

Guide d'utilisation du système Dell™ PowerConnect™ 5324

[Présentation](#)

[Description matérielle](#)

[Installation du périphérique PowerConnect](#)

[Mise en route et configuration du périphérique](#)

[Utilisation de Dell OpenManage Switch Administrator](#)

[Configuration des informations système](#)

[Configuration des informations du périphérique](#)

[Affichage des statistiques](#)

[Configuration de la qualité de service](#)

[Caractéristiques techniques](#)

[Glossaire](#)

Remarques, avis et précautions



REMARQUE : Une REMARQUE indique une information importante qui peut vous aider à mieux utiliser votre ordinateur.



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



PRÉCAUTION : Une PRÉCAUTION indique un risque potentiel de dommages matériels ou corporels, ou de mort.

Les informations contenues dans ce document sont sujettes à modification sans préavis.

© 2003 - 2007 Dell Inc. Tous droits réservés.

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

Marques utilisées dans ce document : *Dell, Dell OpenManage, le logo DELL, Inspiron, Dell Precision, Dimension, OptiPlex, PowerConnect, PowerApp, PowerVault, Axim, DellNet et Latitude* sont des marques de Dell Inc. *Microsoft et Windows* sont des marques déposées de Microsoft Corporation.

D'autres marques et noms commerciaux peuvent être utilisés dans ce document pour faire référence aux entités se réclamant de ces marques et de ces noms ou à leurs produits. Dell Inc. rejette tout intérêt propriétaire dans les marques et les noms commerciaux autres que les siens.

Mai 2007

[Retour à la page du sommaire](#)

Mise en route et configuration du périphérique

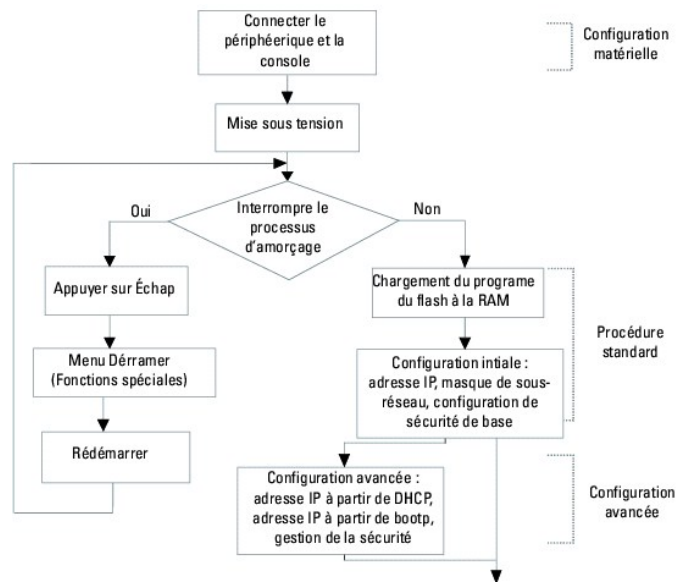
Guide d'utilisation du système Dell™ PowerConnect™ 5324

- [Configuration du terminal](#)
- [Amorçage du périphérique](#)
- [Présentation de la configuration](#)
- [Configuration initiale](#)
- [Nom d'utilisateur](#)
- [Chaînes de communauté SNMP](#)
- [Configuration avancée](#)
- [Récupération d'une adresse IP à partir d'un serveur DHCP](#)
- [Réception d'une adresse IP à partir d'un serveur BOOTP](#)
- [Gestion de la sécurité et configuration du mot de passe](#)
- [Configuration de mots de passe de sécurité](#)
- [Procédures de démarrage](#)

Une fois toutes les connexions externes terminées, vous devez connecter un terminal au périphérique pour configurer celui-ci et effectuer différentes procédures. Pour la configuration initiale, une configuration de périphérique standard est réalisée.

REMARQUE : Avant de continuer, lisez les notes de mise à jour pertinentes à ce produit. Les notes de mise à jour peuvent être téléchargées sur le site www.support.dell.com.

Figure 4-12. Organigramme des procédures d'installation et de configuration



Configuration du terminal

Pour configurer le périphérique, le terminal doit exécuter un logiciel d'émulation de terminal.


Assurez-vous que le logiciel d'émulation de terminal est configuré de la façon suivante :

1. Sélectionnez le port série approprié (port série 1 ou 2) à relier à la console.
2. Configurez le taux de transfert des données à 9600 bauds.

3. Configurez le format de données à 8 bits de données, 1 bit d'arrêt et aucune parité.
4. Paramétrez le contrôle du flux sur **none** (aucun).
5. Sous **Propriétés**, sélectionnez le mode **VT100 pour émulation**.
6. Sélectionnez **Touches du terminal** pour **les touches de fonction, de direction et Ctrl**. Assurez-vous que le paramètre est configuré sur **Touches du terminal** (et non sur **Touches Windows**).

 **AVIS** : Lorsque vous utilisez HyperTerminal avec le système d'exploitation Microsoft® Windows 2000, assurez-vous d'avoir préalablement installé Windows® 2000 Service Pack 2 ou une version plus récente. Windows 2000 Service Pack 2 vous permet d'utiliser les touches de direction dans l'émulation HyperTerminal VT100. Rendez-vous à l'adresse www.microsoft.com pour obtenir des informations sur les service packs de Windows 2000.

Amorçage du périphérique

 **REMARQUE** : Les données conventionnelles pour l'amorçage sont les suivantes :

- o Le périphérique est fourni avec une configuration par défaut.
- o Le périphérique n'est pas configuré avec un nom d'utilisateur et un mot de passe par défaut.

Pour amorcer le périphérique, procédez comme suit :

1. Assurez-vous que le port série du périphérique est connecté à un terminal ASCII ou au connecteur série d'un système de bureau exécutant un logiciel d'émulation de terminal.
2. Trouvez une prise secteur.
3. Éteignez la prise secteur.
4. Connectez le périphérique sur la prise secteur. Reportez-vous à la section [«Connexion d'un périphérique sur un bloc d'alimentation»](#).
5. Allumez la prise secteur.

Lorsque le périphérique est mis sous tension alors que le terminal local est déjà connecté, il effectue un POST (auto-test de démarrage). Le POST s'effectue chaque fois que le périphérique est initialisé et vérifie les composants matériels afin de déterminer si le périphérique fonctionne totalement avant de poursuivre l'initialisation. Si un problème critique est détecté, le flux du programme s'arrête. Si le POST est exécuté avec succès, une image exécutable valide est chargée dans la mémoire RAM. Les messages de POST qui s'affichent sur le terminal indiquent la réussite ou l'échec du test.

1. Assurez-vous que le câble ASCII est connecté au terminal et que les paramètres sur l'émulation de logiciel sont configurés correctement.
2. Connectez le bloc d'alimentation au périphérique.
3. Mettez le périphérique sous tension.
4. À l'amorçage du périphérique, le test d'amorçage recense tout d'abord la mémoire disponible, puis continue le processus d'amorçage. Vous trouverez ci-dessous un exemple des informations qui s'affichent lors du POST :

```
----- Auto-test de démarrage (POST) -----
```

```
Test bouclage canal UART.....OK
```

```
Test SDRAM système.....OK
```

```
Test Somme de Contrôle Amorçage1.....OK
```

```
Test Somme de Contrôle Amorçage2.....OK
```

```
Test Validation Image Flash.....OK
```

```
Version logiciel AMORÇAGE 1.0.0.20 Créée le 22-Jan-2004 15:09:28
```

Processeur : FireFox 88E6218 ARM946E-S , 64 Mo SDRAM.

I-Cache 8 Ko. D-Cache 8 Ko. Cache activé.

Amorçage automatique dans 2 secondes - appuyez sur RETOUR ou Échap pour abandonner et accéder à la mémoire PROM.

Préparation à la décompression...

Le processus d'initialisation dure environ 90 secondes.

Le message d'amorçage automatique qui apparaît à la fin du POST (voir les dernières lignes ci-dessus) indique qu'aucun problème n'a été rencontré.

Au cours de l'amorçage, le menu **Démarrer** peut être utilisé pour exécuter des procédures particulières. Pour accéder au menu **Démarrer**, appuyez sur <Échap> ou <Entrée> moins de deux secondes après l'affichage du message d'amorçage automatique.

Si le processus d'amorçage du système ne s'arrête pas lorsque vous appuyez sur <Échap> ou <Entrée>, le processus continue à décompresser et à charger le code dans la RAM. Le code démarre à partir de la mémoire RAM et la liste des numéros de port disponibles ainsi que leur état (disponible ou non disponible) s'affichent.

L'écran suivant est un exemple de configuration. Les éléments tels que les adresses, les versions et les dates peuvent être différents pour chaque périphérique.

Décompression logiciel à partir d'image-2

78c000

OK

Exécution depuis mémoire RAM...

*** Exécution logiciel Ver. 1.0.0.15 Date 03-Mar-2004 Heure 10:41:14 ***

Version matériel : 00.01.07

Adresse MAC Base : 00:00:07:77:77:77

Taille DRAM : 64 Mo

Taille premier bloc DRAM : 40 960 Ko

Premier PTR DRAM : 0x1800000

Taille mémoire Flash : 16 Mo

Configuration périphérique :

Système basé sur Prestera

Emplacement 1 - Neyland24 HW Rév. 0.1

Version Tapi : v1.2.9

Version Noyau : v1.2.9

01-Jan-2000 01:01:32 %INIT-I-InitCompleted: Initialisation terminée

console> 01-Jan-2000 01:01:35 %LINK-W-Down: g1

01-Jan-2000 01:01:35 %LINK-W-Down: g2

01-Jan-2000 01:01:35 %LINK-W-Down: g3

01-Jan-2000 01:01:35 %LINK-W-Down: g4

01-Jan-2000 01:01:35 %LINK-W-Down: g5

01-Jan-2000 01:01:35 %LINK-W-Down: g6

01-Jan-2000 01:01:35 %LINK-W-Down: g7

01-Jan-2000 01:01:35 %LINK-W-Down: g8

01-Jan-2000 01:01:35 %LINK-W-Down: g9

01-Jan-2000 01:01:35 %LINK-W-Down: g10

01-Jan-2000 01:01:35 %LINK-W-Down: g11

01-Jan-2000 01:01:35 %LINK-W-Down: g12

01-Jan-2000 01:01:35 %LINK-W-Down: g13

01-Jan-2000 01:01:36 %LINK-W-Down: g14

01-Jan-2000 01:01:36 %LINK-W-Down: g15

01-Jan-2000 01:01:36 %LINK-W-Down: g16

01-Jan-2000 01:01:36 %LINK-W-Down: g17

01-Jan-2000 01:01:36 %LINK-W-Down: g18

01-Jan-2000 01:01:36 %LINK-W-Down: g19

01-Jan-2000 01:01:36 %LINK-W-Down: g20

01-Jan-2000 01:01:36 %LINK-W-Down: g21

01-Jan-2000 01:01:36 %LINK-W-Down: g22

01-Jan-2000 01:01:36 %LINK-I-Up: VLAN 3000

01-Jan-2000 01:01:36 %LINK-I-Up: VLAN 1

01-Jan-2000 01:01:36 %LINK-I-Up: g1

01-Jan-2000 01:01:36 %LINK-I-Up: g13

01-Jan-2000 01:01:36 %LINK-I-Up: g14

01-Jan-2000 01:01:36 %LINK-I-Up: g19

01-Jan-2000 01:01:36 %LINK-I-Up: g20

01-Jan-2000 01:01:36 %LINK-I-Up: g21

01-Jan-2000 01:01:36 %LINK-W-Down: g23

01-Jan-2000 01:01:36 %LINK-W-Down: g24

```
01-Jan-2000 01:01:36 %LINK-W-Down: canall
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: VLAN 1000
```

```
01-Jan-2000 01:01:36 %TRUNK-I-PORTADDED: Port g24 ajouté à canall
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: g22
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: g23
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: g24
```

```
01-Jan-2000 01:01:36 %LINK-I-Up: canall
```

```
01-Jan-2000 01:01:36 %LINK-W-Down: g1
```

```
01-Jan-2000 01:03:42 %INIT-I-Startup: Démarrage à froid
```

```
console>
```

Lorsque le périphérique démarre correctement, une invite système permettant de configurer le périphérique s'affiche (`console>`). Avant de configurer le périphérique, assurez-vous que vous y avez installé la dernière version du logiciel. Si nécessaire, téléchargez et installez la dernière version. Pour plus d'informations sur le téléchargement de la dernière version, reportez-vous à la section [«Téléchargement des logiciels»](#).

Présentation de la configuration

Avant d'affecter une adresse IP statique au périphérique, récupérez les informations suivantes :

- 1 L'adresse IP spécifique qui a été affectée au périphérique pour qu'il soit configuré.
- 1 Le chemin par défaut.
- 1 Le masque du réseau.

Il existe deux types de configuration :


- 1 **Configuration initiale** — Fonctions de base en matière de configuration et de sécurité.
- 1 **Configuration avancée** — Inclut la configuration de l'adresse IP dynamique et des fonctions de sécurité plus évoluées.




REMARQUE : Si vous modifiez la configuration, vous devez l'enregistrer avant de redémarrer le système. Pour enregistrer la configuration, entrez :

```
console# copy running-config startup-config
```

Configuration initiale

 **REMARQUE** : Avant de continuer, lisez les notes de mise à jour pertinentes à ce produit. Les notes de mise à jour peuvent être téléchargées sur le site Web de support de Dell à l'adresse support.dell.com.

 **REMARQUE** : La configuration simple initiale tient compte des hypothèses suivantes :

- o Le périphérique PowerConnect n'a jamais été configuré et est dans le même état que lorsqu'il a été reçu.
- o L'initialisation du périphérique PowerConnect a réussi.
- o La connexion série est établie et l'invite de console s'affiche à l'écran d'un terminal VT100. (Appuyez plusieurs fois sur la touche <Entrée> pour vérifier que l'invite s'affiche correctement.)
- o Le périphérique n'est pas configuré avec un nom d'utilisateur et un mot de passe par défaut.

La configuration initiale du périphérique se fait via le port série. Après la configuration initiale, le périphérique peut être géré soit par le port série déjà connecté, soit à distance via une interface définie pendant la configuration initiale.

La configuration initiale consiste à :

- 1 Paramétrer le nom d'utilisateur 'admin', le mot de passe 'dell' avec le plus haut niveau de privilège : 15.
- 1 Configurer l'adresse IP statique et la passerelle par défaut.
- 1 Configurer la chaîne de communauté SNMP de lecture/écriture.
- 1 Affecter l'adresse IP allouée par le serveur DHCP.

Avant d'effectuer la procédure de configuration initiale du périphérique PowerConnect, récupérez les informations suivantes auprès de l'administrateur de réseau :

- 1 L'adresse IP à affecter à un VLAN par lequel le périphérique est géré.
- 1 Le masque de sous-réseau IP du réseau.
- 1 L'adresse IP passerelle par défaut.
- 1 La communauté SNMP.

Adresse IP statique et masque de sous-réseau

L'adresse IP peut être configurée sur n'importe quelle interface, comme un VLAN, un LAG ou un port physique. Une fois la commande de configuration saisie, il est recommandé de vérifier qu'un port a été configuré avec l'adresse IP en saisissant la commande **show ip interface**.


Important : Si une adresse IP est configurée sur un LAG ou un port physique (ex. : g10), cette interface est supprimée du VLAN 1.

Configuration du chemin statique

Pour gérer le périphérique à partir d'un réseau à distance, vous devez configurer un chemin statique, qui est l'adresse IP où les paquets sont envoyés lorsque aucune entrée n'est trouvée dans les tables de périphériques. L'adresse IP configurée doit appartenir au même sous-réseau que celle des interfaces IP du périphérique.

Pour configurer un chemin statique, à l'invite du système, tapez la commande comme indiqué dans l'exemple de configuration ci-dessous, où 100.1.1.1 (masque 24) est la station de gestion spécifique et 100.1.1.10 est le chemin statique utilisé comme une passerelle par défaut.

Affectation d'adresses IP statiques sur une interface intrabande

 **REMARQUE** : Dans le cas de cet exemple, les conditions suivantes doivent être remplies :

- o L'adresse IP à affecter à l'interface VLAN PowerConnect est 192.168.1.123
- o Le masque de sous-réseau IP du réseau est 255.255.255.0
- o L'adresse IP du chemin par défaut est 192.168.1.1
- o La chaîne de communauté SNMP de lecture/écriture est «private» (privée)


```

console> enable

console#configure

console(config)# username admin password dell level 15

console(config)# interface vlan 1

console (config-if) # ip address 192.168.1.123 /24

console (config-if)#exit

console (config)# ip default-gateway 192.168.1.1

console (config) # snmp-server community private rw

console(config)# exit

console#

```

Vérification de l'adresse IP et de l'adresse de passerelle par défaut

Assurez-vous que l'adresse IP et la passerelle par défaut sont correctement assignées en exécutant la commande ci-dessous et en analysant le résultat :


Commande

```
console# show ip interface vlan 1
```

Sortie


Adresse IP de la passerelle	État activité	
-----	-----	
192.168.1.1	Actif	
Adresse IP	Interface	Type

-----	-----	-----
192.168.1.123 /24	VLAN 1	Statique

 **REMARQUE** : Nous vous recommandons de télécharger la dernière révision de la documentation utilisateur sur le site Web de support de Dell à l'adresse support.dell.com.

Nom d'utilisateur

Pour gérer le périphérique à distance, par exemple via une session SSH, Telnet ou l'interface Web, vous devez configurer un nom d'utilisateur. Pour obtenir le contrôle administratif total du périphérique, utilisez le niveau de privilège le plus élevé (15).

 **REMARQUE** : Seul l'administrateur (super-utilisateur) possédant le niveau de privilège le plus élevé (15) est autorisé à gérer le périphérique via l'interface du navigateur Web.

Pour plus d'informations sur le niveau de privilège, reportez-vous au «Guide de référence CLI».

Le nom d'utilisateur configuré est saisi en tant que nom de connexion pour les sessions de gestion à distance. Pour configurer un nom d'utilisateur et un niveau de privilège, tapez la commande à l'invite du système, comme indiqué dans l'exemple de configuration ci-dessous :


```
console> enable
console# configure
console(config)# username admin password abc level 15
```

Chaînes de communauté SNMP

Le protocole SNMP (Simple Network Management Protocol - protocole de gestion de réseau simple) fournit une méthode de gestion des périphériques réseau. Les périphériques SNMP exécutent un logiciel local, appelé «agent». Les agents SNMP gèrent une liste de variables, qui sont utilisées pour gérer le périphérique. Ces variables sont définies dans la MIB (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 ainsi que par des chaînes de communauté SNMP.

Le périphérique est compatible SNMP et contient un agent SNMP qui prend en charge un jeu de variables MIB standard et privées. Les développeurs des stations de gestion ont besoin de la structure exacte de l'arborescence MIB et de la totalité des informations relatives aux variables MIB privées avant de pouvoir gérer les MIB.

Tous les paramètres peuvent être gérés à partir de n'importe quelle plate-forme de gestion SNMP, à l'exception de l'adresse IP de la station de gestion SNMP, du nom de la communauté et des droits d'accès. L'accès de gestion SNMP au périphérique est désactivé si aucune chaîne de communauté n'existe.

 **REMARQUE** : Le périphérique est fourni sans aucune chaîne de communauté configurée. Les protocoles SNMPv1 et SNMPv2 sont pris en charge sur le périphérique. Cette section décrit les paramètres de configuration des protocoles SNMPv1/v2.

L'écran suivant présente la configuration par défaut du périphérique :

Console# show snmp		
Chaîne de communauté	Accès de communauté	Adresse IP
-----	-----	-----

Interruptions activées.		
L'interruption d'authentification est activée.		
Adresse dest. interruption	Communauté dest. interruption	Version
Contact système :		
Emplacement système :		

La chaîne de communauté, l'accès à la communauté et l'adresse IP peuvent être paramétrés via le terminal local lors de la procédure de configuration initiale.

