sur 5 et qu'un utilise tente de se connecter à cinq reprises à l'aide d'un mot de passe incorrect, l'unité exclut l'utilisateur à la sixième tentative. Les valeurs possibles vont de 1 à 5.

Définition de la gestion des mots de passe

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

La gestion des mots de passe est définie et l'unité est mise à jour.

Gestion des mots de passe à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page Password Management (Gestion des mots de passe).

Tableau 6-31. Gestion des mots de passe à l'aide de commandes CLI

Commande CLI	Description
password min-length *longueur*	Définit la longueur minimum du mot de passe.
password history numéro	Définit le nombre de modifications du mot de passe nécessaires pour pouvoir le réutiliser.
password lock-out *numéro*	Définit le nombre de saisies d'un mot de passe incorrect avant que l'utilisateur soit exclu de l'unité.
show password configuration	Affiche les informations sur la gestion des mots de passe.

Voici un exemple de commandes CLI :

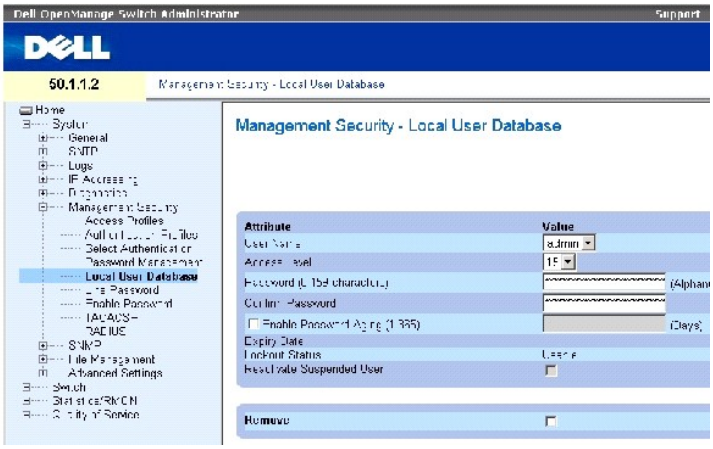
```
console # show passwords configuration

Minimal length: 0

History: Disabled

History hold time: no limit

Lockout control: disabled

Enable Passwords
```

Level	Password Aging	Password Expiry date	Lockout	
-----	--------	----------	-------	
1	-	-	-	
15	-	-	-	
Line Passwords				
Line	Password Aging	Password Expiry date	Lockout	
-------	--------	----------	-------	
Telnet	-	-	-	
SSH	-	-	-	
Console	-	-	-	
console # **show users accounts**				
Username	Privilege	Password Aging	Password Expiry Date	Lockout
--------	---------	--------	----------	-------
nim	15	39	18-Feb-2005	

Définition des bases de données d'utilisateurs locales

La page Local User Database (Base de données d'utilisateurs locale) contient des champs permettant de définir les utilisateurs, les mots de passe et les niveaux d'accès. Pour ouvrir la page Local User Database (Base de données d'utilisateurs locale), cliquez sur System (Système) → Management Security (Sécurité de gestion) → Local User Database (Bases de données d'utilisateurs locales) dans l'arborescence.

Figure 6-46. Local User Database (Base de données d'utilisateurs locale)



La page Local User Database (Base de données d'utilisateurs locale) 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 des utilisateurs est **1** et le plus élevé est **15**. Les utilisateurs disposant d'un accès de niveau 15 sont des utilisateurs privilégiés et autorisés à utiliser le programme OpenManage Switch Administrator.

Password (0-159 Characters) (Mot de passe [0 à 32 caractères]) : mot de passe défini par l'utilisateur.

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

Enable Password Aging (1-365) (Activer le délai d'expiration du mot de passe [1 à 365]) : définit le délai d'expiration d'un mot de passe.

Expiry Date (Date d'expiration) : indique la date d'expiration du mot de passe défini par l'utilisateur.

Lockout Status (État de l'exclusion) : spécifie le nombre de tentatives d'authentification infructueuses depuis la dernière connexion réussie, lorsque la case **Enable Login Attempts** (Activer les tentatives de connexion) est cochée à la page Password Management (Gestion des mots de passe). Spécifie l'état **LOCKOUT** (Exclusion) lorsque le compte de l'utilisateur est bloqué.

Reactivate Suspended User (Réactiver un utilisateur exclu) : réactive les droits d'accès de l'utilisateur spécifié. Les droits d'accès peuvent être suspendus après des tentatives de connexion infructueuses.

Remove (Supprimer) : supprime des utilisateurs de la liste **User Name** (Nom d'utilisateur).

Attribution de droits d'accès à un utilisateur

1. Affichez la page Local User Database (Base de données d'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).

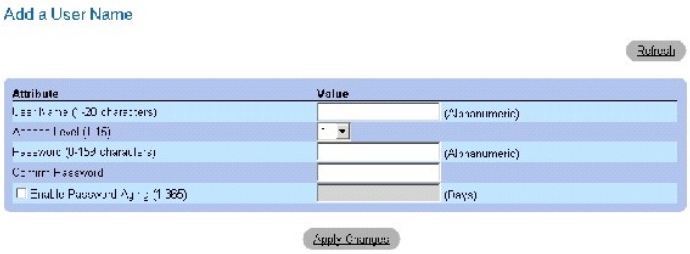
Les droits d'accès et mots de passe des utilisateurs sont définis et l'unité est mise à jour.

Définition d'un nouvel utilisateur

1. Affichez la page Local User Database (Base de données d'utilisateurs locale).
2. Cliquez sur **Add** (Ajouter).

La page **Add User** (Ajouter un utilisateur) s'affiche.

Figure 6-47. Add a User (Ajout d'un utilisateur)



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

Le nouvel utilisateur est défini et l'unité est mise à jour.

Affichage de la table des utilisateurs locaux

1. Affichez la page Local User Database (Base de données d'utilisateurs locale).
2. Cliquez sur **Show All** (Afficher tout).

La page Local User Table (Table des utilisateurs locaux) s'affiche.

Figure 6-48. Local User Table (Table des utilisateurs locaux)

Réactivation d'un utilisateur exclu

1. Affichez la page Local User Database (Base de données d'utilisateurs locale).
2. Cliquez sur **Show All** (Afficher tout).

La page Local User Table (Table des utilisateurs locaux) s'affiche.

3. Sélectionnez un **nom d'utilisateur**.
4. Cochez la case **Reactivate Suspended User** (Réactiver un utilisateur exclu).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les droits d'accès des utilisateurs sont réactivés et l'unité est mise à jour.

Suppression de comptes utilisateur

1. Affichez la page Local User Database (Base de données d'utilisateurs locale).
2. Cliquez sur **Show All** (Afficher tout).

   La page Local User Table (Table des utilisateurs locaux) s'affiche.
3. Sélectionnez un **nom d'utilisateur**.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

   L'utilisateur sélectionné est supprimé et l'unité est mise à jour.

Attribution d'utilisateurs à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page Local User Database (Base de données d'utilisateurs locale).

Tableau 6-32. Commandes CLI de la base de données d'utilisateurs locale

Commande CLI	Description
username nom [password mot de passe] [level niveau] [encrypted]	Définit un système d'authentification reposant sur des noms d'utilisateurs.
set username nom **active**	Réactive les droits d'accès d'un utilisateur exclu.

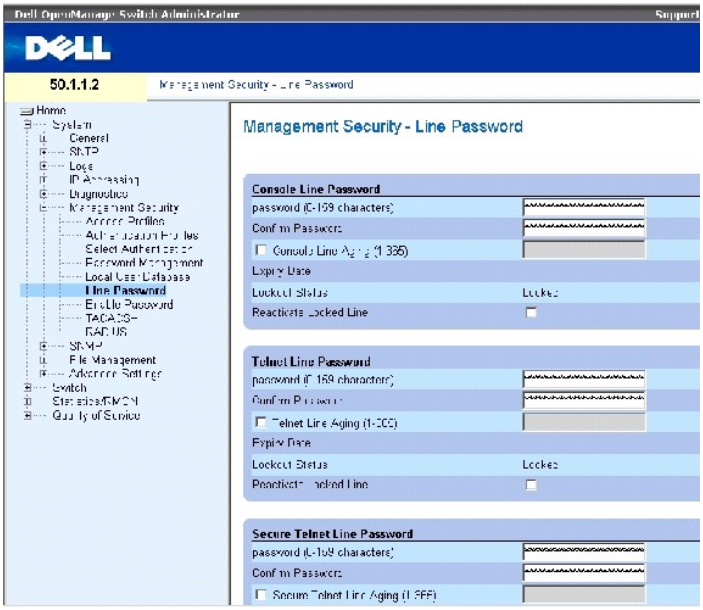
Voici un exemple de commandes CLI :

```
console(config)# username
bob password lee level 15



console# set username bob
active
```

Définition de mots de passe en ligne

La page Line Password (Mot de passe en ligne) contient des champs permettant de définir des mots de passe en ligne pour les méthodes de gestion. Pour ouvrir la page Line Password (Mot de passe en ligne), cliquez sur System (Système) → Management Security (Sécurité de gestion) → Line Passwords (Mots de passe en ligne) dans l'arborescence.

Figure 6-49. Line Password (Mot de passe en ligne)



La page Line Password (Mot de passe en ligne) contient les champs suivants :

Line Password for Console / Telnet / Secure Telnet (Mot de passe en ligne pour la session Console/Telnet/Telnet sécurisée) : mot de passe en ligne permettant d'accéder à l'unité par le biais d'une session Console, Telnet ou Telnet sécurisée.

Confirm Password for Console / Telnet / Secure Telnet (Confirmer le mot de passe pour la session Console/Telnet/Telnet sécurisée) : confirme le nouveau mot de passe en ligne. Le mot de passe s'affiche sous la forme *****.

Line Aging (1-365) for Console / Telnet / Secure Telnet (Expiration du mot de passe en ligne pour la session Console/Telnet/Telnet sécurisée) : indique le délai d'expiration (en jours) d'un mot de passe en ligne.

Expiry Date for Console / Telnet / Secure Telnet (Date d'expiration de la session Console/Telnet/Telnet sécurisée) : indique la date d'expiration du mot de passe en ligne.

Lockout Status for Console / Telnet / Secure Telnet (État de l'exclusion pour la session Console/Telnet/Telnet sécurisée) : spécifie le nombre de tentatives d'authentification infructueuses depuis la dernière connexion réussie, si la case **Enable Login Attempts** (Activer les tentatives de connexion) a été cochée dans la page Password Management (Gestion des mots de passe). Spécifie l'état **LOCKOUT** (Exclusion) lorsque le compte de l'utilisateur est bloqué.

Reactivate Locked Line for Console / Telnet / Secure Telnet (Réactiver la ligne bloquée pour la session Console/Telnet/Telnet sécurisée) : réactive le mot de passe en ligne pour une session Console/Telnet/Telnet sécurisée. Les droits d'accès peuvent être suspendus après des tentatives de connexion infructueuses.

Définition de mots de passe en ligne pour les sessions de console

1. Affichez la page Line Password (Mot de passe en ligne).
2. Définissez le champ **Console Line Password** (Mot de passe en ligne pour la console).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mot de passe en ligne à utiliser pour les sessions de console est défini et l'unité est mise à jour.

Définition de mots de passe en ligne pour les sessions Telnet

1. Affichez la page Line Password (Mot de passe en ligne).

2. Définissez le champ Telnet Line Password (Mot de passe en ligne pour une session Telnet).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mot de passe en ligne à utiliser pour les sessions Telnet est défini et l'unité est mise à jour.

Définition de mots de passe en ligne pour les sessions Telnet sécurisées

1. Affichez la page Line Password (Mot de passe en ligne).
2. Définissez le champ **Secure Telnet Line Password** (Mot de passe en ligne pour une session Telnet sécurisée).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mot de passe en ligne à utiliser pour les sessions Telnet sécurisées est défini et l'unité est mise à jour.

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

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page Line Password (Mot de passe en ligne).

Tableau 6-33. Commandes CLI relatives aux mots de passe en ligne

Commande CLI	Description
password mot de passe [encrypted]	Définit un mot de passe en ligne.

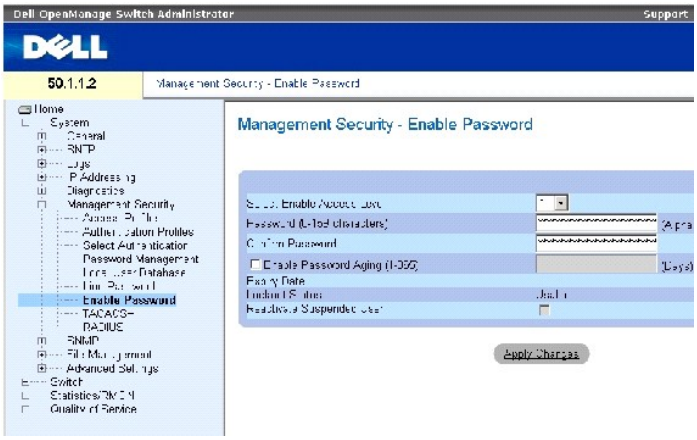
Voici un exemple de commandes CLI :

```
console(config-line)#
password dell
```

Définition de mots de passe Enable

La page Enable Password (Mot de passe Enable) définit un mot de passe local permettant de contrôler l'accès pour les utilisateurs disposant de droits normaux ou de privilèges. Pour ouvrir la page Enable Password (Mot de passe Enable), cliquez sur System (Système) → Management Security (Sécurité de gestion) → Enable Passwords (Mots de passe Enable) dans l'arborescence.

Figure 6-50. Enable Password (Mot de passe Enable)



La page Enable Password (Mot de passe Enable)contient les champs suivants :

Select Enable Access Level (Sélectionner le niveau d'accès Enable) : niveau d'accès associé au mot de passe Enable. Les valeurs possibles vont de 1 à 15.

Password (0-159 Characters) (Mot de passe [0 à 159 caractères]) : mot de passe Enable en cours.

Confirm Password (Confirmer le mot de passe) : confirme le nouveau mot de passe Enable. Ce mot de passe s'affiche sous la forme *****.

Enable Password Aging (1-365) (Activer le délai d'expiration du mot de passe [1 à 365]) : définit le délai d'expiration d'un mot de passe.

Expiry Date (Date d'expiration) : indique la date d'expiration du mot de passe Enable.

Lockout Status (État de l'exclusion) : spécifie le nombre de tentatives d'authentification infructueuses depuis la dernière connexion réussie, si la case **Enable Login Attempts** (Activer les tentatives de connexion) a été cochée dans la page Password Management (Gestion des mots de passe). Spécifie l'état **LOCKOUT** (Exclusion) lorsque le compte de l'utilisateur est bloqué.

Reactivate Suspended User (Réactiver un utilisateur exclu) : réactive les droits d'accès de l'utilisateur spécifié. Les droits d'accès peuvent être suspendus après une tentative de connexion infructueuse.

Définition d'un nouveau mot de passe Enable

1. Affichez la page Enable Password (Mot de passe Enable).
2. Complétez les champs avec les valeurs appropriées.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau mot de passe Enable est défini et l'unité est mise à jour.

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

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page Enable Password (Mot de passe Enable).

Tableau 6-34. Commandes CLI permettant la modification du mot de passe Enable

Commande CLI	Description
enable password [level niveau] mot de passe [encrypted]	Définit un mot de passe local permettant de contrôler l'accès aux niveaux Utilisateurs et Droits d'accès.

Voici un exemple de commandes CLI :

```
console(config)# enable
password level 15 secret
```

Définition des paramètres TACACS+

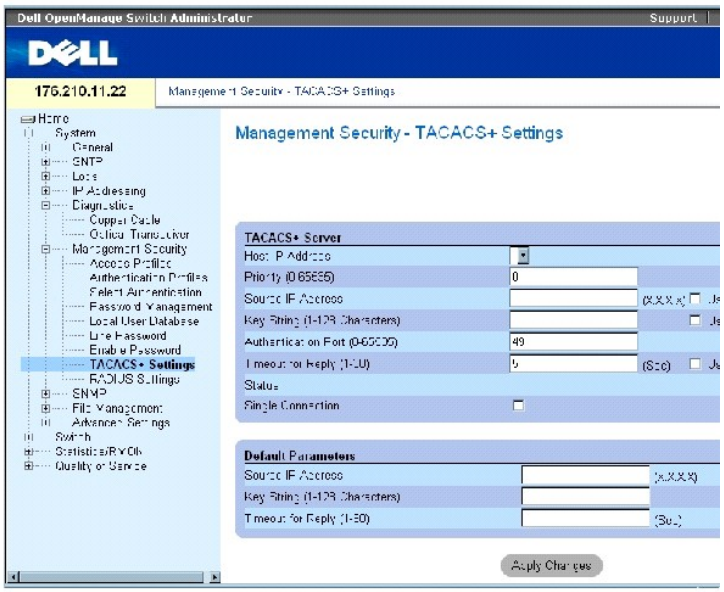
Les unités prennent en charge le client Terminal Access Controller Access Control System (TACACS+). TACACS+ permet une gestion sécurisée et centralisée de la validation des utilisateurs qui accèdent à l'unité.

TACACS+ offre un système de gestion centralisé des utilisateurs tout en restant compatible avec le système RADIUS et d'autres processus d'authentification. TACACS+ propose les services suivants :

- Authentication (Authentification) : fournit une authentification lors de la connexion et à l'aide de noms d'utilisateurs et de mots de passe définis par l'utilisateur.
- Authorization (Autorisation) : effectuée lors de la connexion. Une fois la session d'authentification terminée, une session d'autorisation commence avec le nom d'utilisateur authentifié. Le serveur TACACS+ vérifie les droits de l'utilisateur.

Le protocole TACACS+ vérifie l'intégrité du réseau via des échanges de protocole chiffrés entre l'unité et le serveur TACACS+. Pour ouvrir la page TACACS+ Settings (Paramètres TACACS+), cliquez sur **System** (Système) → **Management Security** (Sécurité de gestion) → **TACACS+** dans l'arborescence.

Figure 6-51. TACACS+ Settings (Paramètres TACACS+)



La page TACACS+ Settings (Paramètres TACACS+)contient les champs suivants :

Host IP Address (Host IP Address) : indique l'adresse IP du serveur TACACS+.

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

Source IP Address (Adresse IP source) : adresse IP source de l'unité utilisée pour la session TACACS+ entre l'unité et le serveur TACACS+.

Key String (0-128 Characters) (Clé de codage [1 à 128 caractères]) : définit la clé d'authentification et de codage pour les communications TACACS+ entre l'unité et le serveur TACACS+. Cette clé doit correspondre à la clé de codage utilisée sur le serveur TACACS+. Cette clé est codée.

Authentication Port (0-65535) (Port d'authentification [0 à 65535]) : numéro de port de la session TACACS+. Le port par défaut est le 49.

Timeout for Reply (1-30) (Délai de réponse [1 à 30]) : délai qui s'écoule avant que la connexion entre l'unité et le serveur TACACS+ n'expire. La plage de valeurs est comprise entre 1 et 30 secondes.

Status (État) : état de la connexion entre l'unité et le serveur TACACS+. Ce champ peut prendre les valeurs suivantes :

Connected (Connectée) : l'unité est actuellement connectée au serveur TACACS+.

Not Connected (Non connectée) : l'unité n'est pas connectée au serveur TACACS+.

Single Connection (Connexion unique) : gère une connexion ouverte unique entre l'unité et le serveur TACACS+

Les paramètres TACACS+ par défaut sont définis par l'utilisateur. Les paramètres par défaut sont appliqués aux nouveaux serveurs TACACS+ définis. Si les valeurs par défaut ne sont pas définies, les valeurs système par défaut sont appliquées aux nouveaux serveurs TACACS+.

Voici les valeurs TACACS+ par défaut :

Source IP Address (Adresse IP source) : adresse IP source par défaut de l'unité utilisée pour la session TACACS+ entre l'unité et le serveur TACACS+. L'adresse IP source par défaut est de 0.0.0.0.

Key String (0-128 Characters) (Clé de codage [1 à 128 caractères]) : clé de codage par défaut utilisée pour authentifier et crypter toutes les communications entre l'unité et le serveur TACACS+. Cette clé est codée.

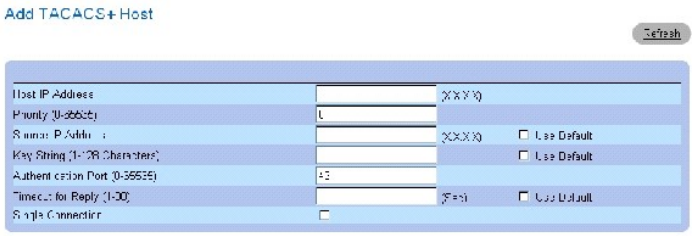
Timeout for Reply (1-30) (Délai de réponse [1 à 30]) : délai par défaut qui s'écoule avant que la connexion entre l'unité et le serveur TACACS+ n'expire. La valeur par défaut est de 5 secondes.

Ajout d'un serveur TACACS+

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

La page Add TACACS+ Host (Ajout d'un hôte TACACS+) s'affiche.

Figure 6-52. Add TACACS+ Host (Ajout d'un hôte TACACS+)



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

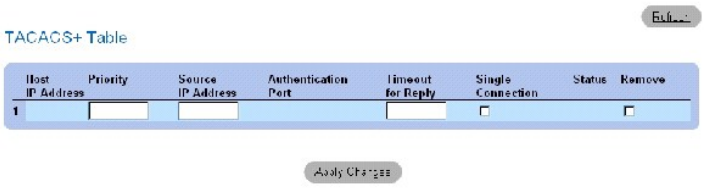
Le serveur TACACS+ est ajouté et l'unité est mise à jour.

Affichage de la page TACACS+ Table (Table TACACS+)

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

La page TACACS+ Table (Table TACACS+) s'affiche.

Figure 6-53. TACACS+ Table (Table TACACS+)



Suppression d'un serveur TACACS+

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

   La page TACACS+ Table (Table TACACS+) s'affiche.
3. Sélectionnez une entrée de la page TACACS+ Table (Table TACACS+).
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

   Le serveur TACACS+ est supprimé et l'unité est mise à jour.

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

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page TACACS+ Settings (Paramètres TACACS+).

Tableau 6-35. Commandes CLI TACACS+

Commande CLI	Description
tacacs-server host {*adresse-ip* | *nom d'hôte*} [**single-connection**] [**port** *numéro-port*] [**timeout** *délai d'attente*] [**key** *clé-codage*] [**source** *source*] [**priority** *priorité*]	Indique un hôte TACACS+.
tacacs-server key clé_codage	Définit la clé d'authentification et de codage utilisée pour toutes les communications TACACS+ entre l'unité et le serveur TACACS+. Cette clé doit correspondre à la clé de codage utilisée sur le démon TACACS+. (Plage : 0 à 128 caractères.)
tacacs-server timeout délai d'attente	Indique le délai d'attente en secondes. (Plage : 1 - 30.)
tacacs-server source-ip source	Indique l'adresse IP source. (Plage : adresse IP valide.)
show tacacs [*adresse_ip*]	Affiche la configuration et les statistiques d'un serveur TACACS+.

Voici un exemple de commandes CLI :

```
console# show tacacs

Device Configuration

IP address      Status      Port  Single Connection  TimeOut  Source IP  Priority
--------------  ----------  ----  -----------------  -------  ---------  --------
12.1.1.2        Not         49    Yes                1        12.1.1.1   1
```

	Connected					
Global values						

TimeOut : 5						
Device Configuration ----------						
Source IP : 0.0.0.0						
console#						

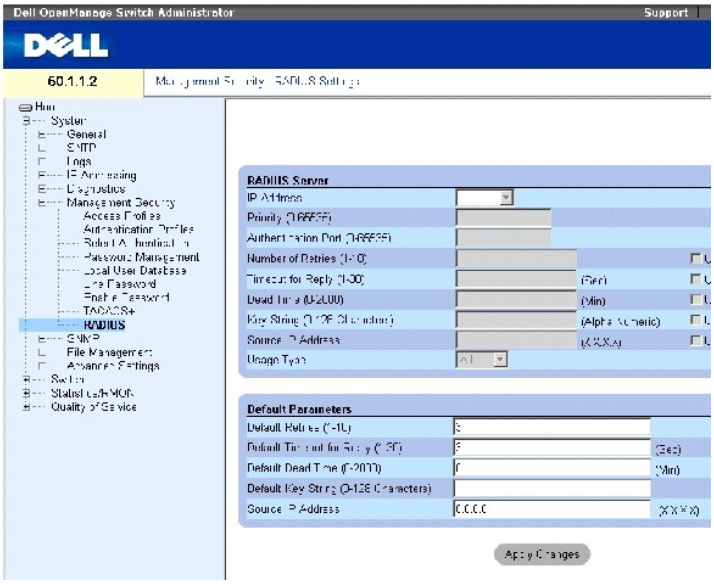
Configuration des paramètres RADIUS

Les serveurs RADIUS (Remote Authorization Dial-In User Service) permettent d'accroître la sécurité des réseaux. Vous pouvez définir jusqu'à quatre serveurs RADIUS. Ces serveurs assurent une méthode d'authentification centralisée pour :

- les accès Telnet ;
- les accès Secure Shell ;
- les accès Web ;
- les accès Console.

Pour ouvrir la page RADIUS Settings (Paramètres RADIUS), cliquez sur System (Système) → Management Security (Sécurité de gestion) → RADIUS dans l'arborescence.

Figure 6-54. RADIUS Settings (Paramètres RADIUS)



La page RADIUS Settings (Paramètres RADIUS) contient les champs suivants :

IP Address (Adresse IP) : liste des adresses IP de serveurs d'authentification.

Priority (0-65535) (Priorité [1 à 65535]) : priorité du serveur. Les valeurs autorisées sont comprises entre 0 et 65535, 0 correspondant à la valeur la plus élevée. Cette valeur est utilisée pour définir l'ordre d'interrogation des serveurs.

Authentication Port (Port d'authentification) : identifie le port d'authentification. Ce port s'utilise pour vérifier l'authentification du serveur RADIUS.

Number of Retries (1-10) (Nombre de tentatives [1à10]) : indique le nombre de demandes de transmission envoyées au serveur RADIUS avant échec. Les valeurs possibles vont de 1 à 10.

Timeout for Reply (1-30) (Délai de réponse [1 à 30]) : indique le délai, en secondes, pendant lequel l'unité attend une réponse du serveur RADIUS avant de renvoyer la requête ou de basculer sur le serveur suivant. Les valeurs possibles vont de 1 à 30.

Dead Time (0-2000) (Délai d'inactivité [0 à 2000]) : indique la durée (en minutes) pendant laquelle un serveur RADIUS est détourné pour répondre à des demandes de service. La plage est comprise entre 0 et 2000.

Key String (1-128 Characters) (Clé de codage [1 à 128 caractères]) : clé de codage utilisée pour authentifier et crypter toutes les communications RADIUS entre l'unité et le serveur RADIUS. Cette clé est codée.

Source IP Address (Adresse IP source) : indique l'adresse IP source utilisée pour la communication avec les serveurs RADIUS.

Usage Type (Type d'utilisation) : indique le type d'utilisation du serveur. Ce champ peut prendre l'une des valeurs suivantes : login, 802.1x ou all (Tous). La valeur par défaut est "all".

Les valeurs RADIUS par défaut sont définies à l'aide des champs suivants :

REMARQUE : si aucune valeur n'a été définie pour les délais, le nombre de tentatives ou le délai d'inactivité, les valeurs générales par défaut sont appliquées à chaque hôte.

Default Retries (1-10) (Tentatives par défaut [1 à 10]) : indique le nombre de demandes de transmission par défaut envoyées au serveur RADIUS avant échec.

Default Timeout for Reply (1-30) (Délai d'attente par défaut pour les réponses [1 à 30]) : définit la durée (en secondes) pendant laquelle l'unité attend une réponse du serveur RADIUS avant expiration. La valeur par défaut est de 5 secondes.

Default Dead Time (0-2000) (Délai d'inactivité par défaut [0 à 2000]) : indique la durée par défaut (en minutes) pendant laquelle un serveur RADIUS est détourné pour répondre à des demandes de service. La plage est comprise entre 0 et 2000.

Default Key String (1-128 Characters) (Clé de codage par défaut [1 à 128 caractères]) : clé de codage par défaut utilisée pour authentifier et crypter toutes les communications RADIUS entre l'unité et le serveur RADIUS. Cette clé est codée.

Source IP Address (Adresse IP source) : indique l'adresse IP source par défaut utilisée pour la communication avec les serveurs RADIUS. L'adresse IP source par défaut est 0.0.0.0.

Définition des paramètres RADIUS

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

Les paramètres RADIUS sont mis à jour sur l'unité.

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 6-55. Add RADIUS Server (Ajouter un serveur RADIUS)

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

Le nouveau serveur RADIUS est ajouté et l'unité est mise à jour.

Affichage de la liste de serveurs RADIUS

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

La page RADIUS Servers List (Liste de serveurs RADIUS) s'affiche.

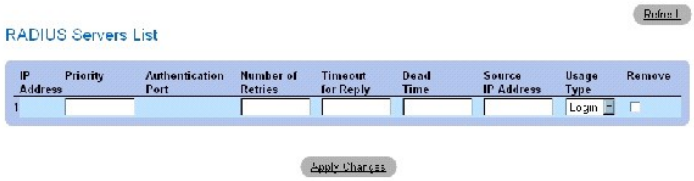


Figure 6-56. RADIUS Servers List (Liste de serveurs RADIUS)

Suppression d'un serveur RADIUS

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

La page RADIUS Servers List (Liste de serveurs RADIUS) s'affiche.

3. Sélectionnez une entrée de la page RADIUS Servers List (Liste de serveurs RADIUS).
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le serveur RADIUS est supprimé et l'unité est mise à jour.

Définition de serveurs RADIUS à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page RADIUS Settings (Paramètres RADIUS).

Tableau 6-36. Commandes CLI relatives au serveur RADIUS

Commande CLI	Description
radius-server timeout *délai d'attente*	Définit la durée pendant laquelle un routeur attend une réponse d'un serveur hôte.
radius-server retransmit *tentatives*	Définit le nombre de tentatives de recherche de la liste de serveurs RADIUS hôtes.
radius-server deadtime délai d'inactivité	Définit les serveurs non disponibles à ignorer.
radius-server key *clé-codage*	Définit la clé de codage d'authentification et de cryptage utilisée pour toutes les communications RADIUS entre le routeur et le serveur RADIUS.
radius-server host *adresse-ip* [**auth-port** *numéro-port-aut*] [**timeout** délai d'attente] [**retransmit** *tentatives*] [**deadtime** *délai d'inactivité*] [**key** *clé-codage*] [**source** *source*] [**priority** *priorité*]	Spécifie un serveur RADIUS hôte.
show radius-servers	Affiche les paramètres des serveurs RADIUS.

Voici un exemple de commandes CLI :

```
Console(config)# radius-
server timeout 5


Console(config)# radius-
```

```
server retransmit 5



Console(config)# radius-
server deadtime 10



Console(config)# radius-
server key dell-server



Console(config)# radius-
server host 196.210.100.1
auth-port 127 timeout 20



Console# show radius-
servers



IP address Auth Acct
TimeOut Retransmit
Deadtime Source IP
Priority



-------- ---- ---- ------
--------- ------- -------
------



172.16.1.1 164 51646 3 3 0
01 172.16.1.2 164 51646 3
3 0 02
```

Définition des paramètres SNMP

Le protocole SNMP (Simple Network Management Protocol) fournit une méthode de gestion d'unités en réseau. Le commutateur prend en charge les versions SNMP suivantes :

- SNMPv1 (version 1)
- SNMPv2 (version 2)
- SNMPv3 (version 3)

SNMP v1 et v2

Les agents SNMP gèrent une liste de variables qui sont utilisées pour gérer le commutateur. Ces variables sont définies dans la MIB (Management Information Base, base d'informations de gestion). La MIB affiche les variables gérées par l'agent. L'agent SNMP définit un format de spécifications MIB ainsi que le format utilisé pour accéder aux informations sur le réseau. Les droits d'accès aux agents SNMP sont contrôlés par des chaînes d'accès.

SNMP v1 et v2 sont activées par défaut.

SNMP v3

SNMP v3 applique également un contrôle d'accès et un nouveau mécanisme d'interruption aux PDU SNMPv1 et SNMPv2. En outre, un modèle USM (User Security Model) est défini pour SNMPv3. Ce modèle inclut les fonctions suivantes :

- **Authentication** (Authentification) : vérifie l'intégrité des données et authentifie leur origine.
- **Privacy** (Confidentialité) : garantit la confidentialité des informations contenues dans le message. Cipher Block-Chaining (CBC) est la méthode de codage utilisée. Vous pouvez appliquer uniquement le mode d'authentification à un message SNMP ou les deux modes d'authentification et de

confidentialité. Cependant, le mode confidentialité ne peut pas être appliqué sans le mode authentification.

- **Timeliness** (Précision) : offre une protection contre le retard dans la transmission des messages ou la transmission de messages redondants. L'agent SNMP compare le message entrant et les informations d'horodatage.
- **Key Management** (Gestion des clés) : définit la création, les mises à jour et l'utilisation des clés.

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

- Sécurité
- Contrôle des accès aux fonctionnalités
- Interruptions

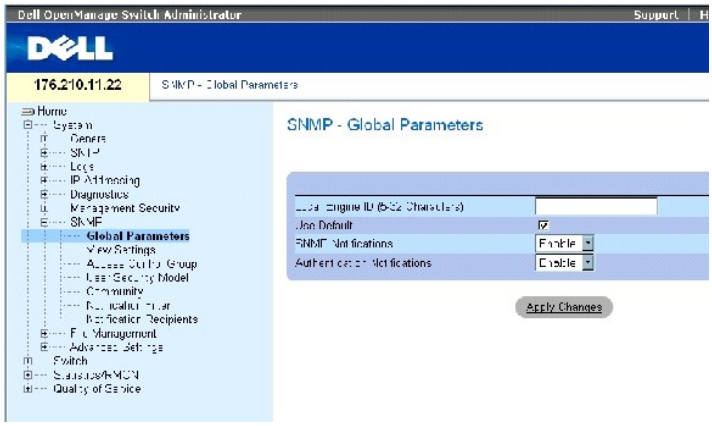
Les clés d'authentification ou de confidentialité sont modifiées dans le modèle USM (User Security Model).

SNMPv3 peut être activé si l'ID du moteur local est activé.

Définition des paramètres globaux SNMP

La page SNMP Global Parameters (Paramètres globaux SNMP) permet d'activer les notifications SNMP et d'authentification. Pour ouvrir la page SNMP Global Parameters (Paramètres globaux SNMP), cliquez sur System (Système) → SNMP → Global Parameters (Paramètres globaux) dans l'arborescence.

Figure 6-57. SNMP Global Parameters (Paramètres globaux SNMP)



La page SNMP Global Parameters (Paramètres globaux SNMP) contient les champs suivants :

Local Engine ID (ID du moteur local) : indique l'ID du moteur local de l'unité. La valeur de ce champ est une chaîne hexadécimale. Chaque octet correspond à deux chiffres hexadécimaux. Chaque octet peut être séparé par un point ou deux points. L'ID du moteur doit être défini avant l'activation de SNMPv3.

Pour les unités autonomes, sélectionnez un ID de moteur par défaut composé du numéro Enterprise et de l'adresse MAC par défaut.

Pour un système empilable, configurez l'ID du moteur et vérifiez qu'il est unique dans le domaine d'administration. Cela évite que deux unités d'un réseau possèdent le même ID de moteur.

Use Defaults (Utiliser les valeurs par défaut) : utilise l'ID de moteur généré pour l'unité. L'ID de moteur par défaut, basé sur l'adresse MAC de l'unité, est défini comme suit :

First 4 octets (4 premiers octets) : premier bit = 1, le reste étant le numéro IANA Enterprise = 674.

Fifth octet (Cinquième octet) : défini sur 3 pour indiquer l'adresse MAC qui suit.

Last 6 octets (6 derniers octets) : adresse MAC de l'unité.

SNMP Notifications (Notifications SNMP) : active ou désactive le routeur qui envoie des notifications SNMP.

Authentication Notifications (Notifications d'authentification) : active ou désactive le routeur qui envoie des interruptions SNMP lorsque l'authentification échoue.

Activation des notifications SNMP

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

Les notifications SNMP sont activées et l'unité est mise à jour.

Activation des notifications d'authentification

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

Activation des notifications SNMP à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher les champs de la page SNMP Global Parameters (Paramètres globaux SNMP).

Tableau 6-37. Commandes relatives aux notifications SNMP

Commande CLI	Description
snmp-server enable traps	Permet au routeur d'envoyer des interruptions SNMP.
snmp-server trap authentication	Permet au routeur d'envoyer des interruptions SNMP lorsque l'authentification échoue.
show snmp	Vérifie l'état des communications SNMP.
snmp-server engine ID local {*chaîne_id moteur* | **default**}	Indique l'ID du moteur local de l'unité. Les valeurs de ce champ représentent une chaîne hexadécimale. Chaque octet correspond à deux chiffres hexadécimaux. Chaque octet peut être séparé par un point ou deux points. L'ID du moteur doit être défini avant l'activation de SNMPv3.

Voici un exemple de commandes CLI :

```
Console(config)# snmp-server enable traps

Console(config)# snmp-server trap authentication

Console# show snmp
```

```
Community-String    Community-Access    View name    IP address
---------------     ----------------    ---------    ----------
public              read only           view-1       All

Community-String    Group name          IP address   Type
---------------     ----------          ----------   ----

Traps are enabled.

Authentication-failure trap is enabled.

Version 1,2 notifications

Target Address  Type  Community  Version  Udp Port  Filter name  To Sec  Retries
-------         ----  ---------  -------  ----      ------       ---     -------

Version 3 notifications

Target Address  Type  Username   Security Level  Udp Port  Filter name  To Sec  Retries
--------        ----  ---------  --------        ---- -    ------ -     ---     -------

System Contact: Robert

System Location: Marketing
```

Définition des paramètres des vues SNMP

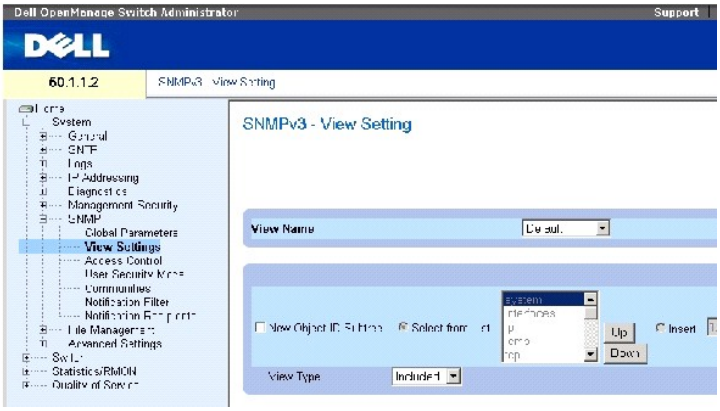
Les vues SNMP permettent ou bloquent l'accès aux fonctions de l'unité ou aux paramètres de ces fonctions. Par exemple, une vue peut être définie pour indiquer que le groupe SNMP A dispose d'un accès en lecture seule (R/O) aux groupes de multidiffusion, tandis que le groupe SNMP B dispose d'un accès en lecture-écriture (R/W). L'accès aux fonctions s'effectue à l'aide du nom MIB ou de l'ID objet MIB.

Les flèches Haut et Bas permettent de parcourir l'arborescence MIB et ses sous-sections.

Pour ouvrir la page SNMPv3 View Settings (Paramètres de la vue SNMPv3), cliquez sur **System** (Système) → **SNMP** → **View Settings** (Paramètres de la vue)

dans l'arborescence.

Figure 6-58. SNMPv3 View Settings (Paramètres de la vue SNMPv3)



La page SNMPv3 View Settings (Paramètres de la vue SNMPv3) contient les champs suivants :

View Name (Nom de la vue) : contient une liste de vues définies par l'utilisateur. Le nom de la vue peut contenir jusqu'à 30 caractères alphanumériques.

New Object ID Subtree (Nouvelle sous-arborescence ID d'objet) : indique l'OID de la fonction de l'unité incluse ou exclue de la vue SNMP sélectionnée.

Selected from List (Sélectionné dans la liste) : sélectionnez l'OID de la fonction de l'unité à l'aide des touches **Haut** et **Bas** pour parcourir la liste de tous les OID de l'unité.

Insert (Insérer) : spécifiez l'OID de la fonction de l'unité.

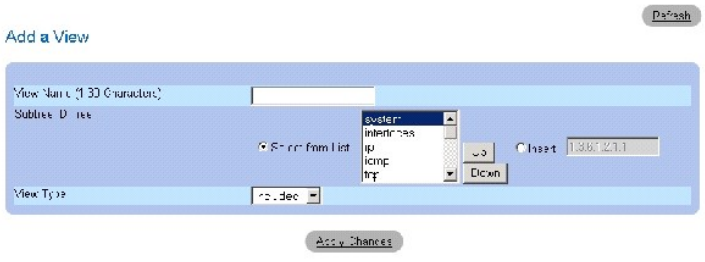
View Type (Type de vue) : indique si la partie de l'arborescence correspondant à l'OID défini sera incluse ou exclue de la vue SNMP sélectionnée.

Ajout d'une vue

1. Affichez la page SNMPv3 View Settings (Paramètres de la vue SNMPv3).
2. Cliquez sur Add (Ajouter).

La page Add A View (Ajout d'une vue) s'affiche.

Figure 6-59. Add A View (Ajout d'une vue)



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

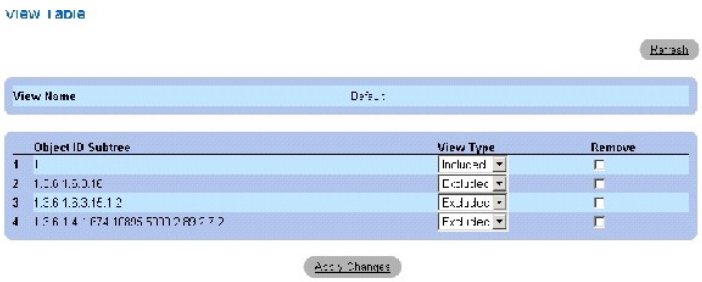
La vue SNMP est ajoutée et l'unité est mise à jour.

Affichage de la table des vues

1. Affichez la page SNMPv3 View Settings (Paramètres de la vue SNMPv3).
2. Cliquez sur Show All (Afficher tout).

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

Figure 6-60. View Table (Table des vues)



Définition de vues SNMPv3 à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page SNMPv3 View Settings (Paramètres de la vue SNMPv3).

Tableau 6-38. Commandes CLI relatives à la vue SNMP

Commande CLI	Description
snmp-server view *nom- vue arborescence-oid* {**included** | **excluded**}	Crée ou met à jour une entrée de la vue.
show snmp views [*nom de la vue]*	Affiche la configuration des vues.

Voici un exemple de commandes CLI :

```
Console(config)# snmp-server view user1
1 included

Console(config)# end

Console# show snmp views

Name        OID Tree            Type
----------- ------------------- --------
-
```

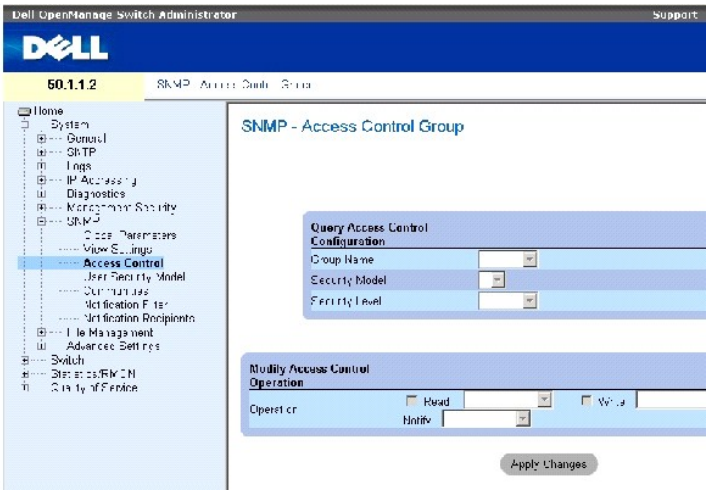
user1	iso	included
Default	iso	included
Default	snmpVacmMIB	excluded
Default	usmUser	excluded
Default	rndCommunityTable	excluded
DefaultSuper	iso	included

Définition du contrôle d'accès SNMP

La page Access Control (Contrôle d'accès) fournit des informations sur la création de groupes SNMP et l'affectation de droits de contrôle d'accès SNMP aux groupes SNMP. Les groupes permettent aux administrateurs réseau d'octroyer des droits d'accès à des fonctions spécifiques de l'unité ou des paramètres de fonctions.

Pour ouvrir la page Access Control Group (Groupe de contrôle d'accès), cliquez sur System (Système) → SNMP → Access Control (Contrôle d'accès) dans l'arborescence.

Figure 6-61. Access Control Group (Groupe de contrôle d'accès)



La page Access Control Group (Groupe de contrôle d'accès) contient les champs suivants :

Group Name (Nom du groupe) : groupe défini par l'utilisateur auquel s'appliquent les règles de contrôle d'accès. Ce nom peut contenir jusqu'à 30 caractères.

SNMP Version (Version SNMP) : définit la version SNMP associée au groupe. Ce champ peut prendre les valeurs suivantes :

SNMPv1 : SNMPv1 est définie pour le groupe.

SNMPv2 : SNMPv2 est définie pour le groupe.

SNMPv3 : SNMPv3 est définie pour le groupe.

Security Level (Niveau de sécurité) : niveau de sécurité associé au groupe. Les niveaux de sécurité s'appliquent uniquement à SNMPv3. Ce champ peut prendre les valeurs suivantes :

No Authentication (Aucune authentification) : les niveaux de sécurité Authentication (Authentification) ou Privacy (Confidentialité) ne sont pas associés au groupe.

Authentication (Authentification) : authentifie les messages SNMP et vérifie que leur origine est authentifiée.

Privacy (Confidentialité) : crypte le message SNMP.

Operation (Fonctionnement) : définit les droits d'accès des utilisateurs. Ce champ peut prendre les valeurs suivantes :

Read (Lecture) : l'accès à la station de gestion s'effectue en lecture seule et aucune modification ne peut être apportée à la vue SNMP associée.

Write (Écriture) : l'accès à la station de gestion s'effectue en lecture-écriture et des modifications peuvent être apportées à la vue SNMP associée.

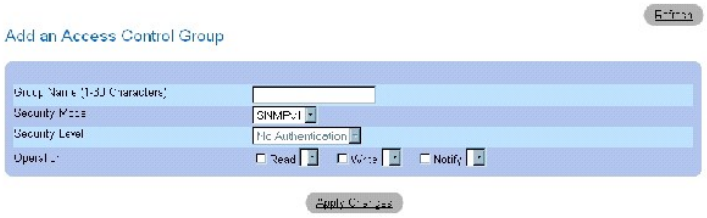
Notify (Notifier) : envoie des interruptions pour la vue SNMP associée.

Définition des groupes SNMP

1. Affichez la page Access Control Group (Groupe de contrôle d'accès).
2. Cliquez sur Add (Ajouter).

La page **Add an Access Control Group** (Ajouter un groupe de contrôle d'accès) s'affiche.

Figure 6-62. Add an Access Control Group (Ajout d'un groupe de contrôle d'accès)



3. Remplissez les champs de la page Add an Access Control Group (Ajout d'un groupe de contrôle d'accès).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le groupe est ajouté et l'unité est mise à jour.

Affichage de la table d'accès

1. Affichez la page Access Control Group (Groupe de contrôle d'accès).
2. Cliquez sur Show All (Afficher tout).

La page Access Table (Table d'accès) s'affiche.

Figure 6-63. Access Table (Table d'accès)

Suppression de groupes SNMP

1. Affichez la page Access Control Group (Groupe de contrôle d'accès).
2. Cliquez sur Show All (Afficher tout).

   La page Access Table (Table d'accès) s'affiche.
3. Sélectionnez un groupe SNMP.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

   Le groupe SNMP est supprimé et l'unité est mise à jour.

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

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page Access Control Group (Groupe de contrôle d'accès).

Tableau 6-39. Commandes CLI du contrôle d'accès SNMP

Commande CLI	Description
snmp-server group *nom du groupe* {**v1 | v2 | v3** {**noauth | auth | priv**}} [**read** *vue lecture*] [**write** *vue écriture*] [**notify** *vue notifier*]	Configure un nouveau groupe Simple Network Management Protocol (SNMP) ou une table qui associe des utilisateurs SNMP à des vues SNMP.
show snmp groups [*nom du groupe*]	Affiche la configuration des groupes.

Voici un exemple de commandes CLI :

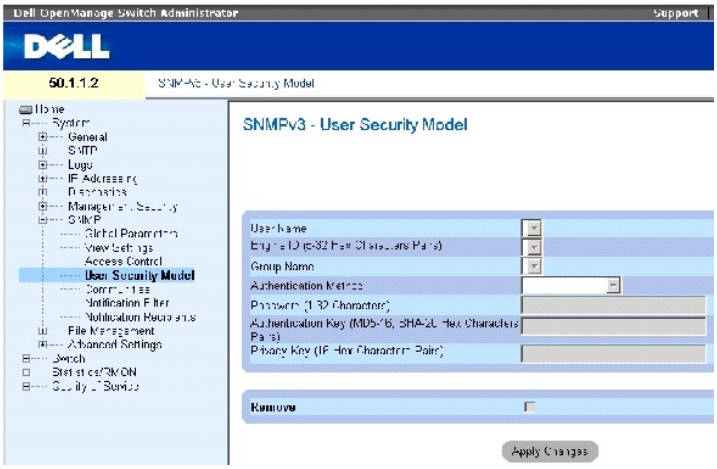
```
console (config)# snmp-
server group user-group v3
priv read user- view
```

Affectation d'un modèle de sécurité aux utilisateurs SNMP

La page SNMPv3 User Security Model (Modèle de sécurité utilisateur SNMPv3) permet d'associer des utilisateurs système à des groupes SNMP et de définir la méthode d'authentification des utilisateurs.