Les options de configuration SNMP sont les suivantes :

- 1 Community string (Chaîne de communauté).
 - o **Read Only** (lecture seule) — Indique que les membres de la communauté peuvent consulter des informations de configuration sans pouvoir les modifier.
 - o **Read/Write** (lecture et écriture) — Indique que les membres de la communauté peuvent consulter et modifier des informations de configuration.
 - o **Super** — Indique que les membres de la communauté ont un accès administration.
- 1 Configurable IP address (Adresse IP configurable). Si l'adresse IP n'est pas configurée, cela signifie que tous les membres de la communauté possédant le même nom de communauté bénéficient des mêmes droits d'accès.

La norme actuellement utilisée consiste à se servir de deux chaînes de communauté pour le périphérique — l'une (publique) avec un accès en lecture seule et l'autre (privée) avec un accès en lecture et en écriture. La chaîne publique permet aux stations de gestion autorisées d'extraire des objets MIB, tandis que la chaîne privée permet aux stations de gestion autorisées d'extraire et de modifier des objets MIB.

Lors de la configuration initiale, il est recommandé de configurer l'unité conformément aux exigences de l'administrateur réseau et liées à l'utilisation d'une station de gestion SNMP.

Configuration de SNMP

Pour configurer une adresse IP et des chaînes de communauté d'une station SNMP pour les tables générales de routeurs du périphérique, effectuez la procédure suivante :

1. À l'invite de la console, tapez la commande **Enable**. L'invite s'affiche sous la forme #.
2. Tapez la commande **configure** et appuyez sur <Entrée>.
3. En mode de configuration, tapez la commande de configuration SNMP avec les paramètres incluant le nom de la communauté (privée), les droits d'accès de la communauté (lecture et écriture) et l'adresse IP, comme indiqué dans l'exemple ci-dessous :

```
console# configure
```

```
config(config)# snmp-server community private rw 11.1.1.2
```

Affichage des tables de communauté SNMP

Pour afficher l'adresse IP et les tables de communauté de la station SNMP :

1. À l'invite de la console, tapez la commande **exit**. L'invite s'affiche sous la forme #.

2. En mode Privileged Exec (EXEC privilégié), tapez la commande show comme indiqué dans l'exemple ci-dessous :

Les paramètres configurés permettent de poursuivre la configuration du périphérique à partir d'un emplacement distant.

Console# show snmp		
Chaîne de communauté	Accès de communauté	Adresse IP
-----	-----	-----
privée	lecture écriture	11.1.1.2
Interruptions activées.		
L'interruption d'authentification est activée.		
Adresse dest. interruption	Communauté dest. interruption	Version
Contact système :		
Emplacement système :		

Configuration avancée

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

- 1 Configuration des adresses IP via DHCP
- 1 Configuration des adresses IP via BOOTP
- 1 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.

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

Lorsque le protocole DHCP est utilisé pour obtenir une adresse IP, le périphérique agit en tant que client DHCP. Lorsque le périphérique est réinitialisé, la commande DHCP est enregistrée dans le fichier de configuration, mais pas l'adresse IP. Pour obtenir une adresse IP à partir d'un serveur DHCP :

- 1. Sélectionnez et connectez n'importe quel port au serveur DHCP ou à un sous-réseau possédant un serveur DHCP, de manière à obtenir l'adresse IP.

2. Tapez les commandes ci-après pour utiliser le port sélectionné pour la réception de l'adresse IP. Dans cet exemple, les commandes sont basées sur le type de port utilisé pour la configuration.

1 Allocation d'adresses IP dynamiques :

```

console# configure

console(config)# interface ethernet g1

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

console(config-if)# exit

console(config)#

```

1 Affectation d'adresses IP dynamiques (sur un VLAN) :

```

console# configure

console(config)# interface ethernet vlan 1

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

console(config-if)# exit

console(config)#

```


3. Pour vérifier l'adresse IP, tapez la commande `show ip interface` à l'invite du système, comme dans l'exemple ci-après.


Console# show ip interface		
Adresse IP de la passerelle	État activité	
-----	-----	
10.7.1.1	Actif	
Adresse IP	Interface	Type
-----	-----	-----
10.7.1.192/24	VLAN 1	Statique

10.7.2.192/24

VLAN 2

DHCP

 **REMARQUE** : Il n'est pas nécessaire de supprimer la configuration du périphérique pour obtenir une adresse IP à partir du serveur DHCP.

 **REMARQUE** : Lorsque vous copiez des fichiers de configuration, évitez d'utiliser un fichier de configuration contenant une instruction permettant d'activer le protocole DHCP sur une interface reliée au même serveur DHCP ou à un serveur possédant la même configuration. Dans cet exemple, le périphérique obtient le nouveau fichier de configuration et l'utilise pour démarrer. Le périphérique active ensuite le DHCP comme il est demandé dans le nouveau fichier de configuration et le DHCP lui demande de charger à nouveau le même fichier.


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

Le protocole standard BOOTP est pris en charge, ce qui permet au périphérique de télécharger automatiquement la configuration IP de son hôte à partir de n'importe quel serveur BOOTP standard sur le réseau. Dans ce cas, le périphérique joue le rôle d'un client BOOTP.

Pour obtenir 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** pour supprimer la configuration de démarrage de la mémoire Flash.

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

 **REMARQUE** : Une fois que l'amorçage du périphérique a commencé, le fait d'entrer des données sur le terminal ASCII ou sur le clavier fait avorter le processus et le périphérique ne reçoit pas d'adresse IP de la part du serveur BOOTP.

L'exemple suivant présente le processus :

```
console> enable
```

```
console# delete startup-config
```

```
Le fichier de démarrage a été supprimé
```

```
console# reload
```

```
Vous n'avez pas enregistré vos modifications. Êtes-vous certain de vouloir continuer (y/n) [n] ?
```

```
Cette commande réinitialisera tout le système et vous déconnectera de la session en cours. Êtes-vous certain de vouloir continuer (y/n) [n] ?
```

```
*****
```

```
/* redémarrage du commutateur */
```

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

Le périphérique est maintenant paramétré 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, and 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 configuré : 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 **Démarrer**. Cette procédure est disponible uniquement sur le terminal local et permet d'accéder une seule fois au périphérique sans saisir de mot de passe.

Configuration de mots de passe de sécurité

Vous pouvez configurer des mots de passe de sécurité pour les services suivants :

- 1 Terminal
- 1 Telnet
- 1 SSH
- 1 HTTP
- 1 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. Même si les noms d'utilisateur peuvent avoir le niveau de privilège 15 sans mot de passe nécessaire, il est recommandé de leur en assigner un automatiquement. Si aucun mot de passe n'est défini, les utilisateurs privilégiés peuvent accéder à l'interface Web sans mot de passe.

Configuration d'un mot de passe terminal initial

Pour configurer un mot de passe terminal initial, entrez les commandes suivantes :

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line console
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password george
```

- 1 Lorsque vous vous connectez à un périphérique pour la première fois via une session de terminal, tapez `george` à l'invite du mot de passe.
- 1 Lorsque vous modifiez le mode du périphérique de `disable` (désactiver) à `enable` (activer), 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
```

- 1 Lorsque vous vous connectez à un périphérique pour la première fois via une session Telnet, tapez `bob` à l'invite du mot de passe.
- 1 Lorsque vous modifiez le mode du périphérique de `disable` (désactiver) à `enable` (activer), 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.
```

- 1 Lorsque vous vous connectez à un périphérique pour la première fois via une session SSH, tapez `jones` à l'invite du mot de passe.
- 1 Lorsque vous modifiez le mode du périphérique de disable (désactiver) à enable (activer), 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 une fois les commandes suivantes lorsque vous configurez une session 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 Démarrer

Les procédures exécutées à partir du menu Démarrer concernent le téléchargement du logiciel, la gestion de la mémoire Flash et la récupération du mot de passe. Les procédures de diagnostic doivent être exécutées par le personnel du support technique et ne sont pas détaillées dans ce document.

Vous pouvez accéder au menu Démarrer au cours de l'amorçage du périphérique – une entrée utilisateur doit être faite immédiatement après le POST.

Pour accéder au menu Démarrer :

1. Mettez le périphérique sous tension et observez le message d'amorçage automatique.

***** RÉINITIALISATION SYSTÈME *****

----- Auto-test de démarrage (POST) -----

Test bouclage canal UART.....OK

Test SDRAM système.....OK

Test Somme de Contrôle Amorçage1.....OK

Test Somme de Contrôle Amorçage2.....OK

Test Validation Image Flash.....OK

Version logiciel AMORÇAGE 1.0.0.20 Créée le 22-Jan-2004 15:09:28

Processeur : FireFox 88E6218 ARM946E-S , 64 Mo SDRAM.

I-Cache 8 Ko. D-Cache 8 Ko. Cache activé.

Amorçage automatique dans 2 secondes - appuyez sur RETOUR ou Échap pour abandonner et accéder à la mémoire PROM.

Préparation à la décompression...

2. Lorsque le message d'amorçage automatique s'affiche, appuyez sur <Entrée> pour entrer dans le menu Démarrer. Les procédures du menu Démarrer peuvent être lancées à l'aide du terminal ASCII ou de l'HyperTerminal Windows.

[1] Download Software (Téléchargement des logiciels)

[2] Erase Flash File (Effacement du fichier FLASH)

[3] Password Recovery Procedure (Procédure de récupération des mots de passe)


[4] Enter Diagnostic Mode (Mode Diagnostic)

[5] Set Terminal Baud-Rate (Configuration du débit du terminal)

[6] Back (Retour)

Tapez votre choix ou appuyez sur 'ÉCHAP' pour sortir

Les sections qui suivent décrivent les options disponibles du menu Démarrer.

 **REMARQUE** : Lorsque vous sélectionnez une option dans le menu Démarrer, vous devez tenir compte d'un délai : Si aucune sélection n'est faite dans les 35 secondes (valeur par défaut), la temporisation expire. Cette valeur par défaut peut être modifiée via l'interface de ligne de commande.


Téléchargement des logiciels

La procédure de téléchargement des logiciels est exécutée lorsqu'une nouvelle version doit être téléchargée pour remplacer des fichiers corrompus, mettre à jour ou mettre à niveau le logiciel du système. Pour télécharger un logiciel via le menu Démarrer :

1. À partir du menu Démarrer, appuyez sur [1]. L'invite suivante apparaît :

Téléchargement du code via XMODEM

2. Lorsque vous utilisez HyperTerminal, cliquez sur **Transfer** (Transfert) dans la barre de menus d'HyperTerminal.
3. Dans le champ **Filename** (Nom du fichier), tapez le chemin du fichier à télécharger.
4. Assurez-vous que le protocole Xmodem est sélectionné dans le champ **Protocol** (Protocole).
5. Cliquez sur **Send** (Envoyer). Le logiciel est téléchargé.

 **REMARQUE** : Une fois le logiciel téléchargé, le périphérique est réamorçé automatiquement.

 **REMARQUE** : Le temps de téléchargement varie suivant l'outil utilisé.

Effacement du fichier FLASH

Dans certains cas, la configuration du périphérique doit être effacée. Si la configuration est effacée, tous les paramètres configurés via l'interface CLI, l'interface de gestion Web ou SNMP doivent être reconfigurés.

Effacement de la configuration du périphérique

1. À partir du menu Démarrer, tapez [2] dans les deux secondes pour effacer le fichier de mémoire Flash. Le message suivant s'affiche :

Avertissement ! Vous êtes sur le point d'effacer un fichier FLASH.

Êtes-vous certain de vouloir continuer (Y/N) ? y

2. Tapez Y. Le message suivant s'affiche.

Nom du fichier Flash d'écriture (8 caractères max, Entrée pour aucun) : config

Le fichier de config (si présent) sera effacé après initialisation du système

=====
Appuyez sur Entrée pour continuer
=====

3. Saisissez config comme nom de fichier FLASH. La configuration est effacée et le périphérique redémarre.
4. Répétez la configuration initiale du périphérique.


Récupération des mots de passe

Si un mot de passe est perdu, la procédure de Récupération des mots de passe peut être appliquée à partir du menu Démarrer. Cette procédure permet d'entrer dans le périphérique une seule fois sans mot de passe.

Pour récupérer un mot de passe perdu (terminal local uniquement) :

1. À partir du menu Démarrer, tapez 3 et appuyez sur <Entrée>.

Le mot de passe est supprimé.

 **REMARQUE** : Pour garantir la sécurité du périphérique, redéfinissez les mots de passe des méthodes de gestion applicables.

Téléchargement de logiciels via un serveur TFTP

Cette section contient des instructions pour le téléchargement des logiciels du périphérique (images système et d'amorçage) via un serveur TFTP. Le serveur TFTP doit être configuré avant de commencer à télécharger le logiciel.

Téléchargement de l'image système

Le périphérique s'amorce et s'exécute lorsqu'il décompresse l'image système de la zone de mémoire Flash où une copie de l'image système est enregistrée. Lorsqu'une nouvelle image est téléchargée, elle est enregistrée dans une autre zone réservée à l'autre copie de l'image système.

Au prochain amorçage, le périphérique décompressera et exécutera l'image système active, sauf indication contraire.

Pour télécharger une image système via le serveur TFTP :

1. Assurez-vous qu'une adresse IP est assignée à au moins un port du périphérique et que des pings peuvent être envoyés à un serveur TFTP.
2. Assurez-vous que le fichier à télécharger est enregistré dans le serveur TFTP (le fichier `zos`).
3. Tapez `show version` pour vérifier la version du logiciel installée sur le périphérique. Vous trouverez ci-dessous un exemple des informations qui

s'affichent :

```
console# show version
```

```
Version logiciel 1.0.0.42 (date 22-Juil-2004 heure 13:42:41)
```

```
Version amorçage 1.0.0.18 (date 01-Juin-2004 heure 15:12:20)
```

```
Version matériel
```

4. Tapez `show bootvar` pour vérifier l'image système active. Vous trouverez ci-dessous un exemple des informations qui s'affichent :

```
console# sh bootvar
```

```
Images actuellement disponibles dans la mémoire Flash
```

```
Image-1 active (sélectionnée pour le prochain amorçage)
```

```
Image-2 inactive
```

```
console#
```

5. Tapez `copy tftp://{adresse tftp}/{nom de fichier} image` pour copier une nouvelle image système dans le périphérique. La nouvelle image téléchargée est enregistrée dans la zone réservée à la copie de l'image système (image-2 dans notre exemple). Vous trouverez ci-dessous un exemple des informations qui s'affichent :

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

```
Accès au fichier `file1' sur 176.215.31.3
```

```
Chargement de file1 depuis 176.215.31.3:
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
La copie s'est effectuée en 00:01:11 [hh:mm:ss]
```

Les points d'exclamation (!) indiquent que le processus de copie est en cours. Chaque symbole (!) correspond à 512 octets transférés avec succès. Un point indique que la temporisation du processus de copie est dépassée. La présence de plusieurs points sur une ligne indique que le processus de copie a échoué.

6. Sélectionnez l'image qui sera utilisée au prochain amorçage en tapant la commande système `boot`. Ensuite, tapez `show bootvar` pour vérifier que la copie indiquée comme paramètre dans la commande `boot system` est sélectionnée pour le prochain amorçage.

Voici un exemple des informations qui s'affichent.

```
console# boot system image-2
```

```
console# sh boot
```

```
Images actuellement disponibles dans la mémoire Flash
```

```
Image-1 active
```

```
Image-2 inactive (sélectionnée pour le prochain amorçage)
```

Si l'image pour le prochain amorçage n'est pas sélectionnée à l'aide de la commande `boot system`, le système s'amorce à partir de l'image actuellement active.

7. Tapez la commande `reload`. Le message suivant s'affiche :

```
console# reload
```

```
Cette commande réinitialisera tout le système et vous déconnectera de la session
```

```
en cours. Êtes-vous certain de vouloir continuer (y/n) [n] ?
```

8. Tapez `y`. Le périphérique redémarre.

Téléchargement d'une image d'amorçage

Vous pouvez mettre à jour l'image d'amorçage en chargeant une nouvelle image d'amorçage à partir du serveur TFTP et en la programmant dans la mémoire Flash. L'image d'amorçage est chargée lorsque le périphérique est mis sous tension. L'utilisateur ne peut pas contrôler les copies d'image d'amorçage. Pour télécharger une image d'amorçage via le serveur TFTP :

1. Assurez-vous qu'une adresse IP est assignée à au moins un port du périphérique et que des pings peuvent être envoyés à un serveur TFTP.
2. Assurez-vous que le fichier à télécharger est enregistré dans le serveur TFTP (le fichier `rfb`).
3. Tapez `show version` pour vérifier la version du logiciel installée sur le périphérique. Vous trouverez ci-dessous un exemple des informations qui

s'affichent :

```
console# sh ver
```

Version logiciel 1.0.0.42 (date 22-Juil-2004 heure 13:42:41)

Version amorçage 1.0.0.18 (date 01-Juin-2004 heure 15:12:20)

Version matériel 00.00.01 (date 01-Mai-2004 heure 12:12:20)

4. Tapez `copy tftp://{adresse tftp}/{nom de fichier} boot` pour copier l'image d'amorçage dans le périphérique. Vous trouverez ci-dessous un exemple des informations qui s'affichent :

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

Effacement du fichier... terminé.

!!

Copie : 2 739 187 octets copiés en 00:01:13 [hh:mm:ss]

5. Tapez la commande `reload`. Le message suivant s'affiche :

```
console# reload
```

Cette commande réinitialisera tout le système et vous déconnectera de la session

en cours. Êtes-vous certain de vouloir continuer (y/n) [n] ?

6. Tapez `y`.

Le périphérique redémarre.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Glossaire

Guide d'utilisation du système Dell™ PowerConnect™ 5324

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [L](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#)

Ce glossaire contient des mots-clés techniques.

A

Adresse IP

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 qui permet d'identifier chaque noeud du réseau.

Agrégation de liaisons

Optimise l'utilisation des ports en reliant des ports de façon à former un faisceau unique (groupes agrégés).

Apprentissage de l'adresse MAC

L'apprentissage de l'adresse MAC se fait via un pont d'apprentissage où l'adresse MAC source des paquets est enregistrée. Les paquets destinés à cette adresse sont transmis uniquement à l'interface du pont où se situe l'adresse. Les paquets adressés à des adresses inconnues sont transmis à chaque interface de pont. L'apprentissage de l'adresse MAC réduit le trafic sur les LAN rattachés.

ARP

Protocole de résolution d'adresses. Protocole TCP/IP qui convertit les adresses IP en adresses physiques.

ASIC

Circuit intégré dédié à une application. Puce personnalisée conçue pour une application spécifique.

Attributions de bande passante

Quantité de bande passante attribuée à une application, un utilisateur et/ou une interface spécifiques.

Au mieux

Le trafic est assigné à la file d'attente de priorité la plus basse et la livraison des paquets n'est pas garantie.

B

Bande passante

La bande passante désigne la quantité de données pouvant être transmises au cours d'une période déterminée. Pour les périphériques numériques, la bande passante est définie en bps (bits par seconde) ou en octets par seconde.

Baud

Nombre d'éléments de signalisation transmis chaque seconde.

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 l'amorce d'un périphérique.

BPDU

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 périphérique avec la configuration Spanning Tree. Les paquets BPDU contiennent des informations sur les ports, les adresses, les priorités et les coûts de transmission.

C

CDB

Base de données de configuration. Fichier contenant des informations relatives à la configuration du périphérique.

Classe de service

Classe de service (CdS). La classe de service est le schéma de priorité 802.1p. La CdS fournit une méthode de marquage de paquets avec des informations de priorité. Une valeur de CdS située entre 0 et 7 est ajoutée à l'en-tête de couche II des paquets, zéro étant la priorité la plus basse et sept la priorité la plus élevée.

CLI

Interface de ligne de commande. Ensemble de commandes en ligne utilisées pour configurer le système. Pour plus d'informations sur l'utilisation de la CLI, reportez-vous à la section Utilisation de la 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

Filtre et transmet les paquets entre les segments de réseau local. Les commutateurs prennent en charge tous les types de protocoles par paquets.

Configuration de démarrage

Conserve la configuration exacte du périphérique lors de sa mise hors tension ou de son redémarrage.

Contre-pression

Mécanisme utilisé en mode Semi-duplex et permettant à un port de ne pas recevoir de message.

Contrôle de flux

Permet aux périphériques fonctionnant à une vitesse inférieure de communiquer avec des périphériques fonctionnant à une vitesse supérieure, c'est-à-dire que ces derniers n'envoient pas de paquets de données.

Couche 2

Couche de liaison de données ou couche MAC. Contient l'adresse physique d'une station serveur ou client. Le traitement de couche 2 est plus rapide que le traitement de couche 3 car il y a moins d'informations à traiter.

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

Unité centrale (UC). 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 transmission de paquets à tous les ports d'un réseau.

Domaine

Groupe d'ordinateurs et de périphériques d'un réseau possédant des règles et des procédures communes.

Domaine de diffusion

Ensemble de tous les dispositifs qui reçoivent des trames de diffusion provenant de n'importe quel des dispositifs faisant partie de cet ensemble. Les domaines de diffusion sont délimités par des routeurs parce que ces derniers ne réacheminent pas de trames de diffusion.

DSCP

DiffServe Code Point (DSCP). Le DSCP fournit une méthode de marquage de paquets IP avec des 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

La norme Ethernet suit la directive IEEE 802.3. Ethernet est la norme LAN la plus utilisée. Prend en charge les transferts de données à 10, 100 ou 1000 Mbps.

EWS

Web Server intégré. Permet la gestion du périphérique via un navigateur Web standard. Les Web Server 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 périphérique. Le fichier de sauvegarde est mis à jour lors de la copie du fichier de configuration d'exécution ou du fichier de démarrage dans le fichier de sauvegarde.

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 hors tension ou au redémarrage du périphérique, toutes les commandes stockées dans le fichier de configuration d'exécution sont perdues.

Fichier image

Des images du système sont enregistrées dans deux secteurs de mémoire FLASH appelés images (Image 1 et Image 2). L'image active stocke la copie active pendant que l'autre image stocke une deuxième copie.

FIFO

First In First Out (Premier entré premier sorti). Processus de mise en file d'attente où le premier paquet de la file d'attente est le premier paquet sortant.

Flapping

Le flapping 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 la perte du trafic.

Fond de panier

Bus principal transportant des informations dans le périphérique.

Fragment

Paquets Ethernet inférieurs à 576 bits.

G

Gigabit Ethernet

Le Gigabit Ethernet effectue des transmissions à 1000 Mbps et est compatible avec les normes Ethernet 10/100 Mbps.

H

HOL

Head of Line (Tête de ligne). Les paquets sont mis en file d'attente. Les paquets en tête de file sont transmis avant les paquets en fin de ligne.

Hôte

Ordinateur qui agit comme une source d'informations ou de services pour les autres ordinateurs.

HTTP

Protocole de transfert hypertexte. Transmet des documents HTML entre les serveurs et les clients sur Internet.

I

IC

Circuit intégré. Les circuits intégrés sont de petits dispositifs électroniques composés de matériaux semiconducteurs.

ICMP

Protocole de contrôle des messages sur Internet. Permet à un hôte passerelle ou de destination de communiquer avec un hôte source, pour reporter une erreur de traitement, par exemple.

IEEE

Institute of Electrical and Electronics Engineers. 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 MAC pour empêcher la formation de boucles.

IEEE 802.1p

Accorde la priorité au trafic du 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

Extrait 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 transmet au port approprié.

IPX

Internetwork Packet Exchange (Échange de paquets entre réseaux). Transmet des communications sans connexion.

L

LAG

Link Aggregated Group (Groupe de liaisons agrégées). Agrège des ports ou des VLAN dans un seul port ou VLAN virtuel.

Pour plus d'informations sur les LAG, reportez-vous à la section **Définition de l'appartenance à un LAG**.

LAN

Local Area Network (Réseau local). Réseau compris dans une pièce, un bâtiment, un campus ou toute autre zone géographique délimitée.

M

Masque à caractères génériques

Indique les bits de l'adresse IP à utiliser et les bits à ignorer. Un masque à caractères génériques 255.255.255.255 indique 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 bits sont ignorés.

Masque de sous-réseau

Utilisé pour 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 avec plus de sécurité. MD5 vérifie l'intégrité de la communication et identifie son origine.

MDI

Media Dependent Interface (Interface dépendante du média). Câble utilisé pour les stations terminales.

MDIX

Media Dependent Interface with Crossover (Interface croisée dépendante du média). Câble utilisé pour les concentrateurs et les commutateurs.

MIB

Base de données MIB. Les MIB contiennent des informations décrivant certains aspects spécifiques des composants du réseau.

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 jusqu'à un port de contrôle.

Pour plus d'informations sur la mise en miroir des ports, reportez-vous à la section **Définition des sessions de mise en miroir des ports**.

Mode d'accès

Indique la méthode d'accès au système accordée à l'utilisateur.

Mode Duplex

Permet la transmission et la réception de données simultanées. Il existe deux sortes de modes Duplex :

- 1 **Mode Duplex intégral** — Permet une communication binaire synchrone, avec un téléphone par exemple. Les deux parties peuvent transmettre des informations au même moment.
- 1 **Mode Semi-duplex** — Permet une communication asynchrone, avec un talkie-walkie par exemple. Une seule partie à la fois peut transmettre des informations.

Monodiffusion

Type de routage qui transmet un seul paquet à un seul utilisateur.

Multidiffusion

Transmet des copies d'un paquet unique à plusieurs ports.

N

Négociation automatique

Permet aux ports Ethernet 10/100 Mbps ou 10/100/1000 Mbps d'établir les fonctions suivantes :

- 1 Mode Duplex/Semi-duplex
- 1 Contrôle de flux
- 1 Vitesse

NMS

Système de gestion de réseau. Interface qui fournit une méthode de gestion du système.

Nœud

Point d'extrémité d'une connexion réseau ou jonction de plusieurs lignes dans un réseau. Les noeuds peuvent être les éléments suivants :

- 1 Processeurs

- 1 Contrôleurs
- 1 Stations de travail

Numéro d'inventaire

Indique la référence attribuée au périphérique par l'utilisateur.

O

OID

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.

P

Paquets

Blocs d'informations permettant la transmission dans des systèmes à commutation de paquets.

PDU

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 si une adresse IP spécifique est disponible. Un paquet est envoyé à une autre adresse IP et attend une réponse.

Pont

Périphérique qui relie deux réseaux. Les ponts dépendent du matériel et sont indépendants du protocole. Les ponts agissent au niveau des couches 1 et 2.

Port

Les ports physiques offrent des composants de connexion qui permettent aux microprocesseurs de communiquer avec des équipements périphériques.

Port d'entrée

Port sur lequel le trafic du réseau est reçu.

Port combo

Port logique unique avec deux connexions physiques : une connexion RJ-45 et une connexion SFP.

Ports de sortie

Ports à partir desquels le trafic du réseau est transmis.

Profils d'accès

Permettent aux gestionnaires de réseau de définir des profils et des règles d'accès au périphérique. L'accès aux fonctions de gestion peut être limité à un groupe d'utilisateurs, défini par les critères suivants :

- 1 Interfaces d'entrée
- 1 Adresse IP source et/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 qui définissent la façon dont les périphériques échangent des informations sur les réseaux.

Protocole GARP

Protocole d'enregistrement générique GARP. Enregistre les stations clientes dans un domaine de multidiffusion.

Protocole GVRP

Protocole d'enregistrement VLAN GARP. Enregistre les stations clientes dans un VLAN.

Protocole Spanning Tree

Empêche la formation de boucles dans le trafic réseau. Le STP (protocole Spanning Tree) fournit une topographie en arborescence de la présentation des ponts. Le protocole STP fournit un chemin unique entre les stations terminales sur un réseau et élimine ainsi la formation de boucles.

Q

QoS

Qualité de service. La QoS permet aux gestionnaires de réseau de choisir le trafic de réseau et de déterminer la façon dont il sera transmis en fonction de priorités, de types d'applications et d'adresses source et de destination.

R

RADIUS

Service d'authentification distant 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 de réseau à récupérer à partir d'une seule station de travail.

Routeur

Périphérique relié à des réseaux séparés. Les routeurs transmettent les paquets entre plusieurs réseaux. Les routeurs fonctionnent au niveau de la couche 3.

RSTP

Protocole Rapid Spanning Tree. 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 qui fournit des services aux autres ordinateurs sur un réseau. Ces services sont notamment le stockage de fichiers et l'accès aux applications.

SNMP

Simple Network Management Protocol (Protocole de gestion de réseau simple). Gère les réseaux locaux. Un logiciel basé sur SNMP communique avec des périphériques réseau et des agents SNMP intégrés. Les agents SNMP collectent des informations relatives à l'état du périphérique et à l'activité du réseau et renvoient ces informations vers une station de travail.

SNTP

Simple Network Time Protocol (Protocole de temps de réseau simple). Le protocole SNTP assure une synchronisation de l'heure de l'horloge du commutateur réseau avec une précision d'une milliseconde.

SoC

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

Sous-réseau. Les sous-réseaux sont des portions de réseau qui partagent un composant d'adresse commun. Dans les réseaux TCP/IP, les périphériques qui partagent un préfixe font partie du même sous-réseau. Par exemple, tous les périphériques avec un préfixe 157.100.100.100 font partie du même sous-réseau.

SSH

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.

Système terminal

Périphérique de l'utilisateur final sur un réseau.

T

TCP/IP

Transmissions Control Protocol (Protocole de contrôle de transmission). 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

Protocole d'émulation de terminal. Permet aux utilisateurs d'un système de se connecter à des ressources de réseaux distants et de les utiliser.

Tempête de diffusion

Quantité excessive de messages de diffusion transmis simultanément sur un réseau à travers un seul port. Les réponses aux messages transmises sont chargées sur le réseau, ce qui se traduit par une surcharge des ressources réseau ou par un dépassement de délai du réseau.

Pour plus d'informations sur les tempêtes de diffusion, reportez-vous à la section [«Définition des paramètres des LAG»](#).

TFTP

Trivial File Transfer Protocol (Protocole de transfert de fichiers simple). Utilise le protocole UDP (protocole de datagramme utilisateur) sans fonctions de sécurité pour transférer des fichiers.

Trames

Paquets contenant les informations d'en-tête et de queue de bande requises par le support physique.

Trames Jumbo

Permettent de transporter les données identiques sur un nombre réduit de trames. Les trames Jumbo permettent d'éviter la surcharge, de réduire le temps de traitement et de diminuer les interruptions.

U

UDP

User Data Protocol (Protocole de datagramme utilisateur). Transmet les paquets mais ne garantit pas leur livraison.

V

Version d'amorce

Version de l'amorce.

Vitesse de port

Désigne la vitesse du port. Les différentes vitesses de port sont les suivantes :

- 1 Ethernet 10 Mbps
- 1 Fast Ethernet 100 Mbps
- 1 Gigabit Ethernet 1000 Mbps

VLAN

Virtual Local Area Networks (Réseaux locaux virtuels). Sous-groupes logiques d'un LAN (réseau local) créés par le biais d'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

Réseaux étendus. Réseaux couvrant une vaste zone géographique.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Description matérielle

Guide d'utilisation du système Dell™ PowerConnect™ 5324

- [Configurations des ports du périphérique](#)
- [Dimensions](#)
- [Signification des DEL](#)
- [Composants matériels](#)

Configurations des ports du périphérique

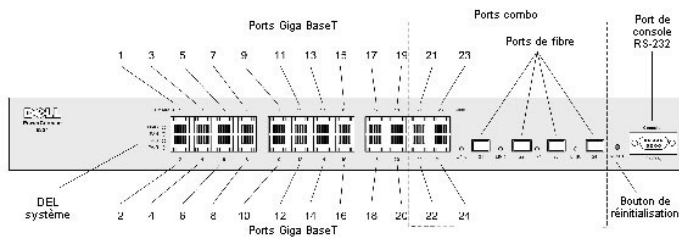
Description des ports du panneau avant du PowerConnect 5324

Le périphérique PowerConnect 5324 est configuré avec les ports suivants :

- 1 24 ports en cuivre — Ports RJ-45 utilisés comme des ports Gigabit Ethernet 10/100/1000 BaseT
- 1 4 ports de fibre — Utilisés comme des ports Gigabit
- 1 Port de terminal — Port de console RS-232

La figure ci-dessous illustre le panneau avant du PowerConnect 5324.

Figure 2-3. Panneau avant du PowerConnect 5324



Les ports 1 à 24 du panneau avant sont des ports RJ-45 en cuivre utilisés comme des ports 10/100/1000 Mbps qui prennent en charge les modes Semi-duplex et Duplex intégral. Quatre ports de fibre SFP (21 à 24) sont utilisés comme des ports combo. Les ports combo sont des ports simples avec deux connexions physiques. Une seule connexion physique peut être activée à la fois, donc soit les ports en cuivre, soit les ports en fibre 21 à 24. Les ports de la première rangée sont numérotés de 1 à 23 (chiffres impairs) et ceux de la deuxième rangée sont numérotés de 2 à 24 (chiffres pairs).

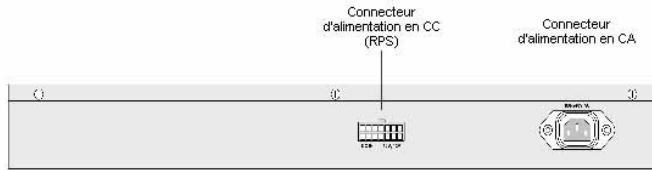
Le panneau avant contient également un port de console RS-232, toutes les DEL du périphérique et un bouton de réinitialisation utilisé pour réinitialiser manuellement le périphérique.

Le périphérique détecte automatiquement si le câble connecté à un port RJ-45 est croisé ou direct et fonctionne dans les deux cas.

Description des ports du panneau arrière du PowerConnect

Le panneau arrière du périphérique contient les connecteurs d'alimentation, comme illustré à la [Figure 2-4](#).

Figure 2-4. Panneau arrière du périphérique



Le panneau arrière du périphérique contient deux connecteurs d'alimentation. Le connecteur d'alimentation en CA peut être relié à des sources d'alimentation en 110 V ou 220 V.

Le connecteur d'alimentation en CC doit être relié à une alimentation redondante (RPS) pour être activé automatiquement en cas de coupure de courant CC.

Ports du périphérique

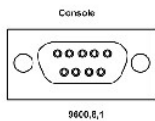
Ports SFP

Le port SFP (à faible encombrement) est un émetteur-récepteur optique remplaçable à chaud haute vitesse et compact, utilisé comme un port 1000Base-SX ou LX.

Port de console RS-232

Connecteur DB-9 pour une connexion série, utilisé pour le débogage, le téléchargement du logiciel, etc. Le débit par défaut est 9600 bps. Le débit peut être configuré entre 2400 bps et 38 400 bps.

Figure 2-5. Port de console



Ports combo

Un port combo est un port logique simple avec deux connexions physiques :

- 1 Une connexion RJ-45 pour le câblage en cuivre des paires torsadées
- 1 Une connexion SFP pour différents modules à fibres

Une seule connexion physique de port combo peut être utilisée en même temps. Les fonctions et les commandes de port disponibles dépendent de la connexion physique utilisée.

Le système détecte automatiquement le support utilisé sur un port combo et utilise cette information pour toutes les opérations et interfaces de commande.

Lorsque vous avez un port RJ-45 et un port SFP et qu'un connecteur est inséré dans le port SFP, c'est le port SFP qui est activé, à moins que le connecteur en cuivre du port Base-T portant le même numéro soit inséré et possède une liaison.

Le système peut basculer du port RJ-45 au port SFP (et inversement) sans redémarrage ni réinitialisation du système.

Dimensions

Les dimensions du périphérique sont les suivantes :

- 1 Hauteur — 44 mm (1,73 pouce)
 - 1 Largeur — 440 mm (17,32 pouces)
 - 1 Profondeur — 255 mm (10,03 pouces)
-

Signification des DEL

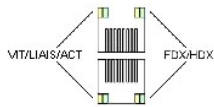
Le panneau avant comporte des diodes électro-luminescentes (DEL) qui indiquent l'état des liaisons, des blocs d'alimentation, des ventilateurs et fournissent des diagnostics sur le système.

DEL des ports

DEL des ports 10/100/1000 Base-T

Chaque port 10/100/1000 Base-T possède deux DEL. La DEL de gauche donne des indications sur la vitesse/liaison/activité et la DEL de droite donne des indications sur le mode Duplex.

Figure 2-6. DEL des ports RJ-45 en cuivre 10/100/1000 BaseT



Les indications des DEL de port RJ-45 sont expliquées dans le tableau suivant :

Tableau 2-1. Indications des DEL de port RJ-45 en cuivre 10/100/1000BaseT

DEL	Couleur	Description
DEL de gauche	Vert fixe	Le port est connecté à 1000 Mbps.
	Vert clignotant	Le port transmet ou reçoit des données à 1000 Mbps.
	Orange fixe	Le port est connecté à 10 ou 100 Mbps.
	Orange clignotant	Le port transmet ou reçoit des données à 10 ou 100 Mbps.
	ÉTEINT	Le port fonctionne en mode Semi-duplex.

DEL SFP

Les ports SFP possèdent chacun une DEL portant la marque LNK.

Figure 2-7.



DEL de port SFP

Les indications des DEL de port SFP sont expliquées dans le tableau suivant :

Tableau 2-2. Indications des DEL de port SFP

DEL	Couleur	Description
SFP	Vert fixe	Le port est activé.
	Vert clignotant	Le port transmet ou reçoit des données.
	ÉTEINT	Le port est désactivé.

Lorsque le port SFP est connecté, la DEL Duplex du port combo en cuivre correspondant s'allume en vert.

DEL système

Les DEL système, situées sur le côté gauche du panneau avant, indiquent l'état des blocs d'alimentation, des ventilateurs, des conditions de température et fournissent des diagnostics. La [Figure 2-8](#) illustre les DEL système.

Figure 2-8. DEL système



Le tableau suivant décrit les indications des DEL système.

Tableau 2-3. Indications des DEL système

DEL	Couleur	Description
Diagnostics (DIAG)	Vert clignotant	Le système exécute un test de diagnostic.
	Vert fixe	Le système a réussi le test de diagnostic.
	Rouge fixe	Le système n'a pas réussi le test de diagnostic.
Ventilateur (FAN)	Vert fixe	Les ventilateurs du périphérique fonctionnent normalement.
	Rouge fixe	Un ou plusieurs ventilateurs ne fonctionnent pas.
Alimentation redondante (RPS)	Vert fixe	L'alimentation redondante fonctionne actuellement.
	Rouge fixe	L'alimentation redondante ne fonctionne pas.
	ÉTEINT	L'alimentation redondante ne fonctionne pas actuellement.
Bloc d'alimentation principal (PWR)	Vert fixe	Le bloc d'alimentation principal fonctionne normalement.
	ÉTEINT	Le bloc d'alimentation principal ne fonctionne pas actuellement.
	Rouge	Le bloc d'alimentation principal est en panne.

Composants matériels

Blocs d'alimentation

Le périphérique possède une unité d'alimentation interne (unité CA) et un connecteur permettant de relier le périphérique à une unité d'alimentation externe (unité CC). L'unité externe permet la redondance de l'alimentation et est appelée unité RPS. Pour alimenter le périphérique, un seul bloc d'alimentation est nécessaire. Le fonctionnement avec les deux unités d'alimentation est contrôlé via le partage de charge.

Le partage de charge consiste à répartir les exigences d'alimentation du périphérique entre les deux blocs d'alimentation. En cas de coupure d'électricité sur l'un des deux blocs d'alimentation, l'autre continue automatiquement à fournir de l'électricité au périphérique.

Les DEL d'alimentation donnent des indications sur l'état du bloc d'alimentation. Pour plus d'informations sur les DEL, reportez-vous à la section [«Signification des DEL»](#).

Bloc d'alimentation en CA

Le bloc d'alimentation en CA convertit le 220/110 VCA 50/60 Hz standard en 5 VCC à 5 A et 12 VCC à 3 A. L'unité détecte automatiquement la valeur nominale de tension disponible (110 ou 220 V) et aucun paramétrage n'est nécessaire.

Le bloc d'alimentation en CA utilise un connecteur CA 220/110 V standard. Sa DEL se situe sur le panneau avant et indique si l'unité en CA est connectée.

Bloc d'alimentation en CC

Un bloc d'alimentation en CC externe est utilisé comme unité d'alimentation redondante. Le fonctionnement est possible avec l'alimentation fournie depuis cette unité uniquement. Un connecteur de type RPS600 est utilisé. Aucune configuration n'est requise. Sa DEL se situe sur le panneau avant et indique si l'unité en CC est connectée.

Lorsque le périphérique est connecté à une source d'alimentation différente, la probabilité d'avoir une panne en cas de coupure d'électricité diminue.

Bouton de réinitialisation

Le bouton de réinitialisation situé sur le panneau avant permet de réinitialiser manuellement le périphérique.

Système de ventilation

Le périphérique utilise un système de ventilateurs pour le refroidissement. L'état opérationnel des ventilateurs peut être contrôlé grâce aux indications des DEL. Pour plus d'informations, reportez-vous à la section [«Signification des DEL»](#).

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Installation du périphérique PowerConnect

Guide d'utilisation du système Dell™ PowerConnect™ 5324

- [Précautions d'installation](#)
- [Exigences du site](#)
- [Déballage](#)
- [Montage du périphérique](#)
- [Connexion du périphérique](#)
- [Connexions des ports, câbles et informations sur le brochage](#)
- [Paramètres par défaut des ports](#)

Cette section contient des informations sur le déballage du périphérique, son emplacement, son installation et le raccordement des câbles.

Précautions d'installation

PRÉCAUTION Avant d'exécuter toute procédure, lisez et suivez les consignes de sécurité du Guide d'informations du système fourni dans la documentation Dell.

PRÉCAUTION Observez les points suivants avant d'effectuer les procédures de cette section :

- 1 Assurez-vous que le rack ou le placard où se situe le périphérique est correctement fixé afin d'éviter qu'il ne bouge ou ne tombe.
 - 1 Assurez-vous que les circuits d'alimentation électrique sont correctement mis à la terre.
 - 1 Observez et suivez les marquages de la maintenance. N'effectuez la maintenance d'un périphérique vous-même qu'en adhérant strictement aux explications fournies dans la documentation de votre système. Si vous ouvrez et retirez les panneaux dotés d'un symbole triangulaire illustré d'un éclair, vous risquez de vous faire électrocuter. Seuls les techniciens de service qualifiés sont habilités à manipuler ces composants.
 - 1 Assurez-vous que le câble d'alimentation, le câble d'extension et/ou la prise ne sont pas endommagés.
 - 1 Assurez-vous que le périphérique est à l'abri de l'eau.
 - 1 Assurez-vous que le périphérique est éloigné des radiateurs et/ou de toute autre source de chaleur.
 - 1 Assurez-vous que les grilles de refroidissement ne sont pas obstruées.
 - 1 N'introduisez pas de corps étranger dans le périphérique, vous risquez de provoquer un incendie ou de vous faire électrocuter.
 - 1 Utilisez le périphérique uniquement avec l'équipement homologué.
 - 1 Laissez le périphérique refroidir avant de retirer les panneaux ou de toucher l'équipement interne.
 - 1 Assurez-vous que le périphérique ne surcharge pas les circuits d'alimentation, le câblage et la protection contre les surintensités. Pour connaître la capacité des circuits d'alimentation, additionnez les valeurs nominales d'ampérage de tous les commutateurs installés sur le même circuit que le périphérique. Comparez le total obtenu avec la limite de valeur nominale du circuit.
 - 1 N'installez pas le périphérique dans un environnement où la température de fonctionnement pourrait dépasser 40° C (122° F).
 - 1 Assurez-vous que le flux d'air à l'avant, sur les côtés et à l'arrière du périphérique peut circuler librement.
-

Exigences du site

Le périphérique peut être monté dans un rack standard de 19 pouces ou bien installé sur une surface plane. Avant d'installer le périphérique, vérifiez que l'emplacement choisi répond aux exigences du site.

- 1 **Général** — Assurez-vous que le bloc d'alimentation est correctement installé.
- 1 **Alimentation** — Le périphérique est installé à moins d'1,5 m (5 pieds) d'une prise 220/110 VCA, 50/60 Hz mise à la terre et facilement accessible.
- 1 **Dégagement** — Il y a suffisamment d'espace devant pour que l'opérateur puisse y accéder. Assurez-vous de laisser de l'espace pour le câblage, les branchements électriques et la ventilation.
- 1 **Câblage** — Le chemin des câbles évite les sources de bruit électrique comme les émetteurs-transmetteurs radio, les amplificateurs de diffusion, les lignes d'alimentation et les platines de lumière fluorescente.
- 1 **Environnement** — La plage de températures de fonctionnement de l'unité se situe entre 0° et 40° C (32° et 104° F), avec une humidité relative de 10 à 90 %, sans condensation. Vérifiez que le boîtier de l'unité est à l'abri de l'eau et de l'humidité.

Déballage


Contenu de l'emballage


Pendant le déballage de l'unité, assurez-vous que les articles suivants sont inclus :

- 1 Le périphérique
- 1 Un câble d'alimentation en CA
- 1 Un câble de jonction RS-232
- 1 Des tampons en caoutchouc autocollants
- 1 Un kit de montage pour une installation en rack
- 1 Le CD de documentation

Déballage du périphérique

Pour déballer le périphérique :

 **REMARQUE** : Avant de déballer le périphérique, inspectez l'emballage et signalez immédiatement tout signe de dommage.

 **REMARQUE** : Nous ne fournissons pas de bracelet ESD ; il est cependant recommandé d'en porter un pour effectuer la procédure suivante.

1. Placez le conteneur sur une surface plane et propre et coupez toutes les sangles.
2. Ouvrez le conteneur ou retirez la partie supérieure du conteneur.
3. Retirez soigneusement le périphérique du conteneur et placez-le sur une surface stable et propre.
4. Retirez tout le matériel d'emballage.
5. Inspectez le périphérique. Signalez immédiatement tout signe de dommage.

Montage du périphérique

Présentation

Les connecteurs d'alimentation du périphérique se situent sur le panneau arrière. Si vous le pouvez, utilisez une alimentation redondante CC (UPS). Le connecteur CC UPS se situe sur le panneau arrière du périphérique.

Montage du système

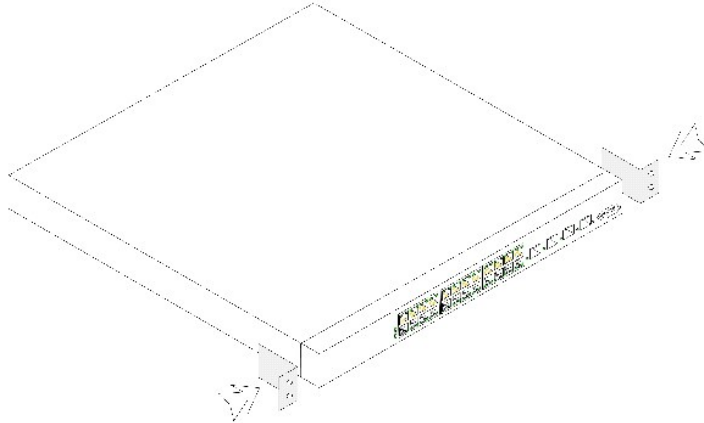
Installation du rack du périphérique

 **PRÉCAUTION** : Débranchez tous les câbles de l'unité avant de monter le périphérique dans un rack ou une armoire.

 **PRÉCAUTION** : Si vous montez plusieurs périphériques dans un rack, faites-le en commençant par le bas.

1. Placez la languette métallique de montage sur rack sur un côté du périphérique en vous assurant que les trous de montage sont alignés sur les trous de montage de la languette métallique de montage sur rack. La [Figure 3-9](#) illustre le montage des languettes métalliques.

Figure 3-9. Languettes métalliques de montage sur rack de connexion



2. Insérez les vis fournies dans les trous de montage du rack et serrez-les à l'aide d'un tournevis.
3. Répétez ce processus pour la languette métallique de montage sur rack à installer sur l'autre côté du périphérique.