Pour ouvrir la page SNMPv3 User Security Model (Modèle de sécurité utilisateur SNMPv3), cliquez sur **System** (Système) → **SNMP** → **User Security Model** (Modèle de sécurité utilisateur) dans l'arborescence.

Figure 6-64. SNMPv3 User Security Model (Modèle de sécurité utilisateur SNMPv3)



La page SNMPv3 User Security Model (Modèle de sécurité utilisateur SNMPv3) contient les champs suivants :

User Name (Nom de l'utilisateur) : contient une liste de noms définis par l'utilisateur. Ce nom peut contenir jusqu'à 30 caractères alphanumériques.

Engine ID (ID du moteur) : indique l'entité SNMP locale ou distante à laquelle l'utilisateur est connecté. La modification ou la suppression de l'ID du moteur SNMP local supprime la base de données d'utilisateurs SNMPv3.

Local (Locale) : indique que l'utilisateur est connecté à une entité SNMP locale.

Remote (Distante) : indique que l'utilisateur est connecté à une entité SNMP distante. Si l'ID du moteur est défini, les unités distantes reçoivent des messages d'informations.

Group Name (Nom du groupe) : contient une liste de groupes SNMP définis par l'utilisateur. Les groupes SNMP sont définis à la page Access Control Group (Groupe de contrôle d'accès).

Authentication Method (Méthode d'authentification) : méthode utilisée pour authentifier les utilisateurs. Ce champ peut prendre les valeurs suivantes :

MD5 Key (Clé MD5) : les utilisateurs sont authentifiés à l'aide de l'algorithme HMAC-MD5.

SHA Key (Clé SHA) : les utilisateurs sont authentifiés à l'aide du niveau d'authentification HMAC-SHA-96.

MD5 Password (Mot de passe MD5) : indique que le mot de passe HMAC-MD5-96 est utilisé pour l'authentification. L'utilisateur doit saisir un mot de passe.

SHA Password (Mot de passe SHA) : les utilisateurs sont authentifiés à l'aide du niveau d'authentification HMAC-SHA-96. L'utilisateur doit saisir un mot de passe.

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

Password (0-32 Characters) (Mot de passe [0 à 32 caractères]) : modifie le mot de passe défini par l'utilisateur pour un groupe. Les mots de passe peuvent contenir jusqu'à 32 caractères alphanumériques.

Authentication Key (MD5-16; SHA-20 hexa chars) (Clé d'authentification [MD5 : 16 caractères hexadécimaux ; SHA : 20 caractères hexadécimaux]) : définit le niveau d'authentification HMAC-MD5-96 ou HMAC-SHA-96. Les clés d'authentification et de confidentialité permettent de définir la clé d'authentification. Si seule l'authentification est nécessaire, 16 octets sont définis pour MD5. Si la confidentialité et l'authentification sont toutes deux requises, 32 octets sont définis pour MD5. Chaque octet correspond à deux chiffres hexadécimaux. Chaque octet peut être séparé par un point ou deux points.

Privacy Key (16 hexa characters) (Clé de confidentialité [16 caractères hexadécimaux]) : si seule l'authentification est nécessaire, 20 octets sont définis. Si la confidentialité et l'authentification sont toutes deux requises, 16 octets sont définis. Chaque octet correspond à deux chiffres hexadécimaux. Chaque octet peut être séparé par un point ou deux points.

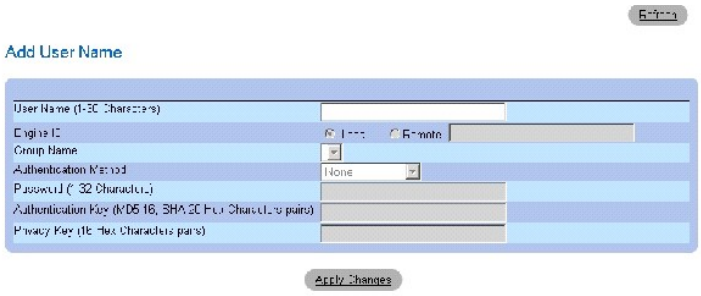
Remove (Supprimer) : permet de supprimer des utilisateurs du groupe spécifié.

Ajout d'utilisateurs à un groupe

1. Affichez la page SNMPv3 User Security Model (Modèle de sécurité utilisateur SNMPv3).
2. Cliquez sur Add (Ajouter).

La page Add SNMPv3 User Name (Ajout d'un nom d'utilisateur SNMPv3) s'affiche.

Figure 6-65. Add SNMPv3 User Name (Ajout d'un nom d'utilisateur SNMPv3)



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

L'utilisateur est ajouté au groupe et l'unité est mise à jour.

Affichage de la table User Security Model (USM)

1. Affichez la page SNMPv3 User Security Model (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 6-66. User Security Model Table (Table du modèle de sécurité utilisateur)

Suppression d'une entrée de la table USM

1. Affichez la page SNMPv3 User Security Model (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.
3. Sélectionnez une entrée de la page User Security Model Table (Table du modèle de sécurité utilisateur).
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

   L'entrée est supprimée de la page User Security Model Table (Table du modèle de sécurité utilisateur) et l'unité est mise à jour.

Définition d'utilisateurs SNMPv3 à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page SNMPv3 User Security Model (Modèle de sécurité utilisateur SNMPv3).

Tableau 6-40. Commandes CLI des utilisateurs SNMPv3

Commande CLI	Description
snmp-server user *nom d'utilisateur nom du groupe* [**remote** id moteur- chaîne][**auth-md5** mot de passe | **auth-sha mot de passe** | **auth-md5-key** *clé- des-md5* | **clé-SHA-auth** *clé- DES-sha*]	Configure un nouvel utilisateur SNMP V3.
show snmp users [*nom d'utilisateur*]	Affiche la configuration des utilisateurs.

Voici un exemple de commandes CLI :

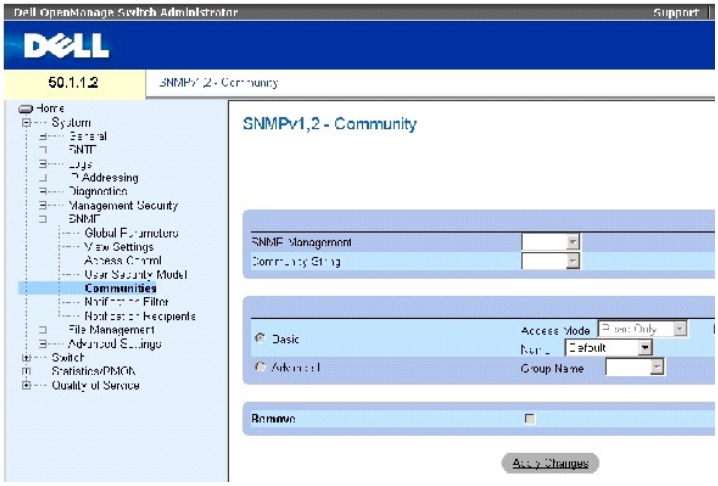
```
console (config)# snmp-server user John user-group auth-md5 1234

console (config)# end

console# show snmp users

                                                    

Name    Group Name  Auth Method  Remote
------  ----------  -----------  ------
```

John	user-group	md5	

Définition de communautés SNMP

Les droits d'accès sont gérés en définissant des communautés à l'aide de la page SNMPv1,2 Community (Communauté SNMPv1 et 2). Lorsqu'un nom de communauté est modifié, les droits d'accès qui lui sont associés le sont également. Les communautés SNMP sont définies uniquement pour SNMP v1 et v2. Pour ouvrir la page SNMPv1,2 Community (Communauté SNMPv1 et 2), cliquez sur **System** (Système) → **SNMP** → **Communities** (Communautés) dans l'arborescence.

Figure 6-67. SNMPv1,2 Community (Communauté SNMPv1 et 2)



La page SNMPv1,2 Community (Communauté SNMPv1 et 2)contient les champs suivants :

SNMP Management Station (Station de gestion SNMP) : adresse IP de la station pour laquelle la communauté SNMP est définie.

Community String (Chaîne de communauté) : remplit la même fonction qu'un mot de passe et permet d'authentifier la station de gestion sur l'unité.

Basic (De base) : active le mode SNMP de base pour une communauté sélectionnée. Ce champ peut prendre les valeurs suivantes :

Access Mode (Mode d'accès) : définit les droits d'accès de la communauté. Ce champ peut prendre les valeurs suivantes :

Read Only (Lecture seule) : l'accès à la station de gestion s'effectue en lecture seule et aucune modification ne peut être apportée à la communauté.

Read Write (Lecture/écriture) : l'accès à la station de gestion s'effectue en lecture/écriture et des modifications peuvent être apportées à la configuration de l'unité, mais pas à la communauté.

SNMP-Admin (Administrateur SNMP) : l'utilisateur a accès à toutes les options de configuration de l'unité, et il peut également modifier la communauté.

View Name (Nom de la vue) : contient une liste de vues SNMP définies par l'utilisateur.

Name (Nom) : spécifie le nom de la communauté utilisé pour SNMPv1 et v2.

Advanced (Avancé) : contient une liste de groupes définis par l'utilisateur. Lorsque le mode SNMP avancé est sélectionné, les règles de contrôle d'accès SNMP du groupe sont appliquées à la communauté sélectionnée. Le mode avancé active également des groupes SNMP pour des communautés SNMP spécifiques. Le mode SNMP avancé est défini uniquement avec SNMPv3. Ce champ peut prendre les valeurs suivantes :

Group Name (Nom du groupe) : spécifie le nom du groupe en mode SNMP avancé.

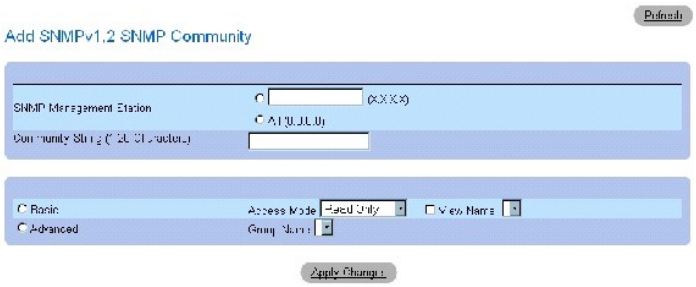
Remove (Supprimer) : supprime une communauté.

Définition d'une nouvelle communauté

1. Affichez la page SNMPv1,2 Community (Communauté SNMPv1 et 2).
2. Cliquez sur **Add** (Ajouter).

La page **Add SNMP Community** (Ajout d'une communauté SNMP) s'affiche.

Figure 6-68. Add SNMP Community (Ajout d'une communauté SNMP)



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

La nouvelle communauté est enregistrée et l'unité est mise à jour.

Suppression de communautés

1. Affichez la page SNMPv1,2 Community (Communauté SNMPv1 et 2).
2. Cliquez sur **Show All** (Afficher tout).

La page **Community Table** (Table des communautés) s'affiche.

3. Sélectionnez une communauté et cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La communauté est supprimée et l'unité est mise à jour.

Configuration de communautés à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher les champs de la page SNMPv1,2 Community (Communauté SNMPv1 et 2).

Tableau 6-41. Commandes CLI relatives aux communautés SNMP

Commande CLI	Description
snmp-server community *communauté* [**ro** | **rw** | **su**] [*adresse-ip*][**view** *nom-vue*]	Configure la chaîne d'accès à la communauté afin d'autoriser les accès au protocole SNMP.
snmp-server community-group *communauté nom-groupe* [*adresse-ip*]	Configure la chaîne d'accès à la communauté afin d'autoriser un accès limité au protocole SNMP en fonction des droits d'accès du groupe.
show snmp	Affiche la configuration SNMP actuelle de l'unité.

Voici un exemple de commandes CLI :

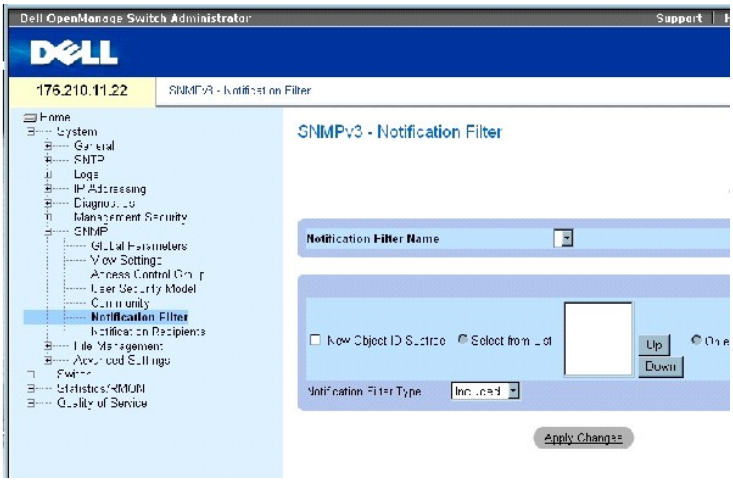
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

Définition des filtres de notification SNMP

La page Notification Filter (Filtre de notification) permet de filtrer les interruptions en fonction des OID. Chaque OID est associé à une fonction de l'unité ou un paramètre de cette fonction. La page Notification Filter (Filtre de notification) permet également aux administrateurs réseau de filtrer les notifications.

Pour ouvrir la page Notification Filter (Filtre de notification), cliquez sur **System** (Système) → **SNMP** → **Notification Filters** (Filtres de notification) *dans l'arborescence*.

Figure 6-69. Notification Filter (Filtre de notification)



La page Notification Filter (Filtre de notification) contient les champs suivants :

Notification Filter Name (Nom du filtre de notification) : filtre de notification défini par l'utilisateur.

New Object Identifier Tree (Nouvelle arborescence de l'identificateur objet) : l'OID pour lequel des notifications sont envoyées ou bloquées. Si un filtre est associé à un OID, les interruptions ou les informations sont générées et envoyées à leurs destinataires. Les OID sont sélectionnés à partir de la liste de sélection ou de la liste des OID.

Notification Filter Type (Type de filtre de notification) : indique si des informations ou des interruptions concernant l'OID sont envoyées aux destinataires des

interruptions.

Excluded (Exclues) : limite l'envoi d'interruptions ou d'informations sur l'OID.

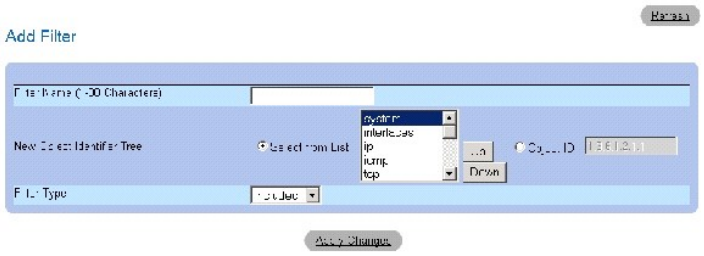
Included (Incluses) : envoie des interruptions ou des informations sur l'OID.

Ajout de filtres SNMP

1. Affichez la page Notification Filter (Filtre de notification).
2. Cliquez sur Add (Ajouter).

La page Add Filter (Ajout d'un filtre) s'affiche.

Figure 6-70. Add Filter (Ajout d'un filtre)



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

Le nouveau filtre est ajouté et l'unité est mise 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) s'affiche.

Figure 6-71. Filter Table (Table des filtres)

Suppression d'un filtre

1. Affichez la page Notification Filter (Filtre de notification).
2. Cliquez sur Show All (Afficher tout).

La page Filter Table (Table des filtres) s'affiche.

3. Sélectionnez une entrée de la Filter Table (Table des filtres).
4. Cochez la case **Remove** (Supprimer).

Le filtre est supprimé et l'unité est mise à jour.

Configuration des filtres de notification à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page Notification Filter (Filtre de notification).

Tableau 6-42. Commandes CLI des filtres de notification SNMP

Commande CLI	Description
snmp-server filter nom-filtre arborescence {**included** | **excluded**}	Crée ou met à jour un filtre de notification SNMP.
show snmp filters [nom du filtre]	Affiche la configuration des filtres de notification SNMP

Voici un exemple de commandes CLI :

```
Console (config)# snmp-server filter user1 iso included

Console(config)# end

Console # show snmp filters

Name          OID Tree      Type
----------    ------------  --------
user1         iso           Included
```

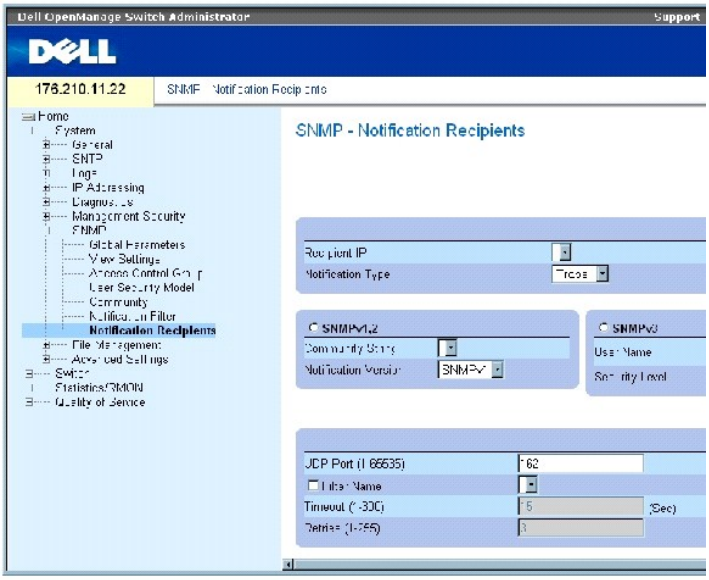
Définition des destinataires de la notification SNMP

La page Notification Recipients (Destinataires de la notification) contient des informations permettant de définir des filtres qui déterminent si des interruptions sont envoyées à des utilisateurs spécifiques et quel type d'interruption est envoyé. Les filtres de notification SNMP fournissent les services suivants :

- Identification des cibles des interruptions de gestion
- Filtrage des interruptions
- Sélection des paramètres de création des interruptions
- Vérification du contrôle d'accès

Pour ouvrir la page Notification Recipients (Destinataires de la notification), cliquez sur **System** (Système) → **SNMP** → **Notification Recipient** (Destinataire de la notification) dans l'arborescence.

Figure 6-72. Notification Recipients (Destinataires de la notification)



La page Notification Recipients (Destinataires de la notification) contient les champs suivants :

Recipient IP (IP destinataire) : indique l'adresse IP à laquelle les interruptions sont envoyées.

Notification Type (Type de notification) : notification envoyée. Ce champ peut prendre les valeurs suivantes :

Trap (Interruption) : des interruptions sont envoyées.

Inform (Information) : des informations sont envoyées.

SNMPv1,2 (SNMPv1 et 2) : les versions de protocole SNMP 1 et 2 sont activées pour le destinataire sélectionné. Complétez les champs suivants pour les protocoles SNMPv1 et SNMPv2 :

Community String (1-20 Characters) (Chaîne de communauté [1 à 20 caractères]) : identifie la chaîne de communauté du gestionnaire d'interruption.

Notification Version (Version de la notification) : détermine le type d'interruption. Ce champ peut prendre les valeurs suivantes :

SNMP V1 : des interruptions de type SNMP Version 1 sont envoyées.

SNMP V2 : des interruptions de type SNMP Version 2 sont envoyées.

SNMPv3 : SNMPv3 est utilisé pour envoyer et recevoir des interruptions. Complétez les champs suivants pour le protocole SNMPv3 :

User Name (Nom d'utilisateur) : utilisateur auquel les notifications SNMP sont envoyées.

Security Level (Niveau de sécurité) : définit la méthode d'authentification du paquet. Ce champ peut prendre les valeurs suivantes :

No Authentication (Aucune authentification) : le paquet n'est ni authentifié ni codé.

Authentication (Authentification) : le paquet est authentifié.

Privacy (Confidentialité) : le paquet est authentifié et codé.

UDP Port (1-65535) (Port UDP [1 à 65535]) : port UDP utilisé pour l'envoi des notifications. 162 est la valeur par défaut.

Filter Name (Nom du filtre) : inclut ou exclut des filtres SNMP.

Timeout (1-300) (Délai [1 à 300]) : durée (en secondes) pendant laquelle l'unité attend avant de renvoyer des informations. La valeur par défaut est de 15 secondes.

Retries (1-255) (Tentatives [1 à 255]) : nombre de fois où l'unité renvoie une demande d'informations. La valeur par défaut est de 3.

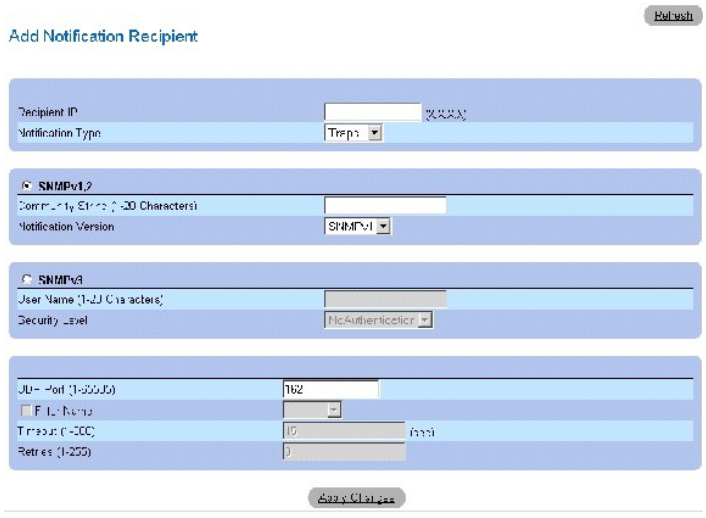
Remove Notification Recipient (Supprimer le destinataire de la notification) : supprime les destinataires de la notification sélectionnés.

Ajout d'un nouveau destinataire d'interruption

1. Affichez la page Notification Recipients (Destinataires de la notification).
2. Cliquez sur Add (Ajouter).

La page Add Notification Recipients (Ajout de destinataires de la notification) s'affiche.

Figure 6-73. Add Notification Recipients (Ajout de destinataires de la notification)



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

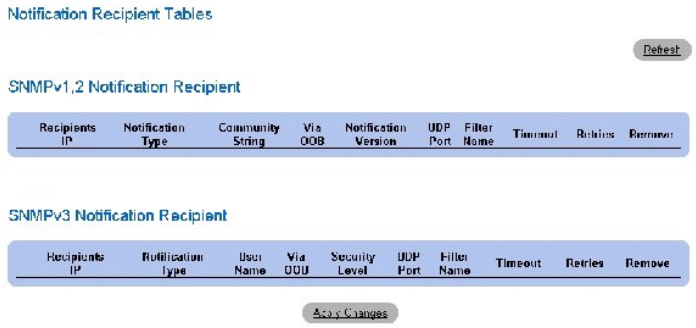
Le destinataire de la notification est ajouté et l'unité est mise à jour.

Affichage des tables des destinataires de la notification

1. Affichez la page Notification Recipients (Destinataires de la notification).
2. Cliquez sur Show All (Afficher tout).

La page Notification Recipients Tables (Tables des destinataires de la notification) s'affiche.

Figure 6-74. Notification Recipients Tables (Tables des destinataires de la notification)



Suppression de destinataires de la notification

1. Affichez la page Notification Recipients (Destinataires de la notification).
2. Cliquez sur Show All (Afficher tout).

La page Notification Recipients Tables (Tables des destinataires de la notification) s'affiche.

3. Sélectionnez un destinataire de la notification dans la table **Destinataire de la notification SNMPV1,2** ou **Destinataire de la notification SNMPv3**.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le destinataire est supprimé et l'unité est mise à jour.

Configuration des destinataires de la notification SNMP à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher les champs de la page Notification Recipients (Destinataires de la notification).

Tableau 6-43. Commandes CLI de la communauté SNMP

Commande CLI	Description
snmp-server host {adresse ip | nom d'hôte} *chaîne-communauté* [**traps** | **informs**] [**1** | **2**] [**udp-port** port] [**filter** nom du filtre] [**timeout** secondes] [**retries** tentatives]	Crée ou met à jour un destinataire qui reçoit des notifications dans SNMP version 1 ou 2.
snmp-server v3-host {adresse_ip | nom d'hôte} *nom d'utilisateur* [**traps** | **informs**] {**noauth** | **auth** | **priv**} [**udp-port** *port*] [**filter** nom du filtre] [**timeout** secondes] [**tentatives** retries]	Crée ou met à jour un destinataire qui reçoit des notifications dans SNMP version 3.
show snmp	Affiche la configuration SNMP en cours.

Voici un exemple de commandes CLI :

```
console(config)# snmp-server host 172.16.1.1
private

console(config)# end

console# show snmp
```

Community-String	Community-Access	View name	IP address
public	read only	user-view	All
private	read write	default	172.16.1.1
private	su	DefaultSuper	172.17.1.1

Gestion des fichiers

Utilisez la page **File Management** (Gestion des fichiers) pour gérer les logiciels de l'unité, le fichier image et les fichiers de configuration. Les fichiers peuvent être téléchargés ou chargés via un serveur TFTP.

Présentation des fichiers de gestion

La structure des fichiers de gestion s'établit comme suit :

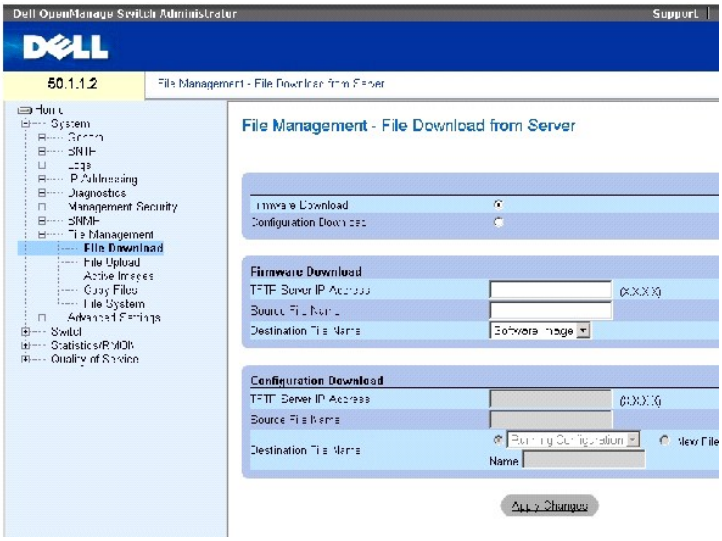
- Fichier de configuration de démarrage : contient les commandes nécessaires à la configuration de l'unité au démarrage ou après redémarrage. Ce fichier est créé en copiant les commandes de configuration du fichier de configuration en cours d'exécution ou du fichier de configuration de sauvegarde.
- Fichier de configuration en cours d'exécution : contient toutes les commandes du fichier de configuration de démarrage, ainsi que les commandes entrées pendant la session en cours. À la mise sous tension ou au redémarrage de l'unité, toutes les commandes enregistrées dans le fichier de configuration en cours d'exécution sont perdues. Pendant le processus de démarrage, toutes les commandes du fichier de configuration de démarrage sont copiées dans le fichier de configuration en cours d'exécution et appliquées à l'unité. Durant la session, toutes les nouvelles commandes sont ajoutées aux commandes existantes dans le fichier de configuration en cours d'exécution. Pour mettre le fichier de configuration de démarrage à jour, le fichier de configuration en cours d'exécution doit être copié dans le fichier de configuration de démarrage avant la mise sous tension de l'unité.
- Fichier de configuration de sauvegarde : contient une copie de sauvegarde de la configuration de l'unité. Vous pouvez enregistrer jusqu'à cinq fichiers de configuration de sauvegarde sur l'unité à l'aide de noms définis par l'utilisateur. Ces fichiers sont créés lorsque l'utilisateur copie le fichier de configuration en cours d'exécution ou le fichier de configuration de démarrage dans un fichier défini par l'utilisateur. Le contenu du fichier de configuration de sauvegarde peut être copié dans le fichier de configuration en cours d'exécution ou dans le fichier de configuration de démarrage.
- Fichiers image : des images du fichier système sont enregistrées dans deux fichiers Flash appelés Image 1 et Image 2. L'image active stocke la copie active et l'autre image une deuxième copie. L'unité démarre et s'exécute à partir de l'image active. Si l'image active est endommagée, le système démarre automatiquement à partir de l'image non active. Ce mécanisme de sécurité permet de remédier aux défaillances susceptibles de se produire lors du processus de mise à niveau des logiciels.

Pour ouvrir la page File Management (Gestion des fichiers), cliquez sur System (Système) → File Management (Gestion des fichiers) dans l'arborescence.

Téléchargement de fichiers

La page File Download from Server (Téléchargement de fichiers à partir du serveur) contient des champs permettant de télécharger des fichiers image système et des fichiers de configuration de l'unité à partir du serveur TFTP. Pour ouvrir la page File Download from Server (Téléchargement de fichiers à partir du serveur), cliquez sur System (Système) → File Management (Gestion des fichiers) → File Download (Téléchargement de fichiers) dans l'arborescence.

Figure 6-75. File Download from Server (Téléchargement de fichiers à partir du serveur)



La page File Download from Server (Téléchargement de fichiers à partir du serveur) contient les champs suivants :

Firmware Download (Téléchargement de micro-code) : le fichier de micro-code est téléchargé. Lorsque l'option **Firmware Download** (Téléchargement de micro-code) est sélectionnée, les champs **Configuration Download** (Téléchargement de configuration) sont grisés.

Configuration Download (Téléchargement de configuration) : le fichier de configuration est téléchargé. Lorsque l'option **Configuration Download** (Téléchargement de configuration) est sélectionnée, les champs **Firmware Download** (Téléchargement de micro-code) sont grisés.

Téléchargement de micro-code

TFTP Server IP Address (Adresse IP du serveur TFTP) : adresse IP du serveur TFTP à partir duquel les fichiers de micro-code sont téléchargés.

Source File Name (Nom du fichier source) : indique le fichier à télécharger.

Destination File Name (Nom du fichier de destination) : type du fichier de destination vers lequel le fichier est téléchargé. Ce champ peut prendre les valeurs suivantes :

Software Image (Image du logiciel) : télécharge le fichier image.

Boot Code (Code d'amorçage) : télécharge le fichier d'amorçage.

Téléchargement de configuration

TFTP Server IP Address (Adresse IP du serveur TFTP) : adresse IP du serveur TFTP à partir duquel les fichiers de configuration sont téléchargés.

Source File Name (Nom du fichier source) : indique les fichiers de configuration à télécharger.

Destination File Name (Nom du fichier de destination) : fichier de destination vers lequel le fichier de configuration est téléchargé. Ce champ peut prendre les valeurs suivantes :

Running Configuration (Configuration en cours d'exécution) : télécharge les commandes dans le fichier de configuration en cours d'exécution.

Startup Configuration (Configuration de démarrage) : télécharge le fichier de configuration de démarrage en écrasant le fichier existant.

Backup Configuration (Configuration de sauvegarde) : télécharge le fichier de configuration de sauvegarde défini par l'utilisateur en écrasant le fichier existant.

New File Name (Nouveau nom de fichier) : télécharge un nouveau fichier de configuration de sauvegarde pouvant servir de fichier de destination.

REMARQUE : le fichier image remplace l'image non active. Il est recommandé de préciser que l'image non active deviendra active après la réinitialisation, puis de réinitialiser l'unité suite au téléchargement.

Une boîte de dialogue affiche la progression du téléchargement du fichier image. Cette fenêtre se ferme automatiquement à la fin du téléchargement.

Téléchargement de fichiers

1. Affichez la page File Download from Server (Téléchargement de fichiers à partir du serveur).
2. Définissez le type du fichier à télécharger.
3. Complétez les champs avec les valeurs appropriées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le logiciel est téléchargé sur l'unité.

REMARQUE : pour activer le fichier image sélectionné, réinitialisez l'unité. Pour plus d'informations sur la réinitialisation de l'unité, consultez la section "Basculement entre unités maîtres".

Téléchargement de fichiers à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page File Download from Server (Téléchargement de fichiers à partir du serveur).

Tableau 6-44. Commandes CLI de téléchargement des fichiers

Commande CLI	Description
copy url_source url_destination	Copie un fichier d'une source vers une destination.

Voici un exemple de commandes CLI :

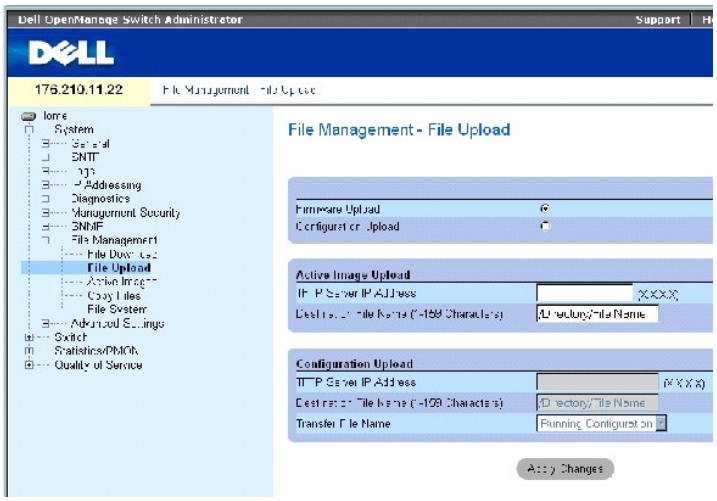
```
console# copy
tftp://10.6.6.64/pp.txt
startup-config



....!



Copy: 575 bytes copied in
00:00:06 [hh:mm:ss]



01-Jan-2000 06:41:55 %
COPY-W-TRAP: The copy
operation was completed
successfully
```

REMARQUE : chaque point d'exclamation (!) indique que dix paquets ont été correctement transférés.

Chargement de fichiers

La page File Upload to Server (Chargement de fichiers sur le serveur) contient des champs permettant de charger les logiciels sur le serveur TFTP à partir de l'unité. Le fichier image peut également être chargé à partir de la page File Upload to Server (Chargement de fichiers sur le serveur). Pour ouvrir la page File Upload to Server (Chargement de fichiers sur le serveur), cliquez sur System (Système) → File Management (Gestion des fichiers) → File Upload (Chargement de fichiers) dans l'arborescence.

Figure 6-76. File Upload to Server (Chargement de fichiers sur le serveur)



La page File Upload to Server (Chargement de fichiers sur le serveur) contient les champs suivants :

Firmware Upload (Chargement de micro-code) : le fichier de micro-code est chargé sur le serveur. Lorsque l'option **Firmware Upload** (Chargement de micro-code) est sélectionnée, les champs **Configuration Upload** (Chargement de configuration) sont grisés.

Configuration Upload (Chargement de configuration) : le fichier de configuration est chargé. Lorsque l'option **Configuration Upload** (Chargement de configuration) est sélectionnée, les champs **Active Image Upload** (Chargement de l'image active) sont grisés.

Chargement de l'image active

TFTP Server IP Address (Adresse IP du serveur TFTP) : adresse IP du serveur TFTP vers lequel l'image du logiciel est chargée.

Destination File Name (1-159 Characters) (Nom du fichier de destination [1 à 159 caractères]) : indique le chemin du fichier image vers lequel le fichier est chargé.

Chargement de configuration

TFTP Server IP Address (Adresse IP du serveur TFTP) : adresse IP du serveur TFTP vers lequel le fichier de configuration est chargé.

Destination File Name (1-159 Characters) (Nom du fichier de destination [1 à 159 caractères]) : indique le chemin du fichier de configuration vers lequel le fichier est chargé.

Transfer File Name (Nom du fichier de transfert) : fichier vers lequel la configuration est chargée. Ce champ peut prendre les valeurs suivantes :

Running Configuration (Configuration en cours d'exécution) : charge le fichier de configuration en cours d'exécution.

Startup Configuration (Configuration de démarrage): charge le fichier de configuration de démarrage.

List of User Defined Configuration Files (Liste des fichiers de configuration définis par l'utilisateur) : charge un fichier de configuration défini par l'utilisateur.

REMARQUE : cette liste de fichiers de configuration définis par l'utilisateur apparaît uniquement si ce dernier a créé des fichiers de configuration de sauvegarde. Par exemple, si l'utilisateur a copié le fichier de configuration en cours d'exécution dans un fichier nommé BACKUP-SITE-1, cette liste s'affiche à la page File Upload to Server (Chargement de fichiers sur le serveur) et le fichier de configuration BACKUP- SITE-1 figure dans la liste.

Chargement de fichiers

1. Affichez la page File Upload to Server (Chargement de fichiers sur le serveur).
2. Définissez le type de fichier à charger.
3. Complétez les champs avec les valeurs appropriées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le logiciel est chargé sur le serveur TFTP.

Chargement de fichiers à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page File Upload to Server (Chargement de fichiers sur le serveur).

Tableau 6-45. Commandes CLI de chargement des fichiers

Commande CLI	Description
copy url_source url_destination	Copie un fichier d'une source vers une destination.

Voici un exemple de commandes CLI :

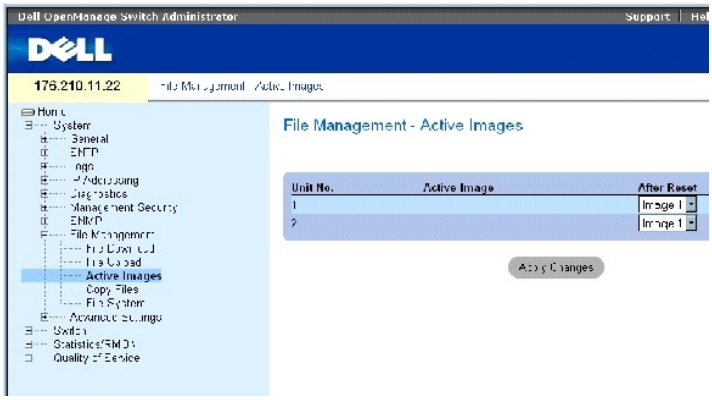
```
console# copy image tftp://10.6.6.64/uploaded.ros

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy: 4234656 bytes copied in 00:00:33 [hh:mm:ss]
```

```
01-Jan-2000 07:30:42 %COPY-W-TRAP: The copy operation was
completed successfully
```

Activation des fichiers image

La page Active Images (Images actives) permet aux administrateurs réseau de sélectionner et réinitialiser des fichiers image. Il est possible de sélectionner individuellement le fichier image actif de chaque unité d'une configuration d'empilage. Pour ouvrir la page Active Images (Images actives), cliquez sur System (Système) → File Management (Gestion des fichiers) → Active Images (Images actives) dans l'arborescence.

Figure 6-77. Active Images (Images actives)



La page Active Images (Images actives) contient les champs suivants :

Unit No. (Numéro d'unité) : numéro de l'unité pour laquelle le fichier image est sélectionné.

Active Image (Image active) : fichier image actif sur l'unité.

After Reset (Après réinitialisation) : fichier image actif après réinitialisation de l'unité. Ce champ peut prendre les valeurs suivantes :

Image 1 : active le fichier image 1 après réinitialisation de l'unité.

Image 2 : active le fichier image 2 après réinitialisation de l'unité.

Sélection d'un fichier image

1. Affichez la page Active Images (Images actives).
2. Sélectionnez le fichier image à associer à une unité spécifique dans le champ **After Reset** (Après réinitialisation).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le fichier image est sélectionné. Il n'est rechargé qu'à la réinitialisation suivante. Le fichier image en cours continue d'être exécuté jusqu'à la réinitialisation suivante de l'unité.

Utilisation du fichier d'image active à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant d'afficher les champs de la page Active Images (Images actives).

Tableau 6-46. Commandes CLI de chargement des fichiers

Commande CLI	Description
boot system [**unit** | *unité*] {**image-1** | **image-2**}	Indique l'image système que l'unité charge au démarrage.
show version [**unit** *unité*]	Affiche les informations de version du système.

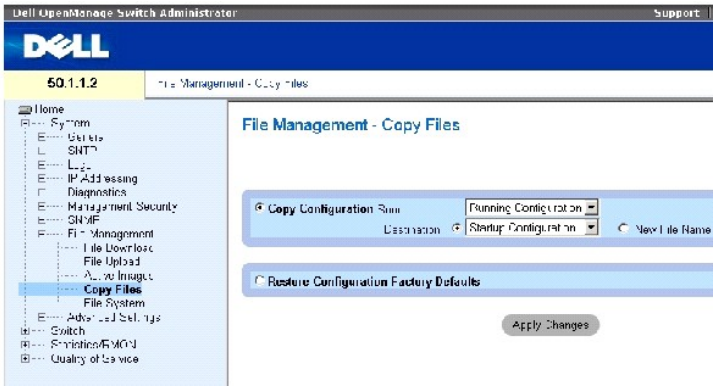
Voici un exemple de commandes CLI :

```
Console# boot system
image-1
```

Copie de fichiers

Vous pouvez copier et supprimer des fichiers à partir de la page Copy Files (Copier des fichiers). Pour ouvrir la page Copy Files (Copier des fichiers), cliquez sur System (Système) → File Management (Gestion des fichiers) → Copy Files (Copier des fichiers) dans l'arborescence.

Figure 6-78. Copy Files (Copier des fichiers)



La page Copy Files (Copier des fichiers) contient les champs suivants :

Copy Configuration (Copier la configuration) : permet de copier le fichier de configuration en cours d'exécution, de démarrage ou de sauvegarde du fichier maître dans le fichier de destination.

Source : indique le type de fichier à copier dans le fichier de destination. Sélectionnez le fichier de configuration en cours d'exécution, de démarrage ou de sauvegarde ou un des fichiers de configuration de sauvegarde définis par l'utilisateur.

Destination : indique le fichier de configuration de destination dans lequel le fichier source est copié. Les fichiers ne peuvent pas être copiés dans le fichier de sauvegarde de l'unité maître de secours. Les fichiers de sauvegarde apparaissent dans le champ **Destination Unit** (Unité de destination) uniquement s'ils ont été définis. Cochez la case New File Name (Nom du nouveau fichier) et indiquez le nom du nouveau fichier afin de copier le fichier source dans un nouveau fichier de configuration de sauvegarde.

New File Name (Nom du nouveau fichier) : indique le nom du nouveau fichier de configuration de sauvegarde.

Restore Configuration Factory Defaults (Restaurer la configuration d'origine) : indique que la configuration actuelle doit être remplacée par la configuration d'origine définie en usine. Si cette option est désactivée, la configuration actuelle est conservée.

Copie de fichiers

1. Affichez la page Copy Files (Copier des fichiers).
2. Complétez les champs **Source** et **Destination**.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le fichier est copié et l'unité est mise à jour.

Restauration de la configuration d'origine

1. Affichez la page Copy Files (Copier des fichiers).
2. Cliquez sur **Restore Configuration Factory Defaults** (Restaurer la configuration d'origine).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres d'origine par défaut sont rétablis et l'unité est mise à jour.

Copie et suppression de fichiers à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page Copy Files (Copier des fichiers).

Tableau 6-47. Commandes CLI de copie des fichiers

Commande CLI	Description
copy *url_source url_destination*	Copie un fichier d'une source vers une destination.
delete startup-config	Supprime le fichier de configuration de démarrage.

Voici un exemple de commandes CLI :

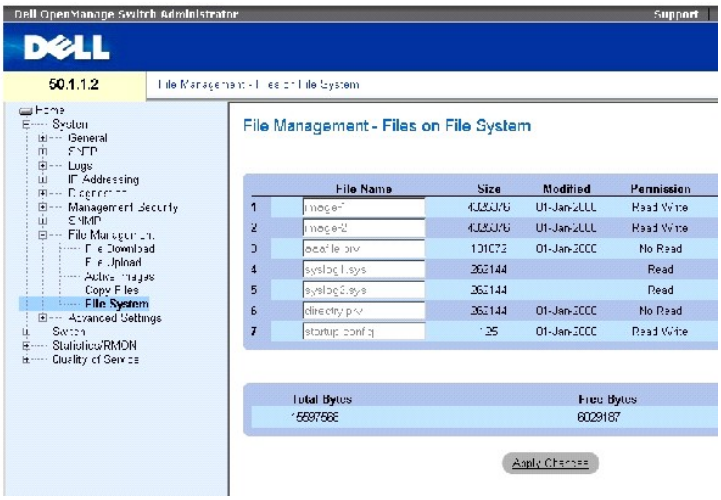
```
console# delete startup-
config


Startup file was deleted


console#


console# copy running-
config startup-config


01-Jan-2000 06:55:32 %
COPY-W-TRAP: The copy
operation was completed
successfully


Copy succeeded


console#
```

Gestion des fichiers de l'unité

La page Files on File System (Fichiers du système de fichiers) fournit des informations relatives aux fichiers stockés sur le système : nom, taille, modifications et

droits d'accès. Le système de fichiers permet de gérer jusqu'à cinq fichiers d'une taille totale de 3 Mo. Pour ouvrir la page Files on File System (Fichiers du système de fichiers), cliquez sur System (Système) → File Management (Gestion des fichiers) → File System (Système de fichiers) dans l'arborescence.

Figure 6-79. Files on File System (Fichiers du système de fichiers)



La page Files on File System (Fichiers du système de fichiers) contient les champs suivants :

File Name (Nom du fichier) : indique le fichier stocké dans le système de gestion de fichiers.

Size (Taille) : indique la taille du fichier.

Modified (Modifié) : indique la date de la dernière modification du fichier.

Permission (Autorisation) : indique le type d'autorisation du fichier. Ce champ peut prendre les valeurs suivantes :

Read Only (Lecture seule) : indique un fichier en lecture seule.

Read Write (Lecture-écriture) : indique un fichier accessible en lecture et en écriture.

Remove (Supprimer) : permet de supprimer le fichier.

Rename (Renommer) : permet de renommer le fichier. Le nom du fichier est modifié dans le champ **File Name** (Nom du fichier).

Total Bytes (Nb total d'octets) : indique l'espace total utilisé.

Free Bytes (Octets disponibles) : indique l'espace disponible.

Gestion des fichiers à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la gestion des fichiers système.

Tableau 6-48. Commandes CLI de copie des fichiers

Commande CLI	Description
dir	Affiche la liste des fichiers dans un système de fichiers flash.

Voici un exemple de commandes CLI :

```
console# dir

Directory of flash:

File Name       Permis-  Flash   Data    Modified
                sion     Size    Size
--------------  ------   ------  ------  ------------------
3.txt           rw       524288  523776  22-Feb-2005 18:49:27
setup           rw       524288  95      22-Feb-2005 15:58:19
setup2          rw       524288  95      22-Feb-2005 15:58:35
image-1         rw       4325376 4325376 06-Feb-2005 17:55:32
image-2         rw       4325376 4325376 06-Feb-2005 17:55:31
test.txt        rw       524288  95      22-Feb-2005 12:16:44
aaafile.prv     --       131072  --      06-Feb-2005 19:09:02
syslog1.sys     r-       262144  --      22-Feb-2005 18:49:27
syslog2.sys     r-       262144  --      22-Feb-2005 18:49:27
directory.prv   --       262144  --      06-Feb-2005 17:55:31
```

startup-config	rw	524288	347	22-Feb-2005 11:56:03
Total size of flash: 16646144 bytes				
Free size of flash: 4456448 bytes				

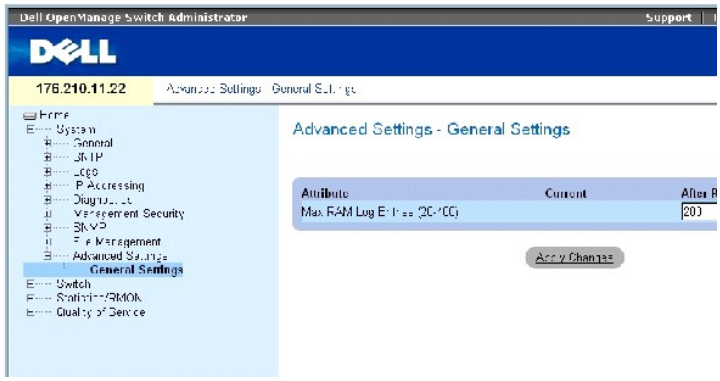
Configuration des paramètres globaux

Utilisez les paramètres avancés pour définir d'autres attributs globaux du commutateur. Les modifications apportées à ces attributs sont appliquées uniquement après la réinitialisation du commutateur. Cliquez sur **System** (Système) → **Advanced Settings** (Paramètres avancés) dans l'arborescence pour ouvrir la page **Advanced Settings** (Paramètres avancés).

La page **Advanced Settings** (Paramètres avancés) affiche un lien permettant de configurer les paramètres globaux.

La page General Settings (Paramètres globaux) fournit des informations permettant de définir les paramètres globaux de l'unité. Pour ouvrir la page General Settings (Paramètres globaux), cliquez sur System (Système) → Advanced Settings (Paramètres avancés) → General Settings (Paramètres globaux) dans l'arborescence.

Figure 6-80. General Settings (Paramètres globaux)



La page General Settings (Paramètres globaux) contient les champs suivants :

Attribute (Attribut) : attribut du paramètre global.

Current (En cours) : valeur configurée en cours.

After Reset (Après réinitialisation) : valeur après réinitialisation. Lorsqu'une valeur est saisie dans la colonne After Reset (Après réinitialisation), la table de champs reçoit une allocation de mémoire.

Max RAM Log Entries (20-400) (Nombre max d'entrées de journal en RAM [1 à 400]) : nombre maximum d'entrées de journal en RAM. Lorsque le maximum est atteint, le journal est effacé et le fichier journal réinitialisé.

Affichage du compteur d'entrées de journal en RAM à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI équivalentes permettant de définir les champs de la page General Settings (Paramètres globaux).

Tableau 6-49. Commandes CLI des paramètres globaux

Commande CLI	Description
logging buffered size nombre	Définit le nombre de messages syslog stockés dans la mémoire tampon interne (RAM).

Voici un exemple de commandes CLI :

```
console(config)# logging
buffered size 300
```

Retour au sommaire

Retour au sommaire

Configuration des informations du commutateur

Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

Cette section contient toutes les informations relatives à l'exploitation du système et les informations générales nécessaires à la configuration de la sécurité du réseau, des ports, des tables d'adresses, du protocole GARP, des VLAN, du protocole STP, de l'agrégation des ports et de la prise en charge de la multidiffusion.