4. Insérez l'unité dans le rack de 19 pouces en vous assurant que les trous de montage sur rack du périphérique sont alignés sur le trou de montage du rack.
5. Fixez l'unité au rack au moyen des vis de rack (non fournies). Serrez la paire inférieure de vis avant la paire supérieure de vis. Le poids de l'unité sera réparti uniformément pendant l'installation. Assurez-vous que les trous de ventilation ne sont pas obstrués.

Installation du périphérique sans rack

Le périphérique doit être installé sur une surface plane s'il n'est pas installé dans un rack. La surface doit pouvoir soutenir le poids du périphérique et de ses câbles.

1. Installez les pieds en caoutchouc fournis avec le périphérique.
2. Posez le périphérique sur une surface plane, en laissant 5,08 cm (2 pouces) de part et d'autre et 12,7 cm (5 pouces) derrière.
3. Assurez-vous que le périphérique est bien aéré.

Connexion du périphérique

Pour configurer le périphérique, vous devez le relier à un terminal.

Connexion d'un périphérique à un terminal

Le périphérique contient un port de console qui permet une connexion à un terminal de bureau exécutant un logiciel d'émulation de terminal destiné à la surveillance et à la configuration du périphérique. Le connecteur de port console est en fait un connecteur DB-9 mâle, qui sert de connecteur d'équipement de terminal de données (DTE).

Pour utiliser le port console, vous aurez besoin :

- 1 Un terminal compatible VT100 ou un système de bureau ou portable avec un port série et un logiciel d'émulation de terminal VT100.
- 1 Un câble simulateur de modem RS-232 avec un connecteur DB-9 femelle pour le port de console et le connecteur correspondant pour le terminal.

Pour connecter un terminal au port console du périphérique :

1. Raccordez un câble de jonction RS-232 au terminal fonctionnant sous un logiciel d'émulation de terminal VT100.
2. Assurez-vous que le logiciel d'émulation de terminal est configuré de la façon suivante :
 - a. Sélectionnez le port série approprié (port série 1 ou 2) à relier à la console.
 - b. Configurez le taux de transfert des données à 9600 bauds.

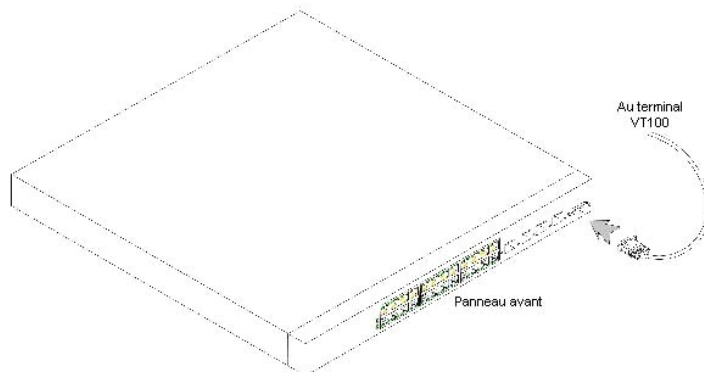
- c. Configurez le format de données à 8 bits de données, 1 bit d'arrêt et aucune parité.
- d. Paramétrez le contrôle du flux sur none (aucun).
- e. Sous **Propriétés**, sélectionnez le mode **VT100 pour émulation**.
- f. Sélectionnez **Touches du terminal** pour les **touches de fonction, de direction et Ctrl**. Assurez-vous que le paramètre est configuré sur **Touches du terminal** (et non sur **Touches Windows**).

➔ **AVIS** : Lorsque vous utilisez HyperTerminal avec le système d'exploitation Microsoft® Windows 2000, assurez-vous d'avoir préalablement installé Windows® 2000 Service Pack 2 ou une version plus récente. Lorsque le Service Pack 2 de Windows 2000 est installé, les touches de direction fonctionnent correctement avec l'émulation VT100 d'HyperTerminal. Rendez-vous à l'adresse www.microsoft.com pour obtenir des informations sur les service packs de Windows 2000.

3. Reliez le connecteur femelle du câble simulateur de modem RS-232 directement au port de console du périphérique et serrez les vis captives.

Le port de console du périphérique se situe sur le panneau avant.

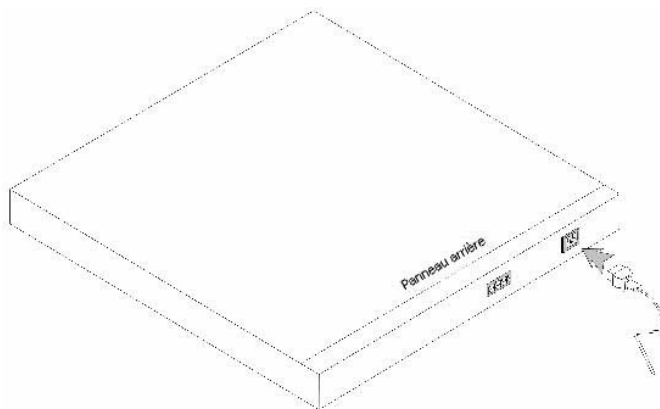
Figure 3-10. Connexion au port de console du PowerConnect 5324



Connexion d'un périphérique sur un bloc d'alimentation

1. Reliez un câble d'alimentation standard d'1,5 m (5 pieds) correctement mis à la terre au connecteur CA situé sur le panneau arrière.
2. Connectez le câble d'alimentation à une prise de courant CA mise à la terre.

Figure 3-11. Connexion au connecteur d'alimentation du périphérique



Vérifiez que le périphérique est connecté et fonctionne correctement en examinant les DEL du panneau avant.

Connexions des ports, câbles et informations sur le brochage

Cette section décrit les interfaces physiques du périphérique et contient des informations sur les connexions des ports. Les types de connecteurs, les ports et les câbles sont répertoriés dans Ports, Connecteurs et Câbles. Les diagnostics pris en charge sont Copper Cable (câble cuivre) et Optical Transceiver (émetteur-récepteur optique).

Connexions RJ-45 pour les ports 10/100/1000BaseT

Les ports 10/100/1000BaseT sont des ports à paire torsadée en cuivre.

Pour établir une liaison pour les ports à paire torsadée, la paire Tx d'une extrémité de câble doit être connectée à la paire Rx de l'autre extrémité du câble et inversement. Si le câblage est fait de telle façon que la paire Tx d'une extrémité est reliée à la paire Tx de l'autre extrémité (ou Rx à Rx), la liaison ne peut pas s'établir.

Pour connecter les ports du périphérique à leurs homologues en réseau, utilisez des câbles directs entre le périphérique et une station et des câbles simulateurs de modem entre les périphériques de transmission (commutateur ou concentrateur). Les câbles directs et simulateurs de modem font partie de la catégorie 5.

Lorsqu'un port est connecté, sa DEL de liaison s'allume.

Tableau 3-4. Ports, Connecteurs et Câbles

Connecteur	Port/Interface	Câble
RJ-45	Port 10/100/1000BaseT	Cat. 5

Les numéros de broche RJ-45 affectés aux ports 10/100/1000BaseT sont détaillés dans le tableau ci-dessous.

Tableau 3-5. Numéros de broche RJ-45 affectés aux ports Ethernet 10/100/1000BaseT

N° de broche	Fonction
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx 3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

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 du flux sur des ports de commutation 10/100/1000BaseT. Par défaut, la négociation automatique est activée sur chaque port.

La négociation automatique est un mécanisme établi entre deux partenaires de liaison qui permet à un port de publier sa vitesse de transmission, son mode Duplex et ses capacités de contrôle de flux (le contrôle du flux par défaut est désactivé) à son partenaire. Les deux ports fonctionnent alors à leur plus haut dénominateur commun.

Si vous connectez un NIC qui ne prend pas en charge la négociation automatique ou qui n'est pas configuré pour la négociation automatique, le port de commutation du périphérique et le NIC doivent être configurés manuellement à la même vitesse et en mode Duplex.

Si la station située à l'autre extrémité de la liaison tente une négociation automatique avec un port de périphérique 10/100/1000BaseT configuré en mode

Duplex intégral, la station tente de fonctionner en mode Semi-duplex.

MDI /MDIX

Le périphérique 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

Le périphérique prend en charge le contrôle du 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

Le périphérique 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 des ports de commutation

Le tableau ci-dessous répertorie les paramètres par défaut des ports.

Tableau 3-6. Paramètres par défaut des ports

Fonction	Paramètre par défaut
Vitesse et mode du port	Cuivre 10/100/1000BaseT : négociation automatique 100 duplex intégral
État de transfert du port	Activé
Marquage du port	Pas de marquage
Contrôle de flux	Désactivé (en entrée)
Contre-pression	Désactivée (en entrée)

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Présentation

Guide d'utilisation du système Dell™ PowerConnect™ 5324

- [PowerConnect 5324](#)
- [Fonctions](#)
- [Documentation CLI supplémentaire](#)

➡ **AVIS** : Avant toute chose, lisez les notes de mise à jour relatives à ce produit. Les notes de mise à jour peuvent être téléchargées du site Web support.dell.com.

Ce guide d'utilisation contient les informations nécessaires pour l'installation, la configuration et la maintenance du périphérique PowerConnect.

PowerConnect 5324

Le PowerConnect 5324 possède 24 ports Gigabit Ethernet. Il possède également quatre ports de fibre SFP qui sont des ports combo utilisés en remplacement des ports Ethernet 21 à 24. Les ports combo sont des ports simples avec deux connexions physiques. Lorsqu'une connexion est établie, l'autre est désactivée.

La [Figure 1-1](#) et la [Figure 1-2](#) illustrent les panneaux avant et arrière du PowerConnect 5324.

Figure 1-1. Panneau avant du PowerConnect 5324



Figure 1-2. Panneau arrière du PowerConnect 5324



Fonctions

Cette section décrit les fonctions du périphérique configurées par l'utilisateur. Pour obtenir une liste complète de toutes les fonctions du périphérique mises à jour, reportez-vous aux Notes de mise à jour de la dernière version du logiciel.

Fonctions générales

Blocage en tête de ligne

Le blocage HOL (Tête de ligne) 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.

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.

Prise en charge des trames Jumbo

Les trames Jumbo permettent de transporter les données identiques sur un nombre réduit de trames. Elles permettent d'éviter la surcharge, de réduire le temps de traitement et de diminuer les interruptions.

Pour plus d'informations sur l'activation des trames Jumbo, reportez-vous à la section [«Définition des informations générales relatives au périphérique»](#).

Prise en charge MDI /MDIX

Le périphérique prend en charge la détection automatique entre les câbles croisés et les câbles directs.

Le câblage standard des stations terminales est MDI (Interface dépendante du média) et le câblage standard des concentrateurs et des commutateurs est MDIX (Interface croisée dépendante du média).

Pour plus d'informations sur la configuration de MDI/MDIX pour les ports ou groupes de liaisons agrégées (LAG), reportez-vous à la section [«Définition des paramètres des ports»](#) ou [«Définition des paramètres des LAG»](#).

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

L'option de contrôle du flux permet aux périphériques fonctionnant à une vitesse inférieure 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 plus d'informations sur la configuration du contrôle du flux pour les ports ou les LAG, reportez-vous à la section [«Définition des paramètres 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 au trafic.

Pour plus d'informations sur la configuration de la contre-pression pour les ports ou les LAG, reportez-vous à la section [«Définition des paramètres des ports»](#) ou [«Définition des paramètres des LAG»](#).

Fonctions de l'adresse MAC prises en charge

Prise en charge de la capacité de l'adresse MAC

Le périphérique prend en charge jusqu'à huit mille adresses MAC. Il réserve des adresses MAC spécifiques pour le système.

Apprentissage automatique des adresses MAC

Le périphérique permet l'apprentissage automatique des adresses MAC à partir de paquets entrants. Les adresses MAC sont enregistrées dans la table de pontage.

Expiration automatique des adresses MAC

Les adresses MAC qui ne transmettent pas de trafic pendant un temps déterminé expirent. Cela évite la surcharge de la table de pontage.

Pour plus d'informations sur la configuration de l'expiration des adresses MAC, reportez-vous à la section [«Configuration des tables d'adresses»](#).

Entrées MAC statiques

Les entrées MAC statiques définies par l'utilisateur sont enregistrées dans la **table de pontage**.

Pour plus d'informations, reportez-vous à la section [«Configuration des tables d'adresses»](#).

Commutation basée sur MAC sensible au VLAN

Les paquets provenant d'une adresse source inconnue sont envoyés au microprocesseur, où les adresses source sont ajoutées à la table du matériel. Les paquets adressés à ou en provenance de cette adresse sont transmis plus efficacement à l'aide de la table du matériel.

Prise en charge de la multidiffusion MAC

Le service de multidiffusion est un service de diffusion limitée, qui permet des connexions un seul émetteur/plusieurs récepteurs et plusieurs émetteurs/plusieurs récepteurs pour la distribution des informations. Le service de multidiffusion de couche 2 est un service où une trame est envoyée à une adresse de multidiffusion spécifique, à partir de laquelle des copies de la trame sont transmises aux ports concernés.

Pour plus d'informations, reportez-vous à la section [«Prise en charge du transfert multidiffusion»](#).

Fonctions de couche 2

Surveillance IGMP

La surveillance IGMP (Protocole d'appartenance à un groupe) examine le contenu des trames IGMP, lorsqu'elles sont transmises par le périphérique depuis les stations de travail vers un routeur multidiffusion en amont. À partir de la trame, le périphérique identifie les stations de travail configurées pour des sessions de multidiffusion et les routeurs multidiffusion qui envoient des trames de multidiffusion.

Pour plus d'informations, reportez-vous à 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, reportez-vous à la section [«Définition des sessions de mise en miroir des ports»](#).

Contrôle des tempêtes de diffusion

Le contrôle des tempêtes permet de limiter le nombre de trames de multidiffusion et de diffusion acceptées et transmises par le périphérique.

En cas de transmission de trames de couche 2, les trames de diffusion et de multidiffusion sont acheminées par inondation vers tous les ports du VLAN correspondant. Toute la bande passante est occupée et tous les noeuds connectés sur les ports sont chargés.

Pour plus d'informations, reportez-vous à la section [«Activation de la fonction de contrôle des tempêtes informatiques»](#).

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, reportez-vous à la section [«Configuration des VLAN»](#).

LAN virtuels (VLAN) basés sur les ports

Les VLAN basés sur les ports classifient les paquets entrants dans les VLAN basés sur leur port entrant.

Pour plus d'informations, reportez-vous à la section [«Définition des paramètres des ports VLAN»](#).

LAN virtuels (VLAN) basés sur le protocole IEEE802.1V

Les règles de classification des VLAN sont définies sur la base de l'identification du protocole de la couche Liaison de données (Couche 2). Les VLAN basés sur un protocole isolent le trafic de couche 2 pour différencier les protocoles de couche 3.

Pour plus d'informations, reportez-vous à la section [«Définition des groupes de protocoles 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. L'une des principales exigences de cette norme est la capacité à marquer des trames d'une balise de Classe de service (Cds) (0 à 7).

Prise en charge du protocole GVRP

Le protocole GVRP (Protocole d'enregistrement VLAN GARP) permet l'élagage du VLAN conformément à l'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 sous-jacente active. [«Fonctions du protocole Spanning Tree»](#).

Pour plus d'informations, reportez-vous à la section [«Configuration du protocole GVRP»](#).

Fonctions du protocole Spanning Tree

Protocole Spanning Tree (STP)

Le Spanning Tree respectant le 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, reportez-vous à la section [«Configuration du protocole Spanning Tree»](#).

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, reportez-vous à la section [«Définition des paramètres des ports STP»](#) ou [«Définition des paramètres des LAG STP»](#).

Spanning Tree rapide respectant le standard 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 (Protocole 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, reportez-vous à la section [«Configuration du protocole Rapid Spanning Tree»](#).

Agrégation des liaisons

Pour plus d'informations, reportez-vous à la section [«Agrégation des ports»](#).

Agrégation des liaisons

Un groupe de liaisons agrégées (LAG) peut contenir jusqu'à huit liaisons agrégées, chacune avec huit ports membres. Il présente les caractéristiques suivantes :

- 1 Une tolérance aux pannes dues à la rupture des liaisons physiques
- 1 Des connexions de bande passante supérieures
- 1 Une plus grande granularité de bande passante
- 1 Une connectivité de serveur à large bande passante

Le LAG est composé de ports ayant la même vitesse, configurés en mode Duplex intégral.

Pour plus d'informations, reportez-vous à la section [«Définition de l'appartenance à un 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 atteignable 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, reportez-vous à la section [«Définition des paramètres LACP»](#).

Fonctions de couche 3

Protocole ARP (Protocole de résolution d'adresses)

Le protocole ARP est un protocole TCP/IP qui convertit les adresses IP en adresses physiques. ARP détermine automatiquement les adresses MAC de prochain saut de périphériques de systèmes, y compris celles des systèmes finaux directement connectés. Les utilisateurs peuvent annuler et compléter ce protocole en définissant des entrées supplémentaires dans la table ARP.

Pour plus d'informations, reportez-vous à la section [«Adressage d'hôtes de domaine»](#).

TCP

Les connexions TCP (Protocole de contrôle de transmission) sont définies entre 2 ports par un échange de synchronisation initial. Les ports TCP sont identifiés par une adresse IP et un numéro de port sur 16 bits. Les flux d'octets sont divisés en paquets TCP, chacun portant un numéro de séquence.

Clients BootP et DHCP

Le protocole DHCP (Protocole de configuration dynamique d'hôtes) permet que des paramètres de configuration supplémentaires soient reçus d'un serveur réseau dès le démarrage du système. Le service DHCP est un processus évolutif. Le DHCP est une extension du BootP.

Pour plus d'informations sur le protocole DHCP, reportez-vous à la section [«Définition de paramètres d'interface IP DHCP»](#).

Fonctions de la qualité de service

Prise en charge de la classe de service 802.1p

La technique de signalisation IEEE 802.1p est une norme OSI de couche 2 relative au marquage et à la définition de priorités du trafic réseau au niveau de la sous-couche MAC/liaison de données. Le trafic 802.1p est classifié et envoyé à la 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). La norme 802.1p définit huit niveaux de priorité, similaires au champ binaire IP Precedence IP Header (En-tête IP de priorité IP).

Pour plus d'informations, reportez-vous à la section [«Configuration de la qualité de service»](#).

Fonctions de gestion du périphérique

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'interruption.

Pour plus d'informations sur les alarmes et les interruptions SNMP, reportez-vous à la section [«Définition des paramètres SNMP»](#).

SNMP version 1 et version 2

Protocole SNMP (Protocole de gestion de réseau simple) sur le protocole UDP/IP. Pour contrôler 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.

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. Le système contient un EWS (Serveur Web intégré), qui dessert des 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 du périphérique PowerConnect est enregistrée dans un fichier de configuration. Le fichier de configuration contient la configuration du périphérique dans le système et celle spécifique aux ports. Le système peut afficher les fichiers de configuration comme un ensemble de commandes CLI, enregistrées et manipulées comme des fichiers de texte.

Pour plus d'informations, reportez-vous à la section [«Gestion des fichiers»](#).

Protocole de transfert de fichiers trivial (TFTP)

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

Surveillance à distance

La surveillance à distance (RMON) est une extension du protocole SNMP, qui fournit des fonctions complètes de surveillance du trafic dans le 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, reportez-vous à la section [«Affichage des statistiques RMON»](#).

Interface de ligne de commande

La syntaxe et la sémantique de la CLI (Interface de ligne de commande) sont autant que possible conformes à la pratique de l'industrie. La CLI se compose d'éléments obligatoires et d'éléments facultatifs. L'interprète 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 sur Syslog, reportez-vous à la section [«Gestion des journaux»](#).

SNTP

Le protocole SNTP (Protocole de temps de réseau simple) assure une synchronisation de l'heure de l'horloge du périphérique réseau avec une précision d'une milliseconde. La synchronisation de l'heure se fait via un serveur réseau SNTP. Les sources de temps sont établies par des Stratoms. Les Stratoms 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, reportez-vous à la section [«Configuration des paramètres du SNMP»](#).

Traceroute

Traceroute permet de détecter des routes IP par où les paquets sont passés au cours du processus de transmission. L'utilitaire CLI Traceroute peut être exécuté en mode User-exec (EXEC utilisateur) ou en mode Privileged (EXEC privilégié).

Caractéristiques 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 (Protocole d'authentification extensible).

Pour plus d'informations, reportez-vous à la section [«Configuration de l'authentification basée sur le port»](#).

Prise en charge des ports verrouillés

Les ports verrouillés augmentent la sécurité du réseau en limitant l'accès à un port spécifique aux utilisateurs possédant des adresses MAC spécifiques. Ces adresses sont soit manuellement définies, soit apprises sur ce port. Lorsqu'une trame est vue 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 invoqué.

Pour plus d'informations, reportez-vous à la section [«Configuration de la sécurité de port»](#).

Client RADIUS

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

Pour plus d'informations, reportez-vous à la section [«Configuration de paramètres RADIUS globaux»](#).

SSH

Secure Shell (SSH) est un protocole qui fournit une connexion distante sécurisée à un périphérique. SSH version 1 est actuellement disponible. La fonction de serveur SSH permet à un client SSH d'établir une connexion cryptée et sécurisée avec un périphérique. 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 d'avoir un système de gestion centralisée des utilisateurs, tout en conservant le RADIUS et les autres processus d'authentification.

Pour plus d'informations, reportez-vous à la section [«Définition des paramètres TACACS+»](#).

Documentation CLI supplémentaire

Le Guide de référence CLI, disponible sur le CD de documentation, contient des informations sur les commandes CLI utilisées pour configurer le périphérique. Il fournit des informations sur la CLI : description, syntaxe, valeurs par défaut, consignes et exemples.

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Configuration de la qualité de service

Guide d'utilisation du système Dell™ PowerConnect™ 5324

- [Présentation de la qualité de service \(QoS\)](#)
- [Définition des paramètres globaux de QoS](#)

Cette section contient des informations relatives à la définition et à la configuration des paramètres de qualité de service (QoS). Pour ouvrir la page, cliquez sur **Home** → Quality of Service (Qualité de service) dans l'arborescence.

Présentation de la qualité de service (QoS)

La qualité de service (QoS) permet d'implémenter une QoS et une mise en file d'attente prioritaire dans un réseau. La QoS améliore le flux du trafic réseau grâce à l'utilisation de stratégies, de compteurs de trames et de contexte.

Certains types de trafic comme le trafic vocal, vidéo et en temps réel sont des exemples d'implémentations qui nécessitent une certaine QoS et qui peuvent posséder une file d'attente de priorité élevée, tandis que d'autres types de trafic possèdent une file d'attente de priorité inférieure. Le flux de trafic s'en trouve très amélioré en cas de forte demande.

La QoS est définie par les termes suivants :

- 1 Classification — Indique les champs de paquet qui correspondent à des valeurs spécifiques. Tous les paquets correspondant aux spécifications définies par l'utilisateur sont classés ensemble.
- 1 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 de paquet, telles que la priorité VLAN (VPT) et la valeur DSCP (DiffServ Code Point).

Informations de classification du marqueur VPT

Les marqueurs de priorité VLAN sont utilisés pour classer les paquets en les adressant à l'une des files d'attente de sortie. L'attribution de marqueurs de priorité VLAN aux files d'attente peut également être définie par l'utilisateur. Le tableau ci-dessous détaille les paramètres par défaut du VPT des files d'attente :

Tableau 9-92. Valeurs par défaut de la table d'adressage QoS à file d'attente

Valeur QoS	Valeurs des files d'attente de transfert
0	q2
1	q1 (Priorité la plus faible = Au mieux)
2	q1 (Priorité la plus faible = Au mieux)
3	q2
4	q3
5	q3
6	q4 (Priorité la plus élevée)
7	q4 (Priorité la plus élevée)

Les paquets qui arrivent sans marquage reçoivent un VPT par défaut, configuré en fonction du port. Le VPT affecté est utilisé pour adresser le paquet à la file d'attente de sortie et comme le VPT de sortie.

Les valeurs DSCP peuvent être adressées aux files d'attente de priorité. Le tableau ci-dessous contient l'adressage par défaut de valeurs DSCP aux valeurs des files d'attente de transfert :

Tableau 9-93. Valeurs par défaut de la table d'adressage DSCP à file d'attente

Valeur DSCP	Valeurs des files d'attente de transfert
-------------	--

0-7	q2 (Priorité la plus faible)
8-15	q1
16-23	q1
24-31	q2
32-39	q3
40-47	q3
48-55	q4
55-63	q4 (Priorité la plus élevée)

L'adressage DSCP est activé au niveau du système.

Services CdS

Une fois les paquets assignés à une file d'attente spécifique, des services CdS peuvent être affectés à une ou plusieurs files d'attente. Les files d'attente de sortie sont configurées avec un schéma de planification à l'aide de l'une des méthodes suivantes :

- 1 Strict Priority (Priorité stricte) — Garantit que les applications à durée de vie critique sont toujours transférées par voie accélérée. La priorité stricte permet de classer par ordre de priorité le trafic vital à durée de vie critique par rapport aux applications à durée de vie moins critique. Par exemple, avec une priorité stricte, le trafic voix sur IP est transmis avant le trafic FTP ou SMTP (messagerie électronique). Le trafic des files d'attente restantes est transmis une fois que la file d'attente de priorité stricte est vidée.
- 1 Weighted Round Robin (WRR) — Garantit qu'une seule application ne domine pas la capacité de transfert du périphérique. Weighted Round Robin (WRR) transfère les files d'attente entières selon un schéma de permutation circulaire (Round Robin). Les priorités des files d'attente sont définies par leur longueur. Plus la file d'attente est longue, plus sa priorité de transfert est élevée. Par exemple, si quatre files d'attente présentent une pondération de 1, 2, 3 et 4, les paquets dont la priorité de transfert est la plus élevée sont affectés à la file d'attente 4 et les paquets dont la priorité de transfert est la plus faible sont affectés à la file d'attente 1. Du fait que la priorité de transfert la plus élevée est affectée à la file d'attente 4, la permutation circulaire pondérée (WRR) traite le trafic ayant la priorité la plus élevée et assure que le trafic à faible priorité est transmis de façon satisfaisante.

Le schéma de planification est activé pour tout le système. Les files d'attente affectées à la stratégie de priorité stricte sont automatiquement affectées à la file d'attente dont la priorité est la plus élevée. Par défaut, toutes les valeurs sont définies en tant que priorité stricte. Lorsque le mode WRR est activé, la valeur de pondération par défaut est un. Les valeurs de pondération des files d'attente peuvent être affectées dans n'importe quel ordre à l'aide de WRR. Les valeurs WRR peuvent être affectées au niveau du système. Le trafic en mode «Au mieux» (Best Effort) est toujours affecté à la première file d'attente. Les valeurs WRR doivent être affectées de façon à ce que la file d'attente 1 reste en mode «Au mieux».

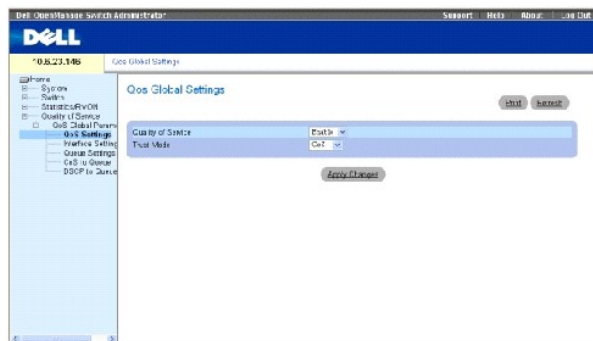
Définition des paramètres globaux de CdS

Les paramètres globaux de classe de service sont définis dans les pages CoS Global Parameter (Paramètres globaux CdS).

Configuration des paramètres globaux de QoS

La page QoS Global Settings (Paramétrages globaux de QoS) contient des champs permettant d'activer ou de désactiver la QoS. Vous pouvez également sélectionner le mode Trust (Confiance). Ce mode se base sur des champs prédéfinis dans le paquet pour déterminer la file d'attente de sortie. Pour ouvrir la page [QoS Settings](#) (Paramétrages de QoS), cliquez sur Quality of Service (Qualité de service) → CoS Global Parameters (Paramètres globaux de CdS) → CoS Settings (Paramétrages de CdS) dans l'arborescence.

Figure 9-130. QoS Settings (Paramétrages de QoS)




Quality of Service (Qualité de service) — Active ou désactive la gestion du trafic réseau à l'aide de la qualité de service.

Trust Mode (Mode Confiance) — Détermine les champs de paquet à utiliser pour la classification des paquets qui intègrent le périphérique. Lorsqu'aucune règle n'est définie, le trafic qui contient le champ de paquet prédéfini (CdS ou DSCP) est adressé en fonction de la table de modes Confiance appropriée. Le trafic ne contenant pas de champ de paquet prédéfini est adressé «au mieux». Les valeurs admises pour le champ Trust Mode sont les suivantes :

CoS (CdS) — Indique que l'affectation de la file d'attente de sortie est déterminée par le numéro de priorité VLAN IEEE802.1p (VPT) ou par le VPT par défaut affecté à un port.

DSCP — Indique que l'affectation de la file d'attente de sortie est déterminée par le champ DSCP.

 **REMARQUE** : La valeur Trust (Confiance) de l'interface remplace la valeur Trust globale.

Activation de la qualité de service :

1. Ouvrez la page [QoS Settings](#) (Paramétrages de QoS).
2. Sélectionnez **Enable** (Activer) dans le champ **CoS Mode** (Mode CdS).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La classe de service est activée sur le périphérique.

Activation du mode Confiance :

1. Ouvrez la page [QoS Settings](#) (Paramétrages de QoS).
2. Sélectionnez **Trust** dans le champ **Trust Mode** (Mode Confiance).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mode Confiance est activé sur le périphérique.

Activation du mode Confiance à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [QoS Settings](#) (Paramétrages QoS).

Tableau 9-94. Commandes CLI de paramétrage de la CdS

Commande CLI	Description
<code>qos trust [cos dscp]</code>	Configure le système en mode de base et l'état Confiance.
<code>no cos trust</code>	Rétablit l'état autre que Confiance.

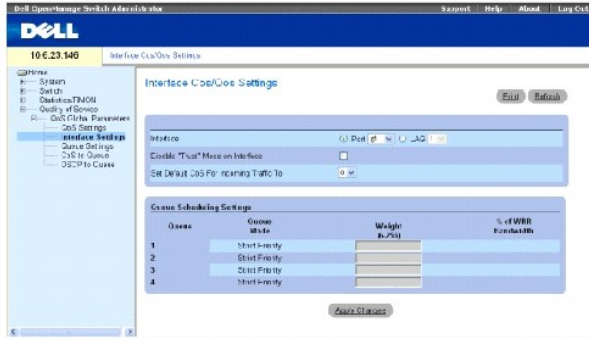
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# cos trust dscp
```

Définition des paramètres de l'interface QoS

La page [Interface Cos/QoS Settings](#) (Paramètres de l'interface CdS/QoS) contient des champs permettant de définir, au niveau de chaque interface, si le mode Trust sélectionné doit être activé. La priorité par défaut pour les paquets non marqués entrants est également sélectionnée dans la page [Interface Cos/QoS Settings](#) (Paramètres de l'interface CdS/QoS). Pour cela, cliquez sur **Quality of Service (Qualité de service)** → **CoS Global Parameters (Paramètres globaux de CdS)** → **Interface Settings (Paramètres de l'interface)** dans l'arborescence.

Figure 9-131. Paramètres de l'interface CdS/QoS



Interface — Désigne le port ou le LAG à configurer :

Disable «Trust» Mode on Interface — Désactive le mode Confiance sur l'interface spécifiée. Ce paramètre remplace la valeur Trust configurée globalement sur le périphérique.

Set Default CoS For Incoming Traffic To (Définir la valeur CdS par défaut pour le trafic entrant) — Définit la valeur de la marque CdS pour les paquets non marqués. Les valeurs des marques CdS sont comprises entre 0 et 7. La valeur par défaut est 0.

Queue (File d'attente) — Numéro de la file d'attente.

Queue Mode (Mode File d'attente) — Indique si la file d'attente est en mode Priorité stricte ou WRR. Ce mode est défini sur l'écran **Queue Settings** (Paramètres de file d'attente).