Configuration de la sécurité du réseau

Utilisez la page **Network Security** (Sécurité réseau) pour définir la sécurité réseau via des listes de contrôle de d'accès et des ports verrouillés. Pour ouvrir la page **Network Security** (Sécurité réseau), sélectionnez **Switch** (Commutateur) → **Network Security** (Sécurité réseau).

Authentification basée sur le port

L'authentification basée sur le port permet d'authentifier des utilisateurs d'un système en fonction du 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 à l'aide du protocole Extensible Authentication Protocol (EAP). L'authentification des ports inclut les éléments suivants :

- **Authenticators** (Authentificateurs) : indique le port de l'unité authentifié avant d'autoriser l'accès au système.
- **Supplicants** (Demandeurs) : indique l'hôte connecté au port authentifié demandant l'accès aux services du système.
- **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 le demandeur est autorisé à accéder aux services du système.

L'authentification basée sur le port crée deux états d'accès :

- **Controlled Access** (Accès contrôlé) : permet la communication entre le demandeur et le système, si le demandeur est autorisé.
- **Uncontrolled Access** (Accès non contrôlé) : permet une communication non contrôlée quel que soit l'état du port.

L'unité prend en charge l'authentification basée sur le port via des serveurs RADIUS.

Authentification avancée basée sur le port

L'authentification avancée basée sur le port :

- Permet de connecter plusieurs hôtes à un port unique.
- Nécessite qu'un seul port soit autorisé pour que tous les hôtes accèdent au système. Si le port n'est pas autorisé, tous les hôtes connectés se voient refuser l'accès au réseau.
- Active l'authentification basée sur l'utilisateur. Des VLAN spécifiques de l'unité sont toujours disponibles, même si des ports spécifiques connectés au VLAN ne sont pas autorisés.
    - Par exemple, le trafic voix sur IP ne nécessite aucune authentification, contrairement au trafic des données. Il est possible de définir des VLAN ne nécessitant aucune autorisation. Ces VLAN sans authentification sont disponibles même si les ports correspondants sont définis comme étant autorisés.

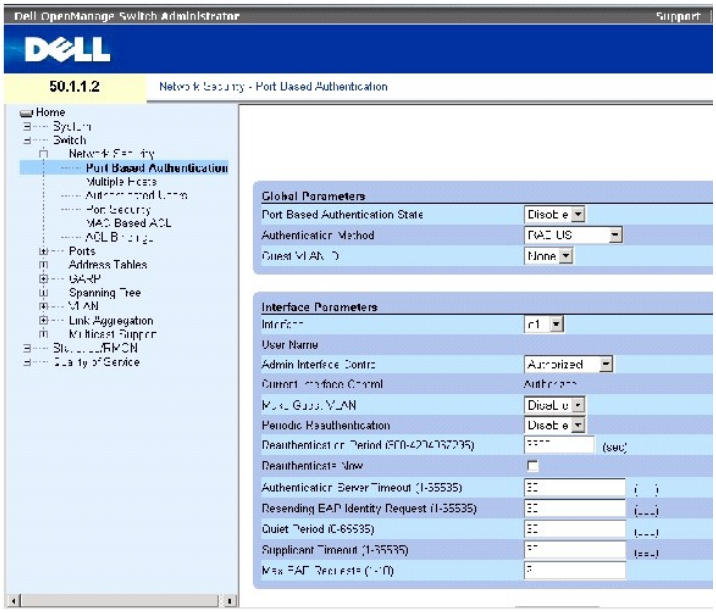
L'authentification avancée basée sur le port est mise en oeuvre dans les modes suivants :

- **Single Host Mode** (Mode hôte unique) : seul l'hôte autorisé peut accéder au port.
- **Multiple Host Mode** (Mode hôtes multiples) : plusieurs hôtes peuvent être connectés à un port unique. Un seul hôte doit être autorisé pour que tous les hôtes puissent accéder au réseau. Si l'authentification de l'hôte échoue ou si un message de fermeture de session EAPOL s'affiche, tous les clients connectés se voient refuser l'accès au réseau.
- **Guest VLANs** (VLAN invités) : fournit un accès réseau limité autorisé aux ports. Si un port se voit refuser l'accès via une autorisation basée sur le port alors que l'option Guest VLANs (VLAN invités) est activée, le port bénéficie d'un accès réseau limité. Par exemple, un administrateur réseau peut utiliser l'option Guest VLAN pour interdire l'accès via une authentification basée sur le port, tout en accordant aux utilisateurs non autorisés l'accès à Internet.

Configuration de l'authentification basée sur le port

La page Port Based Authentication (Authentification basée sur le port) permet aux administrateurs réseau de configurer l'authentification basée sur le port. Pour ouvrir la page Port Based Authentication (Authentification basée sur le port), cliquez sur **Switch** (Commutateur) → **Network Security** (Sécurité réseau) → **Port Based Authentication** (Authentification basée sur le port).

Figure 7-1. Port Based Authentication (Authentification basée sur le port)



La page Port Based Authentication (Authentification basée sur le port) contient les champs suivants :

Port Based Authentication State (État de l'authentification basée sur le port) : active l'authentification basée sur le port au niveau de l'unité. Ce champ peut prendre les valeurs suivantes :

Enable (Activer) : active l'authentification basée sur le port au niveau de l'unité.

Disable (Désactiver) : désactive l'authentification basée sur le port au niveau de l'unité.

Authentication Method (Méthode d'authentification) : indique la méthode d'authentification utilisée. Ce champ peut prendre les valeurs suivantes :

None (Aucune) : indique qu'aucune méthode n'est utilisée pour authentifier le port.

RADIUS : indique que l'authentification des ports s'effectue via le serveur RADIUS.

RADIUS, None (RADIUS, aucune) : indique que l'authentification des ports s'effectue d'abord via le serveur RADIUS. Si le port n'est pas authentifié, aucune méthode d'authentification n'est utilisée et la session est autorisée.

Guest VLANs (VLAN invités) : active l'utilisation d'un VLAN invité pour les ports non autorisés. Si un VLAN est activé, le port non autorisé est automatiquement associé au VLAN sélectionné dans le champ **VLAN List** (Liste des VLAN). La valeur par défaut de ce champ est disabled (désactivé).

Interface : contient une liste d'interfaces pour lesquelles l'authentification basée sur le port est activée.

User Name (Nom d'utilisateur) : indique le nom d'utilisateur du demandeur.

Admin Interface Control (Contrôle de l'interface admin) : définit l'état de l'autorisation des ports. Ce champ peut prendre les valeurs suivantes :

Auto (Automatique) : active l'authentification basée sur le port au niveau de l'unité. L'interface passe de l'état autorisé à l'état non autorisé en fonction des échanges d'authentification entre l'unité et le client.

Authorized (Autorisé) : place l'interface à l'état autorisé sans l'authentifier. L'interface renvoie et reçoit normalement le trafic sans authentifier le client en fonction du port.

Unauthorized (Non autorisé) : refuse à interface sélectionnée l'accès au système en la plaçant à l'état non autorisé. L'interface ne permet pas au client d'utiliser les services d'authentification.

Current Interface Control (Contrôle actuel de l'interface) : état actuel de l'autorisation des ports.

Make Guest VLAN (Créer un VLAN invité) : indique que des utilisateurs non autorisés connectés à cette interface peuvent accéder au VLAN invité.

Periodic Reauthentication (Réauthentification périodique) : permet une réauthentification immédiate du port.

Reauthentication Period (300-4294967295) (Période de réauthentification [300 à 4294967295]) : indique le délai au terme duquel le port sélectionné est réauthentifié. Cette valeur est exprimée en secondes. La valeur par défaut est de 3600 secondes.

Reauthenticate Now (Réauthentification immédiate) : permet une réauthentification immédiate du port.

Authentication Server Timeout (1-65535) (Délai d'authentification du serveur [1 à 65535]) : définit le délai qui s'écoule avant que l'unité renvoie une requête au serveur d'authentification. Cette valeur 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 à 65535]) : définit le délai qui s'écoule avant qu'une requête EAP soit renvoyée. La valeur par défaut est de 30 secondes.

Quiet Period (0-65535) (Période de latence [0 à 65535]) : indique le délai de latence (en secondes) de l'unité après l'échec d'une authentification. La plage de valeurs possibles pour ce champ est 0 à 65535. La valeur par défaut est de 30 secondes.

Supplicant Timeout (1-65535) (Délai pour le demandeur [1 à 65535]) : indique le délai qui s'écoule avant que des requêtes EAP soient renvoyées au demandeur. Cette valeur est exprimée en secondes. La valeur par défaut est de 30 secondes.

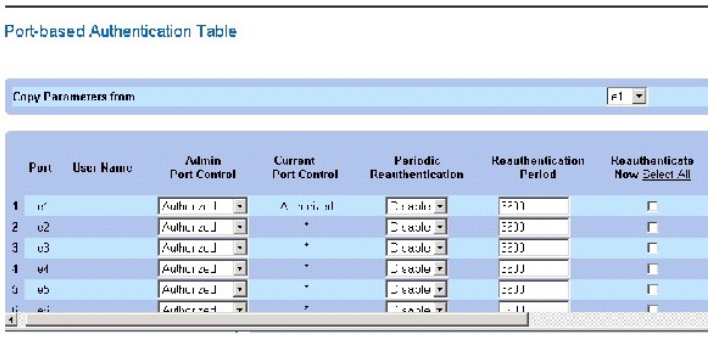
Max EAP Requests (1-10) (Nombre maximum de requêtes EAP [1 à 10]) : indique le nombre total de requêtes EAP envoyées. Si aucune réponse n'est reçue après la période définie, le processus d'authentification est relancé. La valeur par défaut est de 2 tentatives.

Affichage de la table d'authentification basée sur le port

1. Affichez la page Port Based Authentication (Authentification basée sur le port).
2. Cliquez sur Show All (Afficher tout).

La page **Port Based Authentication Table** (Table d'authentification basée sur le port) s'affiche.

Figure 7-2. Port Based Authentication Table (Table d'authentification basée sur le port)



Le **Port Based Authentication Table (Table d'authentification basée sur le port)** contient les champs suivants (en plus de ceux de la page Port Based Authentication - Authentification basée sur le port) :

Unit No. (Numéro d'unité) : sélectionne un membre de la pile.

Copy Parameters from Port No. (Copier les paramètres du port n°) : copie les paramètres du port sélectionné.

Copie de paramètres dans la page Port Based Authentication Table (Table d'authentification basée sur le port)

1. Affichez la page appropriée.
2. Cliquez sur Show All (Afficher tout).

La page **Port Based Authentication Table (Table d'authentification basée sur le port)** s'affiche.

3. Sélectionnez l'interface dans le champ **Copy Parameters from Port No.** (Copier les paramètres du port n°).
4. Sélectionnez une interface dans la page **Port Based Authentication Table (Table d'authentification basée sur le port)**.
5. Cochez la case **Copy to** (Copier vers) pour définir les interfaces vers lesquelles les paramètres d'authentification basée sur le port doivent être copiés.
6. Cliquez sur Apply Changes (Appliquer les modifications).

Activation de l'authentification basée sur le port à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant l'activation de l'authentification basée sur le port, comme indiqué à la page Port Based Authentication (Authentification basée sur le port).

Tableau 7-1. Commandes CLI relatives à l'authentification basée sur le port

Commande CLI	Description
aaa authentication dot1x default *méthode1* [*méthode2*.]	Spécifie une ou plusieurs méthodes AAA (Authentication, Authorization, Accounting) à utiliser dans les interfaces basées sur le protocole IEEE 802.1X.
dot1x max-req *nombre*	Définit le nombre maximum de fois où l'unité envoie une requête EAP au client avant de relancer le processus d'authentification.
dot1x re-authenticate [**ethernet** *interface*]	Lance manuellement une réauthentification de tous les ports 802.1X ou du port 802.1X spécifié.

dot1x re-authentication	Active la réauthentification périodique du client.
dot1x timeout quiet-period secondes	Définit le délai de latence (en secondes) de l'unité après l'échec d'une authentification.
dot1x timeout re-authperiod *secondes*	Définit le nombre de secondes entre les tentatives de réauthentification.
dot1x timeout server-timeout *secondes*	Définit le délai de retransmission des paquets vers le serveur d'authentification.
dot1x timeout supp-timeout *secondes*	Définit le délai de retransmission d'une trame de requête EAP au client.
dot1x timeout tx-period *secondes*	Définit le délai en secondes pendant lequel l'unité attend la réponse à une trame EAP "request" ou "ID" provenant du client avant de renvoyer la requête.
show dot1x [ethernet *interface*]	Affiche l'état 802.1X de l'unité ou de l'interface spécifiée.
show dot1x users [username nom d'utilisateur]	Affiche les utilisateurs 802.1X de l'unité.
dot1x guest-vlan enable	Active l'utilisation d'un VLAN invité pour les ports non autorisés. Si un VLAN est activé, le port non autorisé est automatiquement associé au VLAN sélectionné dans le champ **VLAN List** (Liste des VLAN). La valeur par défaut de ce champ est disabled (désactivé).
dot1x guest-vlan	Contient la liste des VLAN. Le VLAN invité est sélectionné dans la liste des VLAN.

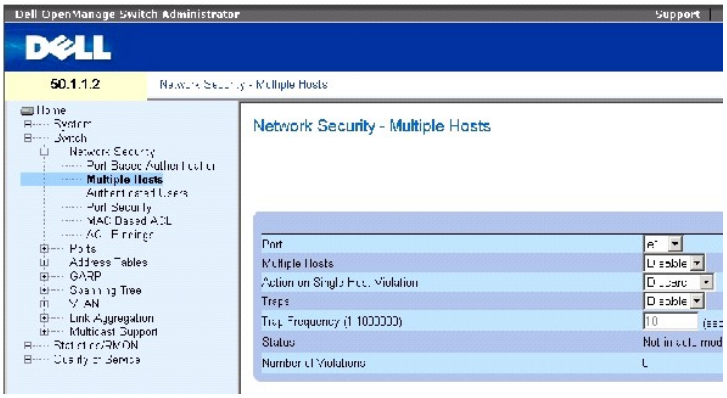
Voici un exemple de commandes CLI :

```
Console# show dot1x

Interface  Admin Mode      Oper Mode     Reauth Control  Reauth Period  Username
---------  --------------  ------------  --------------  -------------  --------
1/e1       Auto            Authorized    Ena             3600           Bob
1/e2       Auto            Authorized    Ena             3600           John
1/e3       Auto            Unauthorized  Ena             3600           Clark
1/e4       Force-auth      Authorized    Dis             3600           n/a
```

Configuration de l'authentification avancée basée sur le port

La page **Multiple Hosts (Hôtes multiples)** fournit des informations permettant de définir les paramètres d'authentification avancée pour des ports et des VLAN spécifiques. Pour plus d'informations sur l'authentification avancée basée sur le port, consultez la section "**Authentification avancée basée sur le port**". Pour ouvrir la page **Multiple Hosts (Hôtes multiples)**, cliquez sur Switch (Commutateur) → Network Security (Sécurité réseau) → Multiple Hosts (Hôtes multiples).

Figure 7-3. Multiple Hosts (Hôtes multiples)



La page **Multiple Hosts (Hôtes multiples)** contient les champs suivants :

Port : numéro du port pour lequel l'authentification avancée basée sur le port est activée.

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 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). Ce champ peut prendre les valeurs 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.

Shutdown (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) (Sec) (Fréquence des interruptions [1 à 1000000 secondes]) : définit la fréquence d'envoi des interruptions à l'hôte. Ce champ peut être défini uniquement si le champ **Multiple Hosts** (Hôtes multiples) est défini sur **Disable** (Désactivé). La valeur par défaut est de 10 secondes.

Status (État) : état de l'hôte. Ce champ peut prendre les valeurs suivantes :

Unauthorized (Non autorisé) : indique que le contrôle du port est défini sur *Force Unauthorized* (Forcé sur non autorisé) ; le lien du port est désactivé ou le contrôle du port est défini sur Auto, mais 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 disposent d'un accès total aux ports.

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 l'option Multiple Host (Hôtes multiples) est activée.

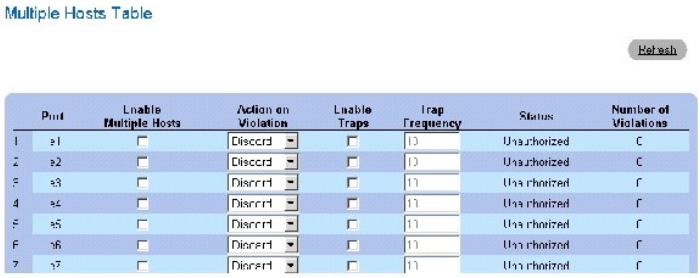
Number of Violations (Nombre de violations) : nombre de paquets reçus sur l'interface en mode hôte unique à partir d'un hôte dont l'adresse MAC n'est pas celle du client (demandeur).

Affichage de la page Multiple Hosts Table (Table des hôtes multiples)

1. Affichez la page **Multiple Hosts (Hôtes multiples)**.
2. Cliquez sur Show All (Afficher tout).

La page **Multiple Hosts Table (Table des hôtes multiples)** s'affiche.

Figure 7-4. Multiple Hosts Table (Table des hôtes multiples)



Activation des hôtes multiples à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant l'activation de l'authentification avancée basée sur le port, comme indiqué à la page **Multiple Hosts (Hôtes multiples)**.

Tableau 7-2. Commandes CLI relatives aux hôtes multiples

Commande CLI	Description
dot1x multiple-hosts	Autorise plusieurs hôtes (clients) sur un port 802.1X pour lequel la commande de configuration de l'interface de contrôle du port dot1x est définie sur Auto.
dot1x single-host-violation {forward |discard |discard-shutdown}[trap secondes]	Configure l'action à exécuter lorsqu'une station dont l'adresse MAC n'est pas celle du client (demandeur) tente d'accéder à l'interface.

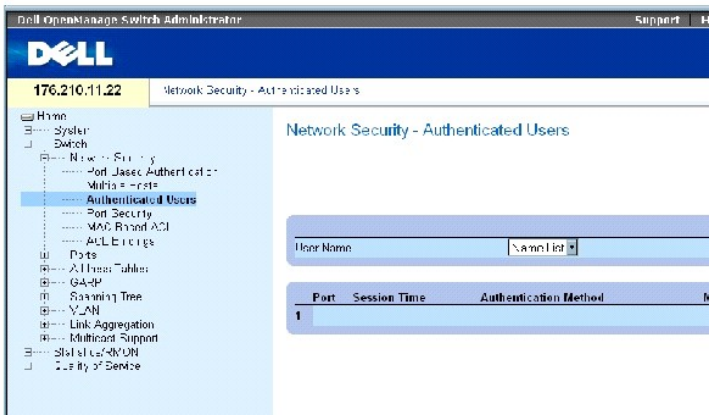
Voici un exemple de commandes CLI.

```
Console (config)#
interface ethernet 1/e1

Console(config-if)# dot1x
multiple-hosts
```

Authentification des utilisateurs

La page Authenticated Users (Utilisateurs authentifiés) affiche la liste d'accès des utilisateurs aux ports. Les listes d'accès des utilisateurs sont définies à la page Add User Name (Ajout d'un nom d'utilisateur). Pour ouvrir la page Authenticated Users (Utilisateurs authentifiés), cliquez sur Switch (Commutateur) → Network Security (Sécurité réseau) → Authenticated Users (Utilisateurs authentifiés).

Figure 7-5. Authenticated Users (Utilisateurs authentifiés)



La page Authenticated Users (Utilisateurs authentifiés) contient les champs suivants :

User Name (Nom d'utilisateur) : liste des utilisateurs autorisés via le serveur RADIUS.

Port : numéro(s) de port utilisé(s) pour l'authentification, par nom d'utilisateur.

Session Time (Durée de la session) : temps de connexion de l'utilisateur sur l'unité. Le format de ce champ est **Jours:heures:minutes:secondes**, par exemple, 3 jours: 2 heures: 4 minutes: 39 secondes.

Authentication Method (Méthode d'authentification) : méthode d'authentification utilisée pour la dernière session. Ce champ peut prendre les valeurs suivantes :

Remote (À distance) : l'utilisateur a été authentifié à partir d'un serveur distant.

None (Aucune) : l'utilisateur n'a pas été authentifié.

MAC Address (Adresse MAC) : adresse MAC du demandeur.

Affichage de la table des utilisateurs authentifiés

1. Affichez la page Authenticated Users (Utilisateurs authentifiés).
2. Cliquez sur Show All (Afficher tout).

La page **Authenticated Users Table** (Table des utilisateurs authentifiés) s'affiche.

Figure 7-6. Authenticated Users Table (Table des utilisateurs authentifiés)

Authentification des utilisateurs à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant d'authentifier les utilisateurs, comme indiqué à la page Authenticated Users (Utilisateurs authentifiés).

Tableau 7-3. Commandes CLI permettant l'ajout d'un nom d'utilisateur

Commande CLI	Description
show dot1x users [username nom d'utilisateur]	Affiche les utilisateurs 802.1X de l'unité.

Voici un exemple de commandes CLI :

```
console# show dot1x users

Port Username Session Time Auth Method MAC Address

---------------------------------------------------------------

1/e11 gili 00:09:27 Remote 00:80:c8:b9:dc:1d
```

Configuration du verrouillage de port

La sécurité réseau peut être améliorée en limitant l'accès à un port spécifique pour les utilisateurs possédant des adresses MAC spécifiques. Les adresses MAC peuvent faire l'objet d'un processus d'apprentissage de façon dynamique jusqu'à ce niveau, ou bien être configurées de façon statique. Le verrouillage de port gère les paquets reçus et ceux ayant fait l'objet d'un apprentissage sur des ports spécifiques. L'accès au port verrouillé est réservé aux utilisateurs disposant d'adresses MAC spécifiques. Ces adresses sont définies manuellement sur le port ou incluses dans la liste des autorisations par le fait qu'elles aient été apprises avant que le port ne soit verrouillé. Lorsqu'un paquet est reçu sur un port verrouillé et que son adresse Mac source n'est pas associée à ce port (parce qu'elle a été apprise sur un port différent ou qu'elle est inconnue du système), le mécanisme de protection est activé. Diverses options sont possibles lorsque des paquets non autorisés arrivent sur un port verrouillé :

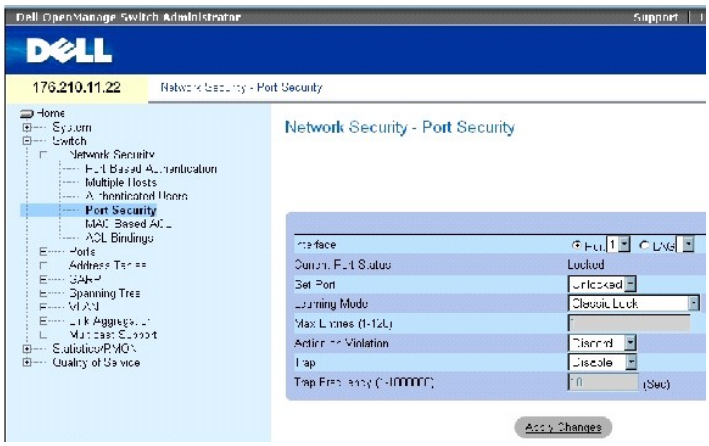
- les paquets sont transmis ;
- les paquets sont rejetés sans interruption ;
- les paquets sont rejetés avec interruption ;
- le port est désactivé.

Le verrouillage du port permet également de stocker une liste d'adresses MAC dans le fichier de configuration. La liste d'adresses MAC peut être restaurée après réinitialisation de l'unité.

REMARQUE : pour activer le verrouillage de port, sélectionnez **Multiple Hosts (Hôtes multiples)** sur les ports requis.

Les ports désactivés sont activés à partir de la page Port Security (Verrouillage de port). La page **Ports** fournit des liens permettant de configurer des fonctionnalités 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 ouvrir la page Port Security (Verrouillage de port), cliquez sur Switch (Commutateur) → Network Security (Sécurité réseau) → Port Security (Verrouillage de port).

Figure 7-7. Port Security (Verrouillage de port)



La page Port Security (Verrouillage de port) contient les champs suivants :

Interface : type d'interface sélectionné, sur lequel l'option Locked Port (Port verrouillé) est activée.

Port : le type d'interface sélectionné est un port.

LAG : le type d'interface sélectionné est un LAG.

Current Port Status (État actuel du port) : état actuel du port configuré.

Set Port (Définir le port) : permet de verrouiller ou de déverrouiller le port. Ce champ peut prendre les valeurs suivantes :

Unlocked (Déverrouillé) : déverrouille le port. Il s'agit de la valeur par défaut.

Locked (Verrouillé) : verrouille le port.

Learning Mode (Mode d'apprentissage) : définit le type de port verrouillé. Le champ **Learning Mode (Mode d'apprentissage)** est activé uniquement si l'option **Locked** (Verrouillé) est sélectionnée dans le champ **Set Port** (Définir le port). Ce champ peut prendre les valeurs suivantes :

Classic Lock (Verrouillage classique) : verrouille le port en utilisant le mécanisme de verrouillage classique. Le port est immédiatement verrouillé, quel que soit le nombre d'adresses déjà apprises.

Limited Dynamic Lock (Verrouillage dynamique limité) : verrouille le port en supprimant les adresses MAC dynamiques qui lui sont actuellement associées. Le port acquiert le nombre maximum d'adresses autorisées sur le port. Le réapprentissage et l'expiration des adresses MAC sont activés.

Max Entries (Nb maximal d'entrées) : indique le nombre d'adresses MAC pouvant être apprises sur le port. Ce champ est activé uniquement si l'option **Locked** (Verrouillé) est sélectionnée dans le champ **Set Port** (Définir le port). En outre, le mode Limited Dynamic Lock (Verrouillage dynamique limité) est sélectionné. La valeur par défaut est de 1.

Action on Violation (Action si violation) : action à appliquer aux paquets qui arrivent sur un port verrouillé. Ce champ peut prendre les valeurs 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.

Shutdown (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 de l'unité.

Trap (Interruption) : active l'envoi d'une interruption lorsqu'un paquet est reçu sur un port verrouillé.

Trap Frequency (1-1000000) : (Fréquence des interruptions [1 à 1000000]) : délai (en secondes) entre deux interruptions. La valeur par défaut est de 10 secondes.

Définition d'un port verrouillé

1. Affichez la page **Port Security (Verrouillage de port)**.
2. Sélectionnez un type et un numéro d'interface.
3. Complétez les champs avec les valeurs appropriées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port verrouillé est ajouté à la page **Port Security Table (Table de verrouillage de port)** et l'unité est mise à jour.

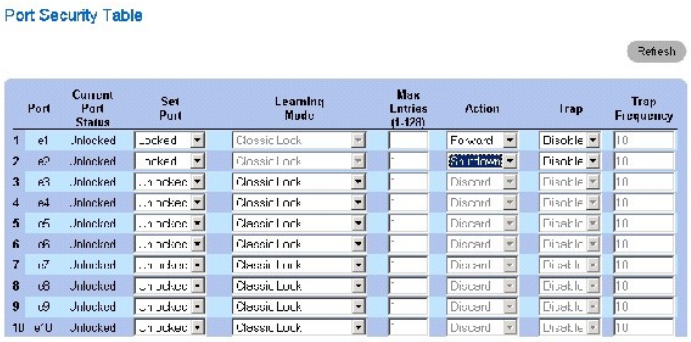
Affichage de la table de verrouillage de port

1. Affichez la page **Port Security (Verrouillage de port)**.
2. Cliquez sur **Show All** (Afficher tout).

La page **Port Security Table (Table de verrouillage de port)** s'affiche.

REMARQUE : les ports verrouillés sont définis dans la page **Port Security Table (Table de verrouillage de port)**.

Figure 7-8. Port Security Table (Table de verrouillage de port)



La page **Port Security Table (Table de verrouillage de port)** contient les champs supplémentaires suivants :

Unit No. (Numéro d'unité) : spécifie l'unité d'empilage pour laquelle les informations du port verrouillé sont affichées.

Copy Parameters from (Copier les paramètres à partir de) : copie les paramètres vers le numéro d'unité sélectionné.

Configuration de l'option de sécurité Locked Port (Port verrouillé) à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la configuration de l'option de sécurité Locked Port (Port verrouillé), comme indiqué dans la page Port Security (Verrouillage de port).

Tableau 7-3. Commandes CLI relatives au verrouillage de port

Commande CLI	Description
shutdown	Désactive les interfaces.
set interface active {ethernet interface | port-channel numéro-canal-port}	Réactive une interface qui a été désactivée pour des raisons de sécurité.
port security learning {disabled | dynamic}	Définit le type de port verrouillé.
port security max adr-max	Spécifie le nombre d'adresses MAC pouvant être apprises sur le port.
port security [forward | discard | discard-shutdown] [trap secondes]	Verrouille l'apprentissage de nouvelles adresses sur une interface.
show ports security {ethernet interface | port-channel numéro-canal-port}	Affiche l'état de verrouillage du port.

Voici un exemple de commandes CLI :

console # **show ports security**

Port	Status	Action	Trap	Frequency	Counter
1/e1	locked	Discard	Enable	100	88
1/e2	locked	Discard, Shutdown	Disable		
1/e3	Unlocked	-	-	-	-

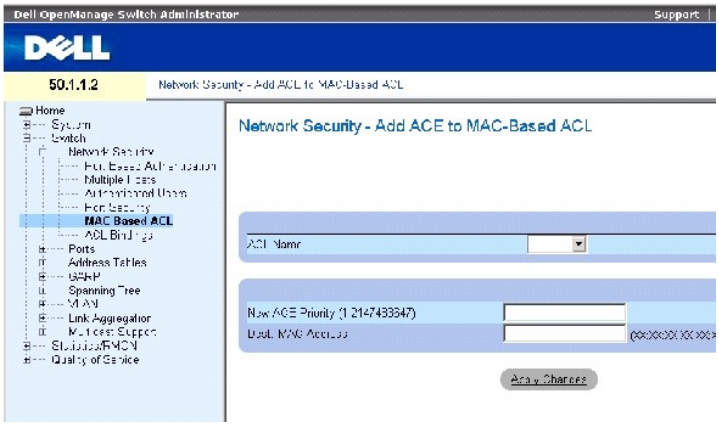
Définition des listes ACL basées sur l'adresse MAC

Les listes de contrôle d'accès (ACL, Access Control Lists) permettent aux administrateurs réseau de définir des actions et des règles de classification pour des ports d'entrée spécifiques. Les listes ACL contiennent plusieurs règles et actions de classification. Chaque règle et action constitue un élément de contrôle d'accès (ACE, Access Control Element). Les ACE sont les filtres qui déterminent les classifications du trafic. Les listes ACL basées sur l'adresse MAC s'appliquent à tous les paquets, y compris les paquets non IP. Les champs de classification se basent uniquement sur les champs L2.

La page MAC Based ACL (ACL basée sur l'adresse MAC) permet de définir une liste ACL basée sur l'adresse MAC. Pour plus d'informations sur les listes ACL, consultez la section "Définition des listes ACL basées sur l'adresse MAC".

Pour ouvrir la page MAC Based ACL (ACL basée sur l'adresse MAC), cliquez sur **Switch** (Commutateur) → **Network Security** (Sécurité réseau) → **MAC based ACL** (ACL basée sur l'adresse MAC).

Figure 7-9. MAC Based ACL (ACL basée sur l'adresse MAC)



La page MAC Based ACL (ACL basée sur l'adresse MAC) contient les champs suivants :

ACL Name (Nom de la liste ACL) : ACL définie par l'utilisateur.

New ACE Priority (1-2147483647) (Priorité des nouveaux éléments ACE [1 à 2147483647]) : index de la règle des ACE dans le champ ACL.

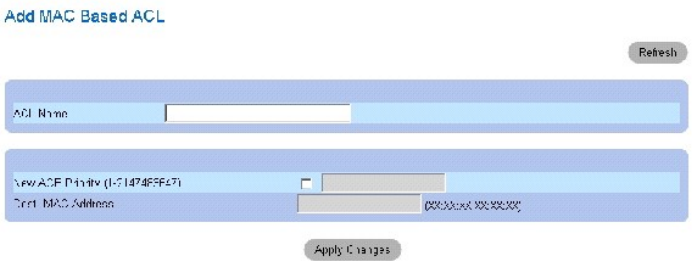
Destination MAC Address (Adresse MAC de destination) : met en correspondance l'adresse MAC de destination à laquelle les paquets sont adressés et l'ACE.

Ajout d'une liste ACL basée sur l'adresse MAC

1. Affichez la page MAC Based ACL (ACL basée sur l'adresse MAC).
2. Cliquez sur **Add** (Ajouter).

La page Add MAC Based ACLs (Ajout de listes ACL basées sur l'adresse MAC) s'affiche.

Figure 7-10. Add MAC Based ACLs (Ajout de listes ACL basées sur l'adresse MAC)



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

La liste ACL basée sur l'adresse MAC est définie et l'unité est mise à jour.

Affichage des ACE associés à une liste ACL

1. Affichez la page MAC Based ACL (ACL basée sur l'adresse MAC).
2. Sélectionnez une liste ACL.
3. Cliquez sur **Show All** (Afficher tout).

La page **ACEs Associated with MAC ACL** (ACE associés à la liste ACL MAC) s'affiche.

Suppression de listes ACL

1. Affichez la page MAC Based ACL (ACL basée sur l'adresse MAC).

REMARQUE : les listes ACL peuvent être supprimées uniquement si elles ne sont pas liées à une interface.

2. Sélectionnez une liste ACL.
3. Cliquez sur **Show All** (Afficher tout).

La page **ACEs Associated with MAC ACL** (ACE associés à la liste ACL MAC) s'affiche.

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

Affectation d'ACE basés sur l'adresse MAC aux ACL à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant l'affectation d'ACE basés sur l'adresse MAC aux ACL, comme indiqué à la page MAC Based ACL (ACL basée sur l'adresse MAC).

Tableau 7-4. Commandes CLI des ACE basés sur l'adresse MAC

Commande CLI	Description
`mac access-list nom`	Crée des listes ACL MAC de couche 2 et passe en mode de configuration des listes d'accès MAC.
`deny destination`	Refuse le trafic si les conditions définies dans la liste ACL basée sur l'adresse MAC sont satisfaites.
`show access-lists [nom]`	Affiche les listes de contrôle d'accès configurées sur l'unité.

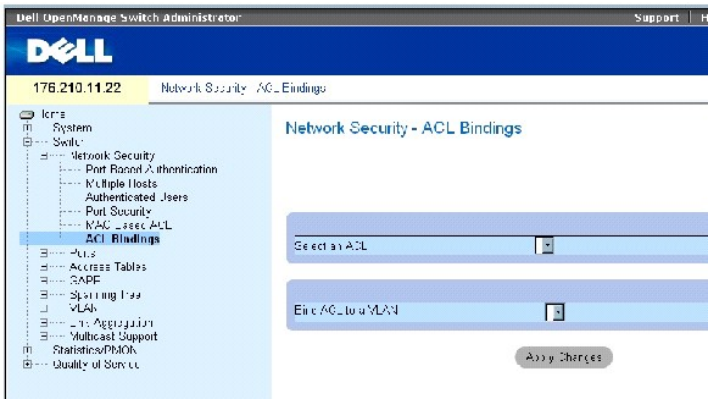
Voici un exemple de commandes CLI :

```
console (config)# mac access-list dell

console (config-mac-al)# deny 00-10-B5-F4-00-01
```

Configuration des liaisons des listes ACL

Une liste ACL est appliquée à l'interface à laquelle elle est associée. Utilisez la page ACL Bindings (Liaisons des listes ACL) pour associer des listes ACL à des méthodes de classification et à des interfaces. Pour ouvrir la page ACL Bindings (Liaisons des listes ACL), cliquez sur **Switch** (Commutateur) → **Network Security** (Sécurité réseau) → **ACL Binding** (Liaisons des listes ACL).

Figure 7-11. ACL Bindings (Liaisons des listes ACL)



La page ACL Bindings (Liaisons des listes ACL) contient les champs suivants :

Select an ACL (Sélectionner une liste ACL) : type de liste ACL auquel sont associés les paquets entrants.

Bind ACL to VLAN (Lier la liste ACL au VLAN) : VLAN auquel la liste ACL est associée.

Affectation d'une liste ACL à une interface

1. Affichez la page ACL Bindings (Liaisons des listes ACL).
2. Sélectionnez le type de liste ACL dans le champ **Select an ACL** (Sélectionner une liste ACL).
3. Sélectionnez le VLAN auquel la liste ACL est associée dans le champ **Bind ACL to an VLAN** (Associer la liste ACL à un VLAN).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La liste ACL est associée à l'interface.

Suppression d'une entrée de la table des liaisons des listes ACL

1. Affichez la page ACL Bindings (Liaisons des listes ACL).
2. Cliquez sur **Show All** (Afficher tout).

La page **ACL Bindings Table** (Table des liaisons des listes ACL) s'affiche.

3. Cochez la case **Remove** (Supprimer) correspondant à l'entrée à supprimer.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée sélectionnée est supprimée de la table et l'unité est mise à jour.

Affichage de la table des liaisons des listes ACL

1. Affichez la page ACL Bindings (Liaisons des listes ACL).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la **table des liaisons des listes ACL**.

Les champs de cette table sont identiques à ceux de la page **ACL Bindings** (Liaisons des listes ACL).

Copie de paramètres dans la table des liaisons des listes ACL

1. Affichez la page ACL Bindings (Liaisons des listes ACL).

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

   La page **ACL Bindings Table** (Table des liaisons des listes ACL) s'affiche.

3. Sélectionnez une interface dans le champ **Copy Parameters from** (Copier les paramètres à partir de).
4. Sélectionnez un VLAN dans le menu déroulant **VLAN**.

   Les définitions de cette interface sont copiées vers les ports ou segments cible sélectionnés.

5. Cochez la case **Copy to** (Copier vers) pour modifier l'entrée ou copier les définitions vers tous les ports ou segments disponibles.
6. Cliquez sur **Select All** (Sélectionner tout).
7. Cliquez sur **Apply Changes** (Appliquer les modifications).

   Les paramètres sont copiés vers les ports ou segments cibles de la *table des liaisons des listes ACL* et l'unité est mise à jour.

Affectation de l'appartenance à une liste ACL à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant l'affectation de l'appartenance à une liste ACL, comme indiqué à la page **ACL Bindings** (Liaisons des listes ACL).

Tableau 7-5. Commandes CLI relatives aux liaisons des listes ACL

Commande CLI	Description
service-acl {**input** *nom-acl*}	Applique une liste d'accès à l'interface.

Voici un exemple de commandes CLI :

```
console(config)# interface vlan 123

console(config-if)# service-acl input dell
```

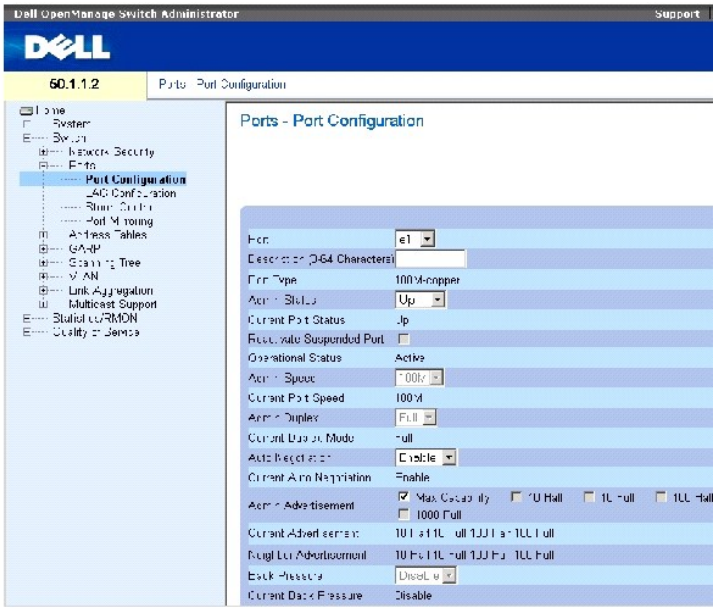
Configuration des ports

La page **Ports** fournit des liens permettant de configurer des fonctionnalités 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 ouvrir la page **Ports**, cliquez sur **Switch** (Commutateurs) → **Ports**.

Définition de la configuration des ports

Utilisez la page **Port Configuration (Configuration des ports)** pour définir les paramètres des ports. Si la configuration d'un port est modifiée alors que celui-ci fait partie d'un LAG, la modification ne prend effet qu'une fois le port supprimé du LAG. Pour ouvrir la page **Port Configuration (Configuration des ports)**, cliquez sur **Switch** (Commutateur) → **Ports** → **Port Configuration** (Configuration des ports) dans l'arborescence.

Figure 7-12. Port Configuration (Configuration des ports)



La page **Port Configuration (Configuration des ports)** contient les champs suivants :

Port : numéro du port pour lequel les paramètres sont définis.

Description (0 - 64 Characters) (Description [0 à 64 caractères]) : brève description de l'interface (par exemple, Ethernet).

Port Type (Type de port) : type du port sélectionné.

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.

Reactivate Suspended Port (Réactiver un port suspendu) : réactive un port si celui-ci a été désactivé par le biais de l'option Locked Port (Port verrouillé).

Operational Status (État opérationnel) : indique l'état opérationnel du port. Ce champ peut prendre les valeurs suivantes :

Suspended (Suspendu) : le port est actif, mais il ne reçoit ni n'envoie aucun trafic.

Active (Actif) : le port est actif, il reçoit et envoie du trafic.

Disable (Désactivé) : le port est désactivé et ne reçoit ni n'envoie aucun trafic.

Admin Speed (Vitesse admin) : débit configuré pour le port. Les options disponibles dépendent du type de port. La vitesse ne peut être définie que lorsque le port est désactivé.

Current Port Speed (Vitesse actuelle du port) : vitesse réelle du port synchronisé (en bps).

Admin Duplex (Duplex admin) : mode duplex du port (en bps). L'option **Full** (Intégral) indique que l'interface prend en charge la transmission entre l'unité et le client dans les deux directions simultanément. L'option **Half** (Semi duplex) indique que l'interface prend en charge la transmission entre le périphérique et le client dans une seule direction à la fois.

Current Duplex Mode (Mode duplex actuel) : 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 qui permet à un port d'annoncer son taux de transmission, son mode duplex et ses capacités de contrôle de flux à son partenaire.

Current Auto Negotiation (Négociation automatique en cours) : configuration actuelle de la négociation automatique.

Admin Advertisement (Annonce admin) : définit la configuration de la négociation automatique annoncée par le port. Ce champ peut prendre les valeurs suivantes :

Max Capability (Capacité maximale) : indique que toutes les vitesses et tous les modes duplex sont 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.

Current Advertisement (Annonce actuelle) : le port annonce sa vitesse au port voisin pour lancer le processus de négociation. Ce champ peut prendre les valeurs spécifiées dans le champ Admin Advertisement (Annonce admin).

Neighbor Advertisement (Annonce du port voisin) : indique les paramètres d'annonce du port voisin. Les valeurs de ce champ sont identiques à celles du champ **Admin Advertisement** (Annonce admin).

Back Pressure (Contre-pression) : active le mode contre-pression sur le port. Le mode contre-pression est utilisé avec le mode semi duplex pour désactiver la capacité des ports à recevoir des messages. Il n'est pas pris en charge par les ports OOB.

Current Back Pressure (Contre-pression en cours) : configuration en cours de la contre-pression.

Flow Control (Contrôle de flux) : active ou désactive le contrôle de flux, ou active la négociation automatique du contrôle de flux sur le port.

Current Flow Control (Contrôle de flux en cours) : configuration en cours du contrôle de flux.

MDI/MDIX (Interface dépendante du média/Interface croisée dépendante du média) : permet à l'unité de distinguer les câbles croisés des câbles directs. Les concentrateurs et les commutateurs sont délibérément câblés de façon opposée à celle des stations terminales, de telle sorte que 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 pour assurer que les paires appropriées sont connectées. La fonction Auto MDIX ne fonctionne pas sur les ports FE si la négociation automatique est désactivée. Ce champ peut prendre les valeurs suivantes :

Auto (Automatique) : utilisez cette option pour détecter automatiquement le type de câble.

MDIX : utilisez cette option pour les concentrateurs et les commutateurs.

MDI : utilisez cette option pour les terminaux.

Current MDI/MDIX (MDI/MDIX en cours) : indique la configuration MDIX en cours de l'unité. Ce champ peut prendre les valeurs suivantes :

MDI (Interface dépendante du média) : la configuration en cours est MDI.

MDIX (Interface croisée dépendante du média) : la configuration en cours est MDIX.

LAG : indique si le port fait partie d'un LAG.

REMARQUE : si la configuration du port est modifiée pendant que le port est membre d'un LAG, cette modification prend effet uniquement une fois que le port a été supprimé du LAG.

Définitions des paramètres des ports

1. Affichez la page **Port Configuration (Configuration des ports)**.
2. Sélectionnez un port dans le champ **Port**.
3. Complétez les champs de la boîte de dialogue.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

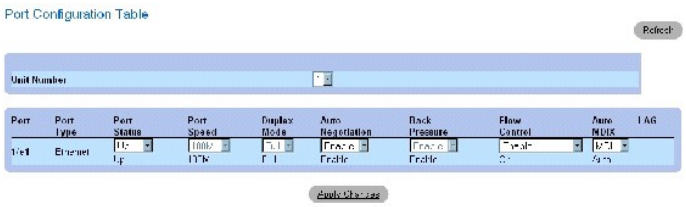
Les paramètres du port sont sauvegardés sur l'unité.

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 7-13. Port Configuration Table (Table de configuration des ports)



Configuration des ports à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la configuration des ports, comme indiqué à la page Port Configuration (Configuration des ports).

Tableau 7-6. Commandes CLI de configuration des ports

Commande CLI	Description
interface ethernet *interface*	Passe en mode de configuration de l'interface afin de configurer une interface de type ethernet.
description *chaîne*	Ajoute une description à une configuration d'interface.
shutdown	Désactive les interfaces qui font partie du contexte en cours de définition.
set interface active {**ethernet** *interface* | **port-channel** *numéro-canal-port*}	Réactive une interface qui a été désactivée pour des raisons de sécurité.
speed *Mbps*	Configure la vitesse d'une interface ethernet donnée lorsque la négociation automatiquement n'est pas utilisée.
duplex {half | full}	Configure le fonctionnement en mode duplex intégral/semi duplex d'une interface ethernet donnée, lorsque la négociation automatiquement n'est pas utilisée.
negotiation [fonction1 [fonction2... fonction5]	Active le fonctionnement de la négociation automatique pour les paramètres de vitesse et de mode duplex d'une interface donnée.
back-pressure	Active le mode contre-pression sur une interface donnée.
flowcontrol {auto | on | off}	Configure le contrôle de flux sur une interface donnée.
mdix {on | auto}	Active automatiquement l'inverseur sur une interface ou un canal de port donné.
show interfaces configuration [**ethernet** *interface* |**port-channel** *numéro-canal-port*]	Affiche la configuration de toutes les interfaces configurées.
show interface advertise	Affiche la configuration d'annonce de négociation de l'interface.
show interfaces status [**ethernet** *interface* | **port-channel** *numéro-canal-port*]	Affiche l'état de toutes les interfaces configurées.
show interfaces description [**ethernet** *interface* | **port-channel** *numéro-canal-port*]	Affiche la description de toutes les interfaces configurées.

Voici un exemple de commandes CLI :

```
console(config)# interface ethernet 1/e3

console(config-if)# description "RD SW#3"

console(config-if)# shutdown

console(config-if)# no shutdown

console(config-if)# speed 100

console(config-if)# duplex full

console(config-if)# negotiation

console(config-if)# back-pressure

console(config-if)# flowcontrol on

console(config-if)# mdix auto

console(config-if)# end

console# show interfaces configuration ethernet 1/e3
```

Port	Type	Duplex	Speed	Neg	Flow Control	Admin State	Back Pressure	Mdix Mode
----	----	------	-----	----	------	-----	------	----
1/e3	100	Full	100	Enabled	On	Up	Enable	Auto

Console# **show interfaces status**

Port	Type	Duplex	Speed	Neg	Flow Control	Link State	Back Pressure	Mdix Mode
----	----	------	-----	----	------	-----	------	----
1/e3	100	Full	100	Auto	On	Up	Enable	On
1/e4	100	Full	1000	Off	Off	Up	Disable	On

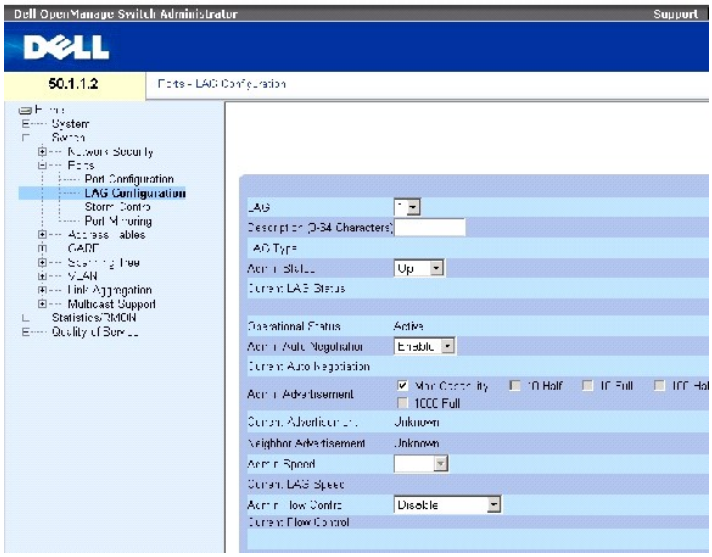
Ch	Type	Duplex	Speed	Neg	Flow Control	Back Pressure	Link State	
---	----	------	-----	-----	-------	--------	------	
1	1000	Full	1000	Off	Off	Disable	Up	

Définition des paramètres des LAG

La page **LAG Configuration (Configuration des LAG)** contient des champs permettant de configurer les paramètres des groupes de liaisons agrégées (LAG). L'unité prend en charge jusqu'à huit ports par LAG et huit LAG par système. Pour plus d'informations sur les LAG et sur l'affectation des ports aux LAG, consultez la section "**Agrégation des ports**".

Pour ouvrir la page **Port Configuration (Configuration des ports)**, cliquez sur Switch (Commutateurs) → Ports → LAG Configuration (Configuration des LAG) dans l'arborescence.

Figure 7-14. LAG Configuration (Configuration des LAG)



La page **LAG Configuration (Configuration des LAG)** contient les champs suivants :

LAG : numéro du LAG.

Description (0 - 64 Characters) (Description [0 à 64 caractères]) : description du LAG définie par l'utilisateur.

LAG Type (Type de LAG) : types de port inclus dans le LAG.

Admin Status (État admin) : active ou désactive le LAG sélectionné.

Current LAG Status (État actuel du LAG) : indique si le LAG est en fonctionnement.

Operational Status (État opérationnel) : active ou désactive le transfert du trafic sur le LAG sélectionné.

Admin Auto Negotiation (Négociation automatique admin) : active ou désactive la négociation automatique sur le LAG. La négociation automatique est un protocole entre deux partenaires de liaison, qui permet à un LAG d'informer son partenaire de sa vitesse de transfert, de son mode duplex et de ses capacités de contrôle de flux (fonction désactivée par défaut).

Current Auto Negotiation (Négociation automatique en cours) : configuration en cours de la négociation automatique.

Admin Advertisement (Annonce admin) : définit la configuration de la négociation automatique annoncée par le LAG. Ce champ peut prendre les valeurs suivantes :

Max Capability (Capacité maximale) : indique que toutes les vitesses et tous les modes Duplex sont acceptés.

10 Half (10 Mbps, semi duplex) : indique que le LAG annonce une vitesse de 10 Mbps en mode semi duplex.

10 Full (10 Mbps, duplex intégral) : indique que le LAG annonce une vitesse de 10 Mbps en mode duplex intégral.

100 Half (100 Mbps, semi duplex) : indique que le LAG annonce une vitesse de 100 Mbps en mode semi duplex.

100 Full (100 Mbps, duplex intégral) : indique que le LAG annonce une vitesse de 100 Mbps en mode duplex intégral.

1000 Full (1000 Mbps, duplex intégral) : indique que le LAG annonce une vitesse de 1000 Mbps en mode duplex intégral.

Current Advertisement (Annonce actuelle) : le LAG annonce sa vitesse au LAG voisin pour lancer le processus de négociation. Ce champ peut prendre les valeurs spécifiées dans le champ Admin Advertisement (Annonce admin).

Neighbor Advertisement (Annonce du LAG voisin) : indique les paramètres d'annonce du LAG voisin. Les valeurs de ce champ sont identiques à celles du champ **Admin Advertisement** (Annonce admin).

Admin Speed (Vitesse admin) : vitesse de fonctionnement du LAG.

Current LAG Speed (Vitesse actuelle du LAG) : vitesse de fonctionnement actuelle du LAG.

Admin Flow Control (Contrôle de flux admin) : active ou désactive le contrôle de flux, ou active la négociation automatique du contrôle de flux pour le LAG. Le mode Flow Control (Contrôle de flux) est activé sur les ports configurés en duplex intégral dans le LAG.

Current Flow Control (Contrôle de flux actuel) : configuration de contrôle de flux définie par l'utilisateur.

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

Les paramètres du LAG sont sauvegardés sur l'unité.

Modification des paramètres des LAG

1. Affichez la page **LAG Configuration (Configuration des LAG)**.
2. Sélectionnez un LAG dans le champ **LAG**.
3. Modifiez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

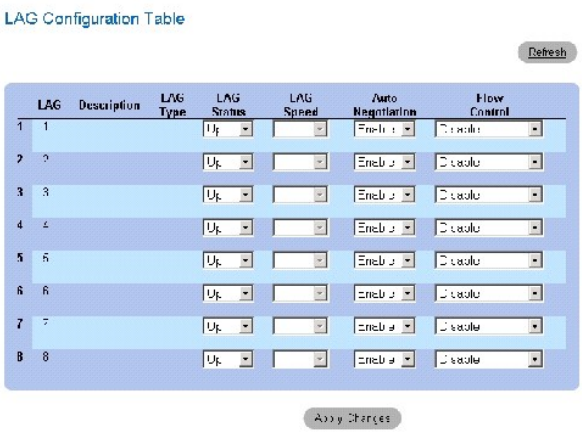
Les paramètres du LAG sont sauvegardés sur l'unité.

Affichage de la table de configuration des LAG

1. Affichez la page **LAG Configuration (Configuration des LAG)**.
2. Cliquez sur **Show All** (Afficher tout).

La page **LAG Configuration Table (Table de configuration des LAG)** s'affiche.

Figure 7-15. LAG Configuration Table (Table de configuration des LAG)



Configuration des LAG à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la configuration des LAG, comme indiqué à la page **LAG Configuration (Configuration des LAG)**.

Tableau 7-8. Commandes CLI relatives à la configuration des LAG

Commande CLI	Description
interface port-channel *numéro-canal-port*	Active le mode de configuration d'interface d'un canal de port spécifique.
description *chaîne*	Ajoute une description à une configuration d'interface.
shutdown	Désactive les interfaces qui font partie du contexte en cours de définition.
speed *bps*	Configure la vitesse d'une interface ethernet donnée lorsque la négociation automatiquement n'est pas utilisée.
negotiation [fonction1 [fonction2... fonction5]	Active la négociation automatique de la vitesse de l'interface.
back-pressure	Active le mode contre-pression sur une interface donnée.
flowcontrol {auto | on | off}	Configure le contrôle de flux sur une interface donnée.
show interfaces configuration [**ethernet** *interface* |**port-channel** *numéro-canal-port*]	Affiche la configuration de toutes les interfaces configurées.
show interfaces status [**ethernet** *interface* | **port-channel** *numéro-canal-port*]	Affiche l'état de toutes les interfaces configurées.
show interfaces description [**ethernet** *interface* |**port-channel** *numéro-canal-port*]	Affiche la description de toutes les interfaces configurées.
show interfaces port-channel [*numéro-canal-port*]	Affiche les informations sur les ports (appartenance à un canal et état actif ou inactif).

Voici un exemple de commandes CLI :

```
console(config)# interface port-channel 2

console(config-if)# no negotiation

console(config-if)# speed 100

console(config-if)# flowcontrol on

console(config-if)# exit
```

```
console(config)# interface port-channel 3

console(config-if)# shutdown

console(config-if)# exit

console(config)# interface port-channel 4

console(config-if)# back-pressure

console(config-if)# description p4

console(config-if)# end

console# show interfaces port-channel
```

Channel	Ports
---------	---------
ch1	Inactive: 1/e(11-13)
ch2	Active: 1/e14

Activation de la fonction 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 à ces messages étant envoyées sur l'ensemble du réseau, elles risquent de surcharger les ressources du réseau ou d'entraîner des dépassements de délai.

La fonction Storm Control est activée au niveau de chaque port, en définissant le type de paquet et la vitesse à laquelle les paquets sont transmis.

Le système mesure la fréquence des trames de diffusion, de monodiffusion et de multidiffusion entrantes séparément sur chaque port. Il rejette les trames lorsque cette fréquence dépasse une limite définie par l'utilisateur.

La page **Storm Control** contient des champs permettant d'activer et de configurer la fonction Storm Control. Pour ouvrir la page **Storm Control**, cliquez sur Switch (Commutateur) → Ports → Storm Control dans l'arborescence.

Figure 7-16. Storm Control

La page **Storm Control** contient les champs suivants :

Port : port sur lequel la fonction Storm Control est activée.

Broadcast Control (Contrôle de diffusion) : permet d'activer ou désactiver le transfert de paquets de diffusion sur l'interface.

Broadcast Mode (Mode diffusion) : indique le mode de diffusion actuellement activé sur l'unité ou la pile. Ce champ peut prendre les valeurs suivantes :

Unknown Unicast, Multicast & Broadcast (Monodiffusion inconnu, Multidiffusion et Diffusion) : comptabilise le trafic de monodiffusion, de multidiffusion et de diffusion.

Multicast & Broadcast (Multidiffusion et Diffusion) : comptabilise simultanément le trafic de diffusion et de multidiffusion.

Broadcast Only (Diffusion uniquement) : comptabilise uniquement le trafic de diffusion.

Broadcast Rate Threshold (70-285000) (Vitesse de diffusion maximale [70 à 285000]) : vitesse maximum (en kilo-octets par seconde) de transfert des paquets inconnus. Les valeurs possibles vont de 70 à 285000 kilo-octets par seconde.

Activation de la fonction Storm Control

1. Affichez la page **Storm Control**.
2. Sélectionnez une interface sur laquelle mettre en uvre la fonction Storm Control.
3. Complétez les champs avec les valeurs appropriées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La fonction Storm Control est activée.

Modification des paramètres des ports pour la fonction Storm Control

1. Affichez la page **Storm Control**.
2. Modifiez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

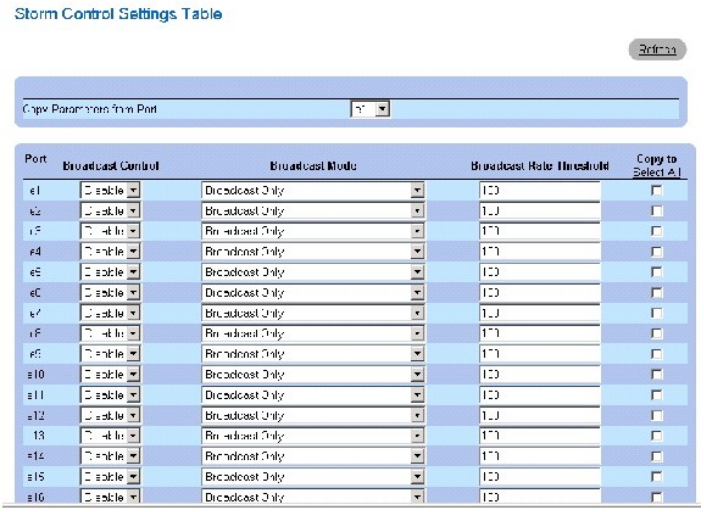
Les paramètres des ports pour la fonction Storm Control sont sauvegardés sur l'unité.

Affichage de la table des paramètres des ports

1. Affichez la page **Storm Control**.
2. Cliquez sur **Show All** (Afficher tout).

La page **Storm Control Settings Table (Table des paramètres Storm Control)** s'affiche.

Figure 7-17. Storm Control Settings Table (Table des paramètres Storm Control)



Outre les champs de la page Storm Control, la page Storm Control Settings Table (Table des paramètres Storm Control) contient les champs supplémentaires suivants :

Copy Parameters from Port (Copier les paramètres à partir du port) : indique le port spécifique à partir duquel les paramètres Storm Control sont copiés.

Copie de paramètres dans la table Storm Control

1. Affichez la page **Storm Control**.
2. Cliquez sur **Show All** (Afficher tout).

La page **Storm Control Settings Table (Table des paramètres Storm Control)** s'affiche.

3. Dans le champ **Copy Parameters from Port** (Copier les paramètres à partir du port), sélectionnez le port à partir duquel les paramètres sont copiés.
4. Cochez la case **Copy to** (Copier vers) pour définir les interfaces vers lesquelles les définitions Storm Control sont copiées, ou cliquez sur **Select All** (Sélectionner tout) pour copier les définitions sur tous les ports.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont copiés vers les ports sélectionnés dans la **table des paramètres Storm Control** et l'unité est mise à jour.

Configuration de la fonction Storm Control à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la configuration de la fonction Storm Control, comme indiqué à la page **Storm Control**.

Tableau 7-7. Commandes CLI relatives à la fonction Storm Control

Commande CLI	Description

`port storm-control include-multicast`	Permet à l'unité de comptabiliser simultanément les paquets multidiffusion, monodiffusion et diffusion.
`port storm-control broadcast enable`	Active la fonction Storm Control.
`port storm-control broadcast rate`	Configure la vitesse de diffusion maximale.
`show ports storm-control` *port*	Affiche la configuration de la fonction Storm Control.

Voici un exemple de commandes CLI :

```
console(config)# port storm-control include-multicast

console(config)# interface ethernet 1/e1

console(config-if)# port storm-control broadcast enable

console(config-if)# port storm-control broadcast rate 100000

console(config-if)# end

console# show ports storm-control
```

Port	Broadcast Storm control [kbyes/sec]
----	----------
1/e1	8000
2/e1	Disabled
3/e2	Disabled

Définition de sessions de mise en miroir des ports

La mise en miroir des ports :

- Contrôle et met en miroir le trafic réseau en transférant des copies des paquets entrants et sortants depuis un port vers un port de contrôle.
- Peut être utilisée comme outil de diagnostic et/ou de débogage.

- Permet de surveiller les performances de l'unité.

Cette mise en miroir est configurée en sélectionnant un port spécifique vers lequel copier tous les paquets, et différents ports à partir desquels les paquets sont dupliqués.

Avant de configurer la fonction de mise en miroir des ports, notez bien ce qui suit :

- La mise en miroir des ports surveille et met en miroir le trafic réseau en transmettant des copies des paquets entrants et sortants, depuis un port contrôlé jusqu'à un port de contrôle.
- Les ports contrôlés ne peuvent pas fonctionner plus rapidement que les ports de contrôle.
- Tous les paquets RX/TX doivent être contrôlés sur le même port.

Les restrictions suivantes s'appliquent aux ports configurés pour être des ports de destination :

- Les ports ne peuvent pas être configurés comme ports sources.
- Les ports ne peuvent pas être membres d'un LAG.
- Des interfaces IP ne sont pas configurées sur le port.
- GVRP n'est pas activé sur le port.
- Le port n'est pas membre d'un VLAN.
- Un seul port de destination peut être défini.

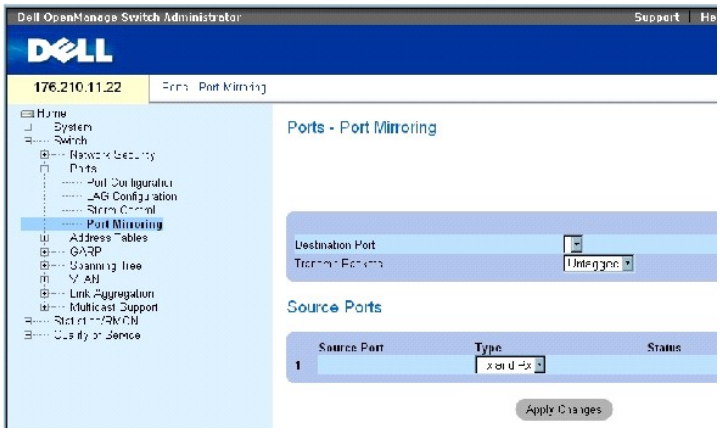
Les restrictions suivantes s'appliquent aux ports configurés pour être des ports sources :

- Les ports sources ne peuvent pas être membres d'un LAG.
- Les ports ne peuvent pas être configurés comme ports de destination.
- Jusqu'à 8 ports sources sont pris en charge.

Pour ouvrir la page **Port Mirroring (Mise en miroir des ports)**, cliquez sur **Switch** (Commutateur) → **Ports** → **Port Mirroring** (Mise en miroir des ports) dans l'arborescence.

REMARQUE : lorsqu'un port est défini comme port cible d'une session de mise en miroir des ports, toutes les opérations courantes sont interrompues sur ce port. Cela inclut Spanning Tree et LACP.

Figure 7-18. Port Mirroring (Mise en miroir des ports)



La page Port Mirroring (Mise en miroir des ports) contient les champs suivants :

Destination Port (Port de destination) : numéro du port vers lequel le trafic est copié.

Transmit Packets (Type de paquets transmis) : définit la méthode de mise en miroir des paquets. Ce champ peut prendre les valeurs suivantes :

Untagged (Non balisés) : met en miroir les paquets en tant que paquets VLAN non balisés. Il s'agit de la valeur par défaut.

Tagged (Balisés) : met en miroir les paquets en tant que paquets VLAN balisés.

Type : indique si les paquets mis en miroir sont de type RX, TX ou RX et TX.

Status(État) : indique si le port est sous contrôle (**Active**) ou non (**Ready**).

Remove (Supprimer) : supprime la session de mise en miroir des ports.

Ajout d'une session de mise en miroir des ports

1. Affichez la page Port Mirroring (Mise en miroir des ports).
2. Cliquez sur **Add** (Ajouter).

La page **Add Source Port** (Ajouter un port source) s'affiche.

3. Définissez les champs **Source Port** (Port source) et **Type**.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).
5. Sélectionnez le port de destination dans le menu déroulant **Destination Port** (Port de destination).
6. Cliquez sur le bouton **Refresh** (Actualiser) de la page Port Mirroring (Mise en miroir des ports).
7. Complétez le champ **Tagged Packets** (Paquets balisés).
8. Complétez le champ **Type**.
9. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau port source est défini et l'unité est mise à jour.

Suppression d'un port de duplication d'une session de mise en miroir des ports

1. Affichez la page Port Mirroring (Mise en miroir des ports).
2. Cochez la case **Remove** (Supprimer).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La session de mise en miroir des ports sélectionnée est supprimée et l'unité est mise à jour.

S'il y a plusieurs ports, seul le port sélectionné est supprimé de la session de mise en miroir des ports.

Le tableau suivant récapitule les commandes CLI équivalentes permettant la configuration d'une session de mise en miroir des ports, comme indiqué à la page Port Mirroring (Mise en miroir des ports).

Tableau 7-8. Commandes CLI relatives à la mise en miroir des ports

Commande CLI	Description
port monitor *src*-interface [**rx** | **tx**]	Démarre une session de surveillance des ports.

Voici un exemple de commandes CLI :

```
console(config)# interface ethernet
1/e1


console(config-if)# port monitor 1/e2


console(config-if)# end


console# show ports monitor
```

Source Port	Destination Port	Type	Status	VLAN Tagging
---	---	---	---	---
1/e2	1/e1	RX, TX	Active	No

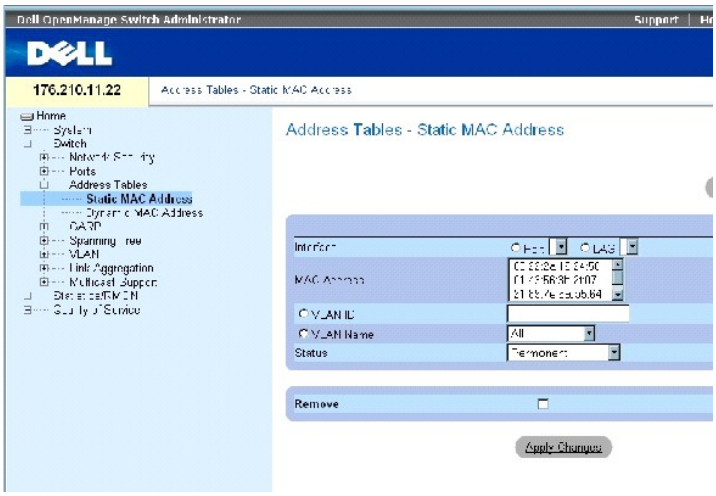
Configuration des tables d'adresses

Les adresses MAC sont stockées soit dans la base de données d'adresses statiques, soit dans la base de données d'adresses dynamiques. Un paquet adressé à une destination stockée dans l'une des bases de données est transmis immédiatement au port. La table des adresses dynamiques peut être triée par interface, par VLAN et par adresse MAC. Les adresses MAC sont apprises de façon dynamique au fur et à mesure que les paquets arrivent sur l'unité. Les adresses sont associées aux ports grâce à l'apprentissage effectué à partir de l'adresse source des trames. Les trames envoyées à une adresse MAC de destination qui n'est associée à aucun port sont acheminées simultanément vers tous les ports du VLAN correspondant. Les adresses statiques sont configurées manuellement. Pour empêcher un débordement de la table de pontage, les adresses MAC dynamiques sont effacées si elles ne sont utilisées par aucun trafic après un certain délai. Pour ouvrir la page Address Tables (Tables d'adresses), cliquez sur Switch (Commutateur) → Address Tables (Tables d'adresses) dans l'arborescence.

Définition d'adresses statiques

La page Static MAC Address Table (Table des adresses MAC statiques) contient une liste d'adresses MAC statiques. Une adresse statique peut être ajoutée et supprimée de la page Static MAC Address Table (Table des adresses MAC statiques). En outre, plusieurs adresses MAC peuvent être définies pour un seul port. Pour ouvrir la page Static MAC Address Table (Table des adresses MAC statiques), cliquez sur Switch (Commutateur) → Address Tables (Tables d'adresses) → Static Address Table (Table des adresses statiques) dans l'arborescence.

Figure 7-19. Static MAC Address Table (Table des adresses MAC statiques)



La page Static MAC Address Table (Table des adresses MAC statiques) contient les champs suivants :

Interface : port ou LAG spécifique auquel l'adresse MAC statique s'applique.

MAC Address (Adresse MAC) : adresses MAC répertoriées dans la liste actuelle des adresses statiques.

VLAN ID (ID du VLAN) : ID du VLAN associé à l'adresse MAC.

VLAN Name (Nom du VLAN) : nom de VLAN défini par l'utilisateur.

Status (État) : état de l'adresse MAC. Ce champ peut prendre les valeurs suivantes :

Secure (Sécurisé) : permet de définir des adresses MAC statiques pour les ports verrouillés.

Permanent : l'adresse MAC est permanente.

Delete on Reset (Supprimer à la réinitialisation) : l'adresse MAC est supprimée lors de la réinitialisation de l'unité.

Delete on Timeout (Supprimer à l'expiration) : l'adresse MAC est supprimée à l'expiration d'un délai.

REMARQUE : pour empêcher la suppression des adresses MAC statiques lors de la réinitialisation de l'unité Ethernet, vérifiez que le port associé à l'adresse MAC est verrouillé.

Remove (Supprimer) : permet de supprimer l'adresse MAC sélectionnée de la table d'adresses MAC.

Ajout d'une adresse MAC statique

1. Affichez la page Static MAC Address Table (Table des adresses MAC statiques).
2. Cliquez sur **Add** (Ajouter).

La page **Add Static MAC Address** (Ajout d'une adresse MAC statique) s'affiche.

3. Complétez les champs.

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

La nouvelle adresse statique est ajoutée à la **table des adresses MAC statiques** et l'unité est mise à jour.

Modification d'une adresse statique dans la table des adresses MAC statiques

1. Affichez la page Static MAC Address Table (Table des adresses MAC statiques).
2. Sélectionnez une interface.
3. Modifiez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse MAC statique est modifiée et l'unité est mise à jour.

Suppression d'une adresse statique de la table des adresses statiques

1. Affichez la page Static MAC Address Table (Table des adresses MAC statiques).
2. Choisissez une interface.
3. Cliquez sur **Show All** (Afficher tout).

La page **Static MAC Address Table** (Table des adresses MAC statiques) s'affiche.

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

L'adresse statique sélectionnée est supprimée et l'unité est mise à jour.

Configuration des paramètres des adresses statiques à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la configuration des adresses statiques, comme indiqué à la page Static MAC Address Table (Table des adresses MAC statiques).

Tableau 7-9. Commandes CLI relatives aux adresses statiques

Commande CLI	Description
bridge address *adresse-mac* [permanent | delete-on-reset | delete-on-timeout | secure] {ethernet interface | port-channel *numéro-canal-port*}	Ajoute une adresse statique source correspondant à une station de couche MAC à la table de pontage.
show bridge address-table [vlan *vlan*] [ethernet *interface* | port-channel *numéro-canal-port*]	Affiche les entrées de la base de données de transfert de pont.

Voici un exemple de commandes CLI :

```
console(config-if)#bridge address 00:60:70:4C:73:FF permanent ethernet g8

console# show bridge address-table

Aging time is 300 sec

vlan    mac address                port    type
```

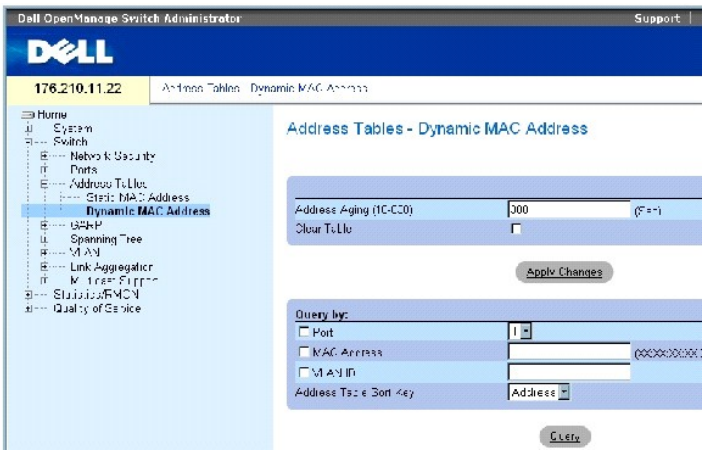
----	----------	----	--------
1	00:60:70:4C:73:FF	1/e8	dynamic
1	00:60:70:8C:73:FF	1/e8	dynamic
200	00:10:0D:48:37:FF	1/e9	static

Affichage des adresses dynamiques

La page **Dynamic MAC Address (Adresse MAC dynamique)** contient des informations pour l'interrogation de la table des adresses dynamiques, notamment le type d'interface, les adresses MAC, le VLAN et le tri de la table. Les paquets transmis à une adresse stockée dans la table des adresses sont transférés directement à ces ports. La page **Dynamic MAC Address (Adresse MAC dynamique)** contient également des informations sur le délai d'expiration avant la suppression d'une adresse MAC dynamique, et inclut des paramètres permettant d'interroger et d'afficher la liste des adresses dynamiques. La table des adresses en cours contient des paramètres d'adresses dynamiques selon lesquels les paquets sont transférés directement aux ports.

Pour ouvrir la page **Dynamic MAC Address (Adresse MAC dynamique)**, cliquez sur Switch (Commutateurs) → Address Tables (Tables d'adresses) → Dynamic **MAC Address** (Adresse MAC dynamique) dans l'arborescence.

Figure 7-20. Dynamic MAC Address (Adresse MAC dynamique)



La page **Dynamic MAC Address (Adresse MAC dynamique)** contient les champs suivants :

Address Aging (10-630) (Expiration de l'adresse [10 à 630]) : indique la durée pendant laquelle l'adresse MAC reste dans la liste Dynamic MAC Address (Adresse MAC dynamique) avant qu'elle n'arrive à expiration si aucun trafic provenant de la source n'est détecté. La valeur par défaut est de 300 secondes.

Clear Table (Effacer la table) : efface la table d'adresses dynamiques.

Port : indique l'interface pour laquelle la table est interrogée. Deux types d'interface sont disponibles.

MAC Address (Adresse MAC) : indique l'adresse MAC pour laquelle la table est interrogée.

VLAN ID (ID du VLAN) : ID du VLAN pour lequel la table est interrogée.

Address Table Sort Key (Clé de tri de la table d'adresses) : indique la méthode de tri appliquée à la table d'adresses dynamiques. La table d'adresses peut être triée par adresse, par VLAN ou par interface.

Redéfinition du délai d'expiration

1. Affichez la page **Dynamic MAC Address (Adresse MAC dynamique)**.
2. Définissez le champ **Aging Time** (Délai d'expiration).
3. Cliquez sur Apply Changes (Appliquer les modifications).

Le délai d'expiration est modifié et l'unité est mise à jour.

Interrogation de la table des adresses dynamiques

1. Affichez la page **Dynamic MAC Address (Adresse MAC dynamique)**.
2. Définissez le paramètre en fonction duquel la **table des adresses dynamiques** doit être interrogée.

Les entrées peuvent être interrogées par **port**, par **adresse MAC** ou par **ID de VLAN**.

3. Cliquez sur **Query** (Interroger).

La table Dynamic MAC Address (Adresse MAC dynamique) est interrogée.

Tri de la table des adresses dynamiques

1. Affichez la page **Dynamic MAC Address (Adresse MAC dynamique)**.
2. Dans le menu déroulant **Address Table Sort Key** (Clé de tri de la table d'adresses), choisissez le type de tri souhaité : par adresse, par ID de VLAN ou par interface.
3. Cliquez sur **Query** (Interroger).

La table Dynamic MAC Address (Adresse MAC dynamique) est triée.

Interrogation et tri des adresses dynamiques à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant l'expiration, l'interrogation et le tri des adresses dynamiques, comme indiqué à la page Dynamic MAC Address (Adresse MAC dynamique).

Tableau 7-10. Commandes CLI d'interrogation et de tri

Commande CLI	Description
bridge aging-time *secondes*	Définit le délai d'expiration de la table d'adresses.
show bridge address-table [**vlan** *vlan*] [**ethernet** *interface* | **port-channel** *numéro-canal-port*]	Affiche les classes des entrées créées de façon dynamique dans la base de données de transfert de pont.

Voici un exemple de commandes CLI :

```
console (config)# bridge aging-time 250

console (config)# end

console# show bridge address-table

```

```
Aging time is 250 sec
```

vlan	mac address	port	type
----	-----------	----	----
1	00:60:70:4C:73:FF	1/e8	dynamic
1	00:60:70:8C:73:FF	1/e8	dynamic
200	00:10:0D:48:37:FF	1/e8	static

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 périphériques intéressés par un attribut de réseau donné, tel qu'un VLAN ou une adresse de multidiffusion.

Lors de la configuration du protocole GARP, vérifiez les points suivants :

- Le délai de sortie (Leave) doit être supérieur ou égal à trois fois le délai de jonction (Join).
- Le délai général de sortie (Leave all) doit être supérieur au délai de sortie (Leave).
- Définissez les mêmes délais GARP pour tous les périphériques de couche 2 connectés. Sinon, l'application GARP ne fonctionnera pas correctement.

Pour ouvrir la page **GARP**, cliquez sur **Switch** (Commutateur) → **GARP** dans l'arborescence.

Définition des temporisateurs GARP

La page GARP Timers (Temporisateurs GARP) contient des champs permettant d'activer GARP sur l'unité. Pour ouvrir la page GARP Timers (Temporisateurs GARP), cliquez sur **Switch** (Commutateur) → **GARP** → **GARP Timers** (Temporisateurs GARP) dans l'arborescence.

Figure 7-21. GARP Timers (Temporisateurs GARP)

La page GARP Timers (Temporisateurs GARP) contient les champs suivants :

Interface : permet de sélectionner un port ou un LAG pour modifier les temporisateurs GARP.

GARP Join Timer (10- 2147483640) (Temporisateur "Join" GARP [10 à 2147483640]) : durée en millisecondes pendant laquelle des PDU sont transmises. La valeur par défaut est de 200 millisecondes.

GARP Leave Timer (10- 2147483640) (Temporisateur "Leave" GARP [10 à 2147483640]) : durée en millisecondes pendant laquelle l'unité 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). La valeur par défaut est de 600 millisecondes.

GARP Leave All Timer (10- 2147483640) (Temporisateur Leave All GARP [10 à 2147483640]) : durée en millisecondes pendant laquelle toutes les unités attendent avant de quitter l'état GARP. Le délai général de sortie (Leave all) doit être supérieur au délai de sortie (Leave). La valeur par défaut est de 10000 millisecondes.

Définition des temporisateurs GARP

1. Affichez la page GARP Timers (Temporisateurs GARP).
2. Sélectionnez une interface.
3. Complétez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres GARP sont sauvegardés sur l'unité.

Copie de paramètres dans la table 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. Sélectionnez le type d'interface dans le champ **Copy Parameters from** (Copier les paramètres à partir de).
4. Sélectionnez une interface dans le menu déroulant **Port** ou **LAG**.

Les définitions de cette interface sont copiées vers les interfaces sélectionnées. Voir l'étape 6.

5. Cochez la case **Copy to** (Copier vers) pour définir les interfaces vers lesquelles les définitions des temporisateurs GARP sont copiées, ou cliquez sur **Select All** (Sélectionner tout) pour copier les définitions vers tous les ports.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont copiés vers les ports ou LAG sélectionnés dans la **table des temporisateurs GARP** et l'unité est mise à jour.

Définition des temporisateurs GARP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la définition des temporisateurs GARP, comme indiqué à la page GARP Timers (Temporisateurs GARP).

Tableau 7-11. Commandes CLI relatives aux temporisateurs GARP

Commande CLI	Description
garp timer {join | leave | leaveall} *valeur_temporisateur*	Règle les valeurs des temporisateurs GARP "Join", "Leave" et "Leave All" de l'application GARP.

Voici un exemple de commandes CLI :

```
```

```
console(config)# interface ethernet 1/e1

console(config-if)# garp timer leave 900

console(config-if)# end

console# show gvrp configuration ethernet 1/e11


GVRP Feature is currently Disabled on the device.

Maximum VLANs: 223
```

Port (s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
1/e11	Disabled	Normal	Enabled	200	900	10000

Configuration du protocole STP

Le protocole STP (Spanning Tree) fournit une topographie en arborescence, quelle que soit l'architecture des ponts. Il fournit un chemin unique entre les stations terminales sur un réseau et élimine ainsi la formation de boucles.

Les boucles se produisent lorsqu'il existe des itinéraires secondaires entre les hôtes. Dans un réseau étendu, elles risquent d'entraîner une réduction des performances, car les ponts transmettent le trafic correspondant indéfiniment.

L'unité prend en charge les versions suivantes du protocole STP :

- Classic STP : fournit un chemin unique entre les stations terminales et élimine ainsi la formation de boucles. Pour plus d'informations sur la configuration du protocole Classic STP, consultez la section "**Définition des paramètres globaux STP**".
- Rapid STP : détecte et utilise des topologies de réseau qui permettent une convergence plus rapide de la topologie Spanning Tree sans création de boucles de transmission. Si le protocole Rapid STP est activé sur l'unité mais que l'unité voisine est configurée en mode STP, l'unité locale utilise le protocole STP.

  Pour plus d'informations sur la configuration du protocole Rapid STP, consultez la section "**Définition de Rapid Spanning Tree (RSTP)**".
- Multiple STP : offre une connectivité totale pour les paquets associés à n'importe quel VLAN. Ce protocole repose sur le protocole RSTP. En outre, il transmet les paquets associés à différents VLAN via des régions MST différentes. Les régions MST se comportent comme un seul pont si le protocole MSTP est activé sur l'unité. Cependant, si RSTP est activé sur l'unité voisine et que l'unité locale utilise les protocoles STP, RSTP et MSTP, les deux unités peuvent interagir.

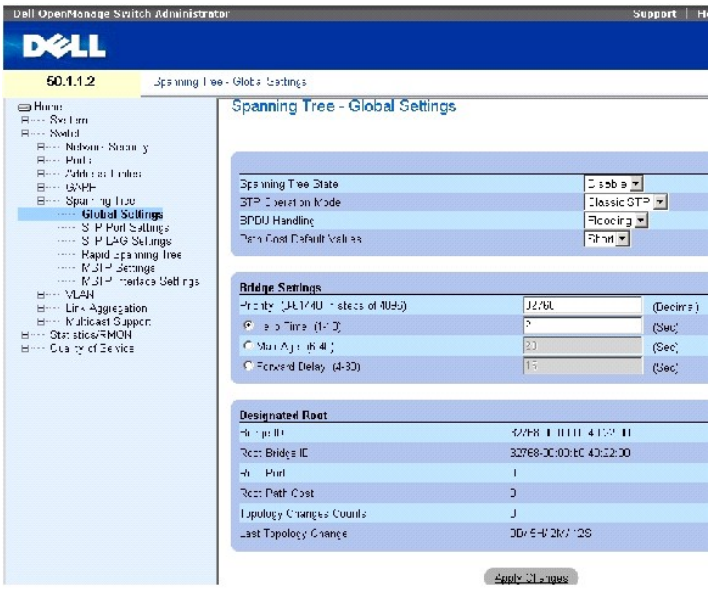
Pour plus d'informations sur la configuration du protocole Multiple STP, consultez la section "**Configuration de Multiple Spanning Tree (MSTP)**".

Pour ouvrir la page **Spanning Tree**, cliquez sur **Switch** (Commutateur) → **Spanning Tree** dans l'arborescence.

Définition des paramètres globaux STP

La page Spanning Tree Global Settings (Paramètres globaux STP) contient des paramètres permettant d'activer le protocole STP sur l'unité. Pour ouvrir la page Spanning Tree Global Settings (Paramètres globaux STP), cliquez sur **Switch** (Commutateur) → **Spanning Tree** → **Global Settings** (Paramètres globaux) dans l'arborescence.

Figure 7-22. Spanning Tree Global Settings (Paramètres globaux STP)



La page Spanning Tree Global Settings (Paramètres globaux STP) contient les champs suivants :

Spanning Tree State (État de la topologie Spanning Tree) : active ou désactive le protocole STP, Rapid STP ou MSTP sur l'unité.

STP Operation Mode (Mode de fonctionnement STP) : indique le mode STP pour lequel STP est activé sur l'unité. Ce champ peut prendre les valeurs suivantes :

Classic STP : active le mode STP classique sur l'unité. Il s'agit de la valeur par défaut.

Rapid STP : active le mode Rapid STP sur l'unité.

Multiple STP : active le mode Multiple STP sur l'unité.

BPDU Handling (Gestion des BPDU) : détermine comment les paquets BPDU sont gérés lorsque le protocole STP est activé sur le port ou l'unité. Les BPDU servent à transmettre les informations relatives au Spanning Tree. Ce champ peut prendre les valeurs suivantes :

Filtering (Filtrage) : filtre les paquets BPDU lorsque le Spanning Tree est désactivé sur une interface. Il s'agit de la valeur par défaut.

Flooding (Acheminement simultané) : achemine simultanément les paquets BPDU lorsque le Spanning Tree est désactivé sur une interface.

Path Cost Default Values (Valeurs par défaut du coût de résolution) : spécifie la méthode utilisée pour associer le coût de résolution par défaut aux ports STP. Ce champ peut prendre les valeurs suivantes :

Short (Court) : spécifie une plage de valeurs comprises entre 1 et 65535 pour le coût de résolution des ports. Il s'agit de la valeur par défaut.

Long (Long) : spécifie une plage de valeurs comprises entre 1 et 200000000 pour le coût de résolution des ports.

Le coût de résolution par défaut associé à une interface varie selon la méthode sélectionnée :

Interface	Long	Court
LAG	20,000	4
1000 Mbps	20,000	4
100 Mbps	200,000	19
10 Mbps	2,000,000	100

Priority (0-65535) (Priorité [0 à 65535]) : indique la valeur de priorité des ponts. Lorsque des commutateurs ou des ponts utilisent le protocole STP, une priorité est affectée à chacun d'eux. Après avoir échangé des BPDU, l'unité possédant la valeur de priorité la plus basse devient le pont racine. La valeur par défaut est de 32768. La valeur de priorité du port est exprimée par incréments de 4096 ; par exemple, 4096, 8192, 12288, etc.

Hello Time (1-10) : indique le délai Hello Time de l'unité. Il s'agit de la durée en secondes pendant laquelle un pont racine attend entre les messages de configuration. La valeur par défaut est de 2 secondes.

Max Age (6-40) (Délai d'attente maximal [6 à 40]) : indique le délai d'attente maximal de l'unité. Le délai d'attente maximal indique la durée en secondes pendant laquelle un pont attend avant d'envoyer des messages de configuration. Le délai d'attente maximal par défaut est de 20 secondes.

Forward Delay (4-30) (Délai avant transfert [4 à 30]) : indique le délai avant transfert observé par l'unité. Le délai avant transfert indique la durée en secondes pendant laquelle un pont reste dans un état d'écoute et d'apprentissage avant de transférer des paquets. La valeur par défaut est de 10 secondes.

Bridge ID (ID pont) : identifie la priorité du pont et l'adresse MAC.

Root Bridge ID (ID pont racine) : identifie la priorité du pont racine et l'adresse MAC.

Root Port (Port racine) : indique le numéro du port qui présente le coût de résolution le plus faible entre ce pont et le pont racine. Cette valeur est significative lorsque le pont n'est pas le pont racine.

Root Path Cost (Coût de résolution racine) : coût de résolution entre ce pont et la racine.

Topology Changes Counts (Nombre de modifications de topologie) : indique le nombre total de modifications de l'état STP qui se sont produites.

Last Topology Change (Dernière modification de topologie) : indique la durée qui s'est écoulée depuis l'initialisation ou réinitialisation du pont ou depuis la dernière modification topographique. L'heure s'affiche au format J/H/M/S, par exemple, 2J/5H/10M/4S.

Définition des paramètres globaux STP

1. Affichez la page appropriée.
2. Sélectionnez **Enable** (Activer) dans le champ **Spanning Tree State** (État de la topologie Spanning Tree).
3. Sélectionnez le mode **STP** dans le champ **STP Operation Mode** (Mode de fonctionnement STP) et définissez les paramètres de pont.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le protocole STP est activé sur l'unité.

Modification des paramètres globaux STP

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

Les paramètres STP sont modifiés et l'unité est mise à jour.

Définition des paramètres globaux STP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la définition des paramètres globaux STP, comme indiqué à la page Spanning Tree Global Settings (Paramètres globaux STP).

Tableau 7-12. Commandes CLI relatives aux paramètres globaux STP

Commande CLI	Description
`spanning-tree`	Active le protocole SPT.
`spanning-tree mode {stp | rstp | mstp}`	Configure le mode du protocole STP.
`spanning-tree priority priorité`	Configure la priorité du protocole SPT.
`spanning-tree hello-time secondes`	Configure le délai Hello Time du réseau, qui correspond à la fréquence à laquelle l'unité diffuse des messages Hello aux autres unités.
`spanning-tree max-age secondes`	Configure le délai d'attente maximal du pont SPT.
`spanning-tree forward- time secondes`	Configure le délai avant transfert du pont SPT, qui correspond à la durée pendant laquelle un port reste dans un état d'écoute et d'apprentissage avant de passer à l'état de transfert.
`show spanning-tree [ethernet interface | port-channel numéro- canal-port] [instance id-instance]`	Affiche la configuration du procole STP.
`show spanning-tree [detail] [active | blockedports] [instance id-instance]`	Affiche des informations détaillées relatives au protocole STP sur les ports actifs ou bloqués.
`show spanning-tree mst- configuration`	Affichage l'identificateur de la configuration MST du protocole STP.

Voici un exemple de commandes CLI :

```
console(config)# spanning-tree

console(config)# spanning-tree mode rstp

console(config)# spanning-tree priority 12288

console(config)# spanning-tree hello-time 5
```

```
console(config)# spanning-tree max-age 12

console(config)# spanning-tree forward-time 25

console(config)# exit

console# show spanning-tree
```

```
Spanning tree enabled mode MSTP

Default port cost method: short

Gathering information .........

###### MST 0 Vlans Mapped:                16-4094

CST Root ID Priority 20480

           Address                        00:30:ab:00:00:08

           Path Cost                      4

           Root Port                      ch2

           This switch is the IST master

           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority                        32768

           Address                        00:00:00:16:00:64

           Max hops                       20
```

Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
1/e2	enabled	128.2	100	DSBL	Dsbl	No	P2p Intr
1/e3	enabled	128.3	100	DSBL	Dsbl	No	P2p Intr
1/e4	enabled	128.4	100	DSBL	Dsbl	No	P2p Intr

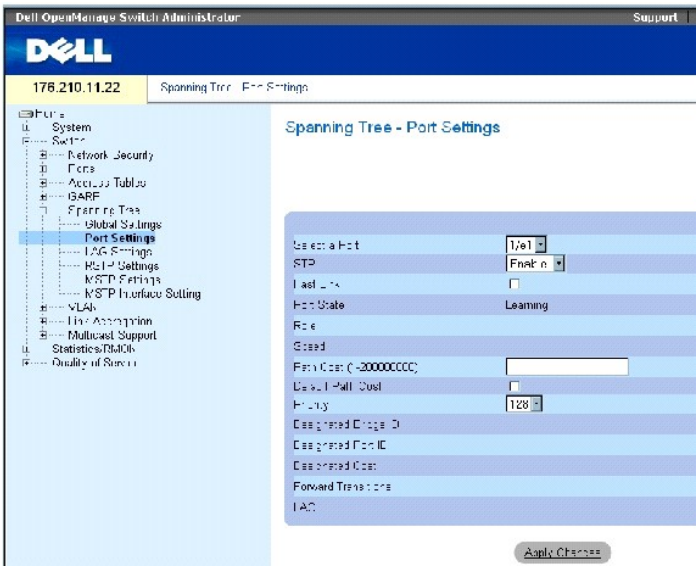
1/e5	enabled	128.5	19	FRW	Desg	Yes	P2p Intr
1/e6	enabled	128.6	100	DSBL	Dsbl	No	P2p Intr
1/e7	enabled	128.7	100	DSBL	Dsbl	No	P2p Intr
1/e8	enabled	128.8	100	DSBL	Dsbl	No	P2p Intr
1/e9	enabled	128.9	100	DSBL	Dsbl	No	P2p Intr
1/e10	enabled	128.10	100	DSBL	Dsbl	No	P2p Intr
1/e11	enabled	128.11	19	DSBL	Desg	Yes	P2p Intr
console# show spanning-tree active							
Spanning tree enabled mode MSTP							
Default port cost method: short							
Gathering information							
###### MST 0 Vlans Mapped: 16-4094							
CST Root ID Priority 20480							
	Address		00:30:ab:00:00:08				
	Path Cost		4				
	Root Port		ch2				
	This switch is the IST master						
	Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec						
Bridge ID Priority			32768				
	Address		00:00:00:16:00:64				
	Max hops		20				
Name	State	Prio.Nbr	Cost	Sts	Role	PortFast	Type
----	-----	-------	----	---	----	-------	----

1/e5	enabled	128.2	19	FRW	Desg	Yes	P2p Intr
1/e7	enabled	128.7	19	DSCR	Altn	No	P2p Bound (STP)
1/e11	enabled	128.11	19	FRW	Desg	Yes	P2p Intr
1/e15	enabled	128.15	19	FRW	Desg	No	P2p Intr
1/e22	enabled	128.22	19	FRW	Desg	Yes	P2p Intr

Définition des paramètres des ports STP

Utilisez la page des paramètres des ports STP pour associer des propriétés STP aux ports. Pour ouvrir la page Spanning Tree Port Settings (Paramètres des ports STP), cliquez sur **Switch** (Commutateur) → **Spanning Tree** → **Port Settings** (Paramètres des ports) dans l'arborescence.

Figure 7-23. Spanning Tree Port Settings (Paramètres des ports STP)



La page Spanning Tree Port Settings (Paramètres des ports STP) contient les champs suivants :

Select a Port (Sélectionner un port) : spécifie le numéro du port dont les paramètres STP seront modifiés.

STP : active ou désactive le protocole STP sur le port.

Fast Link : permet d'activer le mode Fast Link pour le port. Un port en mode Fast Link passe automatiquement à l'état **Forwarding State** (État de transfert) lorsque la liaison est active. 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) : indique l'état STP actuel d'un port. l'état du port détermine quelle action de transfert est effectuée sur le 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 du trafic ou pour apprendre des adresses MAC. Le blocage s'affiche lorsque le protocole Classic STP est activé.

Listening (Écoute) : le port est actuellement en mode d'écoute. Le port ne peut pas transmettre de trafic ni apprendre d'adresses MAC.

Learning (Apprentissage) : le port est actuellement en mode d'apprentissage. Le port ne peut pas transmettre de trafic, mais il peut apprendre de nouvelles adresses MAC.

Forwarding (Transfert) : le port est actuellement en mode de transfert. Le port peut transmettre du trafic et apprendre de nouvelles adresses MAC.

Role (Rôle) : indique le rôle du port attribué par l'algorithme STP fournissant des chemins STP. Ce champ peut prendre les valeurs suivantes :

Root (Racine) : fournit le coût de résolution le plus faible pour le transfert de paquets vers le commutateur racine.

Designated (Désigné) : indique le port sur lequel le commutateur est connecté au LAN.

Alternate (Autre) : fournit un autre chemin vers le commutateur racine à partir de l'interface racine.

Backup (Chemin de secours) : fournit un chemin de secours vers le port désigné en direction des branches du réseau. Les ports de sauvegarde sont créés uniquement lorsque deux ports sont connectés dans une boucle à l'aide d'une liaison point à point. Ils sont également créés 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.

Speed (Vitesse) : vitesse de fonctionnement du port.

Path Cost (1-200000000) (Coût de résolution [1 à 200000000]) : contribution du port au coût de résolution racine. Le coût de résolution est ajusté selon une valeur supérieure ou inférieure et sert à transférer le trafic lorsqu'un chemin est détourné.

Default Path Cost (Coût de résolution par défaut) : coût de résolution par défaut. Les valeurs par défaut du coût de résolution long sont les suivantes :

Ethernet - 2.000.000

Fast Ethernet - 200.000

Gigabit Ethernet - 20.000

Les valeurs par défaut du coût de résolution court sont les suivantes :

Ethernet - 100

Fast Ethernet - 19

Gigabit Ethernet - 4

Priority (0-240, in steps of 16) (Priorité [0 à 240, par incréments de 16]) : valeur de priorité du port. La valeur de priorité influence le choix du port lorsqu'un pont comporte deux ports connectés dans une boucle. La valeur de priorité, exprimée par incréments de 16, est comprise entre 0 et 240.

Designated Bridge ID (ID du pont désigné) : priorité et adresse MAC du pont désigné.

Designated Port ID (ID du port désigné) : priorité et interface du port désigné.

Designated Cost (Coût désigné) : 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.

Forward Transmission (Transfert de transmission) : nombre de fois où le port est passé de l'état **Forwarding** (Transfert) à l'état **Blocking** (Blocage).

LAG : LAG auquel le port est rattaché.

Activation du protocole STP sur un port

1. Affichez la page **Spanning Tree Port Settings** (Paramètres des ports STP).
2. Sélectionnez le port.
3. Sélectionnez **Enabled** (Activé) dans le champ **STP**.
4. Définissez les champs **Fast Link**, **Path Cost** (Coût de résolution) et **Priority** (Priorité).
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 **Spanning Tree Port Settings** (Paramètres des ports STP).
2. Sélectionnez le port.
3. Modifiez les champs correspondants.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des ports STP sont modifiés et l'unité est mise à jour.