- 1 Le mode SP (Priorité stricte) peut être configuré sur toutes les files d'attente 1 à 4.
- 1 Le mode WRR peut être configuré sur toutes les files d'attente 1 à 4.
- 1 Le mode SP peut être configuré sur les files d'attente 1 et 2, avec le mode WRR sur les files d'attente 3 et 4.
- 1 Le mode WRR peut être configuré sur les files d'attente 1 et 2, avec le mode SP sur les files d'attente 3 et 4.

Weight (Pondération) (6-255) — Assigne des pondérations de WRR aux files d'attente. Ce champ est activé uniquement pour les files d'attente en mode WRR.

% of WRR Bandwidth (% de bande passante WWR) — Traduction en pourcentage de la pondération définie dans le champ **Weight (Pondération) (6-255)**.

Affectation de valeurs QoS/CdS pour une interface :

1. Ouvrez la page [Interface Cos/QoS Settings](#) (Paramètres de l'interface CdS/QoS).
2. Sélectionnez une interface dans le champ **Interface**.
3. Renseignez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de CdS sont assignés à l'interface.

Affectation des interfaces CdS à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [Interface Cos/QoS Settings](#) (Paramètres de l'interface CdS/QoS).

Tableau 9-95. Commandes CLI de l'interface CdS

Commande CLI	Description
qos trust	Active l'état Confiance pour chaque port.
qos cos <i>cos-par défaut</i>	Configure la valeur de CdS du port par défaut.
no qos trust	Désactive l'état Confiance sur chaque port.

Vous trouverez ci-dessous un exemple de commande CLI :

```

Console (config)# interface ethernet g5

Console (config-if)# qos trust

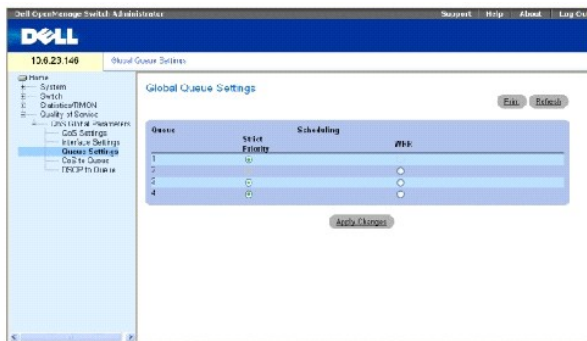
Console (config-if)# qos cos 3

```

Définition des paramètres de file d'attente

La page [Global Queue Setting](#) (Paramètres globaux de file d'attente) contient des champs permettant de configurer la méthode de planification selon laquelle les files d'attente sont maintenues. Pour ouvrir la page [Global Queue Setting](#) (Paramètres globaux de file d'attente), cliquez sur Quality of Service (Qualité de service) → CoS Global Parameters (Paramètres globaux de CdS) → Queue Settings (Paramètres de file d'attente) dans l'arborescence.

Figure 9-132. Paramètres globaux de file d'attente



Queues (Files d'attente) — Numéro de la file d'attente.

Strict Priority (Priorité stricte) — Indique si la planification du trafic est strictement basée sur la priorité des files d'attente. La valeur par défaut est activée.

WRR — Indique si la planification du trafic pour les files d'attente en sortie est basée sur le schéma WRR.

Définition des paramètres de la file d'attente

1. Ouvrez la page [Global Queue Setting](#) (Paramètres globaux de file d'attente).
2. Renseignez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de la file d'attente sont définis et le périphérique est mis à jour.

Affectation des paramètres de file d'attente à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [Global Queue Setting](#) (Paramètres globaux de file d'attente).

Tableau 9-96. Commandes CLI de paramétrage des files d'attente

Commande CLI	Description
<code>wrr-queue bandwidth weight1 weight2...weight_n</code>	Affecte des pondérations WRR (permutation circulaire pondérée) aux files d'attente de sortie.
<code>show qos interface [ethernet interface-number] [queuing]</code>	Affiche les données de l'interface QoS.

Vous trouverez ci-dessous un exemple de commande CLI :

```

Console (config)# wrr-queue bandwidth 10 20 30 40

Console(config)# exit

Console# exit

Console> show qos interface ethernet g1 queuing

Ethernet g1

pondérations bande passante WRR et priorité EF :
```

```

Console (config)# wrr-queue bandwidth 10 20 30 40

Console(config)# exit

Console# exit

Console> show qos interface ethernet g1 queuing

Ethernet g1

pondérations bande passante WRR et priorité EF :
```

qid	pondérations	EF	Priorité
-----	-----	-----	-----
1	125	Désactiver	-

2	125	Désactiver	-
3	125	Désactiver	-
4	125	Désactiver	-
<p>Cos queue map:</p> <p>Cos gid</p> <p>0 2</p> <p>1 1</p> <p>2 1</p> <p>3 2</p> <p>4 3</p> <p>5 3</p> <p>6 4</p> <p>7 4</p>			

Adressage de valeurs CdS aux files d'attente

La page [CoS to Queue Mapping Table](#) (Table d'adressage CdS à file d'attente) contient des champs permettant de classer des paramètres CdS en fonction des files d'attente de trafic. Pour ouvrir la page [CoS to Queue Mapping Table](#) (Table d'adressage CdS à file d'attente), cliquez sur Quality of Service (Qualité de service) → CoS Global Parameters (Paramètres globaux de CdS) → CoS to Queue (CdS à file d'attente) dans l'arborescence.

Figure 9-133. Table d'adressage CdS à file d'attente



Class of Service (Classe de service) — Indique les valeurs des marques de priorité CdS, zéro étant la valeur la plus faible et sept la plus élevée.

Queue (File d'attente) — Indique la file d'attente de transfert de trafic à laquelle la priorité CdS est adressée. Quatre files d'attente de priorité du trafic sont prises en charge.

Restore Defaults (Utiliser les valeurs par défaut) — Restaure les paramètres d'usine du périphérique pour l'adressage de valeurs CdS à une file d'attente de transfert.

Adressage d'une valeur CdS à une file d'attente

1. Ouvrez la page [CoS to Queue Mapping Table](#) (Table d'adressage CdS à file d'attente).
2. Sélectionnez une entrée CdS.
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 CdS est adressée à une file d'attente et le périphérique est mis à jour.

Affectation de valeurs CdS aux files d'attente à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [CoS to Queue Mapping Table](#) (Table d'adressage CdS à file d'attente).

Tableau 9-97. Commandes CLI d'adressage de valeurs CdS à une file d'attente

Commande CLI	Description
<code>wrr-queue cos-map</code> <i>id-file d'attente cos1..cos8</i>	Adresse des valeurs CdS affectées aux files d'attente de sortie.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# wrr-queue cos-map  
4 7
```

Adressage des valeurs DSCP aux files d'attente

La page [DSCP Mapping](#) (Adressage DSCP) contient des champs permettant de définir la file d'attente de sortie qui est affectée en fonction d'un champ DSCP spécifique. Pour ouvrir la page [DSCP Mapping](#) (Adressage DSCP), cliquez sur Quality of Service (Qualité de service) → CoS Global Parameters (Paramètres globaux de CdS) → DSCP Mapping (Adressage DSCP) dans l'arborescence.


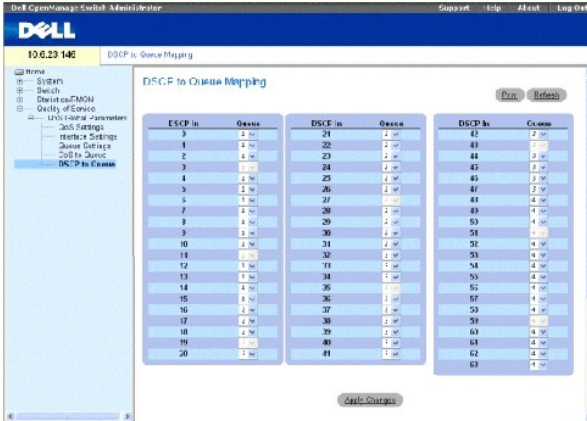
 **REMARQUE** : Pour obtenir la liste des valeurs DSCP adressées par défaut aux files d'attente, reportez-vous au tableau [«Valeurs par défaut de la table d'adressage DSCP à file d'attente»](#).

Figure 9-134. Adressage DSCP



DSCP In (Entrée DSCP) — Valeurs du champ DSCP dans le paquet entrant.

Queue (File d'attente) — File d'attente à laquelle les paquets contenant la valeur DSCP spécifiée sont affectés. Les valeurs sont comprises entre 1 et 4, un étant la valeur la plus faible et quatre la plus élevée.

Adressage d'une valeur DSCP et affectation d'une file d'attente de priorité :

1. Ouvrez la page [DSCP Mapping](#) (Adressage DSCP).
2. Sélectionnez une valeur dans la colonne **DSCP In** (Entrée DSCP).
3. Définissez les champs **Queue** (File d'attente).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La valeur DSCP n'est pas remplacée et elle est affectée à une file d'attente de transfert.

Affectation de valeurs DSCP à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [DSCP Mapping](#) (Adressage DSCP).

Tableau 9-98. Commandes CLI d'adressage de valeurs DSCP à une file d'attente

Commande CLI	Description
<code>qos map dscp-queue liste-dscp to id-file d'attente</code>	Modifie l'adressage DSCP vers file d'attente.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# qos map dscp-queue 33 40 41 to 1
```

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Caractéristiques techniques

Guide d'utilisation du système Dell™ PowerConnect™ 5324

- [Caractéristiques des ports et des câbles](#)
- [Conditions de fonctionnement](#)
- [Caractéristiques physiques du périphérique](#)
- [Caractéristiques de la mémoire du périphérique](#)
- [Caractéristiques des fonctions](#)

Cette annexe contient des informations nécessaires au bon fonctionnement du périphérique.

Caractéristiques des ports et des câbles

Cette section décrit les caractéristiques des ports.

Caractéristiques des ports

Le tableau suivant répertorie les types de ports de périphérique et décrit chaque type de port.

Tableau 10-99.

Périphérique	Caractéristiques
PowerConnect 5324	<ul style="list-style-type: none">1 24 ports GE1 4 ports SFP1 Port de console RS-232
Types de ports	
RJ-45	<ul style="list-style-type: none">1 10 Base-T1 100 Base-T1 1000 Base-T
SFP	Prend en charge le faible encombrement standard Émetteurs-récepteurs à connecteur Gigabit
Paramètres des ports	
	<ul style="list-style-type: none">1 Négociation automatique de la vitesse, du mode Duplex et du contrôle du flux1 Contre-pression1 Blocage en tête de ligne1 MDI/MDIX automatique1 Mise en miroir des ports1 Contrôle des tempêtes de diffusion

Caractéristiques des ports

Conditions de fonctionnement

Cette section décrit les conditions de fonctionnement, notamment les conditions de température et d'humidité.

Tableau 10-100.

Fonction	Caractéristiques
Température de fonctionnement	0° à 40° C / 32° à 104° F
Humidité de fonctionnement	10 à 90 % (sans condensation)

Conditions de fonctionnement

Caractéristiques physiques du périphérique

Cette section décrit les caractéristiques physiques du périphérique.

Tableau 10-101.

Fonction	Caractéristiques
Taille de l'unité	1 Largeur 483 mm (19 pouces) 1 Hauteur 4,445 cm (1 U)
Ventilation	Deux ventilateurs par unité

Caractéristiques physiques du périphérique

Caractéristiques de la mémoire du périphérique

Cette section décrit les caractéristiques de la mémoire du périphérique.

Tableau 10-102.

Type de mémoire	Quantité
DRAM UC	64 Mo
Mémoire Flash	16 Mo
Mémoire tampon de paquet	2 Mo

Caractéristiques de la mémoire du périphérique

Caractéristiques des fonctions

VLAN

- 1 Prise en charge du VLAN pour le marquage et l'authentification basée sur le port, en conformité avec la norme IEEE 802.1Q
- 1 Jusqu'à 4094 VLAN pris en charge
- 1 VLAN réservés pour une utilisation en interne par le système
- 1 VLAN dynamiques avec prise en charge du protocole GVRP
- 1 VLAN basés sur le protocole

Qualité de service

- 1 Mode Confiance de couche 2 (marquage IEEE 802.1p)
- 1 Mode Confiance de couche 3 (DSCP)
- 1 WRR (pondération WRR) réglable
- 1 Planification des files d'attente strictes réglable

Multidiffusion de couche 2

- 1 Prise en charge de la multidiffusion dynamique - jusqu'à 256 groupes de multidiffusion pris en charge dans la surveillance IGMP ou la multidiffusion statique

Sécurité du périphérique

- 1 Protection de l'accès au commutateur par un mot de passe

- 1 Alerte et verrouillage de l'adresse MAC basée sur le port
- 1 Authentification à distance RADIUS pour l'accès à la gestion du commutateur
- 1 TACACS+
- 1 Filtrage de l'accès à la gestion via des profils d'accès de gestion
- 1 Cryptages de gestion SSH/SSL

Fonctions de commutation supplémentaires

- 1 Agrégation de liaisons avec prise en charge de jusqu'à 8 liaisons agrégées par périphérique et jusqu'à 8 ports par liaison agrégée (IEEE 802.3ad)
- 1 Prise en charge du protocole LACP
- 1 Prise en charge des trames Jumbo de 10 K maximum
- 1 Contrôle des tempêtes de diffusion
- 1 Mise en miroir des ports

Gestion du périphérique

- 1 Interface de gestion basée sur le Web
- 1 Accessibilité de la CLI via Telnet
- 1 Prise en charge des protocoles SNMP v1 et SNMP v2
- 1 Prise en charge de 4 groupes RMON
- 1 Transferts par TFTP des fichiers du micrologiciel et de configuration
- 1 Images de micrologiciel doubles intégrées
- 1 Prise en charge des chargements/téléchargements multiples de fichiers de configuration
- 1 Statistiques pour la surveillance des erreurs et l'optimisation des performances
- 1 Prise en charge de la gestion de l'adresse IP DHCP/BootP
- 1 Fonctionnalités de connexion à distance Syslog
- 1 Prise en charge du protocole SNTP
- 1 Traceroute de couche 3
- 1 Client Telnet
- 1 Client DNS

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Configuration des informations du périphérique

Guide d'utilisation du système Dell™ PowerConnect™ 5324

- [Configuration de la sécurité du réseau](#)
- [Configuration des ports](#)
- [Configuration des tables d'adresses](#)
- [Configuration du protocole GARP](#)
- [Configuration du protocole Spanning Tree](#)
- [Configuration des VLAN](#)
- [Agrégation des ports](#)
- [Prise en charge du transfert multidiffusion](#)

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

Le périphérique permet de définir la sécurité du réseau à travers des Access Control Lists (Listes de contrôle d'accès) et des Locked Port (Ports verrouillés). Pour ouvrir la page **Network Security** (Sécurité du réseau), sélectionnez Switch (Commutateur) → Network Security (Sécurité du réseau).

Présentation de la sécurité du réseau

Cette section décrit les fonctions de la sécurité du réseau.

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, à l'aide du protocole EAP (protocole d'authentification extensible). L'authentification basée sur le port est composée des éléments suivants :

- 1 Authenticators (Authentifiants) — Désigne le port authentifié avant d'autoriser l'accès au système.
- 1 Supplicants (Demandeur) — Désigne l'hôte connecté au port authentifié qui demande à accéder aux services du système.
- 1 Authentication Server (Serveur d'authentification) — Désigne le serveur externe, le serveur RADIUS par exemple, qui réalise l'authentification au nom de l'authentifiant et indique si l'utilisateur est autorisé à accéder aux services du système.

L'authentification basée sur le port crée deux états d'accès :

- 1 Controlled Access (Accès contrôlé) — Permet la communication entre l'utilisateur et le système, si l'utilisateur est autorisé.
- 1 Uncontrolled Access (Accès non contrôlé) — Permet une communication non contrôlée sans tenir compte de l'état du port.

Le périphérique prend en charge l'authentification basée sur le port à travers des serveurs RADIUS.

Authentification avancée basée sur le port

L'authentification avancée basée sur le port permet à plusieurs hôtes de se rattacher à un seul port. L'authentification avancée basée sur le port n'a besoin que d'un seul hôte autorisé pour que tous les hôtes puissent accéder au système. Si le port n'est pas autorisé, aucun des hôtes rattachés ne peut accéder au réseau.

L'authentification avancée basée sur le port permet également une authentification basée sur l'utilisateur. Il reste toujours des VLAN spécifiques disponibles sur le périphérique, même si des ports spécifiques rattachés au VLAN ne sont pas autorisés. Par exemple, le trafic Voix sur IP ne nécessite pas d'authentification, contrairement au trafic de données. Vous pouvez définir des VLAN pour lesquels aucune autorisation n'est nécessaire. Les utilisateurs peuvent accéder à des VLAN non authentifiés même si les ports rattachés à ces VLAN sont définis comme autorisés.

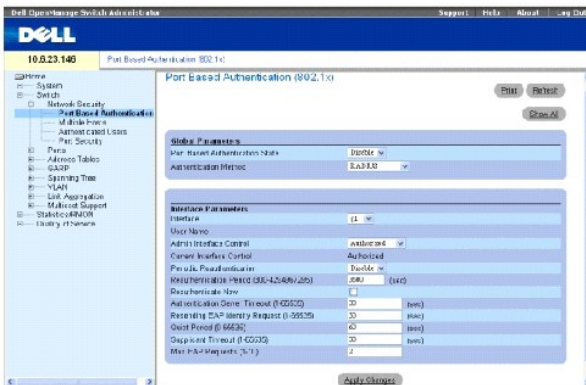
L'authentification avancée basée sur le port est implémentée de la façon suivante :

- 1 **Single Host Mode (Mode Hôte unique)** — Permet uniquement à l'hôte autorisé d'accéder au port.
- 1 **Multiple Host Mode (Mode Hôtes multiples)** — Permet à plusieurs hôtes d'être rattachés à un seul port. Il suffit d'avoir un seul hôte autorisé pour que tous les hôtes puissent accéder au réseau. Si l'authentification de l'hôte échoue ou si un message de déconnexion EAPOL est reçu, tous les clients rattachés se voient refuser l'accès au réseau.

Configuration de l'authentification basée sur le port

La page [Port Based Authentication](#) (Authentification basée sur le port) contient des champs permettant 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 du réseau) → Port Based Authentication (Authentification basée sur le port).

Figure 7-80. Authentification basée sur le port



Port Based Authentication State (État de l'authentification basée sur le port) — Permet l'authentification basée sur le port sur le périphérique. Ce champ peut prendre les valeurs suivantes :

Enable (Activée) — L'authentification basée sur le port est activée sur le périphérique.

Disable (Désactivée) — L'authentification basée sur le port est désactivée sur le périphérique.

Authentication Method (Méthode d'authentification) — Méthode d'authentification utilisée. Ce champ peut prendre les valeurs suivantes :

None (Aucune) — Aucune méthode d'authentification n'est utilisée pour le port.

RADIUS — L'authentification du port est réalisée à l'aide du serveur RADIUS.

RADIUS, None (Aucune) — L'authentification du port est réalisée d'abord à l'aide du serveur RADIUS. Si le port n'est pas authentifié, aucune méthode d'authentification n'est utilisée et la session est autorisée.

Interface — Contient une liste d'interfaces.

User Name (Nom d'utilisateur) — Nom d'utilisateur tel que configuré dans le serveur RADIUS.

Admin Interface Control (Contrôle interface Admin) — Définit l'état d'autorisation du port. Ce champ peut prendre les valeurs suivantes :

Authorized (Autorisé) — Définit l'état de l'interface sur autorisé (permettre le trafic).

Unauthorized (Non autorisé) — Définit l'état de l'interface sur non autorisé (refuser le trafic).

Auto — L'état d'autorisation est défini par la méthode d'autorisation.

Current Interface Control (Contrôle de l'interface en cours) — État d'autorisation du port configuré actuellement.

Periodic Reauthentication (Réauthentification périodique) — Réauthentifie régulièrement le port sélectionné. La période de réauthentification est définie dans le champ **Reauthentication Period (Période de réauthentification) (300-4294967295)**.

Reauthentication Period (300-4294967295) (Période de réauthentification [300-4294967295]) — Indique la période au cours de laquelle le port sélectionné est réauthentifié. La valeur de ce champ est exprimée en secondes. La valeur par défaut est 3600 secondes.

Reauthenticate Now (Réauthentifier maintenant) — Permet la réauthentification immédiate du port.