Affichage de la table des ports STP

1. Affichez la page **Spanning Tree Port Settings** (Paramètres des ports STP).
2. Cliquez sur **Show All** (Afficher tout).

La page **STP Port Table** (Table des ports STP) s'affiche.

Définition des paramètres des ports STP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la définition des paramètres des ports STP, comme indiqué à la page **Spanning Tree Port Settings** (Paramètres des ports STP.

Tableau 7-13. Commandes CLI des paramètres des ports STP

Commande CLI	Description

spanning-tree disable	Désactive le protocole STP sur un port spécifique.
spanning-tree cost coût	Configure le coût de résolution de la topologie Spanning Tree pour un port.
spanning-tree port-priority priorité	Configure la priorité du port.
show spanning-tree [ethernet< interface | port-channel numéro-canal-port] [instance *id-instance*]	Affichage la configuration de la topologie Spanning Tree.
spanning-tree portfast	Active le mode PortFast.
show spanning-tree [detail] [**active** | **blockedports**] [**instance** *id-instance*]	Affiche des informations détaillées relatives au Spanning Tree sur les ports actifs ou bloqués.
show spanning-tree mst- configuration	Affichage l'identificateur de la configuration MST du protocole STP.

Voici un exemple de commandes CLI :

```
console> enable

console# configure

Console(config)# interface ethernet 1/e1

Console(config-if)# spanning-tree disable

Console(config-if)# spanning-tree cost 35000

Console(config-if)# spanning-tree port-priority 96

Console(config-if)# spanning-tree portfast

Console(config-if)# exit

Console(config)# exit

Console# show spanning-tree ethernet 1/e15
```

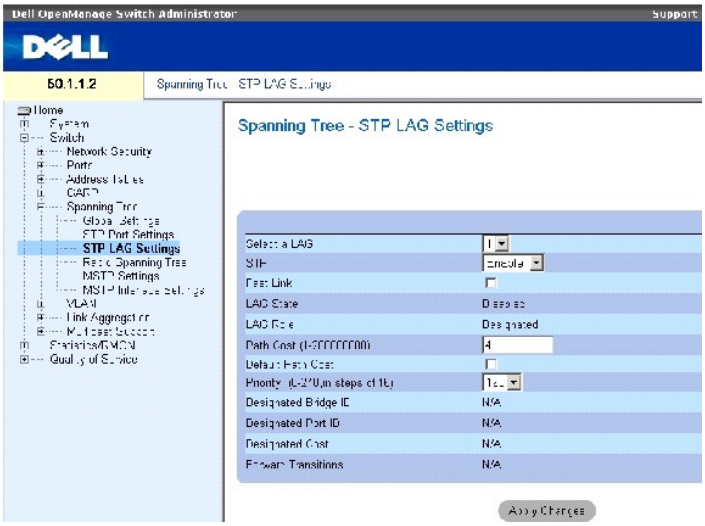
Port 1/e15 enabled					
State: forwarding			Role: designated		

```
Port id: 128.15                                  Port cost: 19
Type: P2p (configured: Auto) Internal Port Fast: No (configured: No)
Designated bridge Priority : 32768               Address: 00:00:00:16:00:64
Designated port id: 128.15                       Designated path cost: 4
Guard root: Disabled
Number of transitions to forwarding state: 2
BPDU: sent 483, received 1037

console# show spanning-tree ethernet 1/e15 instance 12
Port 1/e15 enabled
State: discarding                                Role: alternate
Port id: 128.15                                  Port cost: 19
Type: P2p (configured: Auto) Internal Port Fast: No (configured: No)
Designated bridge Priority : 32768               Address: 00:00:b0:07:07:49
Designated port id: 128.11                       Designated path cost: 0
Guard root: Disabled
Number of transitions to forwarding state: 3
BPDU: sent 482, received 1035
```

Définition des paramètres des LAG STP

Utilisez la page des **paramètres des LAG STP** pour définir les paramètres de ports STP agrégés. Pour ouvrir la page des paramètres des LAG STP, cliquez sur **Switch** (Commutateur) → **Spanning Tree** → **LAG Settings** (Paramètres des LAG) dans l'arborescence.

Figure 7-24. Spanning Tree LAG Settings (Paramètres des LAG STP)



La page **Spanning Tree LAG Settings** (Paramètres des LAG STP) contient les champs suivants :

Select a LAG (Sélectionner un LAG) : numéro du LAG dont vous souhaitez modifier les paramètres STP.

STP : active ou désactive le protocole STP sur le LAG.

Fast Link : active le mode Fast Link pour le LAG. Si le mode Fast Link est activé pour un LAG, l'**État LAG** passe automatiquement à l'état **Forwarding** (Transfert) lorsque le LAG est activé. 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.

LAG State (État du LAG) : état STP actuel d'un LAG. détermine quelle action de transfert est effectuée sur le trafic. Si le pont découvre un LAG défectueux, le LAG passe à l'état **Broken** (Interrompu). Le LAG peut avoir les états suivants :

Disabled (Désactivé) : le protocole STP est désactivé sur le LAG. Le LAG transfère le trafic lorsqu'il apprend des adresses MAC.

Blocking (Blocage): le LAG est bloqué et ne peut pas être utilisé pour transférer du trafic ou pour apprendre des adresses MAC.

RSTP Discarding State (État de rejet RSTP) : dans cet état, le port n'apprend pas les adresses MAC et ne transfert pas les trames.

Il s'agit d'une combinaison des états Blocking (Blocage) et Listening (Écoute) définis dans le protocole STP (802.1.D).

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 apprentissage et ne peut pas transférer le trafic, mais il peut apprendre de nouvelles adresses MAC.

Forwarding (Transfert) : le LAG est en mode transfert : il peut transférer le trafic et apprendre de nouvelles adresses MAC.

Broken (Interrompu) : le LAG ne fonctionnement pas correctement et ne permet pas de transférer le trafic.

LAG Role (Rôle du LAG) : indique le rôle du LAG attribué par l'algorithme STP fournissant des chemins STP. Ce champ peut prendre les valeurs suivantes :

Root (Racine) : fournit le coût de résolution le plus faible pour le transfert de paquets vers le commutateur racine.

Designated (Désigné) : indique le LAG sur lequel le commutateur désigné est connecté au LAN.

Alternate (Autre) : fournit un autre LAG vers le commutateur racine à partir de l'interface racine.

Backup (Chemin de secours) : fournit un chemin de secours vers le port désigné en direction des branches du réseau. Les ports de sauvegarde sont créés uniquement lorsque deux ports sont connectés dans une boucle à l'aide d'une liaison point à point. Ils sont également créés lorsqu'un LAN comporte deux connexions ou plus à un segment partagé.

Disabled (Désactivé) : indique que le LAG ne fait pas partie de la topologie Spanning Tree.

Path Cost (1-200000000) (Coût de résolution [1 à 200000000]) : contribution du LAG au coût de résolution racine. Le coût de résolution est ajusté selon une valeur supérieure ou inférieure et sert à transférer le trafic lorsqu'un chemin est détourné. La valeur du coût de résolution est comprise entre 1 et 200000000.

Default Path Cost (Coût de résolution par défaut) : indique si le coût de résolution par défaut est utilisé. Le coût de résolution par défaut du LAG peut prendre les valeurs suivantes :

Long Method for LAG (Méthode longue pour le LAG) : 20.000

Short Method for LAG (Méthode courte pour le LAG) : 4

Priority (0-240, in steps of 16) (Priorité [0 à 240, par incréments de 16]) : valeur de priorité du LAG. La valeur de priorité influence le choix du port lorsqu'un pont comporte deux ports connectés dans une boucle. La valeur de priorité est comprise entre 0 à 240, par incréments de 16.

Designated Bridge ID (ID du pont désigné) : priorité et adresse MAC du pont désigné.

Designated Port ID (ID du port désigné) : ID de l'interface sélectionnée.

Designated Cost (Coût désigné) : 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.

Forward Transitions (Transfert des transitions) : nombre de fois où l'**état LAG** est passé de l'état **Forwarding** (Transfert) à l'état **Blocking** (Blocage).

Modification des paramètres des LAG STP

1. Affichez la page des **paramètres des LAG STP**.
2. Sélectionnez un LAG dans le menu déroulant **Select a LAG** (Sélectionner un LAG).
3. Modifiez les champs si nécessaire.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des LAG STP sont modifiés et l'unité est mise à jour.

Définition des paramètres des LAG STP à l'aide de commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant de définir les LAG STP.

Tableau 7-14. Commandes CLI des paramètres des LAG STP

Commande CLI	Description
`spanning-tree`	Active le protocole Spanning Tree.
`spanning-tree disable`	Désactive le protocole Spanning Tree sur un LAG spécifique.
`spanning-tree cost` *coût*	Configure le coût de résolution Spanning Tree pour un LAG.
`spanning-tree port-priority` *priorité*	Configure la priorité du port.
`show spanning-tree [`**`ethernet`** `interface |` **`port-channel`** *numéro-canal-port*`] [`**`instance`** *id-instance*`]`	Affiche la configuration du procole STP.
`show spanning-tree [detail] [active | blockedports] [`**`instance`** *id-instance*`]`	Affiche des informations de topologie réseau détaillées sur les ports actifs ou bloqués.

Voici un exemple de commandes CLI :

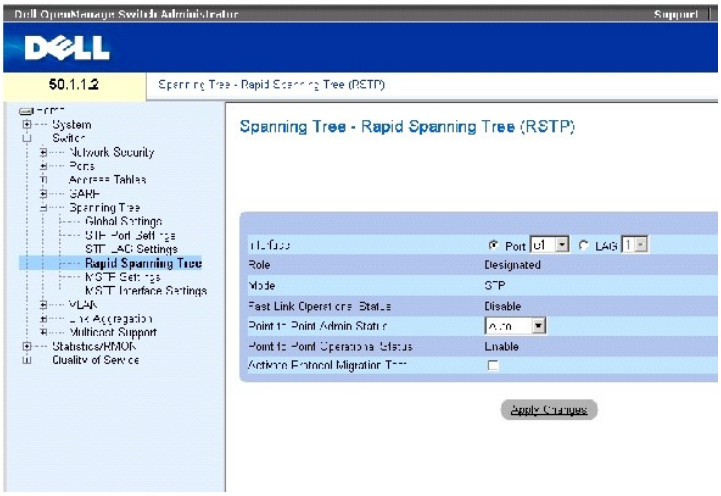
```
console(config)# interface
port-channel 1

console(config-if)#
spanning-tree disable

console(config-if)#
spanning-tree cost 35000

console(config-if)#
spanning-tree port-
priority 96

console(config-if)#
spanning-tree portfast
```

Définition de Rapid Spanning Tree (RSTP)

Le protocole Classic STP empêche les boucles de transfert en couche 2 sur une topologie de réseau générale, mais la convergence peut prendre de 30 à 60 secondes. Ce délai permet de détecter les boucles éventuelles et de répercuter les modifications des états.

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 ouvrir la page des paramètres Rapid Spanning Tree (RSTP), cliquez sur **Switch** (Commutateur) → **Spanning Tree** (STP) → **Rapid Spanning Tree** (RSTP) dans l'arborescence.

Figure 7-25. Rapid Spanning Tree (RSTP) Settings (Paramètres RSTP)



La page des paramètres RSTP contient les champs suivants :

Interface : port ou LAG dont vous pouvez afficher et modifier les paramètres RSTP.

State (État) : désactive l'état RSTP de l'interface sélectionnée.

Role (Rôle) : indique le rôle du port attribué par l'algorithme STP afin de fournir des chemins STP. Ce champ peut prendre les valeurs suivantes :

Root (Racine) : fournit le coût de résolution le plus faible pour le transfert de 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 racine.

Backup (Chemin de secours) : fournit un chemin de secours vers le port désigné en direction des branches du réseau. Les ports de secours sont créés uniquement lorsque deux ports sont connectés dans une boucle à l'aide d'une liaison point à point. Ils sont également créés 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.

Mode : indique le mode STP actuel. Le mode STP est sélectionné à la page Spanning Tree Global Settings (Paramètres globaux STP). Ce champ peut prendre les valeurs suivantes :

Classic STP : indique que le mode Classic STP est activé sur l'unité.

Rapid STP : indique que le mode Rapid STP est activé sur l'unité.

Multiple STP : indique que le mode Multiple STP est activé sur l'unité.

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 une interface, celle-ci passe automatiquement à l'état de transfert (Forwarding).

Point-to-Point Admin Status (État admin point à point) : active ou désactive l'unité afin d'établir une liaison point à point, ou spécifie l'unité pour établir automatiquement une liaison point à point.

Pour établir des communications sur une liaison point à point, le protocole PPP d'origine envoie d'abord des paquets Link Control Protocol (LCP) pour configurer et vérifier la liaison des données. Une fois la liaison établie et les fonctions optionnelles négociées par le protocole LCP, le protocole PPP d'origine envoie des paquets Network Control Protocols (NCP) pour sélectionner ou 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 via la liaison. La liaison reste configurée pour les communications jusqu'à ce que des paquets LCP ou NCP ferment la liaison ou qu'un événement extérieur intervienne. Il s'agit du type réel de liaison du port. Il peut ne pas correspondre à l'état administratif.

Point-to-Point Operational Status (État opérationnel point à point) : état opérationnel point à point.

Activate Protocol Migrational (Activer la migration du protocole) : active l'envoi de paquets LCP (Link Control Protocol) pour configurer et vérifier la liaison des données.

Définition des paramètres RSTP

1. Affichez la page des paramètres RSTP.
2. Sélectionnez une interface.
3. Complétez les champs avec les valeurs appropriées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres RSTP sont définis et l'unité est mise à jour.

Affichage de la table RSTP (Rapid Spanning Tree)

1. Affichez la page des paramètres RSTP.
2. Cliquez sur **Show All** (Afficher tout).

La page **Rapid Spanning Tree (RSTP) Table** (Table RSTP) s'affiche.

Définition des paramètres RSTP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la définition des paramètres RSTP, comme indiqué à la page Rapid Spanning Tree (RSTP).

Tableau 7-15. Commandes CLI relatives aux paramètres RSTP

Commande CLI	Description
`spanning-tree link-type {point-to-point | shared}`	Remplace le paramètre de type de liaison par défaut.
`spanning tree mode {stp | rstp | mstp}`	Configure le protocole STP en cours d'exécution.
`clear spanning-tree detected-protocols [ethernet interface | port-channel numéro- canal-port]`	Relance le processus de migration du protocole.
`show spanning-tree [ethernet interface | port-channel numéro- canal-port]`	Affiche la configuration du procole STP.

Voici un exemple de commandes CLI :

```
console(config)# interface ethernet 1/e5
```

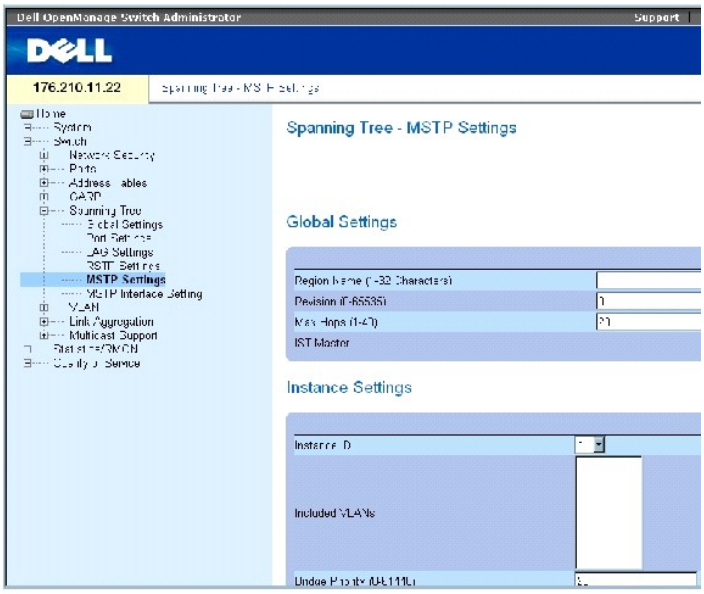
```
console(config-if)# spanning-tree link-type shared

console(config-if)# spanning tree mode rstp
```

Configuration de Multiple Spanning Tree (MSTP)

Le protocole MSTP associe des VLAN à des instances STP. Il fournit un scénario différent d'équilibrage de la charge. Par exemple, si le port A est bloqué dans une instance STP, le même port passe à l'état Forwarding (Transfert) dans une autre instance STP.

En outre, les paquets associés à différents VLAN sont transmis sur des chemins différents dans des régions Multiple Spanning Trees (régions MST). Les régions représentent un ou plusieurs ponts MSTP par lesquels les trames peuvent être transmises. Pour ouvrir la page MSTP Settings (Paramètres MSTP), cliquez sur Switch (Commutateur) → Spanning Tree (STP) → MSTP Settings (Paramètres MSTP) dans l'arborescence.

Figure 7-26. MSTP Settings (Paramètres MSTP)



La page MSTP Settings (Paramètres MSTP) contient les champs suivants :

Region Name (1-32 Characters) (Nom de la région [1 à 32 caractères]) : indique le nom de la région MSTP définie par l'utilisateur.

Revision (0-65535) (Version [0 à 65535]) : définit le chiffre 16 bits non signé qui identifie la version de la configuration MST actuelle. Le numéro de la version est nécessaire à la configuration MST. La plage de valeurs possibles pour ce champ est 0-65535.

Max Hops (1-40) (Nombre maximum de bonds [1 à 40]) : définit le nombre total de bonds qui se produisent dans une région spécifique avant que le BPDU ne soit rejeté. Une fois le BPDU rejeté, les informations du port arrivent à expiration. La plage de valeurs possibles pour ce champ est 1 à 40. La valeur par défaut est de 20 bonds.

IST Master (IST maître) : indique l'ID de l'IST (Internal Spanning Tree) maître. L'IST maître représente la racine de l'instance 0.

Instance ID (ID de l'instance) : définit l'instance MSTP. La plage de ce champ est comprise entre 1 et 15.

Included VLANs (VLAN inclus) : affiche les VLAN associés à l'instance sélectionnée. Chaque VLAN appartient à une instance.

Bridge Priority (0-61440) (Priorité des ponts [0 à 61440] : spécifie la priorité d'unité de l'instance STP sélectionnée. La plage de ce champ est comprise entre 0 et 61440, par incréments de 4096.

Designated Root Bridge ID (ID du pont racine désigné) : indique l'ID du pont racine de l'instance sélectionnée.

Root Port (Port racine) : indique le port racine de l'instance sélectionnée.

Root Path Cost (Coût de résolution racine) : indique le coût de résolution de l'instance sélectionnée.

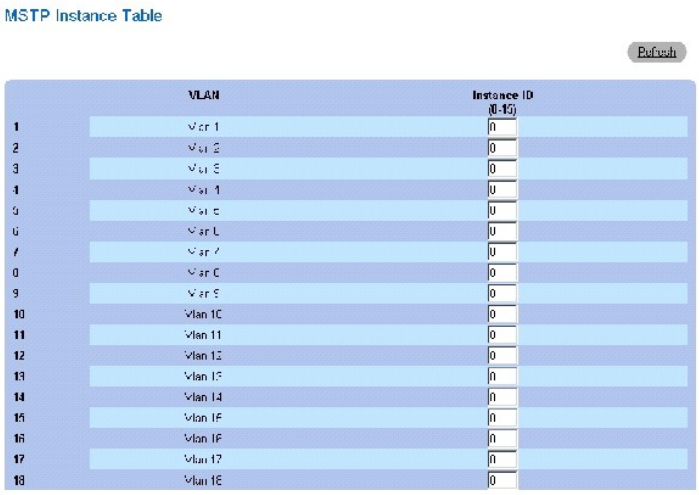
Bridge ID (ID du pont) : indique l'ID du pont de l'instance sélectionnée.

Remaining Hops (Bonds restants) : indique le nombre de bonds restants vers la destination suivante.

Affichage de la page MSTP Instance Table (Table des instances MSTP)

1. Affichez la page MSTP Settings (Paramètres MSTP).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page MSTP Instance Table (Table des instances MSTP).

Figure 7-27. MSTP Instance Table (Table des instances MSTP)



Définition d'instances MST à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la définition des groupes d'instances MST, comme indiqué à la page MSTP Settings (Paramètres MSTP).

Tableau 7-16. Commandes CLI relatives aux instances MSTP

Commande CLI	Description
`spanning-tree mst configuration`	Passe en mode de configuration MST.
	Associe les VLAN à l'instance MST.

instance id-instance {add | remove} vlan plage-vlan	
name chaîne	Définit le nom de la configuration.
revision valeur	Définit le numéro de version de la configuration
spanning-tree **mst** id- instance port-priority priorité	Définit la priorité d'un port.
spanning-tree mst id- instance priority priorité	Définit la priorité d'unité pour l'instance STP spécifiée.
spanning-tree mst max- hops nombre-bonds	Définit le nombre de bonds d'une région MST avant que le BPDU ne soit rejeté et que les informations d'un port n'arrivent à expiration.
spanning-tree mst id- instance **cost** coût	Définit le coût de résolution du port pour les calculs MST
exit	Quitte le mode de configuration de la région MST et applique les modifications apportées à la configuration.
abort	Quitte le mode de configuration de la région MST sans appliquer les modifications apportées à la configuration.
show {current | pending}	Affiche la configuration en cours ou en attente pour la région MST.

Voici un exemple de commandes CLI :

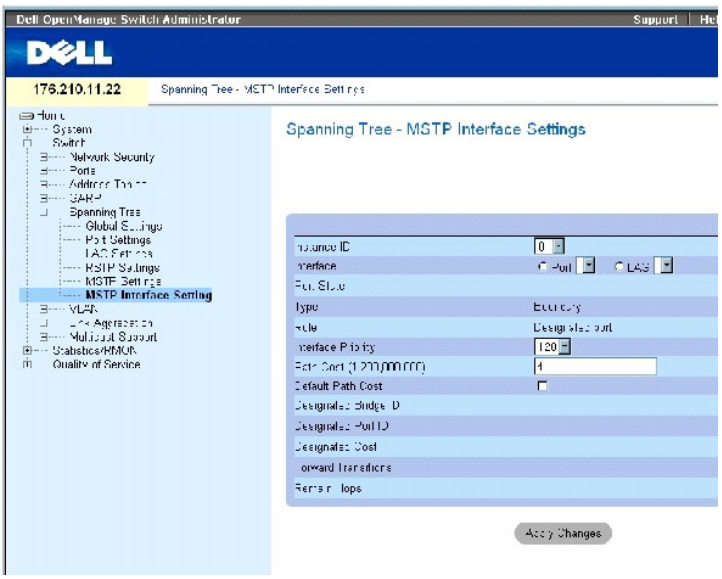
```
console(config)# spanning-tree mst configuration

console(config-mst)# instance 1 add vlan 10-20

console(config-mst)# name region1

console(config-mst)# revision 1

console(config)# spanning-tree mst configuration

console(config-mst)# instance 2 add vlan 21-30

console(config-mst)# name region1

console(config-mst)# revision 1

console(config-mst)# show pending

Pending MST configuration

Name: Region1
```

```
Revision: 1

Instance Vlans Mapped

-------- ------------

0 1-9,31-4094

1 10-20

2 21-30
```

Définition des paramètres d'interface MSTP

La page MSTP Interface Settings (Paramètres d'interface MSTP) contient des champs permettant d'affecter des paramètres MSTP à des interfaces spécifiques. Pour ouvrir la page MSTP Interface Settings (Paramètres d'interface MSTP), cliquez sur Switch (Commutateur) → Spanning Tree (STP) → MSTP Interface Settings (Paramètres d'interface MSTP) dans l'arborescence.

Figure 7-28. MSTP Interface Settings (Paramètres d'interface MSTP)



La page MSTP Interface Settings (Paramètres d'interface MSTP) contient les champs suivants :

Instance ID (ID d'instance) : répertorie les instances MSTP configurées sur l'unité. La plage de valeurs possibles pour ce champ va de 1 à 15.

Interface : associe des ports ou des LAG à l'interface MSTP sélectionnée.

Port State (État du port) : indique si le port est activé ou désactivé dans l'instance spécifique.

Type : 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. Un port maître (Master) offre une connectivité entre une région MSTP et la racine CIST isolée. Un port frontière (Boundary) relie des ponts MST au LAN d'une région isolée. Si le port est un port frontière, il indique également si l'unité située à l'autre extrémité du lien fonctionne en mode RSTP ou STP.

Role (Rôle) : indique le rôle du port attribué par l'algorithme STP afin de fournir des chemins STP. Ce champ peut prendre les valeurs suivantes :

Root (Racine) : fournit le coût de résolution le plus faible pour le transfert de paquets vers l'unité racine.

Designated (Désigné) : indique le port ou LAG sur lequel l'unité désignée est connectée au LAN.

Alternate (Autre) : fournit un autre chemin vers l'unité racine à partir de l'interface racine.

Backup (Chemin de secours) : fournit un chemin de secours vers le port désigné en direction des branches du réseau. Les ports de secours sont créés uniquement lorsque deux ports sont connectés dans une boucle à l'aide d'une liaison point à point. Ils sont également créés 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.

Interface Priority (0-240,in steps of 16) (Priorité d'interface [0 à 240, par incréments de 16]) : définit la priorité de l'interface pour l'instance spécifiée. La valeur par défaut est de 128.

Path Cost- (Coût de résolution) : indique la contribution du port à l'instance STP. La plage devrait toujours être comprise entre 1 et 200.000.000.

Default Path Cost (Coût de résolution par défaut) : indique que le coût de résolution par défaut est appliqué selon la méthode sélectionnée à la page Spanning Tree Global Settings (Paramètres globaux STP).

Designated Bridge ID (ID du pont désigné) : ID du pont qui connecte le lien ou le LAN partagé à la racine.

Designated Port ID (ID du port désigné) : ID du port sur le pont désigné qui connecte le lien ou le LAN partagé à la racine.

Designated Cost (Coût désigné) : coût de résolution du lien ou LAN partagé à la racine.

Forward Transitions (Transitions vers transfert) : nombre de fois où le port est passé à l'état **forwarding** (Transfert).

Remain Hops (Bonds restants) : indique le nombre de bonds restants vers la destination suivante.

Définition des paramètres d'interface MSTP

1. Affichez la page MSTP Interface Settings (Paramètres d'interface MSTP).
2. Sélectionnez une interface.
3. Complétez les champs avec les valeurs appropriées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres MSTP sont définis et l'unité est mise à jour.

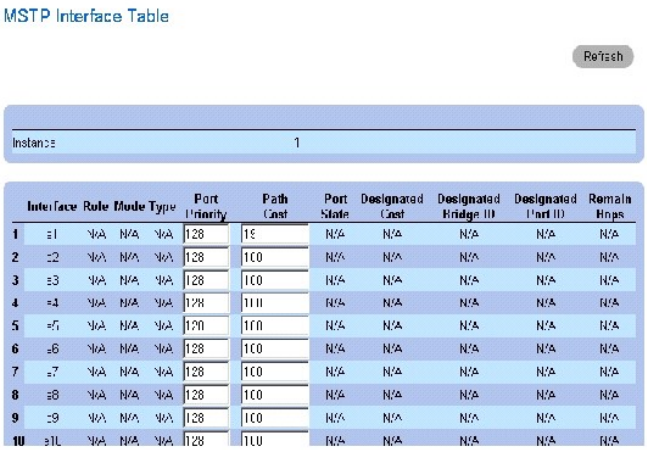
Affichage de la table des interfaces MSTP

1. Affichez la page MSTP Interface Settings (Paramètres d'interface MSTP).

2. Cliquez sur Show All (Afficher tout).

La page MSTP Interface Table (Table des interfaces MSTP) s'affiche.

Figure 7-29. MSTP Interface Table (Table des interfaces MSTP)



Définition d'interfaces MSTP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la définition des interfaces MSTP, comme indiqué à la page MSTP Interface Settings (Paramètres d'interface MSTP).

Tableau 7-17. Commandes CLI relatives aux instances MSTP

Commande CLI	Description
`spanning-tree mst id- instance cost coût`	Définit le coût de résolution du port pour les calculs MST
`spanning-tree mst id- instance priority priorité`	Définit la priorité d'unité pour l'instance STP spécifiée.
`show spanning-tree mst- configuration`	Affiche la configuration MST.

Voici un exemple de commandes CLI :

```
console# show spanning-tree mst-configuration

Gathering information .........

Current MST configuration

Name: Gili

Revision: 65000

Instance        Vlans Mapped                State
                ------------------------    ----------
```

| --- | --- | --- |
0	16-4094	enabled
1	1	enabled
2	2	enabled
3	3	enabled
4	4	enabled
5	5	enabled
6	6	enabled
7	7	enabled
8	8	enabled
9	9	enabled
10	10	enabled
11	11	enabled
12	12	enabled
13	13	enabled
14	14	enabled
15	15	enabled

Configuration des VLAN

Les VLAN sont des sous-groupes logiques d'un LAN créés par le biais d'un logiciel et non par la définition d'une solution matérielle. Ils regroupent des stations utilisateur et des périphériques réseau dans une seule unité, quel que soit le segment de LAN physique auquel ils sont connectés. Les VLAN permettent au trafic réseau de s'acheminer plus efficacement au sein de sous-groupes. Les VLAN gérés au niveau logiciel permettent de réduire le délai d'implémentation des modifications du réseau, des ajouts et des déplacements.

Les VLAN n'ont pas de nombre minimum de ports et peuvent être créés par unité, par périphérique, par pile ou toute autre combinaison de connexions logiques, car ils reposent sur un logiciel et ne sont pas définis par des attributs physiques.

Les VLAN fonctionnent au niveau de la couche 2. Du fait qu'ils isolent le trafic à l'intérieur du VLAN, un routeur fonctionnant au niveau de la couche 3 est nécessaire pour permettre l'acheminement du trafic entre les VLAN. Les routeurs de couche 3 identifient les segments et se coordonnent avec les VLAN. Les VLAN sont des domaines de diffusion et de multidiffusion. Le trafic de diffusion et de multidiffusion est uniquement transmis dans le VLAN où le trafic est généré.

Le balisage VLAN constitue une méthode de transfert des informations VLAN entre les groupes de VLAN. Il consiste à attacher une balise de 4 octets aux en-

têtes de paquets. Cette balise VLAN indique le VLAN auquel le paquet appartient. Les balises VLAN sont attachées au VLAN soit par la station terminale, soit par l'unité réseau. Elles contiennent également les informations de priorité réseau du VLAN.

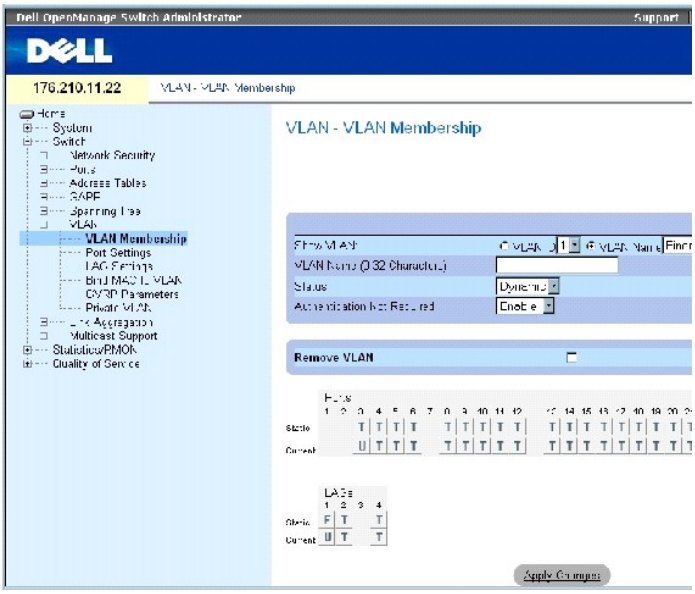
La combinaison des VLAN et du protocole GVRP permet aux administrateurs réseau de définir des noeuds de réseau dans des domaines de diffusion. Le trafic de diffusion et de multidiffusion est confiné au groupe d'origine.

Pour ouvrir la page **VLAN**, cliquez sur **Switch** (Commutateur) → **VLAN** dans l'arborescence.

Définition de l'appartenance à un VLAN

La page **VLAN Membership (Appartenance à un VLAN)** contient des champs permettant de définir des groupes de VLAN. L'unité prend en charge l'adressage de 4094 ID de VLAN à un maximum de 256 VLAN. Un PVID doit être défini pour tous les ports. Si aucune valeur n'est configurée, le PVID VLAN par défaut est utilisé. La valeur par défaut VLAN ID #1 ne peut pas être supprimé du système. Pour ouvrir la page **VLAN Membership (Appartenance à un VLAN)**, cliquez sur **Switch** (Commutateur) → **VLAN** → **VLAN Membership** (Appartenance à un VLAN) dans l'arborescence.

Figure 7-30. VLAN Membership (Appartenance à un VLAN)



La page **VLAN Membership (Appartenance à un VLAN)** contient les champs suivants :

Show VLAN (Afficher le VLAN) : répertorie et affiche des informations spécifiques sur le VLAN en fonction de l'ID ou du nom de VLAN.

VLAN Name (Nom du VLAN [0 à 32 caractères]) : nom de VLAN défini par l'utilisateur.

Status (État) : type de VLAN. Ce champ peut prendre les valeurs suivantes :

Dynamic (Dynamique) : le VLAN a été créé de façon dynamique via le protocole GVRP.

Static (Statique) : le VLAN est défini par l'utilisateur.

Default (Par défaut) : le VLAN est le VLAN par défaut.

Authentication Not Required (Authentification non requise) : accorde ou interdit l'accès à un VLAN aux utilisateurs non autorisés.

Remove VLAN (Supprimer un VLAN) : permet de supprimer le VLAN de la table d'appartenance à un VLAN.

Ajout de nouveaux VLAN

1. Affichez la page **VLAN Membership (Appartenance à un VLAN)**.
2. Cliquez sur **Add** (Ajouter).

   La page **Create New VLAN** (Créer un VLAN) s'affiche.
3. Saisissez l'ID et le nom du VLAN.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

   Le nouveau VLAN est ajouté et l'unité est mise 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 **Show VLAN** (Afficher le VLAN).
3. Modifiez les champs si nécessaire.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

   Les informations relatives à l'appartenance à un VLAN sont modifiées et l'unité est mise à jour.

Suppression de VLAN

1. Affichez la page **VLAN Membership (Appartenance à un VLAN)**.
2. Sélectionnez un VLAN dans le champ **Show VLAN** (Afficher le VLAN).
3. Cochez la case **Remove VLAN** (Supprimer le VLAN).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

   Le VLAN sélectionné est supprimé et l'unité est mise à jour.

Définition des groupes d'appartenance à un VLAN à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la définition des groupes d'appartenance à un VLAN, comme indiqué à la page VLAN Membership (Appartenance à un VLAN).

Tableau 7-18. Commandes CLI relatives aux groupes d'appartenance à un VLAN

Commande CLI	Description
vlan database	Passe en mode de configuration VLAN.
vlan {*plage-vlan*}	Crée un VLAN.
name *chaîne*	Ajoute un nom à un VLAN.

Voici un exemple de commandes CLI :

```
console(config)# vlan
database


console(config-vlan)# vlan
1972


console(config-vlan)# end


console(config)# interface
vlan 1972


console(config-if)# name
Marketing


console(config-if)# end
```

Table d'appartenance des ports à un VLAN

La page **VLAN Port Membership Table** (Table d'appartenance des ports à un VLAN) contient une **table** permettant d'affecter des ports à des VLAN. Les ports sont associés à un VLAN en basculant entre les différentes valeurs **Port Control** (Contrôle des ports). Les ports peuvent avoir les valeurs suivantes :

Tableau 7-21. Table d'appartenance des ports à un VLAN

Contrôle des ports	Définition
T	L'interface est membre d'un VLAN. Tous les paquets transférés par cette interface sont balisés. Les paquets contiennent des informations VLAN.
U	L'interface est membre d'un VLAN, mais les paquets transférés par celle-ci ne sont pas balisés.
F	L'appartenance à un VLAN n'est pas accordée à l'interface.
Néant	L'interface n'est pas membre d'un VLAN. Les paquets associés à l'interface ne sont pas transférés.

La page **VLAN Port Membership Table** (Table d'appartenance des ports à un VLAN) contient les ports et l'état des ports, ainsi que les LAG.

Affectation de ports à un groupe de VLAN

1. Affichez la page VLAN Membership (Appartenance à un VLAN).
2. Cochez la case **VLAN ID** (ID du VLAN) ou **VLAN Name** (Nom du VLAN) et sélectionnez un VLAN dans le menu déroulant.
3. Sélectionnez un port dans la **table d'appartenance des ports** et affectez-lui une valeur.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port est affecté au groupe de VLAN et l'unité est mise à jour.

Suppression d'un VLAN

1. Affichez la page VLAN Membership (Appartenance à un VLAN).
2. Cochez la case **VLAN ID** (ID du VLAN) ou **VLAN Name** (Nom du VLAN) et sélectionnez un VLAN dans le menu déroulant.
3. Cochez la case **Remove VLAN** (Supprimer le VLAN).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le VLAN sélectionné est supprimé et l'unité est mise à jour.

Affectation de ports à des groupes de VLAN à l'aide de commandes CLI

Le tableau suivant récapitule les commandes d'interface de ligne de commande (CLI) équivalentes permettant l'affectation de ports à des groupes de VLAN.

Tableau 7-19. Commandes CLI relatives à l'affectation de ports à un groupe de VLAN

Commande CLI	Description
switchport general acceptable-frame-types tagged-only	Rejette les trames non balisées à l'entrée.
switchport forbidden vlan {add *liste-vlan* | remove *liste-vlan*}	Interdit l'ajout de VLAN spécifiques au port.
switchport mode {accès | trunk | general}	Configure le mode d'appartenance VLAN d'un port.
switchport access vlan id-vlan	Configure l'ID du VLAN lorsque l'interface est en mode d'accès.
switchport trunk allowed vlan {add liste-vlan | remove liste-vlan}	Ajoute ou supprime des VLAN d'un port de jonction.
switchport trunk native vlan id-vlan	Définit le port comme étant membre du VLAN spécifié et l'ID de VLAN comme étant l'ID de VLAN par défaut du port (PVID).
switchport general allowed vlan add liste-vlan [tagged | untagged]	Ajoute ou supprime des VLAN pour un port en mode général.
switchport general pvid id-vlan	Configure le PVID lorsque l'interface est en mode général.

Voici un exemple de commandes CLI :

```
console(config)# vlan
database

console(config-vlan)# vlan
23-25

console(config-vlan)# end

console(config)# interface
vlan 23

console(config-if)# name
Marketing

console(config-if)# end

console(config)# interface
ethernet 1/e8

console(config-if)#
switchport mode access

console(config-if)#
switchport access vlan 23

console(config-if)# end
```

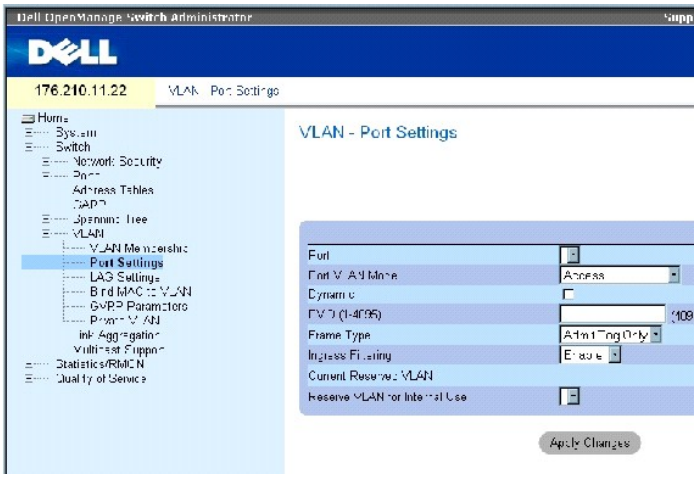
```
console(config)# interface
ethernet 1/e9



console(config-if)#
switchport mode trunk



console(config-if)#
switchport mode trunk
allowed vlan add 23-25



console(config-if)# end



console(config)# interface
ethernet 1/e11



console(config-if)#
switchport mode general



console(config-if)#
switchport general allowed
vlan add 23,25 tagged



console(config-if)#
switchport general pvid 25
```

Définition des paramètres des ports de VLAN

La page VLAN Port Settings (Paramètres des ports de VLAN) contient des champs permettant de gérer des ports faisant partir d'un VLAN. L'ID de VLAN par défaut du port (Port Default VLAN ID, PVID) est configuré à la page VLAN Port Settings (Paramètres des ports de VLAN). Tous les paquets non balisés arrivant à l'unité sont balisés par le PVID du port.

Pour ouvrir la page VLAN Port Settings (Paramètres des ports de VLAN), cliquez sur **Switch** (Commutateur) → **VLAN**→ **Port Settings** (Paramètres des ports) dans l'arborescence.

Figure 7-31. VLAN Port Settings (Paramètres des ports de VLAN)



La page VLAN Port Settings (Paramètres des ports de VLAN) contient les champs suivants :

Port : numéro du port inclus dans le VLAN.

Port VLAN Mode (Mode VLAN du port) : 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 passe en mode d'accès, les types de paquets acceptés sur le port ne peuvent pas être désignés. Le filtrage en entrée ne peut pas être activé ni désactivé sur un port d'accès.

Trunk (Segment) : le port appartient à plusieurs VLAN dont tous les ports ont été balisés (à l'exception d'un port qui peut ne pas être balisé).

PVE Promiscuous (VLAN privé banalisé) : le port appartient à un VLAN privé banalisé.

PVE Community (VLAN privé de communauté) : le port appartient à un VLAN privé de communauté.

PVE Isolated (VLAN privé isolé) : le port appartient à un VLAN privé isolé.

Dynamic (Dynamique) : **associe un port à un VLAN en fonction de l'adresse MAC source hôte connectée au port.**

PVID : affecte un ID de VLAN aux paquets non balisés. La plage des valeurs possibles s'étend de 1 à 4095. Le VLAN 4095 est défini par défaut comme VLAN de rejet. Les paquets faisant référence à ce VLAN sont rejetés.

Frame Type (Type de trame) : type de paquet accepté sur le port. Ce champ peut prendre les valeurs suivantes :

Admit Tag Only (Admettre uniquement les paquets balisés) : seuls les paquets balisés sont acceptés sur le port.

Admit All (Admettre tout) : les paquets balisés et non balisés sont acceptés sur le port.

Ingress Filtering (Filtrage en entrée) : active ou désactive le filtrage en entrée sur le port. Le filtrage en entrée rejette les paquets destinés aux VLAN dont le port ne fait pas partie.

Current Reserved VLAN (VLAN réservé en cours) : VLAN désigné par le système comme VLAN réservé.

Reserve VLAN for Internal Use (VLAN réservé pour utilisation interne) : VLAN sélectionné par l'utilisateur comme VLAN réservé s'il n'est pas utilisé par le système.

Affectation des paramètres de port

1. Affichez la page VLAN Port Settings (Paramètres des ports de VLAN).
2. Sélectionnez le port auquel des paramètres doivent être affectés dans le menu déroulant **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 l'unité est mise à jour.

Affichage de la table des ports de VLAN

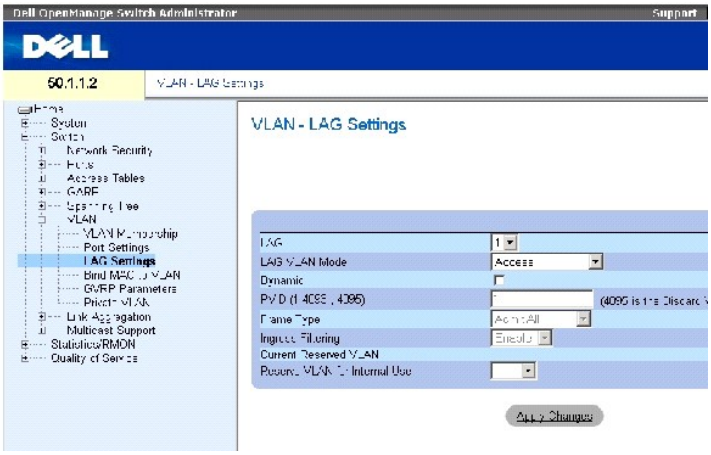
1. Affichez la page VLAN Port Settings (Paramètres des ports de VLAN).
2. Cliquez sur **Show All** (Afficher tout).

La page **VLAN Port Table** (Table des ports de VLAN) s'affiche.

Définition des paramètres des LAG de VLAN

La page VLAN LAG Settings (Paramètres des LAG de VLAN) contient des paramètres relatifs à la gestion des LAG inclus dans un VLAN. Les VLAN peuvent être composés de ports individuels ou de LAG. Les paquets non balisés qui arrivent sur l'unité sont balisés à l'aide des ID de LAG spécifiés par le PVID. Pour ouvrir la page VLAN LAG Settings (Paramètres des LAG de VLAN), cliquez sur **Switch** (Commutateur) → **VLAN**→ **LAG Settings** (Paramètres des LAG) dans l'arborescence.

Figure 7-32. VLAN LAG Settings (Paramètres des LAG de VLAN)



La page VLAN LAG Settings (Paramètres des LAG de VLAN) contient les champs suivants :

LAG : numéro du LAG inclus dans le VLAN.

LAG VLAN Mode (Mode VLAN du LAG) : 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 (Segment) : le LAG appartient à plusieurs VLAN dont tous les ports ont été balisés (à l'exception d'un port qui peut ne pas être balisé).

PVE Promiscuous (VLAN privé banalisé) : le LAG appartient à un VLAN privé banalisé.

PVE Community (VLAN privé de communauté) : le LAG appartient à un VLAN privé de communauté.

PVE Isolated (VLAN privé isolé) : le LAG appartient à un VLAN privé isolé.

Dynamic (Dynamique) : associe un LAG à un VLAN en fonction de l'adresse MAC source hôte connectée au LAG.

PVID (1-4093, 4095) (PVID [1 à 4093, 4095]) : affecte un ID de VLAN aux paquets non balisés. La plage des valeurs possibles s'étend de 1 à 4095. Le VLAN 4095 est défini par défaut comme VLAN de rejet. Les paquets faisant référence à ce VLAN sont rejetés.

Frame Type (Type de trame) : type de paquets accepté par le LAG. Ce champ peut prendre les valeurs suivantes :

Admit Tag Only (Admettre uniquement les paquets balisés) : seuls les paquets balisés sont acceptés par le LAG.

Admit All (Admettre tout) : les paquets balisés et non balisés sont acceptés par le LAG.

Ingress Filtering (Filtrage en entrée) : active ou désactive le filtrage en entrée par le LAG. Le filtrage en entrée rejette les paquets destinés aux VLAN dont le LAG ne fait pas partie.

Current Reserved VLAN (VLAN réservé actuel) : VLAN désigné comme VLAN réservé.

Reserve VLAN for Internal Use (VLAN réservé à un usage interne) : VLAN désigné comme VLAN réservé après réinitialisation de l'unité.

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** et complétez les champs de la page.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des LAG de VLAN sont définis et l'unité est mise 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.

Affectation de LAG à des groupes de VLAN à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant l'affectation de LAG à des groupes de VLAN, comme indiqué à la page VLAN LAG Settings (Paramètres des LAG de VLAN).

Tableau 7-20. Commandes CLI relatives aux affectations de LAG de VLAN

Commande CLI	Description
switchport mode {access | trunk | general}	Configure le mode d'appartenance VLAN d'un LAG.
switchport trunk native vlan *id-vlan*	Définit le port comme étant membre du VLAN spécifié et l'ID de VLAN comme étant l'ID de VLAN par défaut du LAG (PVID).
switchport general pvid *id vlan*	Configure l'ID de VLAN du LAG (PVID) lorsque l'interface est en mode général.
switchport general allowed vlan add *liste-vlan* [**tagged | untagged**]	Ajoute ou supprime des VLAN d'un LAG général.
switchport general acceptable-frame-type tagged-only	Rejette les paquets non balisés à l'entrée.

switchport access vlan dynamic	Associe l'adresse MAC au VLAN.
switchport general ingress-filtering disable	Désactive le filtrage en entrée d'un LAG.

Voici un exemple de commandes CLI :

```
console(config)# interface
port-channel 1

console(config-if)#
switchport mode access

console(config-if)#
switchport access vlan 2

console(config-if)# exit

console(config)# interface
port-channel 2

console(config-if)#
switchport mode general

console(config-if)#
switchport general allowed
vlan add 2-3 tagged

console(config-if)#
switchport general pvid 2

console(config-if)#
switchport general
acceptable-frame-type
tagged-only

console(config-if)#
switchport general
ingress-filtering disable

console(config-if)# exit

console(config)# interface
port-channel 3

console(config-if)#
switchport mode trunk

console(config-if)#
switchport trunk native
vlan 3

console(config-if)#
```

```
switchport trunk allowed
vlan add 2
```

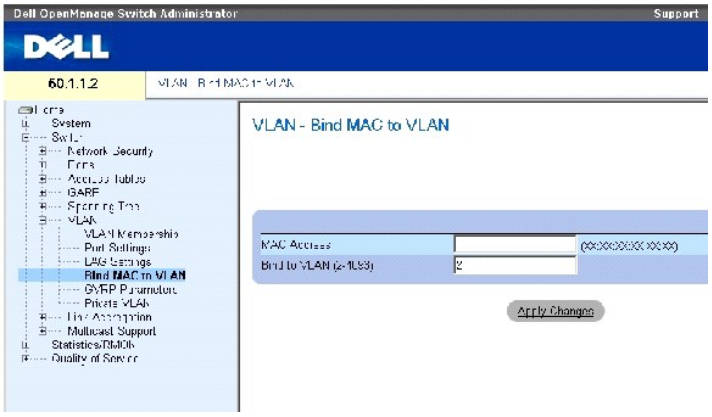
Liaison d'adresses MAC à des VLAN

La liaison d'adresses MAC à des VLAN permet d'associer un port à un VLAN en fonction des adresses MAC. Lorsqu'un VLAN est associé à une adresse MAC et que celle-ci est apprise sur un port, le port est lié au VLAN correspondant. Lorsque l'adresse MAC expire, le port quitte le VLAN. Seuls les VLAN dynamiques peuvent être liés à des adresses MAC.