Authentication Server Timeout (1-65535) (Délai du serveur d'authentification [1-65535]) — Quantité de temps qui s'écoule avant que le périphérique envoie une nouvelle demande au serveur d'authentification. La valeur de ce champ est exprimée en secondes. La valeur par défaut est 30 secondes.

Resending EAP Identity Request (1-65535) (Renvoi demande d'identité EAP [1-65535]) — Quantité de temps qui s'écoule avant que des demandes EAP soient renvoyées. La valeur par défaut est 30 secondes.

Quiet Period (0-65535) (Période de repos [0-65535]) — Nombre de secondes durant lesquelles le périphérique reste au repos après un échec d'authentification. Ce champ peut prendre les valeurs 0 à 65 535. La valeur par défaut est 60 secondes.

Supplicant Timeout (1-65535) (Délai demandeur [1-65535]) — Quantité de temps qui s'écoule avant que des demandes EAP soient renvoyées à l'utilisateur. La valeur de ce champ est exprimée en secondes. La valeur par défaut est 30 secondes.

Max EAP Requests (1-10) (Nbre max. de demandes EAP [1-10]) — Nombre total de demandes EAP envoyées. Si aucune réponse n'est reçue après la période définie, le processus d'authentification est relancé. La valeur par défaut pour ce champ est 2 nouvelles tentatives.

Affichage de la table des authentifications basées sur le port

1. Ouvrez la page [Port Based Authentication](#) (Authentification basée sur le port).
2. Cliquez sur **Show All** (Afficher tout).

La [table des authentifications basées sur le port](#) s'ouvre :

Figure 7-81. Table des authentifications basées sur le port

Port-based Authentication Table

Copy Parameters from

Port	Host Name	Admin Port Config	Current Port Config	Periodic Reauthentication	Reauthentication Period	Reauthentication New 802.1X	Authentication Status	Start Period	Remedy EAP	Max EAP Requests	Significant Success	Server Timeout	Termination Cause	Copy to Selected
1	g1	Authorized	*	Disabled	300	0	Force Authorized	03	08	2	0	30	Not successful yet	<input type="checkbox"/>
2	g2	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
3	g3	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
4	g4	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
5	g5	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
6	g6	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
7	g7	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
8	g8	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
9	g9	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
10	g10	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
11	g11	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
12	g12	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
13	g13	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
14	g14	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
15	g15	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
16	g16	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
17	g17	Authorized	Authorized	Disabled	300	0	Force Authorized	03	08	2	0	30	Not successful yet	<input type="checkbox"/>
18	g18	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
19	g19	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
20	g20	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
21	g21	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
22	g22	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
23	g23	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>
24	g24	Authorized	*	Disabled	300	0	Initiate	03	08	2	0	30	Port re-authorized	<input type="checkbox"/>

Apply Changes

Termination Cause (Cause de l'arrêt) — Raison pour laquelle l'authentification du port s'est terminée.

Copy To Checkbox (Case à cocher Copier vers) — Copie les paramètres d'un port vers les ports sélectionnés.

Select All (Sélectionner tout) — Sélectionne tous les ports de la [table des authentifications basées sur le port](#).

Copie des paramètres dans la table des authentifications basées sur le port

- Ouvrez la page [Port Based Authentication](#) (Authentification basée sur le port).
- Cliquez sur **Show All** (Afficher tout).

La [table des authentifications basées sur le port](#) s'ouvre.

- Sélectionnez l'interface dans le champ **Copy Parameters from** (Copier les paramètres à partir de).
- Sélectionnez une interface dans la [table des authentifications basées sur le port](#).
- Cochez la case **Copy to** (Copier vers) pour définir les interfaces vers lesquelles les paramètres de l'authentification basée sur le port seront copiés.
- Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont copiés dans le port sélectionné de la [table des authentifications basées sur le port](#) et le périphérique est mis à jour.

Activation de l'authentification basée sur le port à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'activation de l'authentification basée sur le port comme sur la page [Port Based Authentication](#) (Authentification basée sur le port).

Tableau 7-49. Commandes CLI de l'authentification basée sur le port

Commande CLI	Description
<code>aaa authentication dot1x default method1 [method2]</code>	Spécifie une ou plusieurs méthodes AAA (authentification, autorisation et comptabilité) à utiliser sur les interfaces qui exécutent IEEE 802.1X.
<code>dot1x max-req compte</code>	Définit le nombre maximum de fois où le périphérique envoie un EAP au client avant de relancer le processus d'authentification.
<code>dot1x re-authenticate [ethernet interface]</code>	Entame manuellement une réauthentification de tous les ports activés 802.1X ou du port activé 802.1X spécifié.
<code>dot1x re-authentication</code>	Active la réauthentification périodique du client.
<code>dot1x timeout quiet-period secondes</code>	Définit le nombre de secondes pendant lesquelles le périphérique reste au repos après un échec d'authentification.
<code>dot1x timeout re-authperiod secondes</code>	Définit le nombre de secondes qui s'écoulent entre deux tentatives de réauthentification.
<code>dot1x timeout server-timeout secondes</code>	Définit la durée de la retransmission de paquets vers le serveur d'authentification.
<code>dot1x timeout supp-timeout secondes</code>	Définit la durée de la retransmission d'une trame de demande EAP au client.

<code>dot1x timeout tx-period</code> secondes	Définit le nombre de secondes durant lesquelles le périphérique attend de la part du client une réponse à une trame d'identité/demande EAP, avant de renvoyer la demande.
<code>show dot1x [ethernet interface]</code>	Affiche l'état 802.1X pour le périphérique ou l'interface spécifiée.
<code>show dot1x users [username nom d'utilisateur]</code>	Affiche les utilisateurs 802.1X pour le périphérique.

Vous trouverez ci-dessous un exemple de commande CLI :

```

Console> enable

Console# show dot1x

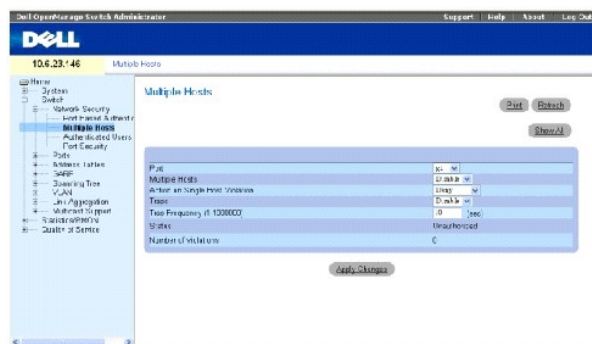
```

Interface	Mode Admin	Mode Oper	Contrôle Réauthent	Période Réauthent	Nom d'utilisateur
-----	-----	-----	-----	-----	-----
g1	Auto	Autorisé	Activ	3600	Bob
g2	Auto	Autorisé	Activ	3600	John
g3	Auto	Non autorisé	Activ	3600	Clark
g4	Aut-forcée	Autorisé	Désact	3600	-

Configuration de l'authentification avancée basée sur le port

La page [Multiple Hosts](#) (Hôtes multiples) fournit des informations permettant de définir des paramètres d'authentification avancée basée sur le port pour des ports spécifiques. Pour ouvrir la page [Multiple Hosts](#) (Hôtes multiples), cliquez sur Switch (Commutateur) → Network Security (Sécurité du réseau) → Multiple Hosts (Hôtes multiples).

Figure 7-82. Hôtes multiples



Port — Numéro du port pour lequel l'authentification avancée basée sur le port est activée.

Multiple Hosts (Hôtes multiples) — Permet ou non à un hôte unique d'autoriser plusieurs hôtes à accéder au système. Ce paramètre doit être activé pour désactiver le filtre en entrée ou pour utiliser la sécurité de verrouillage des ports sur le port sélectionné.

Action on Single Host Violation (Action en cas de violation de l'hôte unique) — Définit l'action à effectuer sur les paquets arrivant en mode Hôte unique, depuis un hôte dont l'adresse MAC n'est pas celle du client (demandeur). Ce champ peut être défini uniquement si le champ **Multiple Hosts** (Hôtes multiples) est paramétré sur **Disable** (Désactivé). Ce champ peut prendre les valeurs suivantes :

Permit (Autoriser) — Transfère les paquets d'une source inconnue, mais l'adresse MAC n'est pas apprise.

Deny (Refuser) — Ignore les paquets provenant d'une source non apprise. Il s'agit de la valeur par défaut.

Shutdown (Arrêt) — Ignore le paquet provenant d'une source non apprise et verrouille le port. Les ports restent verrouillés jusqu'à leur réactivation ou jusqu'à la réinitialisation de l'unité.

Traps (Interruptions) — Active ou désactive l'envoi d'interruptions à l'hôte en cas de violation.

Trap Frequency (1-1000000) (Sec) (Fréquence des interruptions [1-1000000] [s]) — Définit la fréquence d'envoi des interruptions à l'hôte. Ce champ peut être défini uniquement si le champ **Multiple Hosts** (Hôtes multiples) est paramétré sur **Disable** (Désactivé). La valeur par défaut est 10 secondes.

Status (État) — État de l'hôte. Ce champ peut prendre les valeurs suivantes :

Unauthorized (Non autorisé) — Les clients (demandeurs) ont un accès complet au port.

Authorized (Autorisé) — Les clients (demandeurs) ont un accès au port limité.

No single-host (Pas d'hôte unique) — **Multiple Hosts** (Hôtes multiples) est activé.

Number of Violations (Nombre de violations) — Nombre de paquets arrivés sur l'interface en mode Hôte unique, depuis un hôte dont l'adresse MAC n'est pas celle du client (demandeur).

Affichage de la [table des hôtes multiples](#)

1. Ouvrez la page [Multiple Hosts](#) (Hôtes multiples).
2. Cliquez sur **Show All** (Afficher tout).

La [table des hôtes multiples](#) s'ouvre :

Figure 7-83. **Table des hôtes multiples**

Multiples Hosts Table

Port	Enable Multiple Hosts	Action on Violation	Enable Traps	Trap Frequency	Status	Number of Violations
1	g1	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
2	g2	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
3	g3	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
4	g4	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
5	g5	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
6	g6	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
7	g7	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
8	g8	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
9	g9	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
10	g10	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
11	g11	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
12	g12	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
13	g13	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
14	g14	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
15	g15	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
16	g16	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
17	g17	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
18	g18	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
19	g19	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
20	g20	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
21	g21	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
22	g22	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
23	g23	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0
24	g24	Deny	<input checked="" type="checkbox"/>	10	Unauthorized	0

Activation des hôtes multiples à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'activation de l'authentification avancée basée sur le port comme sur la page [Multiple Hosts](#) (Hôtes multiples).

Tableau 7-50. Commandes CLI des hôtes multiples

Commande CLI	Description
<code>dot1x multiple-hosts</code>	Autorise les hôtes multiples (clients) sur un port autorisé 802.1X qui possède la commande de configuration d'interface dot1x port-control paramétrée sur auto.
<code>dot1x single-host-violation {forward discard discard-shutdown} [trap secondes]</code>	Configure l'action à effectuer lorsqu'une station dont l'adresse MAC n'est pas celle du client (demandeur) tente d'accéder à l'interface.

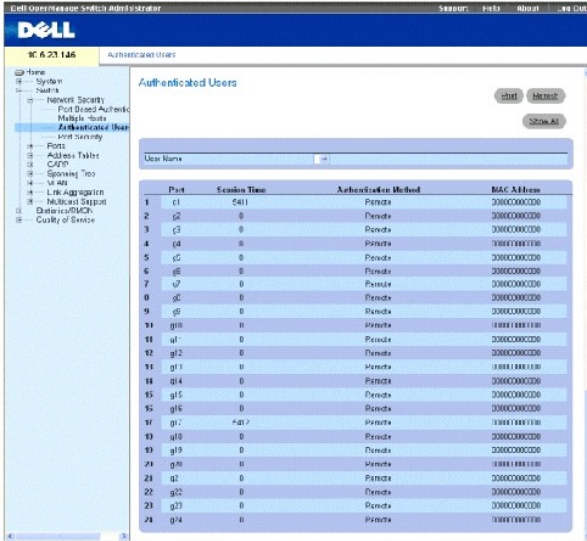
Vous trouverez ci-dessous un exemple de commande CLI.

```
Neyland# configure
Neyland(config)# interface ethernet g1
Neyland(config-if)# dot1x multiple-hosts
```

Authentification d'utilisateurs

La page [Authenticated Users](#) (Utilisateurs authentifiés) affiche des listes d'utilisateurs avec accès au port. Les listes d'utilisateurs avec accès sont définies sur la page Add User Name (Ajouter un nom d'utilisateur). Pour ouvrir la page [Authenticated Users](#) (Utilisateurs authentifiés), cliquez sur Switch (Commutateur) → Network Security (Sécurité du réseau) → Authenticated Users (Utilisateurs authentifiés).

Figure 7-84. Utilisateurs authentifiés



User Name (Nom d'utilisateur) — Liste d'utilisateurs autorisés à l'aide du serveur RADIUS.

Port — Numéro du/des ports utilisés pour l'authentification (par nom d'utilisateur).

Session Time (Durée de session) — Durée de connexion de l'utilisateur au périphérique. Le format de ce champ est Jour:Heure:Minute:Secondes. Exemple : 3 jours: 2 heures: 4 minutes: 39 secondes.

Last Authentication (Dernière authentification) — Temps écoulé depuis la dernière authentification de l'utilisateur. Le format de ce champ est Jour:Heure:Minute:Secondes. Exemple : 3 jours: 2 heures: 4 minutes: 39 secondes.

Authentication Method (Méthode d'authentification) — Méthode utilisée pour la dernière authentification de session. Ce champ peut prendre les valeurs suivantes :

Remote (À distance) — L'utilisateur a été authentifié à partir d'un serveur distant.

None (Aucun) — L'utilisateur n'a pas été authentifié.

MAC Address (Adresse MAC) — Adresse MAC du client (demandeur).

Affichage de la table des utilisateurs authentifiés

1. Ouvrez la page **Add User Name** (Ajouter un nom d'utilisateur).
2. Cliquez sur **Show All** (Afficher tout).

La **table des utilisateurs authentifiés** s'ouvre :

Figure 7-85. Table des utilisateurs authentifiés



Authentification d'utilisateurs à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'authentification des utilisateurs comme sur la page **Add User Name** (Ajouter un nom d'utilisateur).

Tableau 7-51. Commandes CLI d'ajout d'un nom d'utilisateur

Commande CLI	Description
<code>show dot1x users [username nom d'utilisateur]</code>	Affiche les utilisateurs 802.1X pour le périphérique.

Vous trouverez ci-dessous un exemple de commande CLI :

console# show dot1x users					
Nom d'utilisateur	Durée session	Dern Auth	Méthode Auth	Adresse MAC	Interface
-----	-----	-----	-----	-----	-----
Bob	1d3h	58m	À distance	00:08:3b:79:87:87	g1
John	8h19m	2m	Aucun	00:08:3b:89:31:27	g2

Configuration de la sécurité de port

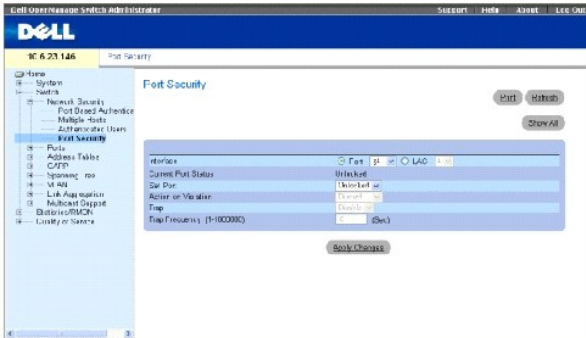
La sécurité du réseau peut être augmentée en limitant l'accès à un port spécifique aux utilisateurs possédant des adresses MAC spécifiques. Les adresses MAC peuvent être apprises de façon dynamique jusqu'à ce point ou bien configurées de façon statique. La sécurité des ports verrouillés contrôle les paquets reçus et appris arrivant à des ports spécifiques. L'accès au port verrouillé est limité aux utilisateurs possédant des adresses MAC spécifiques. Ces adresses sont soit manuellement définies sur le port, soit apprises sur ce port jusqu'à ce qu'il soit verrouillé. Lorsqu'un paquet arrive à un port verrouillé et que son adresse MAC source n'est pas liée à ce port (apprise sur un autre port ou inconnue du système), le mécanisme de protection est utilisé et propose plusieurs possibilités. Les paquets non autorisés arrivant à un port verrouillé peuvent être :

- 1 Forwarded (Transmis)
- 1 Discarded with no trap (Ignorés sans interruption)
- 1 Discarded with a trap (Ignorés avec interruption)
- 1 The ingress port is disabled (Le port d'entrée est désactivé)

Le port verrouillé permet également de stocker une liste d'adresses MAC dans le fichier de configuration. Cette liste peut être restaurée après réinitialisation du périphérique.

Les ports désactivés sont activés à partir de la page **Port Parameters** (Paramètres de port). Reportez-vous à la section [« Définition des paramètres des ports »](#). Pour ouvrir la page **Port Security** (Sécurité de port), cliquez sur Switch (Commutateur) → Network Security (Sécurité du réseau) → Port Security (Sécurité de port).

Figure 7-86. Sécurité de port



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) — Le port est soit verrouillé, soit déverrouillé. 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.

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 (Ignorer) — Ignore les paquets provenant d'une source non apprise. Il s'agit de la valeur par défaut.

Shutdown (Arrêt) — Ignore le paquet provenant d'une source non apprise et verrouille le port. Les ports restent verrouillés jusqu'à leur réactivation ou jusqu'à la 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 [1-1000000])— Indique le délai (en secondes) entre deux interruptions. Ce champ ne s'applique qu'aux ports verrouillés. La valeur par défaut est 10 secondes.

Définition d'un port verrouillé

1. Ouvrez la page [Port Security](#) (Sécurité de port).
2. Sélectionnez un type et un numéro d'interface.
3. Renseignez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port verrouillé est ajouté à la [table de sécurité de port](#) et le périphérique est mis à jour.

Affichage de la table des ports verrouillés

1. Ouvrez la page [Port Security](#) (Sécurité de port).
2. Cliquez sur **Show All** (Afficher tout).

La [table de sécurité de port](#) s'ouvre :

Les ports verrouillés peuvent également être définis à partir de la page Locked Ports Table (Table des ports verrouillés) et de la page [Port Security](#) (Sécurité de port).

Figure 7-87. Table de sécurité de port

Port Security Table

Copy Parameters from: Port: g1, LAG: 1

Port	Current Port Status	Set Port	Action	Trap	Trap Frequency	Copy to Select All
1	g1 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
2	g4 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
3	g3 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
4	g4 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
5	g5 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
6	g6 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
7	g7 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
8	g3 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
9	g9 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
10	g10 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
11	g11 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
12	g12 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
13	g13 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
14	g14 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
15	g15 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
16	g16 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
17	g17 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
18	g18 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
19	g19 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
20	g20 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
21	g21 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
22	g22 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
23	g23 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
24	g24 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
Global System LAGs						
25	LAG 1 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
26	LAG 2 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
27	LAG 3 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
28	LAG 4 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
29	LAG 5 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
30	LAG 6 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
31	LAG 7 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>
32	LAG 8 Unlocked	Unlocked	Discard	Disable	10	<input type="checkbox"/>

Apply Changes

Configuration de l'option de sécurité Locked Port (Port verrouillé) à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration de la sécurité Locked Port (Port verrouillé) comme sur la page [Port Security](#) (Sécurité de port).

Tableau 7-52. Commandes CLI de la sécurité de port

Commande CLI	Description
shutdown	Désactive les interfaces.
set interface active { ethernet <i>interface</i> port-channel <i>numéro-canal-port</i> }	Réactive une interface qui a été arrêtée pour des raisons de sécurité de port.
port security [forward discard discard-shutdown] [trap <i>secondes</i>]	Verrouille l'apprentissage de nouvelles adresses sur une interface.
show ports security { ethernet <i>interface</i> port-channel <i>numéro-canal-port</i> }	Affiche l'état de verrouillage du port.