Pour lier des adresses MAC à un VLAN, vérifiez que les ports de VLAN ont été ajoutés de façon dynamique et ne sont pas statiques.

Pour ouvrir la page **Bind MAC to VLAN (Lier des adresses MAC à des VLAN)**, cliquez sur **Switch** (Commutateur) → **VLAN** → **Bind MAC to VLAN** (Lier des adresses MAC à des VLAN).

Figure 7-33. Bind MAC to VLAN (Lier des adresses MAC à des VLAN)



La page Bind MAC to VLAN (Lier des adresses MAC à des VLAN) contient les champs suivants :

MAC Address (Adresse MAC) : indique l'adresse MAC liée au VLAN.

Bind to VLAN (2-4093) (Lier à un VLAN [2 à 4093]) : indique le VLAN auquel l'adresse MAC est liée.

Affichage de la table de liaison d'adresses MAC à des VLAN

1. Affichez la page Bind MAC to VLAN (Lier des adresses MAC à des VLAN).
2. Cliquez sur **Show All** (Afficher tout).

La page **MAC to VLAN table** (Table de liaison d'adresses MAC à des VLAN) s'affiche.

Liaison d'adresses MAC à des VLAN à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la liaison d'adresses MAC à des VLAN.

Tableau 7-21. Commandes CLI relatives à la liaison d'adresses MAC à des VLAN

Commande CLI	Description

mac-to-vlan adresse-MAC id-vlan	Lie l'adresse MAC au VLAN.
switchport access vlan dynamic	Configure des VLAN privés.
show mac-to-vlan	Affiche la base de données de liaison d'adresses MAC à des VLAN.
no mac-to-vlan adresse-mac	Annule la liaison de l'adresse MAC au VLAN.

Voici un exemple de commandes CLI :

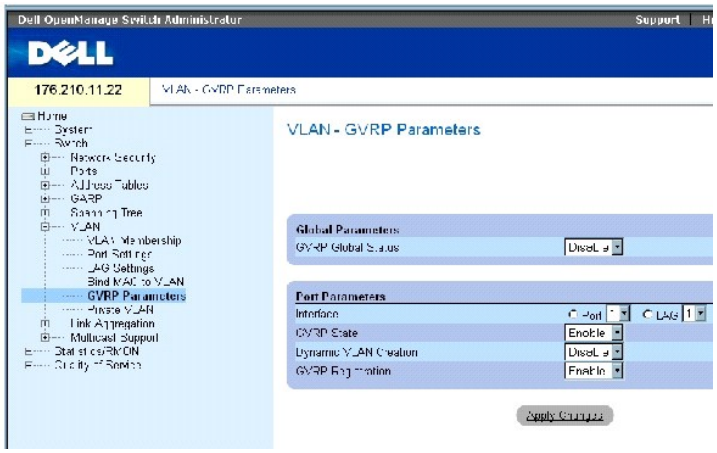
```
console(config-vlan)# mac-to-vlan 0060.704c.73ff 123

console(config-vlan)# exit

console(config)# exit

console# show vlan mac-to-vlan

MAC Address VLAN

------------ ------

0060.704c.73ff 123
```

Configuration des paramètres GVRP

Le protocole GVRP (GARP VLAN Registration Protocol) est fourni spécifiquement pour la diffusion automatique des informations relatives à l'appartenance aux VLAN entre les ponts compatibles VLAN. Le protocole GVRP permet aux ponts compatibles VLAN d'apprendre automatiquement l'adressage VLAN-pont sans avoir à configurer individuellement chaque pont et enregistrer l'appartenance au VLAN.

La page **GVRP Parameters (Paramètres GVRP)** active le protocole GVRP de façon globale. Le protocole GVRP peut également être activé pour chaque interface. Pour ouvrir la page GVRP Parameters (Paramètres GVRP), cliquez sur **Switch (Commutateur)** → **VLAN**→ **GVRP Parameters** (Paramètres GVRP) dans l'arborescence.

Figure 7-34. GVRP Parameters (Paramètres GVRP)



La page GVRP Parameters (Paramètres GVRP) contient les champs suivants :

GVRP Global Status (État global GVRP) : active ou désactive le protocole GVRP sur l'unité. Le protocole GVRP est désactivé par défaut.

Interface : spécifie le port ou LAG concerné par la modification des paramètres GVRP.

GVRP State (État GVRP) : active ou désactive le protocole GVRP sur une interface.

Dynamic VLAN Creation (Création dynamique de VLAN) : active ou désactive la création de VLAN par le biais de GVRP sur une interface.

GVRP Registration (Enregistrement GVRP) : active ou désactive l'enregistrement VLAN par le biais de GVRP sur une interface.

Activation du protocole GVRP sur l'unité

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 l'unité.

Activation de l'enregistrement 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).
3. Sélectionnez **Enable** (Activer) dans le champ GVRP State (État GVRP) pour l'interface de votre choix.
4. Sélectionnez **Enable** (Activer) dans le champ **GVRP Registration** (Enregistrement GVRP).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'enregistrement GVRP des VLAN est activé sur le port et l'unité est mise à jour.

Configuration du protocole GVRP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la configuration du protocole GVRP, comme indiqué à la page GVRP Global Parameters (Paramètres globaux GVRP).

Tableau 7-22. Commandes CLI des paramètres globaux GVRP

Commande CLI	Description
gvrp enable (global**)**	Active GVRP de façon globale.
gvrp enable (interface)	Active GVRP sur une interface.
gvrp vlan-creation-forbid	Active ou désactive la création dynamique de VLAN.
gvrp registration-forbid	Annule l'enregistrement de tous les VLAN dynamiques et empêche l'enregistrement dynamique des VLAN sur le port.
show gvrp configuration [**ethernet** *interface*| **port-channel** *numéro-canal-port*]	Affiche les informations de configuration GVRP, y compris les valeurs des temporisateurs, et indique si le protocole GVRP et la création dynamique de VLAN sont activés et quels ports exécutent GVRP.
show gvrp error-statistics [**ethernet** *interface* | **port-channel** *numéro_canal_port*]	Affiche les statistiques d'erreurs GVRP.
show gvrp statistics [**ethernet** *interface* | **port-channel** *numéro_canal_port*]	Affiche les statistiques GVRP.
clear gvrp statistics [**ethernet** *interface*| **port-channel** *numéro-canal-port*]	Efface toutes les statistiques GVRP.

Voici un exemple de commandes CLI :

```
console(config)# gvrp enable

console(config)# interface ethernet 1/e1

console(config-if)# gvrp enable

console(config-if)# gvrp vlan-creation-forbid

console(config-if)# gvrp registration-forbid

console(config-if)# end

console# show gvrp configuration

GVRP Feature is currently Enabled on the device

Maximum VLANs: 223
```

Port (s)	GVRP-Status	Registration	Dynamic VLAN Creation	Timers (milliseconds) Join	Leave	Leave All
---	---	---	---	---	---	---
1/e11	Enabled	Forbidden	Disabled	200	900	10000
1/e12	Disabled	Normal	Enabled	200	600	10000

Configuration des VLAN privés

Les VLAN privés (PVLAN) augmentent la sécurité du réseau en limitant les communications entre les ports d'un VLAN. Il limitent le trafic réseau au niveau de la couche 2. Les administrateurs réseau définissent un VLAN principal. Ce VLAN principal contient des VLAN isolés et des VLAN de communauté. Les ports des VLAN privés peuvent avoir les états suivants :

- **Promiscuous** (Banalisé) : les ports banalisés peuvent communiquer avec tous les ports d'un VLAN privé. Tous les paquets banalisés sont automatiquement associés aux VLAN isolés et aux VLAN de communauté.
- **Isolated** (Isolés) : les ports isolés sont complètement isolés des autres ports du même VLAN privé. Cependant, les ports isolés peuvent communiquer avec les ports banalisés. En outre, la totalité du trafic à destination et en provenance de ports isolés d'un VLAN est bloquée, à l'exception du trafic provenant de ports banalisés. Tous les ports isolés sont automatiquement associés au VLAn isolé.
- **Community** (Communauté) : les ports de communauté communiquent avec les autres ports de communauté et les ports banalisés. Les ports de communauté sont séparés de toutes les autres interfaces des autres communautés ou des ports isolés du même VLAN privé. Tous les ports de communauté sont automatiquement associés au VLAN de communauté et au VLAN privé.

REMARQUE : les ports ne peuvent pas être définis comme banalisés ou isolés s'ils représentent des membres de VLAN existants.

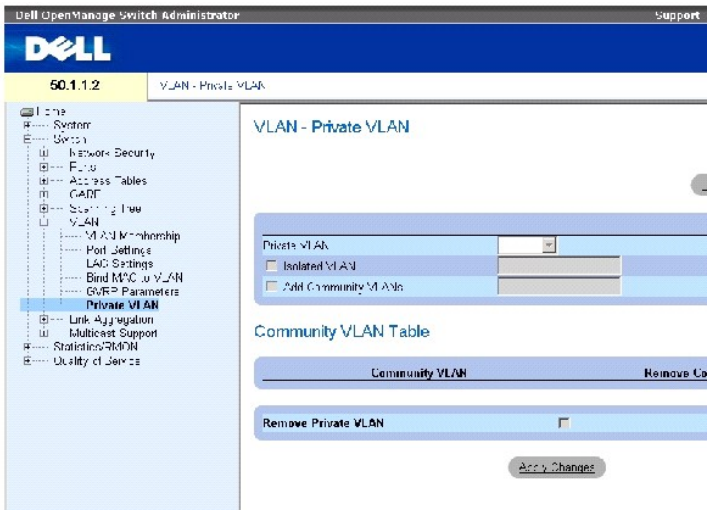
REMARQUE : les VLAN créés précédemment ne peuvent pas être configurés comme des VLAN isolés ou des VLAN de communauté.

REMARQUE : les VLAN isolés et les VLAN de communauté sont inclus dans le nombre total de VLAN.

Si le VLAN principal est supprimé, les VLAN isolés et les VLAN de communauté le sont également. En outre, les VLAN isolés et les VLAN de communauté transfèrent uniquement le trafic non balisé.

Pour ouvrir la page Private VLAN (VLAN privé), cliquez sur **Switch** (Commutateur) → **VLAN** → **Private VLAN** (VLAN privé) dans l'arborescence.

Figure 7-35. Private VLAN (VLAN privé)



La page Private VLAN (VLAN privé) contient les champs suivants :

Private VLAN (VLAN privé) : contient la liste des VLAN privés définis par l'utilisateur. Les VLAN privés sont définis à la page **Add Private VLAN (Ajout de VLAN privés)**.

Isolated VLAN (VLAN isolé) : indique le VLAN auquel les ports isolés sont associés.

Add Community VLANs (Ajouter des VLAN de communauté) : ajoute un VLAN de communauté auquel les ports de communauté sont associés.

Community VLAN (VLAN de communauté) : affiche la liste des VLAN de communauté.

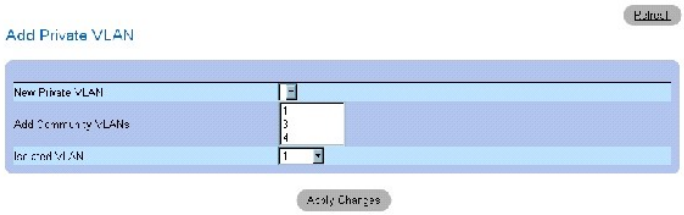
Remove Community (Supprimer un VLAN de communauté) : supprime un VLAN de communauté.

Remove Private VLAN (Supprimer un VLAN privé) : supprime un VLAN privé.

Ajout de VLAN privés

1. Affichez la page Private VLAN (VLAN privé).
2. Cliquez sur **Add** (Ajouter). La page **Add Private VLAN (Ajout de VLAN privés)** s'affiche.

Figure 7-36. Add Private VLAN (Ajout de VLAN privés)



La page Add Private VLAN (Ajout de VLAN privés) contient les champs supplémentaires suivants :

New Private VLAN (Nouveau VLAN privé) : contient la liste des VLAN privés. Les VLAN de communauté sont ajoutés au VLAN privé.

Add Community VLANs (Ajouter des VLAN de communauté) : ajoute un VLAN de communauté au VLAN privé.

Isolated VLAN (VLAN isolé) : ajoute un VLAN isolé au VLAN privé.

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

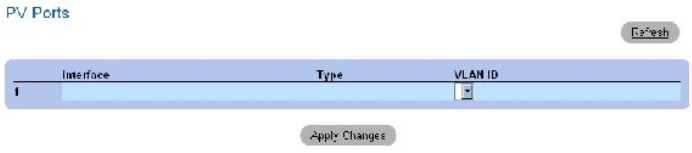
Le VLAN privé est défini et l'unité est mise à jour.

Affichage de la table des ports de VLAN privé

1. Affichez la page Private VLAN (VLAN privé).
2. Cliquez sur **Show PV Ports** (Afficher les ports de VLAN privé).

La page **PV Ports Table (Table des ports de VLAN privé)** s'affiche.

Figure 7-37. PV Ports Table (Table des ports de VLAN privé)



Configuration des VLAN privés à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la configuration des VLAN privés, comme indiqué à la page **Private VLAN (VLAN privé)**.

Tableau 7-23. Commandes CLI relatives aux VLAN privés

Commande CLI	Description
switchport mode private vlan promiscuous	**Ajoute un port banalisé à un VLAN banalisé.**
switchport mode private vlan community	**Ajoute un port de communauté à un VLAN de communauté.**
switchport mode private vlan isolated	**Ajoute un port isolé à un VLAN isolé.**
private-vlan primary	Définit un VLAN principal.
private-vlan community {add liste-vlan-communauté | remove liste-vlan-communauté }	Définit ou supprime un VLAN de communauté du VLAN principal.
private-vlan isolated	Définit un VLAN isolé du VLAN principal.

switchport private-vlan *pvlan* [community *cvlan*]	Définit des ports de VLAN privés.
show vlan private-vlan [primary vlan-id]	Affiche le VLAN principal privé.

Voici un exemple de commandes CLI :

```
console(config)# vlan
database

console(config-vlan)# vlan
2

console(config-vlan)# exit

console(config)# interface
vlan 2

console(config-if)#
private-vlan primary

console(config)# interface
vlan 2

console(config-if)#
private-vlan isolated 10

console(config-if)#
private-vlan community add
20

console# show vlan
private-vlan

console(config-if)# end
```

Agrégation des ports

La fonction d'agrégation des liaisons optimise l'utilisation des ports en reliant entre eux un groupe de ports de façon à former un LAG (groupe agrégé) unique. Elle multiplie la bande passante entre les périphériques, augmente la flexibilité des ports et assure la redondance des liens.

L'unité prend en charge à la fois les LAG statiques et les LAG LACP (Link Aggregation Control Protocol). Les LAG LACP négocient les liens de ports agrégés avec d'autres ports LACP situés sur un périphérique différent. Si les autres ports de l'unité sont également des ports LACP, les périphériques établissent un groupe de liens agrégés (LAG) entre eux.

Tenez compte des informations suivantes lors de l'agrégation des ports :

- Tous les ports d'un LAG doivent correspondre au même type de support.
- Un VLAN n'est pas configuré sur le port.
- Le port n'est pas associé à un autre LAG.
- Le mode de négociation automatique n'est pas configuré sur le port.

- Le port fonctionne en mode duplex intégral.
- Tous les ports du LAG ont le même filtrage en entrée et les mêmes modes balisés.
- Tous les ports du LAG ont la même contre-pression et les mêmes modes de contrôle de flux.
- Tous les ports du LAG ont la même priorité.
- Tous les ports du LAG ont le même type d'émetteur-récepteur.
- L'unité prend en charge jusqu'à huit LAG, et huit ports par LAG.
- Les ports peuvent être configurés comme des ports LACP uniquement s'ils ne font pas partie d'un LAG configuré précédemment.

Les ports ajoutés à un LAG perdent leur configuration individuelle. Lorsque des ports sont supprimés du LAG, la configuration d'origine est appliquée aux ports.

L'unité utilise une fonction de hachage pour déterminer quels paquets sont transmis sur un membre donné d'un LAG. La fonction de hachage effectue un équilibrage de charge à base de statistiques entre les membres des liens agrégés. L'unité considère un lien agrégé comme un seul et même port logique.

Définition des paramètres LACP

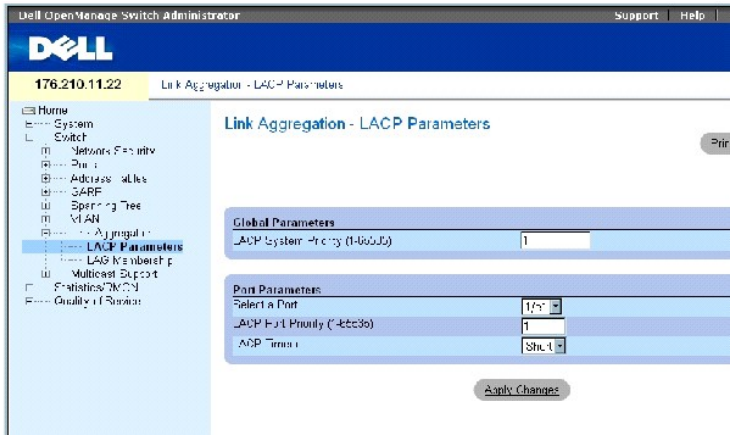
Les ports agrégés peuvent être reliés en groupes de ports à agrégation de liens. Chaque groupe est composé de ports ayant la même vitesse et réglés en mode duplex intégral.

Les ports d'un groupe de liaisons agrégées (LAG) peuvent être composés de différents types de supports s'ils fonctionnent à la même vitesse. Les liens agrégés peuvent être configurés manuellement ou automatiquement en activant le protocole LACP (Link Aggregation Control Protocol) sur les liens appropriés.

Définition des paramètres LACP

La page **LACP Parameters** (Paramètres LACP) contient des champs permettant la configuration des LAG LACP. Les ports agrégés peuvent être reliés en groupes de ports à agrégation de liens. Chaque groupe est composé de ports ayant la même vitesse. Les liens agrégés peuvent être configurés manuellement ou établis automatiquement en activant le protocole Link Aggregation Control Protocol (LACP) sur les liens appropriés. Pour ouvrir la page LACP Parameters (Paramètres LACP), cliquez sur **Switch** (Commutateur) → **Link Aggregation** (Agrégation de liaisons) → **LACP Parameters** (Paramètres LACP) dans l'arborescence.

Figure 7-38. LACP Parameters (Paramètres LACP)



La page LACP Parameters (Paramètres LACP) contient les champs suivants :

LACP System Priority (1-65535) (Priorité du système LACP [1 à 65535]) : valeur de priorité LACP des paramètres globaux. Les valeurs possibles vont de 1 à 65535. La valeur 1 est utilisée par défaut.

Select a Port (Sélectionner un port) : numéro du port auquel les valeurs d'expiration et de priorité sont associées.

LACP Port Priority (1-65535) (Priorité du port LACP [1 à 65535]) : valeur de priorité LACP du port.

LACP Timeout (Délai d'expiration LACP) : délai d'expiration administratif LACP. Ce champ peut prendre les valeurs suivantes :

Short (Court) : spécifie une valeur de délai d'expiration court.

Long : spécifie une valeur de délai d'expiration long.

Définition des paramètres globaux d'agrégation de liaisons

1. Affichez la page LACP Parameters (Paramètres LACP).
2. Complétez le champ **LACP System Priority** (Priorité du système LACP).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont définis et l'unité est mise à jour.

Définition des paramètres des ports à agrégation de liaisons

1. Affichez la page LACP Parameters (Paramètres LACP).
2. Complétez les champs de la zone **Port Parameters** (Paramètres des ports).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont définis et l'unité est mise à jour.

Affichage de la page LACP Parameters Table (Table des paramètres LACP)

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

La page **LACP Port Parameters Table** (Table des paramètres LACP) s'affiche.

Configuration des paramètres LACP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la configuration des paramètres LACP, comme indiqué à la page LACP Parameters (Paramètres LACP).

Tableau 7-27. Commandes CLI relatives aux paramètres LACP

Commande CLI	Description
lacp system-priority *valeur*	Configure la priorité du système.
lacp port-priority *valeur*	Configure la valeur de priorité des ports physiques.
lacp timeout {**long** | **short**}	Affecte un délai d'expiration LACP administratif.
show lacp ethernet *interface* [**parameters** | **statistics** | **protocol-state**]	Affiche les informations LACP des ports ethernet.

Voici un exemple de commandes CLI :

```
Console (config)# lacp
system-priority 120


Console (config)#
interface ethernet 1/e11


Console (config-if)# lacp
port-priority 247


Console (config-if)# lacp
timeout long


Console (config-if)# end


Console# show lacp
ethernet 1/e11 statistics


Port 1/e11 LACP
Statistics:


LACP PDUs sent:2


LACP PDUs received:2
```

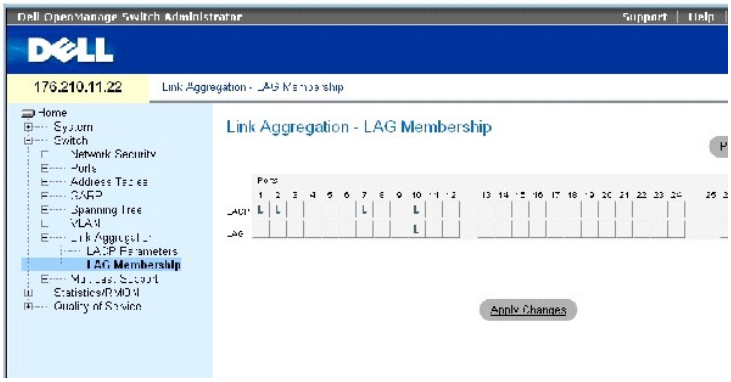
Définition de l'appartenance à un LAG

L'unité prend en charge huit LAG par système, et huit ports par LAG, qu'elle soit autonome ou intégrée à une pile.

Lorsqu'un port est ajouté à un LAG, il adopte automatiquement ses propriétés. Si le port ne peut pas être configuré avec les propriétés du LAG, il n'est pas ajouté au LAG. Un message d'erreur s'affiche. Cependant, si le premier port qui se connecte au LAG ne peut pas être configuré avec les paramètres du LAG, il est ajouté au LAG avec ses paramètres de port par défaut. Un message d'erreur s'affiche. Cependant, comme il s'agit du seul port du LAG, la totalité du LAG utilise les paramètres du port au lieu des paramètres définis pour le LAG.

Utilisez la page **LAG Membership (Appartenance à un LAG)** pour associer des ports aux LAG. Pour ouvrir la page **LAG Membership (Appartenance à un LAG)**, cliquez sur **Switch** (Commutateur) → **Link Aggregation** (Agrégation de liaisons) → **LAG Membership** (Appartenance à un LAG) dans l'arborescence.

Figure 7-39. LAG Membership (Appartenance à un LAG)



La page **LAG Membership (Appartenance à un LAG)** contient les champs suivants :

LACP : agrège le port dans un LAG à l'aide de LACP.

LAG : ajoute un port à un LAG et indique le LAG spécifique auquel le port appartient.

Ajout de ports à un LAG ou LACP

1. Affichez la page **LAG Membership (Appartenance à un LAG)**.
2. À l'aide du bouton de la ligne LAG (deuxième ligne), spécifiez un numéro afin d'agréger ou de supprimer le port sur ce numéro de LAG.
3. À l'aide du bouton de la ligne LACP (première ligne), spécifiez un numéro de port afin d'associer le LACP ou le LAG statique.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port est ajouté au LAG ou LACP et l'unité est mise à jour.

Ajout de ports à des LAG à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant l'affectation de ports à des LAG, comme indiqué à la page **LAG Membership (Appartenance à un LAG)**.

Tableau 7-24. Commandes CLI relatives à l'appartenance à un LAG

Commande CLI	Description
channel-group *numéro-canal-port* **mode** {**on** | **auto**}	Associe un port à un canal de port. Utilisez la forme "no" de cette commande pour supprimer la configuration canal-groupe de l'interface.
show interfaces port-channel [*numéro-canal-port*]	Affiche les informations sur le port/canal.

Voici un exemple de commandes CLI :

```
console(config)# interface
ethernet 1/e11

console(config-if)#
channel-group 1 mode on
```

Prise en charge du transfert multidiffusion

Le transfert multidiffusion permet la diffusion d'un même paquet à plusieurs destinations. Le service de multidiffusion de couche 2 est basé sur une unité de couche 2 recevant un seul paquet destiné à une adresse de multidiffusion spécifique. Le transfert multidiffusion crée des copies de ce paquet et transmets les paquets aux ports appropriés.

Registered Multicast traffic (Trafic multidiffusion enregistré) : si le trafic destiné à un groupe de multidiffusion enregistré s'affiche, il est géré par une entrée de la base de données de filtrage de multidiffusion et transféré uniquement aux ports enregistrés.

Unregistered Multicast traffic (Trafic multidiffusion non enregistré) : si le trafic destiné à un groupe de multidiffusion non enregistré s'affiche, il est géré par une entrée spéciale de la base de données de filtrage de multidiffusion. La configuration par défaut consiste à acheminer tout le trafic de ce type (trafic dans des groupes de multidiffusion non enregistrés).

L'unité prend en charge les opérations suivantes :

- **Forwarding L2 Multicast Packets** (Transfert des paquets multidiffusion de couche 2) : transfère les paquets multidiffusion de couche 2. Le filtrage multidiffusion de couche 2 est activé par défaut et n'est pas configurable par l'utilisateur.

REMARQUE : le système prend en charge le filtrage de multidiffusion de 256 groupes de multidiffusion.

- **Filtering L2 Multicast Packets** (Filtrage des paquets multidiffusion de couche 2) : transfère les paquets de couche 2 vers des interfaces. Si le filtrage de multidiffusion est désactivé, les paquets multidiffusion sont acheminés vers tous les ports correspondants.

Pour ouvrir la page **Multicast Support** (Prise en charge de la multidiffusion), cliquez sur **Switch** (Commutateur) → **Multicast Support** (Prise en charge de la multidiffusion) dans l'arborescence.

Définition des paramètres globaux de multidiffusion

Par défaut, la commutation de couche 2 transmet les paquets multidiffusion vers tous les ports de VLAN appropriés et gère le paquet comme une seule transmission de multidiffusion. Bien qu'opérationnel, ce type de transfert ne constitue pas la solution optimale car les paquets multidiffusion sont également envoyés vers des ports inappropriés. Cela entraîne une augmentation du trafic réseau. Les filtres de transfert de multidiffusion permettent de transférer les paquets de couche 2 vers des sous-ensembles de ports.

Lorsque la surveillance IGMP est activée de façon globale, tous les paquets IGMP sont transférés vers l'UC. L'UC analyse les paquets entrants et détermine :

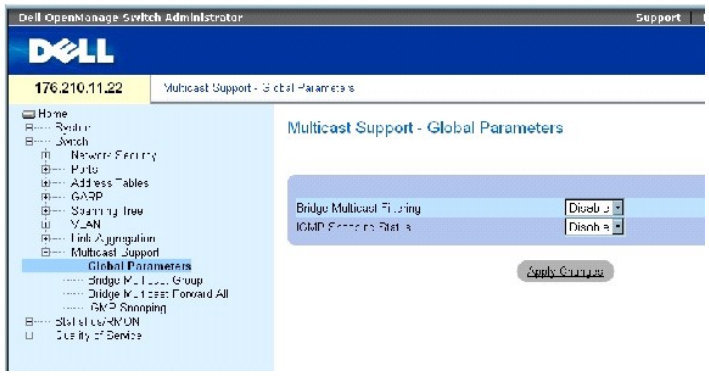
- quels ports veulent se joindre aux groupes de multidiffusion ;
- quels ports possèdent des routeurs multidiffusion générant des requêtes IGMP ;
- quels protocoles de routage transfèrent les paquets et le trafic de multidiffusion.

Les ports souhaitant se joindre à un groupe de multidiffusion spécifique émettent un rapport IGMP indiquant que ce groupe de multidiffusion accepte des membres. Cela entraîne la création de la base de données de filtrage de multidiffusion.

Pour ouvrir la page **Multicast Support** (Prise en charge de la multidiffusion), cliquez sur **Switch** (Commutateur) → **Multicast Support** (Prise en charge de la multidiffusion) dans l'arborescence.

La page **Global Parameters (Paramètres globaux)** contient des champs permettant d'activer la surveillance IGMP sur l'unité. Pour ouvrir la page **Global Parameters (Paramètres globaux)**, cliquez sur **Switch** (Commutateur) → **Multicast Support** (Prise en charge de la multidiffusion) → **Global Parameters** (Paramètres globaux) dans l'arborescence.

Figure 7-40. Global Parameters (Paramètres globaux)



La page **Global Parameters (Paramètres globaux)** 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 de la surveillance IGMP) : active ou désactive la surveillance IGMP sur l'unité. La valeur par défaut est Disabled (Désactivé). La surveillance IGMP peut être activée uniquement si la page **Global Parameters (Paramètres globaux)** est affichée.

Activation du filtrage de multidiffusion par ponts sur l'unité

1. Affichez la page **Global Parameters (Paramètres globaux)**.
2. Sélectionnez **Enable** (Activer) dans le champ **Bridge Multicast Filtering** (Filtrage de multidiffusion par ponts).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le *filtrage* de multidiffusion par ponts est activé sur l'unité.

Activation de la surveillance IGMP sur l'unité

1. Affichez la page **Global Parameters (Paramètres globaux)**.
2. Sélectionnez **Enable** (Activer) dans le champ **IGMP Snooping Status** (État de la surveillance IGMP).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La surveillance IGMP est activée sur l'unité.

Activation du filtrage de multidiffusion et de la surveillance IGMP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant l'activation du filtrage de multidiffusion et de la surveillance IGMP, comme indiqué à la page **Global Parameters (Paramètres globaux)**.

Tableau 7-25. Commandes CLI relatives au filtrage de multidiffusion et à la surveillance

Commande CLI	Description
bridge multicast filtering	Active le filtrage des adresses de multidiffusion.
ip igmp snooping	Active la surveillance IGMP (Internet Group Membership Protocol).

Voici un exemple de commandes CLI :

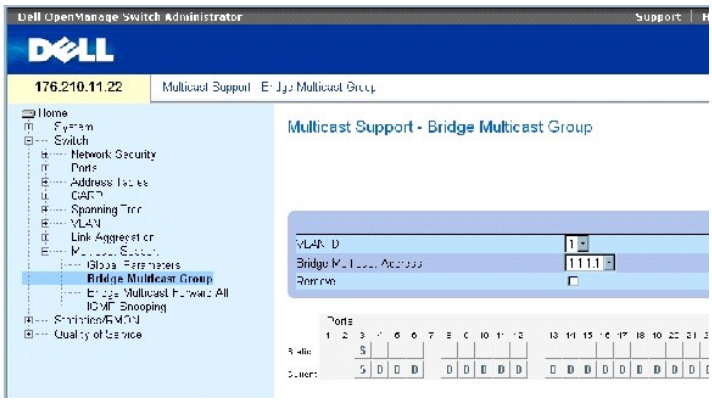
```
console(config)# bridge
multicast filtering

console(config)# ip igmp
snooping
```

Ajout de membres à une adresse de multidiffusion par ponts

La page **Bridge Multicast Group (Groupe de multidiffusion par ponts)** affiche les ports et les LAG connectés au groupe de service de multidiffusion dans les tables **Ports** et **LAG**. Ces tables reflètent également la manière dont le port ou le LAG s'est joint au groupe de multidiffusion. Les ports peuvent être ajoutés soit à des groupes existants, soit à de nouveaux groupes de service de multidiffusion. La page **Bridge Multicast Group (Groupe de multidiffusion par ponts)** permet la création de nouveaux groupes de service de multidiffusion. La page **Bridge Multicast Group (Groupe de multidiffusion par ponts)** permet également d'affecter des ports à un groupe d'adresses de service de multidiffusion spécifique.

Pour ouvrir la page **Bridge Multicast Group (Groupe de multidiffusion par ponts)**, cliquez sur **Switch** (Commutateur) → **Multicast Support** (Prise en charge de la multidiffusion) → **Bridge Multicast Group** (Groupe de multidiffusion par ponts) dans l'arborescence.

Figure 7-41. Bridge Multicast Group (Groupe de multidiffusion par ponts)



La page **Bridge Multicast Group (Groupe de multidiffusion par ponts)** contient les champs suivants :

VLAN ID (ID de VLAN) : identifie un VLAN et contient des informations sur l'adresse du groupe de multidiffusion.

Bridge Multicast Address (Adresse de multidiffusion par ponts) : identifie l'adresse MAC ou IP du groupe de multidiffusion.

Remove (Supprimer) : supprime une adresse de multidiffusion par ponts.

Ports : ports pouvant être ajoutés à un service de multidiffusion.

LAG : LAG pouvant être ajoutés à un service de multidiffusion.

Le tableau suivant contient les paramètres de gestion des membres des ports et des LAG IGMP :

Tableau 7-26. Paramètres de contrôle de la table des membres des ports/LAG IGMP

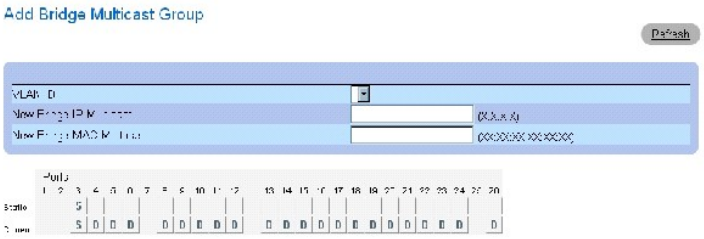
Contrôle du port	Définition
D	Le port/LAG a rejoint le groupe de multidiffusion de façon dynamique à la ligne *Current* (Actuel).
S	Rattache le port au groupe de multidiffusion en tant que membre statique à la ligne *Static* (Statique). Le port/LAG a rejoint le groupe de multidiffusion de façon statique à la ligne *Current* (Actuel).
F	Forbidden (Interdit).
Néant	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 (Ajout d'un groupe de multidiffusion par ponts)** s'affiche.

Figure 7-42. Add Bridge Multicast Group (Ajout d'un groupe de multidiffusion par ponts)



3. Définissez les champs **VLAN ID** (ID de VLAN) et **New Bridge Multicast Address** (Nouvelle adresse de multidiffusion par ponts).
4. Faites basculer un port vers la valeur **S** pour le rattacher au groupe de multidiffusion sélectionné.
5. Faites basculer un port vers la valeur **F** pour interdire l'ajout d'adresses de multidiffusion à un port spécifique.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse de multidiffusion par ponts est affectée au groupe de multidiffusion et l'unité est mise à jour.

Configuration des ports pour la réception d'un service de multidiffusion

1. Affichez la page **Bridge Multicast Group (Groupe de multidiffusion par ponts)**.
2. Définissez les champs **VLAN ID** (ID de VLAN) et **Bridge Multicast Address** (Adresse de multidiffusion par ponts).
3. Faites basculer un port vers la valeur **S** pour le rattacher au groupe de multidiffusion sélectionné.
4. Faites basculer un port vers la valeur **F** pour interdire l'ajout d'adresses de multidiffusion à un port spécifique.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port est affecté au groupe de multidiffusion et l'unité est mise à jour.

Affectation des LAG pour la réception d'un service de multidiffusion

1. Affichez la page **Bridge Multicast Group (Groupe de multidiffusion par ponts)**.
2. Définissez les champs **VLAN ID** (ID de VLAN) et **Bridge Multicast Address** (Adresse de multidiffusion par ponts).
3. Faites basculer le LAG vers la valeur **S** pour le rattacher au groupe de multidiffusion sélectionné.
4. Faites basculer le LAG port vers la valeur **F** pour interdire l'ajout d'adresses de multidiffusion à un LAG spécifique.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le LAG est affecté au groupe de multidiffusion et l'unité est mise à jour.

Gestion des membres du service de multidiffusion à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la gestion des membres du service de multidiffusion, comme indiqué à la page **Bridge Multicast Group (Groupe de multidiffusion par ponts)**.

Tableau 7-27. Commandes CLI relatives aux membres du service de multidiffusion

Commande CLI	Description
bridge multicast address {*adresse-multidiffusion-mac* | *adresse-multidiffusion-ip*}	Enregistre les adresses de multidiffusion de couche MAC dans la table des ponts et ajoute des ports statiques au groupe.
bridge multicast forbidden address {*adresse-multidiffusion-mac* | *adresse-multidiffusion-ip*}[**add** | **remove**] {**ethernet** *liste-interfaces* | **port-channel** *liste-numéros-canal-port*}	Interdit l'ajout d'une adresse de multidiffusion à des ports spécifiques. Utilisez la forme "no" de cette commande pour rétablir les valeurs par défaut.
show bridge multicast address-table [**vlan** *id-vlan*id] [**address** {*adresse-multidiffusion-mac* | *adresse-multidiffusion-ip*}] [**format ip** | **mac**]	Affiche des informations sur la table des adresses MAC de multidiffusion.

Voici un exemple de commandes CLI :

```
Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet 1/e11,1/e12

console(config-if)# end

console # show bridge multicast address-table
```

Vlan	MAC Address	Type	Ports
----	----------	-----	----------
1	0100.5e02.0203	static	1/e11, 1/e12
19	0100.5e02.0208	static	1/e11-16
19	0100.5e02.0208	dynamic	1/e11-12

```
Forbidden ports for multicast addresses:
```

Vlan	MAC Address	Ports	
----	----------	----------	
1	0100.5e02.0203	1/e8	
19	0100.5e02.0208	1/e8	

```
console # show bridge multicast address-table format ip
```

Vlan	IP Address	Type	Ports
----	----------	-----	----------
1	224-239.130|2.2.3	static	1/e11, 1/e12
19	224-239.130|2.2.8	static	1/e11-16

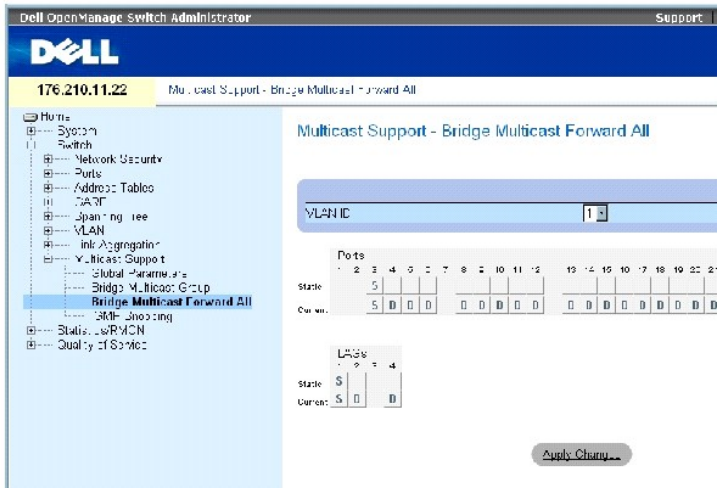
19	224-239.130|2.2.8	dynamic	1/e11-12
Forbidden ports for multicast addresses:			
Vlan	IP Address	Ports	
----	----------	----------	
1	224-239.130|2.2.3	1/e8	
19	224-239.130|2.2.8	1/e8	

Affectation de paramètres de transfert multidiffusion total

La page **Bridge Multicast Forward All (Transfert multidiffusion total par ponts)** contient des champs permettant de rattacher des ports ou des LAG à une unité elle-même rattachée à un routeur ou commutateur multidiffusion voisin. Une fois la surveillance IGMP activée, les paquets multidiffusion sont transférés au port ou au VLAN approprié.

Pour ouvrir la page **Bridge Multicast Forward All (Transfert multidiffusion total par ponts)**, cliquez sur **Switch** (Commutateur) → **Multicast Support** (Prise en charge de la multidiffusion) → **Bridge Multicast Forward All (Transfert multidiffusion total par ponts)** dans l'arborescence.

Figure 7-43. Bridge Multicast Forward All (Transfert multidiffusion total par ponts)



La page Bridge Multicast Forward All (Transfert multidiffusion total par ponts) contient les champs suivants :

VLAN ID (ID de VLAN) : identifie un VLAN.

Ports : ports pouvant être ajoutés à un service de multidiffusion.

LAG : LAG pouvant être ajoutés à un service de multidiffusion.

La page **Gestion de la table des valeurs de contrôle des commutateurs/ports de transfert multidiffusion par ponts** contient les paramètres permettant de gérer la configuration des commutateurs et des ports.

Gestion de la table des valeurs de contrôle des commutateurs/ports de transfert multidiffusion par ponts

Le tableau suivant décrit les paramètres utilisés pour définir les contrôles des ports.

Tableau 7-28. Gestion de la table des valeurs de contrôle des commutateurs/ports de transfert multidiffusion par ponts

Contrôle du port	Définition
D	Rattache le port à un routeur ou commutateur multidiffusion en tant que port dynamique.
S	Rattache le port à un routeur ou commutateur multidiffusion en tant que port statique.
F	Forbidden (Interdit).
Néant	Le port n'est pas rattaché à un routeur ou commutateur multidiffusion.

Rattachement d'un port à un routeur ou commutateur multidiffusion

1. Affichez la page **Bridge Multicast Forward All (Transfert multidiffusion total par ponts)**.
2. Définissez le champ **VLAN ID** (ID de VLAN).
3. Sélectionnez un port dans la table des **ports** et affectez-lui une valeur.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port est rattaché à un routeur ou commutateur multidiffusion.

Rattachement d'un LAG à un routeur ou commutateur multidiffusion

1. Affichez la page **Bridge Multicast Forward All (Transfert multidiffusion total par ponts)**.
2. Définissez le champ **VLAN ID** (ID de VLAN).
3. Sélectionnez un port dans la table des **LAG** et affectez-lui une valeur.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le LAG est rattaché à un routeur ou commutateur multidiffusion.

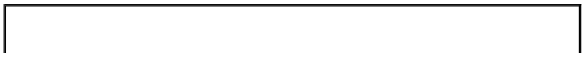
Gestion des LAG et des ports rattachés aux routeurs multidiffusion à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes permettant la gestion des LAG et des ports rattachés aux routeurs multidiffusion, comme indiqué à la page **Bridge Multicast Forward All (Transfert multidiffusion total par ponts)**.

Tableau 7-29. Commandes CLI de gestion des LAG et des ports rattachés aux routeurs multidiffusion

Commande CLI	Description
show bridge multicast filtering *id-vlan*	Affiche la configuration de filtrage de multidiffusion.
bridge multicast forward-all {**add** | **remove**} {**ethernet** *liste-interfaces* | **canal-port** *liste-numéro-canal-port*}	Active le transfert de tous les paquets multidiffusion sur un port. Utilisez la forme "no" de cette commande pour rétablir les valeurs par défaut.

Voici un exemple de commandes CLI :



```
Console(config)# interface vlan 1

Console(config-if)# bridge multicast forward-all add ethernet 1/e3

Console(config-if)# end

Console# show bridge multicast filtering 1

Filtering: Enabled

VLAN:     Forward-All

Port      Static            Status
-------   ----------------  -----------
1/e11     Forbidden         Filter
1/e12     Forward           Forward(s)
1/e13     -                 Forward(d)
```

Surveillance IGMP

La page **IGMP Snooping** (Surveillance IGMP) contient des champs permettant l'activation de la surveillance IGMP pour chaque VLAN et la définition du délai d'expiration des paquets. Pour ouvrir la page **IGMP Snooping (Surveillance IGMP)**, cliquez sur **Switch** (Commutateur) → **Multicast Support** (Prise en charge de la multidiffusion) → **IGMP Snooping** (Surveillance IGMP) dans l'arborescence.

Figure 7-44. IGMP Snooping (Surveillance IGMP)

VLAN ID (ID de VLAN): spécifie l'ID du réseau local virtuel.

IGMP Snooping Status (État de la surveillance IGMP) : active ou désactive la surveillance IGMP sur le VLAN.

Auto Learn (Apprentissage automatique) : active ou désactive l'apprentissage automatique sur l'unité Ethernet.

Host Timeout (1-2147483647) (Délai d'expiration de l'hôte [1 à 2147483647]) : délai avant expiration d'une entrée de surveillance IGMP. La valeur par défaut est de 260 secondes.

Multicast Router Timeout (1-2147483647) (Délai d'expiration du routeur multidiffusion [1 à 2147483647]) : délai d'expiration d'une entrée du routeur multidiffusion. La valeur par défaut est de 300 secondes.

Leave Timeout (0-2147483647) (Délai de sortie [0 à 2147483647]) : délai en secondes entre la réception d'un message de sortie du port et l'expiration d'une entrée. La valeur par défaut est de 10 secondes.

Activation de la surveillance IGMP sur l'unité

1. Affichez la page **IGMP Snooping (Surveillance IGMP)**.
2. Sélectionnez l'ID de VLAN de l'unité sur laquelle la surveillance IGMP doit être activée.
3. Sélectionnez **Enable** (Activer) dans le champ **IGMP Snooping Status** (État de la surveillance IGMP).
4. Remplissez les champs se trouvant sur cette page.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La surveillance IGMP est activée sur l'unité.

Affichage de la page IGMP Snooping Table (Table de surveillance IGMP)

1. Affichez la page **IGMP Snooping (Surveillance IGMP)**.
2. Cliquez sur **Show All** (Afficher tout).

La page **IGMP Snooping Table** (Table de surveillance IGMP) s'affiche.

Configuration de la surveillance IGMP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI permettant de configurer les informations de la page IGMP Snooping (Surveillance IGMP).

Tableau 7-30. Commandes CLI relatives à la surveillance IGMP

Commande CLI	Description
ip igmp snooping	Active la surveillance IGMP (Internet Group Membership Protocol).
ip igmp snooping mrouter learn-pim-dvmrp	Active l'apprentissage automatique des ports des routeurs multidiffusion dans le contexte d'un VLAN spécifique.
ip igmp snooping host-time-out délai-expiration	Configure le délai d'expiration de l'hôte.
ip igmp snooping mrouter-time-out *délai-expiration*	Configure le délai d'expiration du routeur multidiffusion.
ip igmp snooping leave-time-out {*délai-expiration* | **immediate-leave**}	Configure le délai d'expiration de sortie.
show ip igmp snooping groups [**vlan** *id-vlan*] [**address** *adresse-multidiffusion-ip*]	Affiche les groupes de multidiffusion appris par la surveillance IGMP.
show ip igmp snooping interface *id-vlan*	Affiche la configuration de la surveillance IGMP.
show ip igmp snooping mrouter [id-vlan interface]	Affiche des informations sur les interfaces du routeur multidiffusion apprises de façon dynamique.

Voici un exemple de commandes CLI :

```
console> enable
```

```
console# config


console(config)# ip igmp snooping


console(config)# interface vlan 1


console(config-if)# ip igmp
snooping mrouter learn-pim-dvmrp


console(config-if)# ip igmp
snooping host-time-out 300


Console(config-if)# ip igmp
snooping mrouter-time-out 200


console(config-if)# ip igmp
snooping leave-time-out 60


console(config-if)# end


console# show ip igmp snooping
groups
```

Vlan	IP Address	Querier	Ports
1	224-239.130|2.2.3	Yes	1/e11, 1/e12
19	224-239.130|2.2.8	Yes	1/e11-13

```
console# show ip igmp snooping
interface 1/e1


IGMP Snooping is globally enabled


IGMP Snooping is enabled on VLAN 1


IGMP host timeout is 300 sec


IGMP Immediate leave is disabled.
IGMP leave timeout is 60 sec


IGMP mrouter timeout is 200 sec


Automatic learning of multicast
router ports is enabled


console# show ip igmp snooping
```

mrouter

VLAN	Ports		
----	------		
1	1/e11		

Retour au sommaire

Retour au sommaire

Affichage des statistiques

Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

Les pages de **statistiques** fournissent des informations relatives aux interfaces, aux réseaux virtuels dynamiques (GVRP), à Etherlike, à la télésurveillance (RMON) et à l'utilisation de l'unité. Pour ouvrir la page **Statistics** (Statistiques), cliquez sur **Statistics** dans l'arborescence.

REMARQUE : il n'existe aucune commande CLI pour les pages de statistiques.

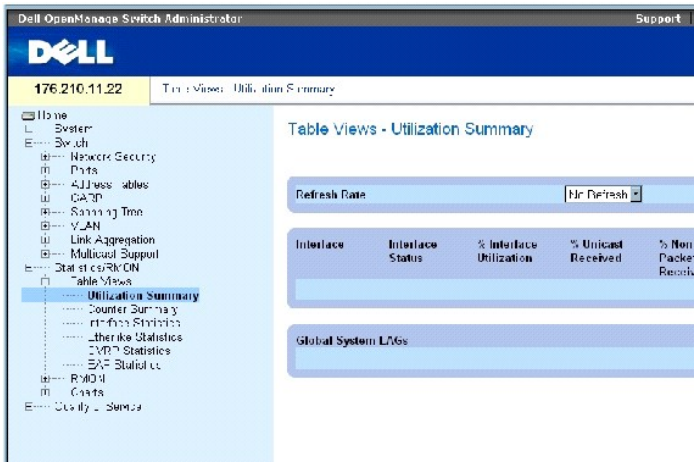
Affichage des tables

La page **Table View** (Vue Tables) contient des liens qui permettent d'afficher les statistiques sous forme de table. Pour ouvrir la page, cliquez sur **Statistics** (Statistiques) → **Table** (Table) dans l'arborescence.

Affichage du récapitulatif de l'utilisation

La page Utilization Summary (Récapitulatif de l'utilisation) contient des statistiques sur l'utilisation de l'interface. Pour ouvrir cette page, cliquez sur **Statistics** (Statistiques) → **Table Views** (Vues Tables) → **Utilization Summary** dans l'arborescence.

Figure 8-1. Utilization Summary (Récapitulatif de l'utilisation)



REMARQUE : l'écran est actualisé régulièrement pour minimiser l'impact de l'affichage sur les ordinateurs dotés d'une faible quantité de mémoire. Il est possible que vous observiez une interruption de l'affichage pendant cette mise à jour.

La page Utilization Summary (Récapitulatif de l'utilisation) contient les champs suivants :

Refresh Rate (Intervalle de rafraîchissement) : indique le délai qui s'écoule entre deux actualisations des statistiques sur les interfaces.

Interface : numéro de l'interface.

Interface Status (État de l'interface) : indique l'état de l'interface.

% Interface Utilization (% d'utilisation de l'interface) : pourcentage d'utilisation de l'interface réseau, basé sur le mode duplex. La plage de valeurs de ce champ s'étend de 0 à 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.

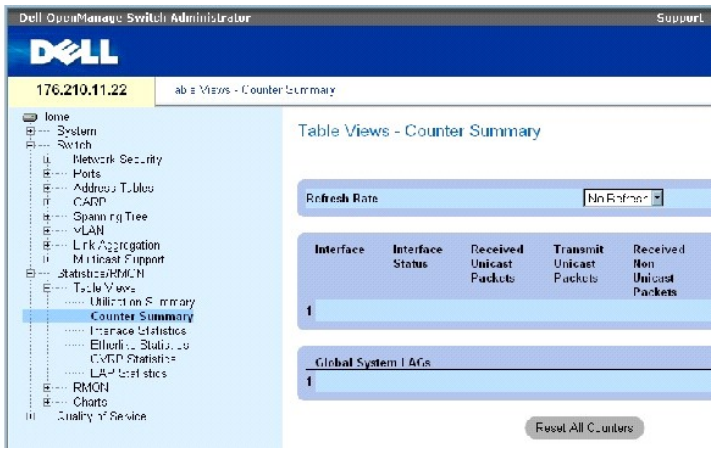
% Error Packets Received (% de paquets avec erreurs reçus) : indique le pourcentage de paquets contenant des erreurs ayant été reçus sur l'interface.

Global System LAGs (LAG système globaux) : indique l'utilisation en cours des LAG globaux.

Affichage du récapitulatif des compteurs

La page **Counter Summary (Récapitulatif des compteurs)** affiche des statistiques sur l'utilisation des ports sous forme numérique et non sous forme de pourcentages. Pour ouvrir la page **Counter Summary (Récapitulatif des compteurs)**, cliquez sur **Statistics / RMON** (Statistiques/RMON) → **Table Views** (Vues Tables) → **Counter Summary** (Récapitulatif des compteurs) dans l'arborescence.

Figure 8-2. Counter Summary (Récapitulatif des compteurs)



La page Counter Summary (Récapitulatif des compteurs) contient les champs suivants :

Refresh Rate (Intervalle de rafraîchissement) : indique le délai qui s'écoule entre deux actualisations des statistiques sur les interfaces.

Interface : numéro de l'interface.

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.

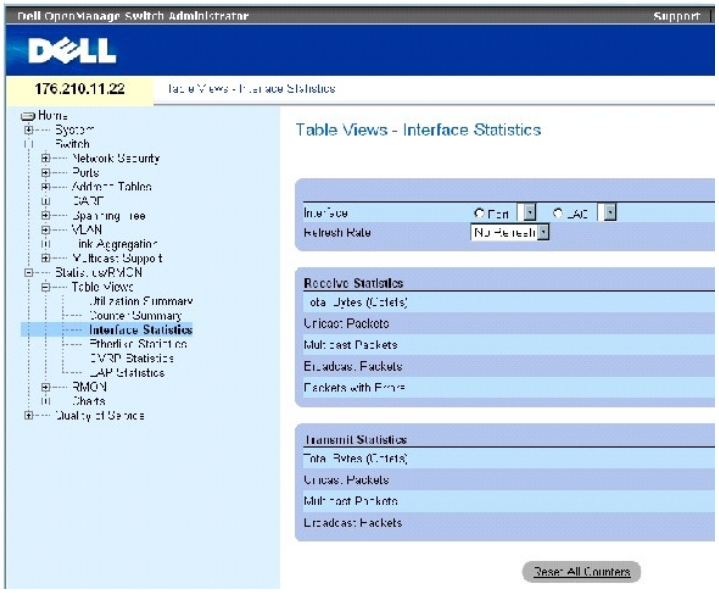
Received Errors (Erreurs reçues) : indique le nombre de paquets contenant des erreurs ayant été reçus sur l'interface.

Global System LAGs (LAG système globaux) : affiche un compteur récapitulatif pour les LAG système globaux.

Affichage des statistiques sur les interfaces

La page **Interface Statistics (Statistiques sur les interfaces)** contient des statistiques sur les paquets reçus et transmis. Les zones relatives à ces deux types de paquets sont identiques. Pour ouvrir la page **Interface Statistics (Statistiques sur les interfaces)**, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Table Views** (Vues Tables) → **Interface Statistics** (Statistiques sur les interfaces) dans l'arborescence.

Figure 8-3. Interface Statistics (Statistiques sur les interfaces)



La page **Interface Statistics (Statistiques sur les interfaces)** contient les champs suivants :

Interface : indique si les statistiques affichées concernent un port ou un LAG.

Refresh Rate (Intervalle de rafraîchissement) : intervalle écoulé entre deux actualisations des statistiques.

Statistiques de réception

Total Bytes (Octets) Received (Nb total d'octets reçus) : affiche le nombre total d'octets reçus sur l'interface sélectionnée.

Unicast Packets (Paquets monodiffusion reçus) : nombre de paquets monodiffusion reçus sur l'interface sélectionnée.

Multicast Packets (Paquets multidiffusion reçus) : nombre de paquets multidiffusion reçus sur l'interface sélectionnée.

Broadcast Packets (Paquets de diffusion reçus) : nombre de paquets de diffusion reçus sur l'interface sélectionnée.

Statistiques de transmission

Total Bytes (Octets) (Nb total d'octets) : affiche le nombre total d'octets transmis à partir de l'interface sélectionnée.

Unicast Packets (Paquets monodiffusion) : nombre de paquets monodiffusion transmis à partir de l'interface sélectionnée.

Multicast Packets (Paquets multidiffusion) : nombre de paquets multidiffusion transmis à partir de l'interface sélectionnée.

Broadcast Packets (Paquets de diffusion) : nombre de paquets de diffusion transmis à partir de l'interface sélectionnée.

Affichage des statistiques sur les interfaces

1. Affichez la page **Interface Statistics (Statistiques sur les interfaces)**.
2. Sélectionnez une interface dans le champ approprié.

Les statistiques relatives à l'interface sélectionnée s'affichent.

Réinitialisation des compteurs de statistiques sur les interfaces

1. Affichez la page **Interface Statistics (Statistiques sur les interfaces)**.
2. Cliquez sur **Reset All Counters** (Réinitialiser tous les compteurs).

Les compteurs sont réinitialisés.

Affichage des statistiques sur les interfaces à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant d'afficher les statistiques sur les interfaces.

Tableau 8-1. Commandes CLI pour l'affichage des statistiques sur les interfaces

Commande CLI	Description
show interfaces counters [**ethernet** *interface* | **port- channel** *numéro_canal_port*]	Affiche le trafic enregistré par l'interface physique.

Voici un exemple de commandes CLI.

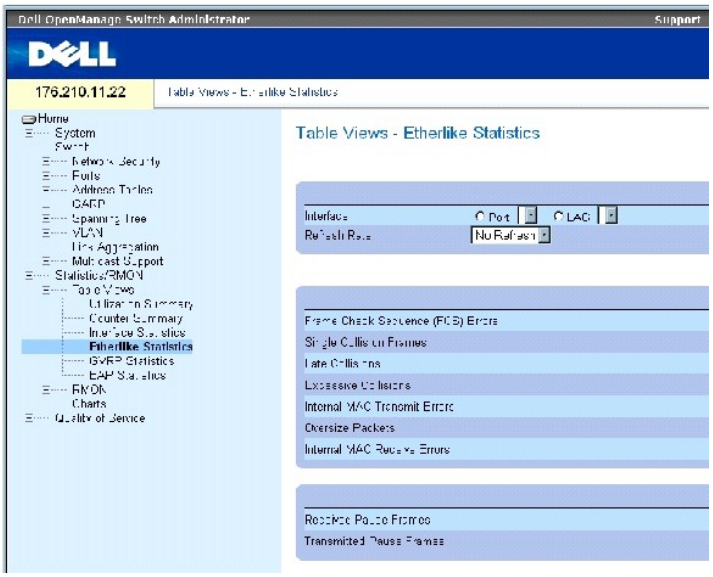
```
console> enable
```

```
console# show interfaces counters

Port InOctets InUcastPkts InMcastPkts InBcastPkts

------ --------- ----------- ----------- -----------

1/e1 0 0 0 0

1/e2 0 0 0 0

1/e3 0 0 0 0

1/e4 0 0 0 0

1/e5 0 0 0 0

1/ e6 0 0 0 0

1/e7 0 0 0 0

1/e8 0 0 0 0

1/e9 0 0 0 0

1/e10 0 0 0 0
```

Affichage des statistiques Etherlike

La page **Etherlike Statistics (Statistiques Etherlike)** contient des statistiques sur les erreurs liées aux interfaces. Pour ouvrir la page **Etherlike Statistics (Statistiques Etherlike)**, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Table Views** (Vues Tables) → **Etherlike Statistics** (Statistiques Etherlike) dans l'arborescence.

Figure 8-4. Etherlike Statistics (Statistiques Etherlike)



La page **Etherlike Statistics (Statistiques Etherlike)** contient les champs suivants :

Interface : indique si les statistiques affichées concernent un port ou un LAG.

Refresh Rate (Intervalle de rafraîchissement) : intervalle écoulé entre deux actualisations des statistiques.

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.

Single Collision Frames (Trames monocollision) : affiche le nombre d'erreurs de trames monocollision reçues sur l'interface sélectionnée.

Late Collision (Collision tardive) : affiche le nombre de collisions tardives reçues sur l'interface sélectionnée.

Oversize Packets (Paquets dépassant la taille limite) : nombre d'erreurs dues à des paquets trop longs sur l'interface sélectionnée.

Internal MAC Transmit Errors (Erreurs de transmission MAC internes) : affiche le nombre d'erreurs de transmission MAC internes reçues sur l'interface sélectionnée.

Received Pause Frames (Trames de pause reçues) : nombre d'erreurs de pause reçues sur l'interface sélectionnée.

Transmitted Pause Frames (Trames de pause transmises) : nombre d'erreurs de pause transmises sur l'interface sélectionnée.

Affichage des statistiques Etherlike sur une interface

1. Affichez la page **Etherlike Statistics (Statistiques Etherlike)**.
2. Sélectionnez une interface dans le champ approprié.

Réinitialisation des statistiques Etherlike

1. Affichez la page **Etherlike Statistics (Statistiques Etherlike)**.

2. Cliquez sur **Reset All Counters** (Réinitialiser tous les compteurs).

Les compteurs Etherlike Statistics (Statistiques Etherlike) sont réinitialisés.

Affichage des statistiques Etherlike à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant d'afficher les statistiques Etherlike.

Tableau 8-2. Commandes CLI pour l'affichage des statistiques Etherlike

Commande CLI	Description
show interfaces counters [**ethernet** *interface* | **port- channel** numéro_canal_port]	Affiche le trafic enregistré par l'interface physique.

Voici un exemple de commandes CLI.

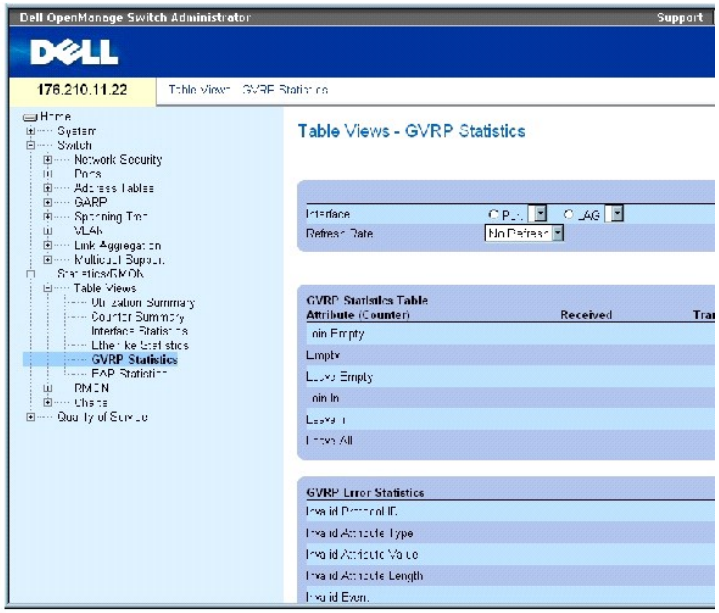
```
Console# show interfaces counters ethernet 1/1

Port    IN Octets   InUcastPkts   InMcastPkts   InBcastPkts
----    ---------   -----------   -----------   -----------
1/e1    183892      1289          987           8

Port    OUT         OutUcastPkts  OutMcastPkts  OutBcastPkts
        Octets
----    ----------  ------------  ------------  ------------
1/e1    9188        9             8             0

FCS Errors: 8

Single Collision Frames: 0

Multiple Collision Frames: 0

SQE Test Errors: 0

Deferred Transmissions: 0

Late Collisions: 0
```

Excessive Collisions: 0	
Internal MAC Tx Errors: 0	
Carrier Sense Errors: 0	
Oversize Packets: 0	
Internal MAC Rx Errors: 0	
Received Pause Frames: 0	
Transmitted Pause Frames: 0	

Affichage des statistiques GVRP

La page **GVRP Statistics (Statistiques GVRP)** contient des statistiques relatives aux réseaux virtuels dynamiques (GVRP). Pour ouvrir cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Table Views** (Vues Tables) → **GVRP Statistics** (Statistiques GVRP) dans l'arborescence.

Figure 8-5. GVRP Statistics (Statistiques GVRP)



La page **GVRP Statistics (Statistiques GVRP)** contient les champs suivants :

Interface : indique si les statistiques affichées concernent un port ou un LAG.

Refresh Rate (Intervalle de rafraîchissement) : intervalle écoulé entre deux actualisations des statistiques.

Join Empty : affiche les statistiques "Join Empty" relatives aux réseaux virtuels dynamiques de l'unité.

Leave Empty : affiche les statistiques "Leave Empty" relatives aux réseaux virtuels dynamiques de l'unité.

Empty : affiche les statistiques "Empty" relatives aux réseaux virtuels dynamiques de l'unité.

Join In : affiche les statistiques "Join In" relatives aux réseaux virtuels dynamiques de l'unité.

Leave In : affiche les statistiques "Leave In" relatives aux réseaux virtuels dynamiques de l'unité.

Leave All : affiche les statistiques "Leave All" relatives aux réseaux virtuels dynamiques de l'unité.

Invalid Protocol ID (ID de protocole incorrect) : affiche les statistiques relatives aux ID de protocole GVRP incorrects sur l'unité.

Invalid Attribute Type (Type d'attribut incorrect) : affiche les statistiques relatives aux ID d'attributs GVRP incorrects sur l'unité.

Invalid Attribute Value (Valeur d'attribut incorrecte) : affiche les statistiques relatives aux valeurs d'attributs GVRP incorrectes sur l'unité.

Invalid Attribute Length (Longueur d'attribut incorrecte) : affiche les statistiques relatives aux longueurs d'attributs GVRP incorrectes sur l'unité.

Invalid Events (Événements incorrects) : affiche les statistiques relatives aux événements GVRP incorrects sur l'unité.

Affichage des statistiques GVRP sur un port

1. Affichez la page **GVRP Statistics (Statistiques GVRP)**.
2. Sélectionnez une interface dans le champ approprié.

Les statistiques GVRP relatives à l'interface sélectionnée s'affichent.

Réinitialisation des statistiques GVRP

1. Affichez la page **GVRP Statistics (Statistiques GVRP)**.
2. Cliquez sur **Reset All Counters** (Réinitialiser tous les compteurs).

Les compteurs de statistiques GVRP sont réinitialisés.

Affichage des statistiques GVRP à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant d'afficher les statistiques GVRP.

Tableau 8-3. Commandes CLI pour l'affichage des statistiques GVRP

Commande CLI	Description
show gvrp statistics [**ethernet** *interface* | **port-channel** *numéro_canal_port*]	Affiche les statistiques GVRP.
	Affiche les statistiques d'erreurs GVRP.

show gvrp error- statistics [**ethernet** *interface* | **port-channel** *numéro_canal_port*]

Voici un exemple de commandes CLI :

```
console# show gvrp statistics

GVRP statistics:

---------------

Legend:

rJE: Join Empty Received

rJIn : Join In Received

rEmp : Empty Received

rLIn : Leave In Received

rLE : Leave Empty Received

rLA : Leave All Received

sJE : Join Empty Sent

sJIn : Join In Sent

sEmp : Empty Sent

sLIn : Leave In Sent

sLE : Leave Empty Sent

sLA : Leave All Sent
```

```
Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE
sLA

---- --- ---- ---- ---- --- --- --- --- --- ---- --- --
-
```

```
1/e1 0 0 0 0 0 0 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0 0 0 0 0 00 0
```

```
Console# show gvrp error-statistics

GVRP error statistics:

----------------

Legend:

INVPROT : Invalid Protocol Id

INVPLEN : Invalid PDU Length

INVATYP : Invalid Attribute Type

INVALEN : Invalid Attribute Length

INVAVAL : Invalid Attribute Value

INVEVENT : Invalid Event

Port INVPROT INVATYP INVAVAL INVPLEN INVALEN INVEVENT

---- ------- ------- ------- ------ - ------ - -------

1/e1 0 0 0 0 0 0 0

1/e2 0 0 0 0 0 0 0

1/e3 0 0 0 0 0 0 0

1/e4 0 0 0 0 0 0 0
```

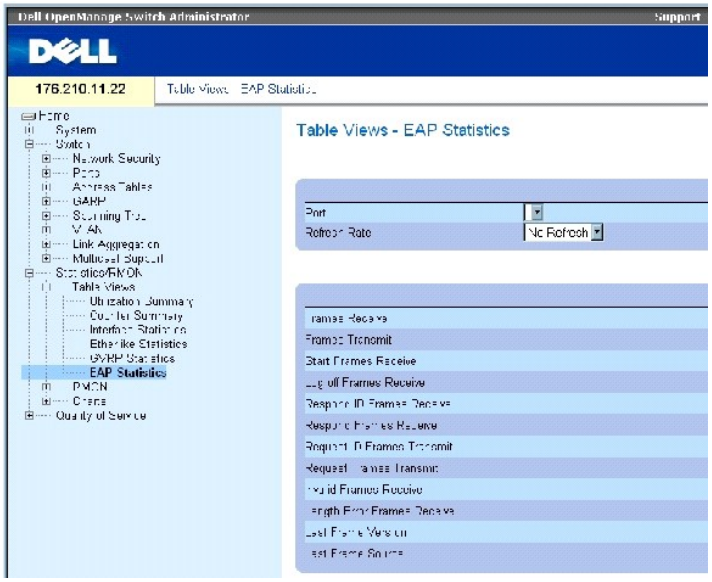
```
sLE : Leave Empty Sent

sLA : Leave All Sent
```

```
Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE
sLA


---- --- ---- ---- ---- --- --- --- --- --- ---- --- --
-


1/e1 0 0 0 0 0 0 0 0 0 0 0 0


1/e2 0 0 0 0 0 0 0 0 0 0 0 0


1/e3 0 0 0 0 0 0 0 0 0 0 0 0


1/e4 0 0 0 0 0 0 0 0 0 0 0 0


1/e5 0 0 0 0 0 0 0 0 0 0 0 0


1/e6 0 0 0 0 0 0 0 0 0 0 0 0


1/e7 0 0 0 0 0 0 0 0 0 0 0 0


1/e8 0 0 0 0 0 0 0 0 0 0 0 0
```

Affichage des 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, consultez la section "**Configuration de l'authentification basée sur le port**". Pour ouvrir la page **EAP Statistics (Statistiques EAP)**, cliquez sur **Statistics / RMON** (Statistiques/RMON) → Table Views (Vues Tables) → **EAP Statistics** (Statistiques EAP) dans l'arborescence.

Figure 8-6. EAP Statistics (Statistiques EAP)



La page **EAP Statistics (Statistiques EAP)** contient les champs suivants :

Port : indique le port sur lequel les données nécessaires aux statistiques sont collectées.

Refresh Rate (Intervalle de rafraîchissement) : intervalle écoulé entre deux actualisations des statistiques.

Frames Receive (Trames reçues) : indique le nombre de trames EAPOL valides reçues sur le port.

Frames Transmit (Trames transmises) : indique le nombre de trames EAPOL transmises par le port.

Start Frames Receive (Trames de début reçues) : indique le nombre de trames EAPOL de début reçues sur le port.

Log off Frames Receive (Trames de déconnexion reçues) : indique le nombre de trames EAPOL de déconnexion reçues sur le port.

Respond ID Frames Receive (Trames "Respond ID" reçues) : indique le nombre de trames EAP "Respond ID" reçues sur le port.

Respond Frames Receive (Trames "Respond" reçues) : indique le nombre de trames EAP "Respond" valides reçues sur le port.

Request ID Frames Transmit (Trames "Request ID" transmises) : indique le nombre de trames EAP "Request ID" transmises par le port.

Request Frames Transmit (Trames "Request" transmises) : indique le nombre de trames EAP "Request" transmises par le port.

Invalid Frames Receive (Trames non valides reçues) : indique le nombre de trames EAPOL non reconnues ayant été reçues sur le port.

Length Error Frames Receive (Trames de longueur incorrecte reçues) : indique le nombre de trames EAPOL de longueur incorrecte reçues sur le port.

Last Frame Version (Version de la dernière trame) : indique le numéro de version du protocole associé à la dernière trame EAPOL reçue.

Last Frame Source (Source de la dernière trame) : indique l'adresse MAC source associée à la dernière trame EAPOL reçue.

Affichage des statistiques EAP pour un port

1. Affichez la page **EAP Statistics (Statistiques EAP)**.
2. Sélectionnez une interface dans le champ approprié.

Les statistiques EAP relatives à l'interface s'affichent.

Pour réinitialiser les statistiques EAP :

1. Affichez la page **EAP Statistics (Statistiques EAP)**.
2. Cliquez sur Reset All Counters (Réinitialiser tous les compteurs).

Les compteurs de statistiques EAP sont réinitialisés.

Affichage des statistiques EAP à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant d'afficher les statistiques EAP.

Tableau 8-4. Commandes CLI pour l'affichage des statistiques EAP

Commande CLI	Description
show dot1x statistics	Affiche les statistiques 802.1X pour l'interface spécifiée.

Voici un exemple de commandes CLI :

```
console# show dot1x statistics ethernet 1/e1

EapolFramesRx: 11

EapolFramesTx: 12

EapolStartFramesRx: 1

EapolLogoffFramesRx: 1

EapolRespIdFramesRx: 3

EapolRespFramesRx: 6

EapolReqIdFramesTx: 3

EapolReqFramesTx: 6

InvalidEapolFramesRx: 0

EapLengthErrorFramesRx: 0

LastEapolFrameVersion: 1

LastEapolFrameSource: 0008.3b79.8787
```

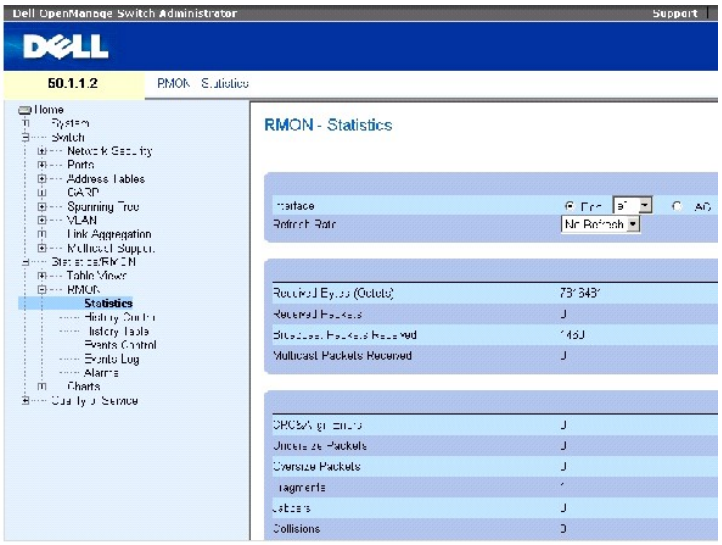
Affichage des statistiques RMON

La télésurveillance (Remote Monitoring, RMON) permet aux administrateurs réseau d'afficher des informations sur le réseau à partir d'un site distant. Pour ouvrir la page **RMON**, cliquez sur **Statistics / RMON** (Statistiques/RMON) → **RMON** dans l'arborescence.

Affichage d'un groupe de statistiques RMON

La page RMON Statistics (Statistiques RMON) permet d'afficher des informations sur l'utilisation de l'unité et sur les erreurs survenues sur celle-ci. Pour ouvrir la page RMON Statistics (Statistiques RMON), cliquez sur **Statistics / RMON** (Statistiques/RMON) → **RMON**→ **Statistics** (Statistiques) dans l'arborescence.

Figure 8-7. RMON Statistics (Statistiques RMON)



La page RMON Statistics (Statistiques RMON) contient les champs suivants :

Interface : identifie le port ou LAG correspondant aux statistiques affichées.

Refresh Rate (Intervalle de rafraîchissement) : intervalle écoulé entre deux actualisations des statistiques.

Received Bytes (Octets) (Nb d'octets reçus) : **affiche le nombre d'octets reçus sur l'interface sélectionnée.**

Received Packets (Nb de paquets reçus) : **affiche le nombre de paquets reçus sur l'interface sélectionnée.**

Broadcast Packets Received (Paquets de diffusion reçus) : nombre de paquets de diffusion valides reçus sur l'interface depuis la dernière actualisation de l'unité. Ce nombre n'inclut pas les paquets multidiffusion.

Multicast Packets Received (Paquets multidiffusion reçus) : nombre de paquets multidiffusion valides reçus sur l'interface depuis la dernière actualisation de l'unité.

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 de l'unité.

Undersize Packets (Paquets de longueur insuffisante) : nombre de paquets de moins de 64 octets ayant été reçus sur l'interface depuis la dernière actualisation de l'unité.

Oversize Packets (Paquets de longueur excessive) : nombre de paquets de plus de 1518 octets ayant été reçus sur l'interface depuis la dernière actualisation de l'unité.

Fragments : 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 de l'unité.

Jabbers (Jabotages) : nombre de jabotages (paquets de plus de 1518 octets) ayant été reçus sur l'interface depuis la dernière actualisation de l'unité.

Collisions : nombre de collisions ayant été reçues sur l'interface depuis la dernière actualisation de l'unité.

Frames of *xx* Bytes (Trames de xx octets) : nombre de trames de *xx* octets ayant été reçues sur l'interface depuis la dernière actualisation de l'unité.

Affichage des statistiques sur les interfaces

1. Affichez la page RMON Statistics (Statistiques RMON).
2. Sélectionnez un type et un numéro d'interface dans le champ **Interface**.

Les statistiques correspondantes s'affichent.

Affichage des statistiques RMON à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant d'afficher les statistiques RMON.

Tableau 8-5. Commandes CLI pour l'affichage des statistiques RMON

Commande CLI	Description
show rmon statistics {**ethernet** *interface* | **port-channel** *numéro_canal_port*}	Affiche les statistiques Ethernet RMON.

Voici un exemple de commandes CLI :

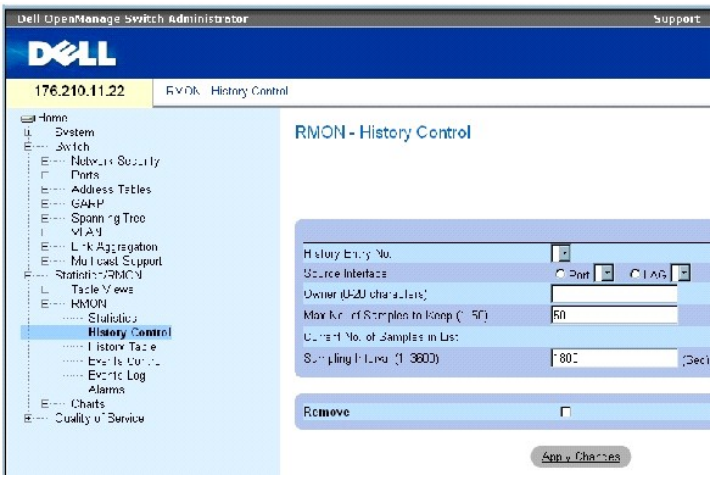
```
console# show rmon statistics ethernet 1/e1

Port 1/e1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0
```

```
Fragments: 0 Jabbers: 0

64 Octets: 98 65 to 127 Octets: 0

128 to 255 Octets: 0 256 to 511 Octets: 0

512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

Affichage des statistiques de contrôle de l'historique RMON

La page **RMON History Control (Contrôle de l'historique RMON)** contient des informations sur les échantillons de données collectés sur les ports (définitions d'interfaces ou périodes d'interrogation, par exemple). Pour ouvrir la page **RMON History Control (Contrôle de l'historique RMON)**, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **RMON**→ **History Control** (Contrôle de l'historique) dans l'arborescence.

Figure 8-8. RMON History Control (Contrôle de l'historique RMON)



La page RMON History Control (Contrôle de l'historique RMON) contient les champs suivants :

History Entry No. (N° d'entrée historique) : numéro d'entrée de la page **History Control** (Contrôle de l'historique).

Source Interface (Interface source) : port ou LAG à partir duquel les échantillons de l'historique ont été collectés.

Owner (Propriétaire) : identifie l'utilisateur ou la station RMON qui a demandé les informations RMON.

Max Number of Samples to Keep (Nombre max d'échantillons à conserver) : indique le nombre d'échantillons à enregistrer. La valeur par défaut est de 50.

Current Number of Samples in List (Nombre actuel d'échantillons dans la liste) : indique le nombre d'échantillons existants.

Sampling Interval (Intervalle d'échantillonnage) : indique, en secondes, la fréquence à laquelle des échantillons sont collectés sur les ports. Les valeurs possibles sont comprises entre 1 et 3600 secondes. La valeur par défaut est de 1800 secondes (30 minutes).

Remove (Supprimer) : supprime l'entrée de la **table de contrôle de l'historique**.

Ajout d'une entrée de contrôle d'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.
3. Complétez les champs de la boîte de dialogue.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

   L'entrée est ajoutée à la **table de contrôle de l'historique**.

Modification d'une entrée de la table de contrôle de l'historique

1. Affichez la page **RMON History Control (Contrôle de l'historique RMON)**.
2. Sélectionnez une entrée dans le champ **History Entry No.** (N° d'entrée historique).
3. Apportez les modifications requises dans les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

   L'entrée est modifiée et l'unité est mise à jour.

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. Sélectionnez une entrée dans le champ **History Entry No.** (N° d'entrée historique).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

   L'entrée sélectionnée est supprimée et l'unité est mise à jour.

Affichage des statistiques d'historique RMON à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant d'afficher les statistiques d'historique RMON.

Tableau 8-6. Commandes CLI pour l'affichage des statistiques d'historique RMON

Commande CLI	Description
rmon collection history index [**owner** *nom_propriétaire* | **buckets** *numéro_bloc*] [**interval** *secondes*]	Active et définit la surveillance RMON sur une interface.
show rmon collection history [**ethernet** *interface* | **port-channel** *numéro-canal-port*]	Affiche les statistiques de l'historique RMON.

Voici un exemple de commandes CLI :

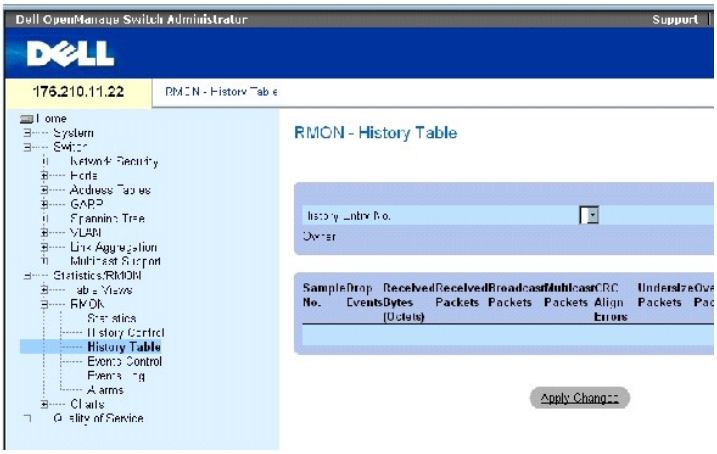
```
console(config)# interface ethernet 1/e8
```

```
console(config-if)# rmon collection history 1 interval
2400
```

Affichage de la table d'historique RMON

La table **RMON History Table (Table d'historique RMON)** contient des échantillons de statistiques réseau relatifs à une interface spécifique. Chaque entrée de la table représente toutes les valeurs des compteurs compilées lors d'un échantillonnage. Pour ouvrir la page **RMON History Table (Table d'historique RMON)**, cliquez sur **Statistics / RMON** (Statistiques/RMON) → **RMON**→ **History Table** (Table d'historique) dans l'arborescence.

Figure 8-9. RMON History Table (Table d'historique RMON)



La page **RMON History Table (Table d'historique RMON)** contient les champs suivants :

REMARQUE : tous les champs n'apparaissent pas dans la table d'historique RMON.

History Entry No. (N° d'entrée historique) : numéro d'entrée de la page **History Control** (Contrôle de l'historique).

Owner (Propriétaire) : identifie l'utilisateur ou la station RMON qui a demandé les informations RMON.

Sample No. (N° d'échantillon) : identifie l'échantillon auquel se rapportent les informations affichées dans la table.

Drop Events (Événements rejetés) : indique le nombre de paquets qui ont été rejetés par manque de ressources réseau durant l'intervalle d'échantillonnage. Cette valeur ne représente pas toujours le nombre exact de paquets rejetés, mais plutôt le nombre de paquets rejetés qui ont été détectés.

Received Bytes (Octets) (Nb d'octets reçus) : affiche le nombre d'octets de données reçus sur le réseau (y compris les paquets non valides).

Received Packets (Paquets reçus) : indique le nombre de paquets reçus durant l'intervalle d'échantillonnage.

Broadcast Packets (Paquets de diffusion) : indique le nombre de paquets de diffusion corrects reçus durant l'intervalle d'échantillonnage.

Multicast Packets (Paquets multidiffusion) : indique le nombre de paquets multidiffusion corrects reçus durant l'intervalle d'échantillonnage.

CRC Align Errors (Erreurs d'alignement CRC) : indique le nombre de paquets de 64 à 1518 octets reçus durant la session d'échantillonnage 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) : nombre de paquets de moins de 64 octets reçus pendant la session d'échantillonnage.

Oversize Packets (Paquets de longueur excessive) : nombre de paquets de plus de 1518 octets reçus pendant la session d'échantillonnage.

Fragments : indique le nombre de paquets de taille inférieure à 64 octets et possédant un FCS qui ont été reçus pendant la session d'échantillonnage.

Jabbers (Jabotages) : nombre de paquets reçus de plus de 1518 octets et possédant un FCS qui ont été reçus pendant la session d'échantillonnage.

Collisions : évalue le nombre total de collisions de paquets survenues pendant la session d'échantillonnage. Des collisions sont détectées lorsque des ports répéteurs détectent plusieurs stations qui effectuent des transmissions simultanées.

Utilization (Utilisation) : évalue l'utilisation des couches principales du réseau physique sur une interface lors de l'échantillonnage de la session. Cette valeur est représentée par un pourcentage.

Affichage des 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.** (N° d'entrée historique).

Les statistiques relatives à l'entrée s'affichent dans la table d'historique RMON.

Affichage des statistiques d'historique RMON à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant d'afficher l'historique RMON.

Tableau 8-7. Commandes CLI de contrôle de l'historique RMON

Commande CLI	Description
show rmon history index {throughput | errors | other} [period secondes]	Affiche l'historique des statistiques Ethernet RMON.

Vous trouverez ci-dessous un exemple des commandes CLI permettant d'afficher des statistiques Ethernet RMON relatives au débit sur l'index 1 :

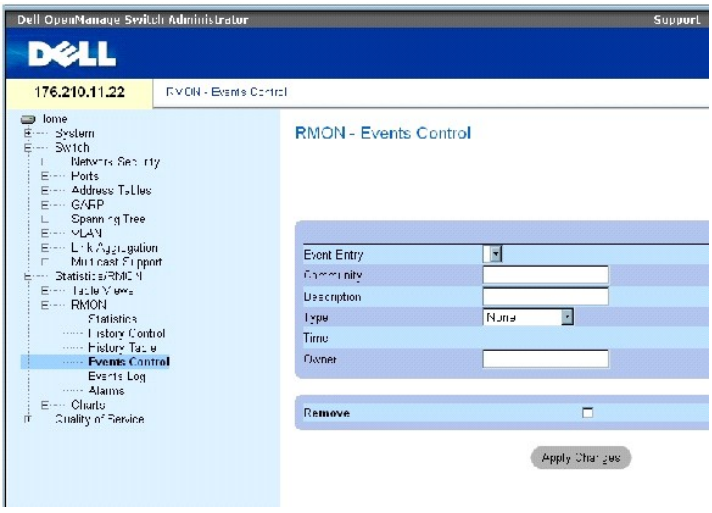
```
console> enable

console# show rmon history 1 throughput

Sample Set: 5 Owner: cli

Interface: 24 interval: 10

Requested samples: 50 Granted samples: 50
```

```
Maximum table size: 270


Time Octets Packets Broadcast Multicast %


------------------ -- ---- -- ------- ------- -- ------
--- ---


09-Mar-2003 18:29:32 0 0 0 0 0


09-Mar-2003 18:29:42 0 0 0 0 0


09-Mar-2003 18:29:52 0 0 0 0 0


09-Mar-2003 18:30:02 0 0 0 0 0


09-Mar-2003 18:30:12 0 0 0 0 0


09-Mar-2003 18:30:22 0 0 0 0 0
```

Définition d'événements RMON sur l'unité

La page **RMON Events Control (Contrôle des événements RMON)** permet de définir des événements RMON. Pour ouvrir la page **RMON Events Control (Contrôle des événements RMON)**, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **RMON**→ **Events Control** (Contrôle des événements) dans l'arborescence.

Figure 8-10. RMON Events Control (Contrôle des événements RMON)



La page **RMON Events Control (Contrôle des événements RMON)** contient les champs suivants :

Event Entry (Entrée événement) : identifie l'événement concerné.

Community (Communauté) : indique la communauté à laquelle l'événement est associé.

Description : affiche la description définie par l'utilisateur pour l'événement.

Type : précise le type de l'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 (Journal et Interruption) : indique que l'événement est à la fois une entrée de journal et une interruption.

None (Aucun) : iI n'y a aucun événement.

Time (Heure) : indique l'heure à laquelle l'événement s'est produit.

Owner (Propriétaire) : identifie l'unité ou l'utilisateur qui a défini l'événement.

Remove (Supprimer) : supprime l'événement de la table des événements RMON.

Ajout d'un événement RMON

1. Affichez la page **RMON Events Control (Contrôle des événements RMON)**.
2. Cliquez sur **Add** (Ajouter).

   La page **Add an Event Entry** (Ajouter une entrée d'événement) s'affiche.
3. Renseignez les informations de la fenêtre de dialogue et cliquez sur **Apply Changes** (Appliquer les modifications).

   L'entrée est ajoutée à la **table des événements** et l'unité est mise à jour.

Modification d'un événement RMON

1. Affichez la page **RMON Events Control (Contrôle des événements RMON)**.
2. Sélectionnez une entrée dans la **table des événements**.
3. Modifiez les champs de la boîte de dialogue et cliquez sur **Apply Changes** (Appliquer les modifications).

   L'entrée est modifiée dans la **table des événements** et l'unité est mise à jour.

Suppression d'entrées d'événements RMON

1. Affichez la page **RMON Events Control (Contrôle des événements RMON)**.
2. Cliquez sur **Show All** (Afficher tout).

   La page **RMON Events Table** (Table des événements RMON) s'affiche.
3. Cochez la case **Remove** (Supprimer) associée à l'événement approprié, puis cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée sélectionnée est supprimée et l'unité est mise à jour.

REMARQUE : il est possible de supprimer une entrée d'événement en cochant la case **Remove** (Supprimer) appropriée dans la page **RMON Events Control** (Contrôle des événements RMON).

Définition des événements de l'unité à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant de définir les événements de l'unité.

Tableau 8-8. Commandes CLI permettant la définition des événements de l'unité

Commande CLI	Description
rmon event *type index* [**community** *texte*] [**description** *texte*] [**owner nom**]	Configure des événements RMON.
show rmon events	Affiche la table des événements RMON.

Voici un exemple de commandes CLI :

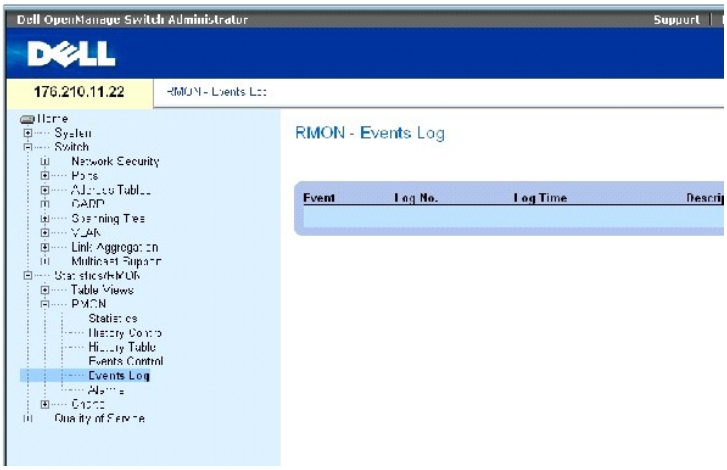
```
console(config)# rmon event 1 log

console(config)# exit

console# show rmon events
```

Index	Description	Type	Community	Owner	Last Time Sent
-----	-----------	---- ----	---------	-------	---------- ----
1	Errors	Log		CLI	Jan 18 2002 23:58:17
2	High Broadcast	Log-Trap	router	Manager	Jan 18 2002 23:59:48

Affichage du journal des événements RMON

La page **RMON Events Log (Journal des événements RMON)** répertorie les événements RMON. Pour ouvrir la page **RMON Events Log (Journal des événements RMON)**, cliquez sur **Statistics / RMON** (Statistiques/RMON) → **RMON**→ **Events Log** (Journal des événements) dans l'arborescence.

Figure 8-11. RMON Events Log (Journal des événements RMON)



La page **RMON Events Log (Journal des événements RMON)** contient les champs suivants :

Event (Événement) : identifie le numéro de l'entrée dans le journal des événements RMON.

Log No. (N° du journal) : indique le numéro du journal.

Log Time (Heure de consignation) : indique l'heure à laquelle l'entrée a été créée dans le journal.

Description : décrit l'entrée de journal.

Définition des événements de l'unité à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant de définir les événements de l'unité.

Tableau 8-9. Commandes CLI permettant la définition des événements de l'unité

Commande CLI	Description
show rmon log [*événement*]	Affiche la table de consignation RMON.

Voici un exemple de commandes CLI :

```
console(config)# rmon event 1 log

Console> show rmon log

Maximum table size: 500

Event Description Time
```

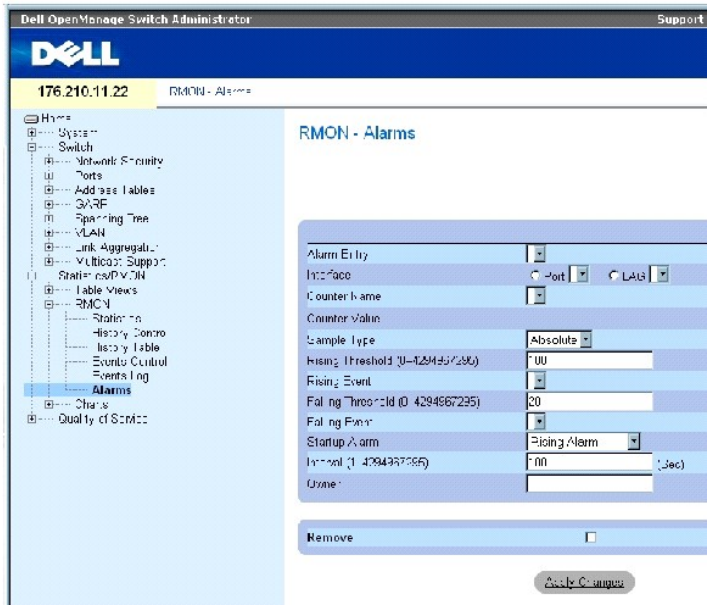
```
----- ---------- ----- --------------


1 Errors Jan 18 2002 23:58:17


2 High Broadcast Jan 18 2002 23:59:48
```

Définition d'alarmes RMON sur l'unité

La page **RMON Alarms (Alarmes RMON)** permet de définir des alarmes réseau. Ces alarmes sont émises en cas de détection d'un problème ou d'un événement sur le réseau. Elles sont générées par la hausse et la baisse de seuils prédéfinis. Pour plus d'informations, consultez la section "Affichage du journal des événements RMON".

Pour ouvrir la page **RMON Alarms (Alarmes RMON)**, cliquez sur **Statistics / RMON** (Statistiques/RMON) → **RMON**→ **Alarms** (Alarmes) dans l'arborescence.

Figure 8-12. RMON Alarms (Alarmes RMON)



La page **RMON Alarms (Alarmes RMON)** contient les champs suivants :

Alarm Entry (Entrée Alarme) : identifie une alarme spécifique.

Interface : indique l'interface dont les statistiques RMON s'affichent.

Counter Name (Nom du compteur) : indique la variable MIB sélectionnée.

Counter Value (Valeur du compteur) : indique la valeur de la variable MIB sélectionnée.

Sample Type (Type d'échantillon) : indique la méthode d'échantillonnage utilisée pour la variable sélectionnée et compare sa valeur aux seuils. Ce champ peut prendre les valeurs suivantes :

Delta (Différence) : soustrait la valeur du dernier échantillon de la valeur en cours. La différence obtenue est comparée au seuil.

Absolute (Absolue) : compare directement les valeurs avec les seuils, au terme de l'intervalle d'échantillonnage.

Rising Threshold (0–4294967295) (Seuil en hausse) : hausse de valeur du compteur qui déclenche l'alarme de seuil en hausse. Le seuil en hausse est représenté sous forme de graphique dans la partie supérieure des histogrammes. Une couleur spécifique est associée à chaque variable contrôlée. La valeur par défaut est de 100 secondes.

Rising Event (Événement hausse) : mécanisme qui signale la présence d'alarmes LOG, TRAP ou les deux. Lorsque l'option LOG est sélectionnée, aucun mécanisme d'enregistrement n'est activé sur l'unité ni dans le système de gestion. Toutefois, si l'unité n'est pas réinitialisée, l'événement est conservé dans la table LOG de l'unité. Si l'option TRAP est sélectionnée, une interruption SNMP est générée et signalée via le mécanisme général des interruptions. L'interruption peut être enregistrée à l'aide de ce même mécanisme.

Falling Threshold (0–4294967295) (Seuil en baisse) : baisse de valeur du compteur qui déclenche l'alarme de seuil en baisse. Le seuil en baisse est représenté sous forme de graphique dans la partie supérieure des histogrammes. Une couleur spécifique est associée à chaque variable contrôlée. La valeur par défaut de ce champ est 20.

Startup Alarm (Alarme de démarrage) : événement qui déclenche l'alarme. La hausse se définit par le passage d'une valeur de seuil faible à une valeur de seuil élevée.

Interval (1–4294967295) **(sec)** (Intervalle) : intervalle en secondes entre deux alarmes. La valeur par défaut est de 100 secondes.

Owner (Propriétaire) : identifie l'unité ou l'utilisateur qui a défini l'alarme.

Remove (Supprimer) : supprime une alarme RMON.

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 entrée d'alarme) s'affiche.

Figure 8-13. Ajout d'une entrée d'alarme

3. Sélectionnez une interface.
4. Complétez les champs.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'alarme RMON est ajoutée et l'unité est mise à jour.

Modification 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** (Entrée d'alarme).
3. Modifiez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est modifiée et l'unité est mise à jour.

Affichage de la table des alarmes

1. Affichez la page **RMON Alarms (Alarmes RMON)**.
2. Cliquez sur **Show All** (Afficher tout).

La **table des alarmes** s'affiche.

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** (Entrée d'alarme).
3. Cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est supprimée et l'unité est mise à jour.

Définition des alarmes de l'unité à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant de définir les alarmes de l'unité.

Tableau 8-10. Commandes CLI de définition des alarmes de l'unité

Commande CLI	Description
rmon alarm *index MIB_Object_ID intervalle seuilh seuilb événementh événementb* [**type** *type*] [**startup** *direction*] [**owner** *nom*]	Configure des conditions d'alarme RMON.
show rmon alarm-table	Affiche un récapitulatif de la table des alarmes.
show rmon alarm	Affiche la configuration des alarmes RMON.

Voici un exemple de commandes CLI :

```
console(config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1
360000 1000000 1000000 10 20
```

```
Console# show rmon alarm-table

Index OID Owner

----- ---------------------- -- -----

1 1.3.6.1.2.1.2.2.1.10.1 CLI

2 1.3.6.1.2.1.2.2.1.10.1 Manager

3 1.3.6.1.2.1.2.2.1.10.9 CLI
```

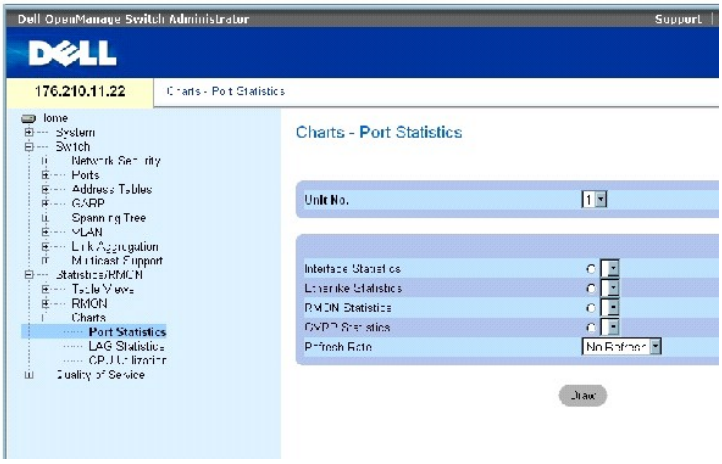
Affichage des graphiques

La page **Charts** (Graphiques) contient des liens qui permettent d'afficher les statistiques sous forme de graphiques. Pour ouvrir cette page, cliquez sur Statistics (Statistiques) → Charts (Graphiques) dans l'arborescence.

Affichage des statistiques sur les ports

La page **Port Statistics (Statistiques sur les ports)** affiche les statistiques relatives aux ports sous forme de graphique. Pour ouvrir la page **Port Statistics (Statistiques sur les ports)**, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Charts** (Graphiques) → **Port Statistics** (Statistiques sur les ports) dans l'arborescence.

Figure 8-14. Port Statistics (Statistiques sur les ports)



La page Port Statistics (Statistiques sur les ports) contient les champs suivants :

Unit No. (Numéro d'unité) : indique l'unité de la pile correspondant aux statistiques affichées.

Interface Statistics (Statistiques d'interface) : sélectionne les statistiques d'interface à afficher.

Etherlike Statistics (Statistiques Etherlike) : sélectionne les statistiques Etherlike à afficher.

RMON Statistics (Statistiques RMON) : sélectionne les statistiques RMON à afficher.

GVRP Statistics (Statistiques GVRP) : sélectionne les statistiques GVRP à afficher.

Refresh Rate (Intervalle de rafraîchissement) : intervalle écoulé entre deux actualisations des statistiques.

Affichage des statistiques sur les ports

1. Affichez la page **Port Statistics (Statistiques sur les ports)**.
2. Sélectionnez la catégorie de statistiques à afficher.
3. Sélectionnez un intervalle de rafraîchissement dans le menu **Refresh Rate** (Intervalle de rafraîchissement).
4. Cliquez sur **Draw** (Dessiner).

Le graphique des statistiques sélectionnées s'affiche.

Affichage des statistiques sur les ports à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant d'afficher les statistiques sur les ports.

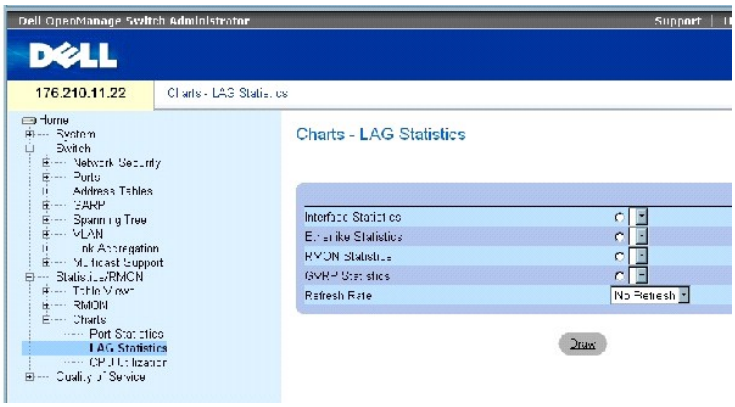
Tableau 8-11. Commandes CLI pour l'affichage des statistiques sur les ports

Commande CLI	Description
show interfaces counters [**ethernet** *interface* | **port- channel** *numéro_canal_port*]	Affiche le trafic enregistré par l'interface physique.
show rmon statistics {**ethernet** *interface* | **port-channel** *numéro_canal_port*}	Affiche les statistiques Ethernet RMON.
show gvrp statistics {**ethernet** *interface* | **port-channel** *numéro_canal_port*}	Affiche les statistiques GVRP.
show gvrp-error statistics {**ethernet** *interface* | **port- channel** *numéro_canal_port*}	Affiche les statistiques d'erreurs GVRP.

Affichage des statistiques sur les LAG

La page **LAG Statistics (Statistiques sur les LAG)** affiche les statistiques relatives aux LAG sous forme de graphique. Pour ouvrir la page **LAG Statistics (Statistiques sur les LAG)**, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Charts** (Graphiques) → **LAG Statistics** (Statistiques sur les LAG) dans l'arborescence.

Figure 8-15. LAG Statistics (Statistiques sur les LAG)



La page LAG Statistics (Statistiques sur les LAG) contient les champs suivants :

Interface Statistics (Statistiques d'interface) : sélectionne les statistiques d'interface à afficher.

Etherlike Statistics (Statistiques Etherlike) : sélectionne les statistiques Etherlike à afficher.

RMON Statistics (Statistiques RMON) : sélectionne les statistiques RMON à afficher.

GVRP Statistics (Statistiques GVRP) : sélectionne les statistiques GVRP à afficher.

Refresh Rate (Intervalle de rafraîchissement) : intervalle écoulé entre deux actualisations des statistiques.

Affichage des statistiques sur les LAG

1. Affichez la page **LAG Statistics (Statistiques sur les LAG)**.
2. Sélectionnez la catégorie de statistiques à afficher.
3. Sélectionnez un intervalle de rafraîchissement dans le menu **Refresh Rate** (Intervalle de rafraîchissement).
4. Cliquez sur **Draw** (Dessiner).

Le graphique des statistiques sélectionnées s'affiche.

Affichage des statistiques sur les LAG à l'aide des commandes CLI

Le tableau ci-après récapitule les commandes CLI permettant d'afficher les statistiques sur les LAG.

Tableau 8-12. Commandes CLI pour l'affichage des statistiques sur les LAG

Commande CLI	Description
show interfaces counters [**ethernet** *interface* | **port- channel** *numéro_canal_port*]	Affiche le trafic enregistré par l'interface physique.
show rmon statistics {**ethernet** *interface* | **port-channel** *numéro_canal_port*}	Affiche les statistiques Ethernet RMON.
show gvrp statistics {**ethernet** *interface* | **port-channel** *numéro_canal_port*}	Affiche les statistiques GVRP.

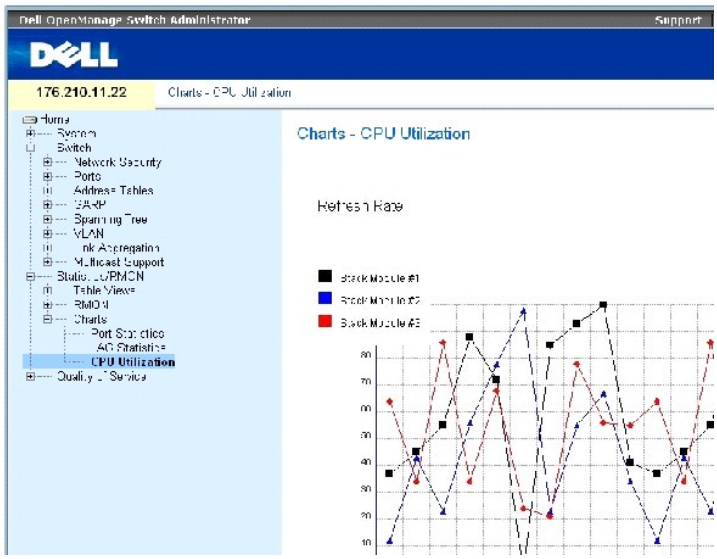
show gvrp-error statistics {**ethernet** *interface* | **port- channel** *numéro_canal_port*}	Affiche les statistiques d'erreurs GVRP.

Affichage de l'utilisation du processeur

La page **CPU Utilization (Utilisation du processeur)** contient des informations sur l'utilisation du processeur et le pourcentage de ressources consommé par chaque membre de la pile. Chaque membre est associé à une couleur dans le graphique.

Pour ouvrir la page **CPU Utilization (Utilisation du processeur)**, cliquez sur **Statistics / RMON** (Statistiques/RMON) → **Charts** (Graphiques) → **CPU Utilization** (Utilisation du processeur) dans l'arborescence.

Figure 8-16. CPU Utilization (Utilisation du processeur)



La page **CPU Utilization (Utilisation du processeur)** contient le champ suivant :

Refresh Rate (Intervalle de rafraîchissement) : intervalle écoulé entre deux actualisations des statistiques.

Retour au sommaire

Retour au sommaire

Configuration de la qualité de service

Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

Cette section contient des informations relatives à la définition et à la configuration des paramètres de la qualité de service (QoS). Pour ouvrir la page Quality of Service (Qualité de service), cliquez sur l'option de même nom dans l'arborescence.

Présentation générale de la qualité de service

La qualité de service permet aux administrateurs réseau de rendre prioritaire le trafic du réseau en fonction de certains critères et d'accorder au trafic spécifique un traitement préférentiel.

Un exemple de mise en oeuvre est le trafic de type vocal, vidéo et en temps réel qui peut être affecté à une file d'attente de priorité élevée, tandis que d'autres types de trafic peuvent être affectés à une file d'attente de priorité inférieure. Le flux de trafic s'en trouve très amélioré en cas de forte demande.

La qualité de service repose sur les principes suivants :

- Classification : indique les champs de paquets qui sont mis en correspondance avec des valeurs spécifiques. Tous les paquets répondant aux spécifications définies par l'utilisateur sont classés ensemble.
- Action : définit la gestion du trafic selon laquelle le transfert de paquets s'effectue en fonction des informations sur les paquets et des valeurs de champs, telles que la balise de priorité VLAN (VPT) et la valeur DSCP (DiffServ Code Point).

Informations de classification de la balise VPT

Les balises de priorité VLAN permettent de classer les paquets en les adressant à l'une des files d'attente de sortie. Ces balises peuvent être définies par l'utilisateur. Le tableau suivant indique les paramètres de l'adressage par défaut de la VPT à la file d'attente.

Tableau 9-1. Valeurs par défaut de la table d'adressage CoS à file d'attente

Valeur CoS	Valeurs des files d'attente de transfert
0	q1 (Priorité la plus faible)
1	q1 (Priorité la plus faible)
2	q1 (Priorité la plus faible)
3	q1 (Priorité la plus faible)
4	q2
5	q2
6	q3
7	q3

REMARQUE : dans une configuration en empilage, la file d'attente 4 (Queue 4) est utilisée pour la transmission du trafic lié à la pile. Par conséquent, l'affectation de trafic supplémentaire à la file d'attente 4 peut interférer avec le transfert du trafic.

Une valeur VPT par défaut est attribuée à tous les paquets entrants non balisés. Cette valeur est définie port par port. Elle permet d'adresser chaque paquet à la file d'attente de sortie.

Les valeurs DSCP peuvent être adressées aux files d'attente de priorité. Le tableau suivant montre la correspondance par défaut entre l'adressage DSCP et les valeurs des files d'attente de sortie.

Tableau 9-2. Valeurs par défaut de la table d'adressage DSCP à file d'attente

Valeur DSCP	Valeurs des files d'attente de transfert
0-15	q1 (Priorité la plus faible)
16-39	q2
40-63	q3

L'adressage DSCP est activé au niveau du système.

Services CoS (classe de service)

Une fois les paquets affectés à une file d'attente de sortie spécifique, les services CoS peuvent être affectés à cette file d'attente. Les files d'attente de sortie sont configurées avec un schéma de planification à l'aide de l'une des méthodes suivantes :

- Strict Priority (Priorité stricte) : garantit le transfert prioritaire des données liées aux applications critiques. Cette option permet de donner la priorité au trafic le plus urgent et important, au détriment d'autres applications ne présentant pas ce caractère d'urgence. Par exemple le trafic voix sur IP est transféré avant le trafic FTP ou SMTP (messagerie électronique).
- Weighted Round Robin (Pondération WRR) : cette méthode garantit qu'aucune application ne monopolise la capacité de transfert de l'unité. Elle transfère les files d'attente dans leur intégralité, l'une après l'autre. Toutes les files d'attente peuvent être incluses dans cette méthode.
  Les files d'attente avec priorité stricte sont traitées avant les files d'attente avec pondération WRR. Si le trafic en cours est minimal et si les files d'attente avec priorité stricte n'occupent pas toute la bande passante allouée à un port, les files d'attente WRR peuvent partager la bande passante avec les files d'attente prioritaires. La bande passante restante est répartie en fonction du taux de pondération. Si la pondération WRR a été sélectionnée, les taux de pondération suivants sont appliqués aux files d'attente : 1, 2, 4, 8.

Définition des paramètres globaux de la qualité de service

La page **QoS Parameters** (Paramètres de la qualité de service) contient des liens vers des pages permettant de définir les paramètres globaux de la qualité de service.

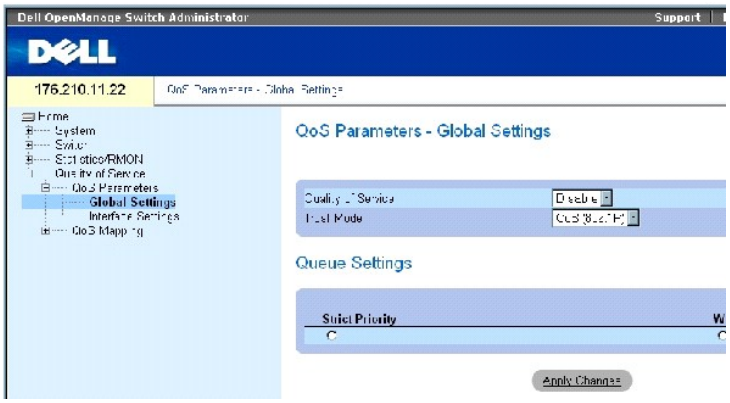
Configuration des paramètres globaux de la qualité de service

La page **Global Settings (Paramètres globaux)** permet d'activer ou de désactiver la qualité de service. Elle permet également de sélectionner le mode Confiance (Trust), qui consiste en l'utilisation de champs prédéfinis d'un paquet pour déterminer sa file de sortie.

La page **Global Settings (Paramètres globaux)** permet en outre de définir des files d'attente avec une priorité stricte ou une pondération WRR.

Pour ouvrir la page **Global Settings (Paramètres globaux)**, cliquez sur Quality of Service (Qualité de service) → QoS Parameters (Paramètres de la qualité de service) → Global Settings (Paramètres globaux) dans l'arborescence.

Figure 9-1. Global Settings (Paramètres globaux)



La page **Global Settings (Paramètres globaux)** contient les sections suivantes :

- Paramètres de la qualité de service
- Paramètres des files d'attente

Paramètres de la qualité de service

Quality of Service (Qualité de service) : active ou désactive l'utilisation de la qualité de service pour la gestion du trafic réseau.

Trust Mode (Mode Confiance) : détermine les champs de paquet à utiliser pour la classification des paquets entrants sur l'unité. Si aucune règle n'est définie, le trafic contenant le champ CoS ou DSCP prédéfini est adressé en fonction du mode Confiance sélectionné. Le trafic ne contenant aucun champ de paquet prédéfini est adressé à la file d'attente "au mieux" (q2). Les valeurs admises pour le champ Trust Mode sont les suivantes :

CoS (802.1p) : la file d'attente de sortie est déterminée par le numéro de priorité VLAN (VPT) IEEE802.1p ou par le VPT par défaut affecté à un port. La valeur par défaut pour l'unité est IEEE802.1p.

DSCP : l'affectation des files d'attente de sortie est déterminée par le champ DSCP.

REMARQUE : les paramètres du mode Confiance associés à l'interface sont prioritaires par rapport à la valeur Trust globale.

Paramètres des files d'attente

Strict Priority (Priorité stricte) : indique que les files d'attente du système sont prioritaires.

WRR (Pondération WRR) : indique que les files d'attente du système sont traitées selon la pondération WRR.

Activation de la qualité de service :

1. Affichez la page **Global Settings (Paramètres globaux)**.
2. Sélectionnez **Enable** (Activer) dans le champ **Quality of Service** (Qualité de service).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La fonction CoS est activée sur l'unité.

Activation du mode Confiance :

1. Affichez la page **Global Settings (Paramètres globaux)**.
2. Activez l'option **Trust Mode** (Mode Confiance).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mode Confiance est activé sur l'unité.

Activation du mode Confiance à l'aide de commandes CLI

Le tableau suivant récapitule les commandes d'interface de ligne de commande (CLI) équivalentes pour la configuration des champs de la page **Global Settings (Paramètres globaux)**.

Tableau 9-3. Commandes CLI permettant de paramétrer la qualité de service

Commande CLI	Description
qos trust [**cos** | **dscp**]	Configure le système en mode Confiance.
no qos trust	Désactive le mode Confiance.

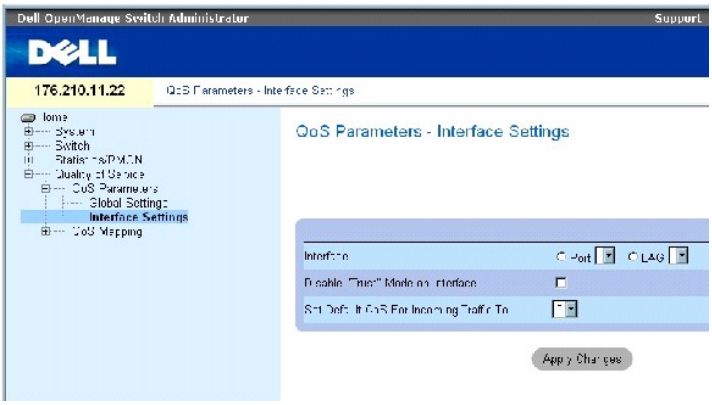
Voici un exemple de commandes CLI :

```
console(config)# qos trust
dscp
```

Définition des paramètres d'interface de la qualité de service

La page **Interface Settings (Paramètres d'interface)** permet de désactiver le mode Confiance et de définir la valeur de classe de service par défaut pour les paquets entrants non balisés. Pour ouvrir la page **Interface Settings (Paramètres d'interface)**, cliquez sur Quality of Service (Qualité de service) → QoS Parameters (Paramètres de la qualité de service) → Interface Settings (Paramètres d'interface) dans l'arborescence.

Figure 9-2. Interface Settings (Paramètres d'interface)



La page **Interface Settings (Paramètres d'interface)** contient les champs suivants :

Interface : port ou LAG spécifique à configurer.

Disable "Trust" Mode on Interface (Désactiver le mode Confiance sur l'interface) : désactive le mode Confiance sur l'interface spécifiée. Ce paramètre remplace le mode Confiance configuré sur l'unité de façon globale.

Set Default CoS For Incoming Traffic To (Définir la valeur CoS par défaut pour le trafic entrant) : définit la valeur par défaut du numéro CoS pour les paquets non balisés. Les valeurs des numéros CoS sont comprises entre 0 et 7. La valeur par défaut est 0.

Affectation de paramètres de qualité de service à une interface

1. Affichez la page **Interface Settings (Paramètres d'interface)**.
2. Sélectionnez une interface dans le champ **Interface**.
3. Complétez les champs avec les valeurs appropriées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les valeurs CoS sont affectées à l'interface.

Affichage des paramètres QoS/CoS

1. Affichez la page **Interface Settings (Paramètres d'interface)**.
2. Cliquez sur **Show All** (Afficher tout).

La table d'interface s'affiche.

Affectation des interfaces QoS à l'aide des commandes CLI

Le tableau suivant récapitule les commandes de l'interface CLI équivalentes pour la configuration des champs de la page **Interface Settings (Paramètres d'interface)**.

Tableau 9-4. Commandes CLI de l'interface QoS

Commande CLI	Description
qos trust	Active le mode Confiance.
no qos trust	Désactive le mode Confiance sur chaque port.

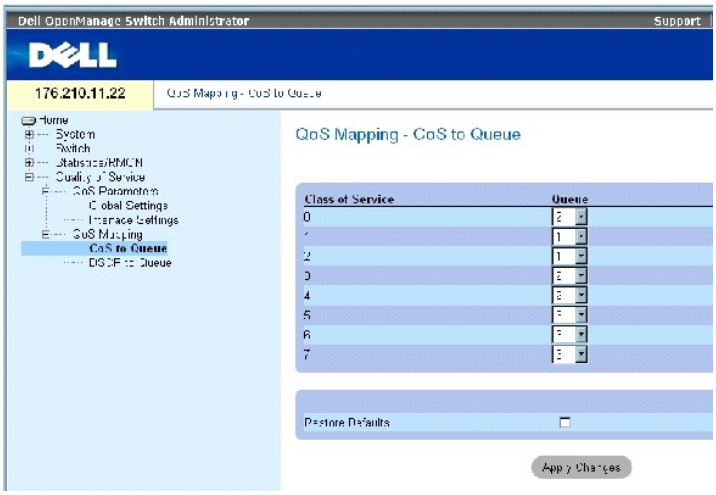
Voici un exemple de commandes CLI :

```
console(config)# interface
ethernet 1/e15


console(config-if)# qos
trust
```

Adressage de valeurs CoS aux files d'attente

La page **CoS to Queue (CoS à file d'attente)** permet d'affecter des paramètres CoS aux files d'attente. Pour ouvrir la page **CoS to Queue (CoS à file d'attente)**, cliquez sur Quality of Service (Qualité de service) → **QoS Mapping** (Adressage QoS) → CoS to Queue (CoS à file d'attente) dans l'arborescence.

Figure 9-3. CoS to Queue (CoS à file d'attente)



La page **CoS to Queue (CoS à file d'attente)** contient les champs suivants :

Class of Service (Classe de service) : indique les valeurs des numéros de priorité CoS, zéro étant la valeur la plus faible et sept la plus élevée.

Queue (File d'attente) : file d'attente à laquelle la priorité CoS est adressée. Quatre files d'attente de priorité du trafic sont prises en charge.

Restore Defaults (Restaurer les valeurs par défaut) : restaure les valeurs par défaut (définies en usine) de l'unité pour l'adressage des valeurs CoS à une file d'attente de sortie.

Adressage d'une valeur CoS à une file d'attente

1. Affichez la page **CoS to Queue (CoS à file d'attente)**.
2. Sélectionnez une entrée CoS.
3. Définissez le numéro de la file d'attente dans le champ **Queue** (File d'attente).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La valeur CoS est adressée à une file d'attente de sortie et l'unité est mise à jour.

Affectation de valeurs CoS aux files d'attente à l'aide de commandes CLI

Le tableau suivant récapitule les commandes de l'interface CLI équivalentes pour la configuration des champs de la page **CoS to Queue (CoS à file d'attente)**.

Tableau 9-5. Commandes CLI des paramètres CoS à file d'attente

Commande CLI	Description
wrr-queue cos-map ID_file_attente cos0.cos7	Adresse les valeurs CoS aux files d'attente de sortie.

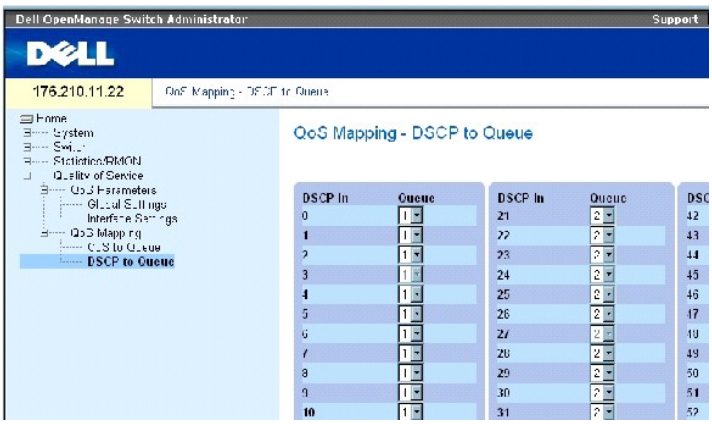
Voici un exemple de commandes CLI :

```
console(config)# wrr-queue
cos-map 4 7
```

Adressage des valeurs DSCP aux files d'attente

La page **DSCP to Queue (DSCP à file d'attente)** permet d'associer des files d'attente de sortie à des champs DSCP spécifiques. Pour ouvrir la page **DSCP to Queue (DSCP à file d'attente)**, cliquez sur Quality of Service (Qualité de service) → **QoS** Mapping (Adressage QoS) → DSCP to Queue (DSCP à file d'attente) dans l'arborescence.

Figure 9-4. DSCP to Queue (DSCP à file d'attente)



La page **DSCP to Queue (DSCP à file d'attente)** contient les champs suivants :

DSCP In (Valeur DSCP entrante) : indique les valeurs du champ DSCP dans le paquet entrant.

Queue (File d'attente) : indique la file d'attente à laquelle les paquets contenant la valeur DSCP spécifiée sont affectés. Les valeurs sont comprises entre 1 et 4, 1 étant la valeur la plus faible et 4 la plus élevée.

Adressage d'une valeur DSCP et affectation d'une file d'attente de priorité

1. Affichez la page **DSCP to Queue (DSCP à file d'attente)**.
2. Sélectionnez une valeur dans la colonne **DSCP In** (Valeur DSCP entrante).
3. Définissez le champ **Queue** (File d'attente).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La valeur DSCP est remplacée et la nouvelle valeur est affectée à une file d'attente de sortie.

Affectation de valeurs DSCP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes de l'interface CLI équivalentes pour la configuration des champs de la page **DSCP to Queue (DSCP à file d'attente)**.

Tableau 9-6. Commandes CLI pour l'attribution de valeurs DSCP aux files d'attente

Commande CLI	Description
qos map dscp-queue liste_dscp **to** ID_file_attente	Modifie l'adressage DSCP vers file d'attente.

Voici un exemple de commandes CLI :

```
console(config)# qos map
dscp-queue 33 40 41 to 1
```

Retour au sommaire

Retour au sommaire

Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

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

AVIS : un AVIS vous avertit d'un dommage ou d'une perte de données potentiels et vous indique comment éviter ce problème.

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

Mars 2005

Retour au sommaire

Retour au sommaire

Informations sur l'interaction entre les fonctions de l'unité

Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

Le tableau suivant contient des informations sur l'interaction entre les différentes fonctionnalités de l'unité.

Fonction	Remarques
VLAN sans authentification 802.1x	Le fonctionnement des VLAN sans authentification 802.1x est restreint lorsqu'ils coexistent avec les éléments suivants : • Guest VLAN 802.1x • VLAN privé • VLAN isolé • VLAN de communauté • VLAN spécial
Port de VLAN sans authentification 802.1x	Le fonctionnement des ports de VLAN sans authentification 802.1x est restreint lorsqu'ils coexistent avec les éléments suivants : • Ports isolés • Ports de communauté • Ports banalisés (mode "promiscuous") • Ports de VLAN basés sur l'adresse MAC • Filtrage en entrée
Listes de contrôle d'accès	Le fonctionnement des ACL (listes de contrôle d'accès) est restreint lorsqu'elles coexistent avec les éléments suivants : • ACL basées sur l'adresse MAC • VLAN spéciaux
Négociation automatique	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Prise en charge de la contre-pression	
Filtrage de multidiffusion par ponts	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Tests des câbles	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Ports de communauté	Le fonctionnement des ports de communauté est restreint lorsqu'ils coexistent avec le verrouillage de port.
VLAN de communauté	Le fonctionnement des VLAN de communauté est restreint lorsqu'ils coexistent avec les éléments suivants : • Adresses MAC statiques • Listes de contrôle d'accès • GVRP • Surveillance IGMP • VLAN spéciaux
DNS	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Mode duplex	
Contrôle de flux	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
GARP	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Guest VLAN	Les Guest VLAN ne peuvent pas fonctionner avec les éléments suivants : • VLAN privé • VLAN isolé • VLAN de communauté • VLAN basé sur l'adresse MAC • VLAN spéciaux
GVRP	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Surveillance IGMP	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Filtrage en entrée	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Port isolé	Les ports isolés ne peuvent pas fonctionner avec les éléments suivants : • Ports de communauté • Ports banalisés (mode "promiscuous") • Verrouillage du port • GVRP • ACL basées sur l'adresse MAC • Filtrage en entrée
VLAN isolé	Les VLAN isolés ne peuvent pas fonctionner avec les éléments suivants : • VLAN de communauté • Adresses MAC statiques

	• Listes de contrôle d'accès • GVRP • Surveillance IGMP • VLAN spéciaux
Statistiques sur les LAG	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Agrégation des liaisons	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions. Cependant, il existe diverses contraintes de configuration. Voir "Définition des paramètres des LAG".
Verrouillage du port	Le verrouillage de port fonctionne de façon restreinte lorsqu'il coexiste avec les éléments suivants : • ACL basées sur l'adresse MAC • Filtrage en entrée
Journalisation	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Prise en charge des adresses MAC	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Détection MDI/MDIX	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Filtrage multidiffusion	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Hôtes multiples	Les hôtes multiples (norme 802.1X) ne fonctionnent pas avec les éléments suivants : • Port isolé • Ports de VLAN basés sur l'adresse MAC
Protocole MST (Multiple Spanning Tree)	Le protocole MST ne fonctionne pas avec les éléments suivants : • Port isolé • Filtrage en entrée
Authentification basée sur le port	L'authentification basée sur le port fonctionne de façon restreinte avec les éléments suivants : • Mode "hôte unique" 802.1 • Port isolé • Verrouillage de port • VLAN basé sur l'adresse MAC • Ports d'entrée
Mise en miroir des ports	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions. Cependant, il existe diverses contraintes de configuration relatives à Storm Control. Voir "Définition de sessions de mise en miroir des ports".
Statistiques sur les ports	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
VLAN privé	Les VLAN privés ne peuvent pas fonctionner avec les éléments suivants : • Ports isolés • Ports de communauté • GVRP • Surveillance IGMP • VLAN spécial
VLAN privé	Les VLAN privés fonctionnent de façon restreinte avec les éléments suivants : • VLAN isolés • GVRP • Surveillance IGMP • VLAN spécial
Ports en mode "promiscuous"	Les ports banalisés (mode "promiscuous") ne peuvent pas fonctionner avec les éléments suivants : • Verrouillage de port • GVRP • Ports de VLAN basés sur l'adresse MAC
Qualité de service	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Statistiques RMON	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Notifications d'authentification SNMP	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Notifications SNMP	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Authentification SNTP	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Spanning Tree	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
VLAN spécial	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
MAC statique	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Storm Control	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Journaux système	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Synchronisation de l'heure système	Aucune restriction ou limitation due à l'interaction avec d'autres fonctions.
Ports de VLAN sans authentification	Les ports de VLAN sans authentification fonctionnent de façon restreinte avec les éléments suivants : • Ports isolés

	• Ports de communauté • Ports banalisés (mode "promiscuous") • GVRP • Ports de VLAN basés sur l'adresse MAC • Filtrage en entrée

Retour au sommaire

Retour au sommaire

Glossaire

Systèmes Dell™ PowerConnect™ 34XX Guide d'utilisation

Ce glossaire contient des termes techniques qui peuvent vous être utiles.

A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | U | V | W

A

Adresse IP

Internet Protocol Address (Adresse de protocole Internet). Adresse unique attribuée à un périphérique réseau avec au moins deux LAN ou WAN interconnectés.

Adresse MAC

Adresse Media Access Control. L'adresse MAC est une adresse matérielle spécifique permettant d'identifier chaque noeud du réseau

Agrégation

Agrégation de liaisons. Optimise l'utilisation des ports en les reliant de façon à former un faisceau unique (groupes agrégés).

Apprentissage d'adresse MAC

L'apprentissage de l'adresse MAC s'effectue via un pont d'apprentissage sur lequel l'adresse MAC source des paquets est enregistrée. Les paquets destinés à cette adresse sont transférés uniquement vers l'interface du pont sur lequel l'adresse se trouve. Les paquets destinés à des adresses inconnues sont transférés à chaque interface de pont. L'apprentissage de l'adresse MAC permet de réduire le trafic sur les LAN rattachés.

ARP

Protocole de résolution d'adresses. Protocole qui convertit les adresses IP en adresses physiques.

ASIC

Application-Specific Internal Circuit. Puce personnalisée conçue pour une application spécifique.

Asset Tag (Numéro d'inventaire)

Indique la référence attribuée au module de commutation par l'utilisateur.

Attribution de bande passante

Quantité de bande passante attribuée à une application, une interface ou un utilisateur donné.

B

Bande passante

Indique la quantité de données pouvant être transférées dans un temps donné. Dans le cas des modules de commutation numériques, la bande passante est définie en bits par seconde (bps) ou en octets par seconde.

Baud

Nombre d'éléments de signalisation transmis chaque seconde.

Best Effort (Au mieux)

Mode de gestion du trafic selon lequel le trafic est dirigé vers la file d'attente ayant la priorité la plus basse. La réception des paquets n'est pas garantie.

BootP

Protocole Bootstrap. Permet à une station de travail de détecter son adresse IP, une adresse IP de serveur BootP sur un réseau ou un fichier de configuration chargé dans la mémoire d'un module commutateur.

BPDU

Bridge Protocol Data Unit (Unité de données de protocole en pont). Fournit des informations de pontage sous forme de message. Les unités BPDU sont envoyées dans des informations sur le module commutateur avec la configuration Spanning Tree. Les paquets BPDU contiennent des informations sur les ports, les adresses, les priorités et les coûts de transmission.

Broadcast Storm

Nombre excessif de messages de diffusion transférés simultanément sur un réseau à travers un seul port. Les réponses à ces messages étant envoyées sur l'ensemble du réseau, elles risquent de surcharger les ressources du réseau ou d'entraîner des dépassements de délai.

Pour plus d'informations, consultez la section "Définition des paramètres des LAG".

C

CDB

Base de données de configuration. Fichier contenant des informations relatives à la configuration de l'unité.

CLI

Interface de ligne de commande. Ensemble de commandes en ligne utilisées pour configurer le système. Pour plus d'informations, consultez la section "Utilisation de l'interface CLI".

Client DHCP

Hôte internet utilisant le protocole DHCP pour obtenir des paramètres de configuration, comme une adresse réseau.

Communauté

Désigne un groupe d'utilisateurs possédant les mêmes droits d'accès au système.

Commutateur

Permet de filtrer et de transférer des paquets entre les segments d'un réseau local. Les commutateurs prennent en charge tous les types de protocoles par paquets.

Configuration de démarrage

Conserve la configuration exacte du module de commutation lors de sa mise hors tension ou de son redémarrage.

Contre-pression

Mécanisme utilisé avec le mode semi duplex et permettant à un port de ne pas recevoir un message.

Contrôle de flux

Le mécanisme de contrôle du flux permet aux périphériques les plus lents de communiquer avec des périphériques fonctionnant à une vitesse supérieure en demandant que ces derniers n'envoient pas de paquets de données.

CoS

Classe de service. Une classe de service correspond à l'ordre de priorité défini dans la norme 802.1p. Elle fournit une méthode permettant de marquer les paquets par l'indication d'informations de priorité. Une valeur de classe de service comprise entre 0 et 7 est ajoutée à l'en-tête de couche 2 des paquets. Zéro correspond à la priorité la plus basse et sept à la plus haute.

Collision : transmission simultanée de plusieurs paquets aboutissant à un conflit. Les données transmises ne peuvent pas être utilisées, et la session est redémarrée.

Couche 2

Couche de liaison de données ou couche MAC. Contient l'adresse physique d'une station client ou serveur. Le traitement en couche 2 est plus rapide qu'en couche 3, car la quantité d'informations à traiter est plus réduite.

Couche 4

Établit une connexion et garantit que toutes les données arrivent à leur destination. Les paquets inspectés au niveau de la couche 4 sont analysés et transmettent des décisions en fonction de leurs applications.

Couche MAC

Sous-couche de la couche DTL (contrôle de liaison).

CPU

Central Processing Unit (Unité centrale). Partie d'un ordinateur qui traite les informations. Les UC sont composées d'une unité de contrôle et d'une unité ALU.

D

Diffusion

Méthode de transfert de paquets à tous les ports d'un réseau.

Domaine

Groupe d'ordinateurs et d'unités inclus dans une même partie d'un réseau et possédant des règles et des procédures communes.

Domaine de diffusion

Ensemble de toutes les unités qui reçoivent des trames de diffusion provenant de toute unité faisant partie d'un ensemble donné. Les domaines de diffusion sont reliés par des routeurs car ces derniers ne transfèrent pas les trames de diffusion.

DRAC/MC

Carte d'accès distant fournissant un point de contrôle unique pour les composants des serveurs modulaires Dell.

DSCP

DiffServe Code Point. Le protocole DSCP fournit une méthode permettant de marquer les paquets IP à l'aide d'informations de priorité QoS.

E

Équilibrage de charge

Permet la distribution des données et/ou le traitement des paquets de façon équitable sur les ressources du réseau disponibles. Par exemple, l'équilibrage de charge peut distribuer les paquets entrants de façon équitable à tous les serveurs ou rediriger les paquets vers le prochain serveur disponible.

Ethernet

Ethernet correspond à la norme IEEE 802.3. Il s'agit de la norme la plus répandue dans les réseaux locaux (LAN). Elle prend en charge les transferts de données à 10, 100 ou 1000 Mbps.

Ethernet Gigabit

Un réseau Ethernet Gigabit effectue des transferts à 1000 Mbps et est compatible avec les normes Ethernet 10/100 Mbps existantes.

EWS

Embedded Web Server (Serveur Web intégré). Permet la gestion de l'unité via un navigateur Web standard. Les serveurs Web intégrés sont utilisés avec ou en remplacement de la CLI ou du NMS.

F

FFT

Fast Forward Table (Table des transmissions rapides). Fournit des informations sur les routes de transmission. Lorsqu'un paquet arrive dans un périphérique avec une route connue, il est transmis via une route listée dans la FFT. Si aucune route n'est connue, l'unité centrale transmet le paquet et met à jour la FFT.

Fichier de configuration de sauvegarde

Contient une copie de sauvegarde de la configuration du module commutateur. Le fichier de sauvegarde est mis à jour lors de la copie du fichier de configuration en cours d'exécution ou du fichier de démarrage dans le fichier de sauvegarde.

Fichier image

Des images du système sont enregistrées dans deux secteurs de mémoire FLASH appelés Image 1 et Image 2. L'image active stocke la copie active et l'autre image une deuxième copie.

Fichier de configuration en cours d'exécution

Contient toutes les commandes du fichier de démarrage, ainsi que les commandes entrées pendant la session en cours. À la mise sous tension ou au redémarrage du module commutateur, toutes les commandes enregistrées dans le fichier de configuration en cours sont perdues.

FIFO

First In First Out (Premier entré premier sorti). Processus de mise en file d'attente où le premier paquet entrant de la file d'attente est le premier paquet sortant.

Fond de panier

Bus principal transportant des informations dans le module commutateur.

Fragment

Paquets Ethernet inférieurs à 576 bits.

G

GARP

General Attributes Registration Procotol (Protocole d'enregistrement générique des attributs). Enregistre les stations clientes dans un domaine de multidiffusion.

GVRP

Protocole d'enregistrement VLAN GARP. Enregistre les stations clientes dans un VLAN.

H

HOL

Head of Line (Tête de ligne). Les paquets sont mis en file d'attente. Les paquets en début de file d'attente sont transmis avant les paquets en fin de file d'attente.

Hôte

Ordinateur agissant comme source d'informations ou de services auprès d'autres ordinateurs.

HTTP

Hypertext Transfer Protocol (Protocole de transport hypertexte). Transfère des documents HTML entre serveurs et clients sur Internet.

I

IC

Integrated Circuit (Circuit intégré). Petit dispositif électronique composé de matériaux semiconducteurs.

ICMP

Internet Control Message Protocol (Protocole de contrôle des messages sur Internet). Permet à un hôte passerelle ou de destination de communiquer avec un hôte source, pour signaler une erreur de traitement, par exemple.

IEEE

Institute of Electrical and Electronics Engineers, Inc. Organisme professionnel dont les activités incluent le développement de normes relatives aux communications et aux réseaux.

IEEE 802.1d

Utilisée dans le protocole Spanning Tree, la spécification IEEE 802.1d prend en charge le pontage basé sur les adresses MAC pour empêcher la formation de boucles.

IEEE 802.1p

Accorde la priorité au trafic réseau au niveau de la sous-couche MAC/liaison de données.

IEEE 802.1Q

Définit le fonctionnement des ponts VLAN qui permet la définition, le fonctionnement et l'administration des VLAN dans des infrastructures LAN en pont.

Interrogation

Opération consistant à extraire des informations d'une base de données pour les utiliser.

Interruption

Message envoyé par le SNMP indiquant qu'un événement système est survenu.

IP

Internet Protocol (Protocole Internet). Désigne le format des paquets et leur méthode d'adressage. Le protocole IP adresse les paquets et les transfère au port approprié.

L

LAG

Link Aggregated Group (Groupe de liaisons agrégées). Agrège des ports ou des VLAN dans un seul port virtuel ou VLAN.

Pour plus d'informations sur les LAG, voir "**Définition de l'appartenance à un LAG**".

LAN

Local Area Network (Réseau local). Réseau étendu à une pièce, un bâtiment, un campus ou toute autre zone géographique limitée.

M

Masque

Filtre acceptant ou rejetant certaines valeurs (des fragments d'adresses IP, par exemple).

Par exemple, si l'unité 1 est insérée 5 minutes après l'unité 2, les deux sont considérées comme ayant la même ancienneté.

Masque à caractères génériques

Indique les bits de l'adresse IP qui sont utilisés et ceux qui sont ignorés. Un masque à caractères génériques de module de commutation indiquant 255.255.255.255 signifie qu'aucun bit n'est important. Un masque à caractères génériques 0.0.0.0 indique que tous les bits sont importants.

Par exemple, si l'adresse IP de destination est 149.36.184.198 et le masque à caractères génériques est 255.36.184.00, les deux premiers bits de l'adresse IP sont utilisés tandis que les deux derniers sont ignorés.

Masque de sous-réseau

Permet de masquer tout ou partie d'une adresse IP utilisée dans une adresse de sous-réseau.

MD5

Message Digest 5. Algorithme qui permet un hachage à 128 bits. MD5 est une variante de MD4 offrant plus de la sécurité. MD5 vérifie l'intégrité de la communication et en authentifie l'origine.

MDI

Media Dependent Interface (Interface dépendante du média). Câble utilisé pour les terminaux.

MDIX

Media Dependent Interface with Crossover (Interface croisée dépendante du média). Câble utilisé pour les concentrateurs et les commutateurs.

MIB

Management Information Base (Base d'informations de gestion). Les MIB contiennent des informations décrivant certains aspects spécifiques des composants du réseau.

Mise en miroir des ports

Contrôle et met en miroir le trafic réseau en transférant des copies des paquets entrants et sortants depuis un port vers un port de contrôle.

Pour plus d'informations, voir "**Mise en miroir des ports**".

Mode d'accès

Indique la méthode par laquelle l'utilisateur est autorisé à accéder au système.

Mode duplex

Permet l'envoi et la réception de données en simultané. Il existe deux sortes de modes duplex :

- **Duplex intégral** : permet une communication binaire synchrone (téléphone, etc.). Les deux parties peuvent transmettre des informations au même moment
- **Semi duplex** : permet une communication asynchrone (talkie-walkie, etc.). Une seule partie à la fois peut transmettre des informations.

Monodiffusion

Type de routage permettant le transfert d'un paquet vers un seul utilisateur.

Multidiffusion

Transfère des copies d'un paquet unique à plusieurs ports.

N

Négociation automatique

Permet aux ports Ethernet 10/100 Mbps ou 10/100/1000 Mbps de fonctionner avec les éléments communs suivants :

- Mode duplex ou semi duplex
- Contrôle de flux
- Vitesse

NMS

Network Management System (Système de gestion de réseau). Interface qui fournit une méthode de gestion du système.

Noeud

Point d'extrémité d'une connexion réseau ou jonction de plusieurs lignes dans un réseau. Les noeuds peuvent être les éléments suivants :

- Processeurs
- Contrôleurs
- Stations de travail

O

OID

Object Identifier (Identifiant d'objet). Utilisé par le protocole SNMP pour identifier les objets gérés. Dans le paradigme de gestion de réseau Gestionnaire/Agent SNMP, chaque objet géré doit posséder un OID permettant de l'identifier.

Oscillation

Le phénomène d'oscillation survient lorsque l'état des interfaces change constamment. Par exemple, un port STP passe de l'état écoute à l'état apprentissage, puis à l'état transmission. Cela peut provoquer une perte du trafic.

P

Paquets

Blocs d'informations transitant dans des systèmes de commutation.

PDU

Protocol Data Unit (Unité de données de protocole). Unité de données spécifiée dans un protocole de couche, constituée d'informations de contrôle de protocole et de données utilisateur de couche.

PING

Packet Internet Groper. Vérifie la disponibilité d'une adresse IP donnée. Un paquet est envoyé vers une adresse IP et attend la réponse.

Pont

Périphérique qui relie deux réseaux. Les ponts sont dépendants du matériel, mais indépendants du protocole. Ils agissent au niveau des couches 1 et 2.

Port

Les ports physiques fournissent des composants de connexion qui permettent aux microprocesseurs de communiquer avec des équipements périphériques.

Port d'entrée

Ports recevant le trafic réseau.

Ports de sortie

Ports à partir desquels le trafic réseau est transféré.

Profils d'accès

Permettent aux administrateurs réseau de définir des profils et des règles d'accès au module commutateur. L'accès aux fonctions de gestion peut être limité à des groupes d'utilisateurs, définis par les critères suivants :

- Interfaces d'entrée
- Adresse IP source ou sous-réseaux IP sources

Profils d'authentification

Ensemble de règles qui permettent la connexion et l'authentification d'utilisateurs et d'applications.

Protocole

Ensemble de règles régissant la façon dont des périphériques traitent l'échange d'informations sur des réseaux.

Protocole Spanning Tree

Empêche la formation de boucles dans le trafic réseau. Le protocole STP fournit une topographie en arborescence, quelle que soit l'architecture des ponts. Il fournit un chemin unique entre les stations terminales sur un réseau et élimine ainsi la formation de boucles.

Q

QoS

Qualité de service. La qualité de service permet aux gestionnaires réseau de déterminer, en fonction de priorités, de types d'applications et d'adresses source et de destination, la façon dont le trafic réseau est transféré.

R

RADIUS

Remote Authentication Dial-In User Service (Service distant d'authentification des utilisateurs entrants). Méthode d'authentification des utilisateurs du système et de suivi du temps de connexion.

RMON

Remote Monitoring (Surveillance à distance). Fournit des informations réseau pouvant être collectées à partir d'une seule station de travail.

Routeur

Périphérique relié à des réseaux séparés. Les routeurs transmettent des paquets de données entre les différents réseaux qu'ils connectent et fonctionnent au niveau de la couche 3.

RSTP

Rapid Spanning Tree Protocol. Détecte et utilise des topologies de réseau qui permettent une convergence plus rapide du Spanning Tree sans création de boucles de transmission.

S

Segmentation

Divise les réseaux locaux en segments de réseaux locaux à des fins de pontage et de routage. La segmentation élimine les limitations de bande passante du réseau local.

Serveur

Ordinateur central fournissant des services aux autres ordinateurs d'un réseau. Ces services comprennent le stockage de fichiers et l'accès à des applications.

SNMP

Simple Network Management Protocol (Protocole de gestion de réseau simple). Permet de gérer des réseaux locaux. Un logiciel basé sur SNMP communique avec les périphériques réseau via des agents SNMP intégrés. Ceux-ci collectent des informations relatives à l'activité du réseau et à l'état de l'unité. Ils renvoient ensuite ces informations vers une station de travail.

SNTP

Simple Network Time Protocol (Protocole simple de synchronisation réseau). Ce protocole assure une synchronisation de l'heure de l'horloge du commutateur réseau avec une précision d'un millième de seconde.

SoC

System on a Chip (Système sur une puce). ASIC contenant un système entier. Par exemple, une application SoC de télécommunications peut contenir un microprocesseur, un DSP (processeur de signal numérique), de la mémoire RAM et de la mémoire ROM.

Sous-réseau

Les sous-réseaux sont des portions de réseau partageant un composant d'adresse commun. Sur les réseaux TCP/IP, les unités partageant un même préfixe font partie du même sous-réseau. Par exemple, toutes les unités ayant le préfixe 157.100.100.100 font partie du même sous-réseau.

SSH

Secure Shell (Environnement sécurisé). Permet de se connecter à un ordinateur à distance via un réseau, d'exécuter des commandes et de transférer des fichiers d'un ordinateur à un autre. Cet environnement permet de sécuriser les méthodes de communication sur des canaux sans protection, et fournit des mécanismes d'authentification avancés.

T

TCP/IP

Transmissions Control Protocol (Protocole de contrôle des transmissions). Permet à deux hôtes de communiquer et d'échanger des flots de données. Le protocole TCP garantit la livraison des paquets dans l'ordre de leur envoi.

Telnet

Terminal Emulation Protocol (Protocole d'émulation de terminal Permet aux utilisateurs d'un système de se connecter à des ressources de réseaux distants et de les utiliser.

Terminal

Unité utilisée par un utilisateur final sur un réseau.

TFTP

Trivial File Transfert Protocol (Protocole de transfert des fichiers simple). Utilise le protocole UDP (User Data Protocol) sans fonctions de sécurité pour transférer les fichiers.

Trame

Paquets contenant les informations d'en-tête et de fin requises par les supports physiques.

Trames Jumbo

Permettent de transporter une quantité de données identique sur un nombre réduit de trames. Les trames Jumbo diminuent les risques de surcharges et d'interruptions, ce qui permet d'obtenir des temps de traitement plus courts.

U

UDP

User Data Protocol (Protocole de datagramme utilisateur). Transmet les paquets mais ne garantit pas leur livraison.

V

Version d'amorçage

Version utilisée au démarrage d'un système.

Vitesse de port

Indique la vitesse d'un port. Les vitesses possibles sont les suivantes :

- Ethernet 10 Mbps
- Fast Ethernet 100 Mbps
- Ethernet Gigabit 1000 Mbps

VLAN

Virtual Local Area Networks (Réseaux locaux virtuels). Sous-groupes logiques d'un LAN créés via un logiciel et non par la définition d'une solution matérielle.

VLAN agrégé

Regroupe plusieurs VLAN dans un seul VLAN agrégé. L'agrégation de VLAN permet aux routeurs de répondre aux demandes ARP de noeuds situés sur des sous-VLAN différents appartenant au même Super VLAN. Les routeurs répondent avec leur adresse MAC.

W

WAN

Wide Area Networks (Réseaux étendus). Réseaux couvrant une vaste zone géographique.

Retour au sommaire