Vous trouverez ci-dessous un exemple de commande CLI :

Console # show ports security					
Port	État	Action	Interruption	Fréquence	Compteur
----	-----	-----	-----	-----	-----
g7	Déverrouillé	Ignorer	Activer	100	88
g8	Déverrouillé	Ignorer, arrêter	Désactiver		
g3	Déverrouillé	-	-	-	-

Configuration des ports

La page **Ports** contient des liens vers des pages de fonctions des ports, notamment des fonctions avancées telles que Storm Control (Contrôle des tempêtes informatiques) et Port Mirroring (Mise en miroir des ports). Pour ouvrir la page **Ports**, cliquez sur **Switch (Commutateur) → Ports**.

Définition des paramètres des ports

La page [Port Configuration](#) (Configuration des ports) contient des champs permettant de définir les paramètres des ports. Pour ouvrir la page [Port Configuration](#) (Configuration des ports), cliquez sur **Switch (Commutateur) → Ports → Port Configuration (Configuration des ports)** dans l'arborescence.

Figure 7-88. Configuration des ports



Port — Numéro du port dont les paramètres sont définis.

Description (0 à 64 caractères) — Brève description de l'interface, par exemple Ethernet.

Port Type (Type de port) — Type du port.

Admin Status (État admin) — Active ou désactive le transfert du trafic à travers le port. Le nouvel état du port s'affiche dans le champ **Current Port Status** (État actuel du port).

Current Port Status (État actuel du port) — Indique si le port est opérationnel ou non.

Re-Activate Port (Réactiver le port) — Réactive un port si celui-ci a été désactivé par le biais de l'option de sécurité **Locked Port** (Port verrouillé).

Operational Status (État opérationnel) — État opérationnel du port. Ce champ peut prendre les valeurs suivantes :

Suspended (Suspendu) — Le port est actuellement activé et ne reçoit ni n'envoie aucun trafic.

Active (Activé) — Le port est actuellement activé et reçoit et envoie du trafic.

Disable (Désactivé) — Le port est actuellement désactivé et ne reçoit ni n'envoie aucun trafic.

Admin Speed (Vitesse admin) — Indique la vitesse de fonctionnement du port. Les options de paramétrage de la vitesse dépendent du type de port sélectionné. La vitesse admin ne peut être paramétrée que si la négociation automatique est désactivée sur le port configuré.

Current Port Speed (Vitesse actuelle du port) — Indique la vitesse du port synchronisé (en bps).

Admin Duplex — Le mode Duplex du port peut être **Full** (Intégral) ou **Half** (Semi-duplex). **Full** (Intégral) indique que l'interface prend en charge la transmission entre le périphérique et son partenaire de liaison dans les deux directions simultanément. **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 actuellement configuré.

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 actuelle) — Indique le paramétrage actuel de la négociation automatique.

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.

Current Back Pressure (Contre-pression actuelle) — Contre-pression actuellement configurée.

Flow Control (Contrôle de flux) — Active ou désactive le contrôle de flux ou active la négociation automatique du contrôle de flux sur le port. Est activé si le port est en mode Duplex **intégral**.

Current Flow Control (Contrôle de flux actuel) — Contrôle de flux actuellement configuré.

MDI/MDIX — Permet au périphérique 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. 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. Ce champ peut prendre les valeurs suivantes :

Auto — Utilisé pour détecter automatiquement le type du câble.

MDI (Interface dépendante du média) — Utilisé pour les stations terminales.

MDIX (Interface croisée dépendante du média) — Utilisé pour les concentrateurs et les commutateurs.

Current MDI/MDIX (MDI/MDIX actuel) — Paramétrage actuel de MDI/MDIX sur le périphérique.

LAG — Indique si le port fait partie d'un LAG.

Définition des paramètres des ports

1. Ouvrez la page [Port Configuration](#) (Configuration des ports).
2. Sélectionnez un port dans le champ **Port**.
3. Définissez les autres champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres du port sont sauvegardés sur le périphérique.

Modification des paramètres des ports

1. Ouvrez la page [Port Configuration](#) (Configuration des ports).
2. Sélectionnez un port dans le champ **Port**.
3. Modifiez les autres champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres du port sont sauvegardés sur le périphérique.

Affichage de la table de configuration des ports :

1. Ouvrez la page [Port Configuration](#) (Configuration des ports).
2. Cliquez sur **Show All** (Afficher tout).

La [Ports Configuration Table](#) (Table de configuration des ports) s'ouvre :

Figure 7-89. Table de configuration des ports

Port Configuration Table

Port	Port Type	Port Status	Port Speed	Duplex Mode	Auto Negotiation	Back Pressure	Flow Control	MDI/MDIX	10G
1	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
2	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
3	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
4	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
5	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
6	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
7	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
8	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
9	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
10	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
11	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
12	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
13	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
14	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
15	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
16	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
17	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
18	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
19	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
20	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
21	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
22	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
23	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
24	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
25	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
26	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
27	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
28	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
29	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
30	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
31	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
32	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
33	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
34	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
35	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
36	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
37	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
38	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
39	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
40	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
41	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
42	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
43	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A
44	100M copper	Up	100	Full	Enable	Disable	Disable	N/A	N/A

Configuration des ports à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des ports comme sur la page [Ports Configuration Table](#) (Table de configuration des ports).

Tableau 7-53. Commandes CLI de configuration des ports

Commande CLI	Description
<code>interface ethernet interface</code>	Passer en mode de configuration de l'interface afin de configurer une interface de type ethernet.
<code>description chaîne</code>	Ajouter une description à une configuration d'interface.
<code>shutdown</code>	Désactiver les interfaces qui font partie du contexte en cours de définition.
<code>set interface active {ethernet interface port-channel numéro-canal-port}</code>	Réactiver une interface qui a été arrêtée pour des raisons de sécurité.
<code>speed bps</code>	Configurer la vitesse d'une interface ethernet donnée lorsque la négociation automatique n'est pas utilisée.
<code>autobaud</code>	Définir la ligne pour la détection automatique de débit.
<code>duplex {half full}</code>	Configurer le fonctionnement en mode Duplex intégral/Semi-duplex d'une interface ethernet donnée lorsque la négociation automatique n'est pas utilisée.
<code>negotiation</code>	Activer le fonctionnement de la négociation automatique pour les paramètres de vitesse et de mode Duplex d'une interface donnée.
<code>back-pressure</code>	Activer le mode Contre-pression sur une interface donnée.
<code>flowcontrol {auto on off rx tx}</code>	Configurer le contrôle de flux sur une interface donnée.
<code>mdix {on auto}</code>	Activer l'inverseur automatique sur une interface ou un canal de port donné.
<code>show interfaces configuration [ethernet interface port-channel numéro-canal-port]</code>	Afficher la configuration de toutes les interfaces configurées.
<code>show interfaces status [ethernet interface port-channel numéro-canal-port]</code>	Afficher l'état de toutes les interfaces configurées.
<code>show interfaces description [ethernet interface port-channel numéro-canal-port]</code>	Afficher la description de toutes les interfaces configurées.

Vous trouverez ci-dessous un exemple de commande CLI :

```

Console (config)# interface ethernet g5

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)# exit

Console (config)# exit

```

```
Console# show interfaces configuration ethernet g5
```

Port	Type	Duplex	Vitesse	Nég	Contrôle de flux	État Admin	Contre-pression	Mode Mdix
----	----	-----	-----	----	-----	-----	-----	----
	-							
g5	1G	Intégral	100	Activée	Sous tension	Opérationnel	Activer	Auto
console#								

```
console# show interfaces status ethernet g5
```

Port	Type	Duplex	Vitesse	Nég	Contrôle de flux	État Liaison	Contre-pression	Mode Mdix
----	----	-----	-----	----	-----	-----	-----	----
	-							
g5	1G	Intégral	100	Activée	Sous tension	Opérationnel	Désactivée	Sous tension
console#								

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

```
Console# show interfaces status
```

Port	Type	Duplex	Vitesse	Nég	Contrôle de flux	État Liaison	Contre-pression	Mode Mdx
----	----	-----	-----	----	-----	-----	-----	----
g1	1G	Intégral	100	Auto	Sous tension	Opérationnel	Activer	Sous tension
g1	100	Intégral	100	Éteint	Éteint	Arrêté	Désactiver	Éteint
g2	100	Intégral	1000	Éteint	Éteint	Opérationnel	Désactiver	Sous tension
Canal	Type	Duplex	Vitesse	Nég	Contrôle de flux	Contre-pression	État Liaison	
---	----	-----	---	-----	-----	-----	-----	
1	1000	Intégral	1000	Éteint	Éteint	Désactiver	Opérationnel	

Définition des paramètres des LAG

La page [LAG Configuration](#) (Configuration des LAG) contient des champs qui permettent de définir des paramètres pour les LAG configurés. Le périphérique prend en charge jusqu'à huit ports par LAG et huit LAG par système.

Pour plus d'informations sur les LAG (Link Aggregated Groups) et sur l'assignation de ports à des LAG, reportez-vous à la section [Agrégation des ports](#).

Pour ouvrir la page [LAG Configuration](#) (Configuration des LAG), cliquez sur Switch (Commutateur) → Ports → LAG Configuration (Configuration des LAG) dans l'arborescence.


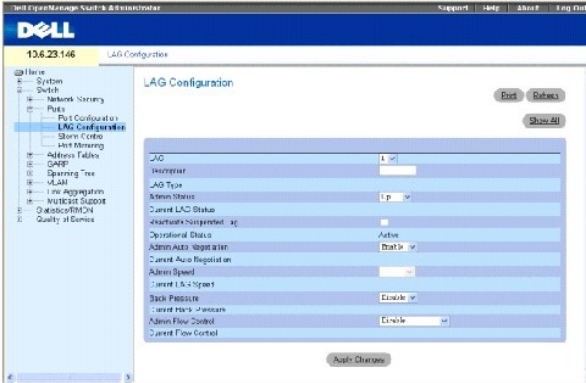
 **REMARQUE** : Si la configuration d'un port est modifiée alors que ce port est membre d'un LAG, cette modification prend effet uniquement après que le port ait été supprimé du LAG.

Figure 7-90. Configuration des LAG



LAG — Indique le numéro de LAG.

Description (0 à 64 caractères) — Contient une description du LAG configuré fournie par l'utilisateur.

LAG Type (Type de LAG) — Indique le type des ports qui constituent le LAG.

Admin Status (État admin) — Active ou désactive le transfert du trafic à travers le LAG sélectionné.

Current LAG Status (État actuel du LAG) — Indique si le LAG est en cours de fonctionnement.

Re-Activate Suspended LAG (Réactiver le LAG suspendu) — Réactive un LAG suspendu.

Operational Status (État opérationnel) — État opérationnel du LAG.

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 de publier sa vitesse de transmission, son mode Duplex et ses capacités de contrôle de flux (le contrôle du flux par défaut est désactivé) à son partenaire.

Current Auto Negotiation (Négociation automatique actuelle) — Indique le paramétrage actuel de la négociation automatique.

Admin Speed (Vitesse admin) — Indique la vitesse de fonctionnement du LAG.

Current LAG Speed (Vitesse actuelle du LAG) — Indique la vitesse actuelle de fonctionnement du LAG.

Admin Back Pressure (Contre-pression admin) — Active ou désactive le mode Contre-pression sur le LAG. Le mode Contre-pression est effectif sur les ports qui fonctionnent en semi-duplex dans le LAG.

Current Back Pressure (Contre-pression actuelle) — Contre-pression actuellement configurée.

Admin Flow Control (Contrôle de flux admin) — Active/désactive le contrôle de flux ou active la négociation automatique du contrôle de flux sur le LAG. Le mode Flow Control (Contrôle du flux) est effectif sur les ports qui fonctionnent en duplex intégral dans le LAG.

Current Flow Control (Contrôle de flux actuel) — Contrôle de flux configuré par l'utilisateur.

Définition des paramètres de LAG

1. Ouvrez la page [LAG Configuration](#) (Configuration des LAG).
2. Sélectionnez un LAG dans le champ LAG.
3. Renseignez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres du LAG sont sauvegardés sur le périphérique.

Modification des paramètres de LAG

1. Ouvrez 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 le périphérique.

Affichage de la table de configuration des LAG :

1. Ouvrez la page [LAG Configuration](#) (Configuration des LAG).
2. Cliquez sur **Show All** (Afficher tout).

La [table de configuration des LAG](#) s'ouvre :

Figure 7-91. Table de configuration des LAG

LAG Configuration Table

LAG	Description	LAG Type	LAG Status	LAG Speed	Auto Negotiation	Eth Port	Flow Control
1	1	Uo	Up	100	Enable	Disable	Disable
2	2	Uo	Up	100	Enable	Disable	Disable
3	3	Uo	Up	100	Enable	Disable	Disable
4	4	Uo	Up	100	Enable	Disable	Disable
5	5	Uo	Up	100	Enable	Disable	Disable
6	6	Uo	Up	100	Enable	Disable	Disable
7	7	Uo	Up	100	Enable	Disable	Disable
8	8	Uo	Up	100	Enable	Disable	Disable

Refresh

Apply Changes

Configuration des LAG à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des LAG comme indiqué dans la page [LAG Configuration](#) (Configuration des LAG).

Tableau 7-54. Commandes CLI de configuration des LAG

Commande CLI	Description
<code>interface port-channel numéro-canal-port</code>	Passer en mode de configuration de l'interface d'un canal de port spécifique.
<code>description chaîne</code>	Ajouter une description à une configuration d'interface.
<code>shutdown</code>	Désactiver les interfaces qui font partie du contexte en cours de définition.
<code>speed bps</code>	Configurer la vitesse d'une interface ethernet donnée lorsque la négociation automatique n'est pas utilisée.

autobaud	Définit la ligne pour la détection automatique de débit.
negotiation	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 rx tx }	Configure le contrôle de flux sur une interface donnée.
show interfaces configuration [ethernet <i>interface</i> port-channel <i>numéro-canal-port</i>]	Affiche la configuration de toutes les interfaces configurées.
show interfaces status [ethernet <i>interface</i> port-channel <i>numéro-canal-port</i>]	Affiche l'état de toutes les interfaces configurées.
show interfaces description [ethernet <i>interface</i> port-channel <i>numéro-canal-port</i>]	Affiche la description de toutes les interfaces configurées.
show interfaces port-channel [<i>numéro-canal-port</i>]	Affiche des informations sur les canaux de port (quels ports sont membres de ce canal de port et s'ils sont actuellement actifs ou non).

Vous trouverez ci-dessous un exemple de commande CLI :

```

console(config-if)# channel-group 1 mode on

console(config-if)#exit

console(config)# interface range e g21-24

console(config-if)# channel-group 1 mode on

console(config-if)# ex

console(config)# interface ethernet g5

console(config-if)# channel-group 2 mode on

console(config-if)#exit

console(config)# exit

```

console# show interfaces port-channel	
Canal	Ports
-----	-----
canal1	Inactif : g(21-24)
canal2	Actif : g5
canal3	

canal4	
canal5	
canal6	
canal7	
canal8	
console#	

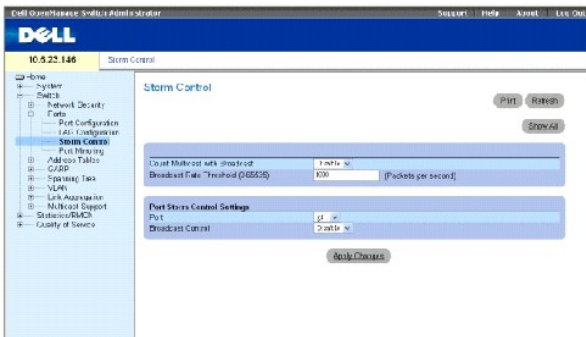
Activation de la fonction de contrôle des tempêtes informatiques

Une Broadcast Storm (Tempête de diffusion) résulte d'une quantité excessive de messages de diffusion transmis simultanément sur un réseau à travers un seul port. Les réponses aux messages transmises sont chargées sur le réseau, ce qui se traduit par un épuisement des ressources réseau ou par un dépassement de délai du réseau.

Le système mesure la fréquence des trames de diffusion et de multidiffusion entrantes séparément sur chaque port et ignore les trames lorsque la fréquence dépasse une limite définie par l'utilisateur.

La page [Storm Control](#) (Contrôle des tempêtes informatiques) contient des champs permettant d'activer et de configurer la fonction Storm Control. Pour ouvrir la page [Storm Control](#) (Contrôle des tempêtes informatiques), cliquez sur Switch (Commutateur) → Ports → Storm Control (Contrôle des tempêtes informatiques) dans l'arborescence.

Figure 7-92. Contrôle des tempêtes informatiques



Count Multicast with Broadcast (Compter les paquets multidiffusion et diffusion) — Compte le trafic diffusion et multidiffusion. Ce champ peut prendre les valeurs suivantes :

- o **Enable** (Activer) — Compte le trafic diffusion et multidiffusion.
- o **Disable** (Désactiver) — Compte uniquement le trafic diffusion.

Broadcast Rate Threshold (1-1000000) (Fréquence seuil diffusion [1-1000000])— Définit la fréquence limite (en paquets par seconde) à laquelle les paquets inconnus sont transmis. La plage s'étend de 0 à 1000000. La valeur par défaut est zéro. Toutes les valeurs sont arrondies au multiple de 64 Kbps supérieur. Si la valeur se situe en-dessous de 64 Kbps, elle est arrondie à 64 Kbps, sauf pour la valeur zéro.

Port — Indique le port à partir duquel la fonction de contrôle des tempêtes informatiques est activée.

Broadcast Control (Contrôle des paquets diffusion) — Active ou désactive la transmission des paquets diffusion sur le périphérique.

Activation de la fonction de contrôle des tempêtes informatiques sur le périphérique

1. Ouvrez la page [Storm Control](#) (Contrôle des tempêtes informatiques).
2. Sélectionnez une interface sur laquelle mettre en œuvre la fonction de contrôle des tempêtes informatiques.
3. Renseignez les champs.
4. Cliquez sur **Show All** (Afficher tout).

La fonction de contrôle des tempêtes informatiques est activée sur le périphérique.

Modification des paramètres des ports pour la fonction de contrôle des tempêtes informatiques

1. Ouvrez la page [Storm Control](#) (Contrôle des tempêtes informatiques).
2. Modifiez les champs.
3. Cliquez sur **Show All** (Afficher tout).

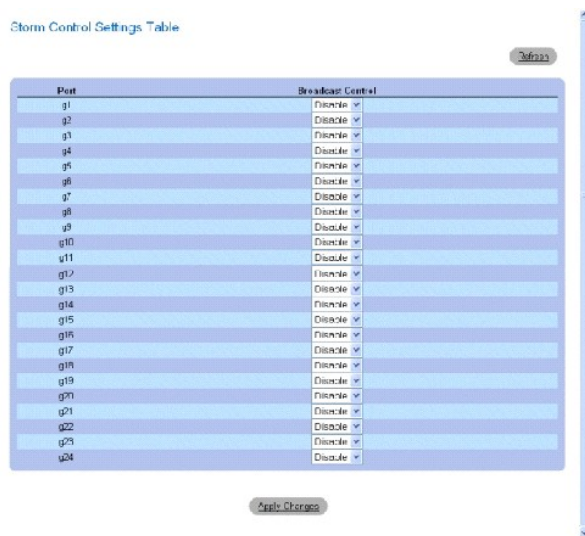
Les paramètres des ports pour la fonction de contrôle des tempêtes informatiques sont sauvegardés sur le périphérique.

Affichage de la table des paramètres des ports

1. Ouvrez la page [Storm Control](#) (Contrôle des tempêtes informatiques).
2. Cliquez sur **Show All** (Afficher tout).

La [table des paramètres de contrôle des tempêtes informatiques](#) s'ouvre :

Figure 7-93. Table des paramètres de contrôle des tempêtes informatiques



Storm Control Settings Table

Port	Broadcast Control
g1	Disable ▾
g2	Disable ▾
g3	Disable ▾
g4	Disable ▾
g5	Disable ▾
g6	Disable ▾
g7	Disable ▾
g8	Disable ▾
g9	Disable ▾
g10	Disable ▾
g11	Disable ▾
g12	Disable ▾
g13	Disable ▾
g14	Disable ▾
g15	Disable ▾
g16	Disable ▾
g17	Disable ▾
g18	Disable ▾
g19	Disable ▾
g20	Disable ▾
g21	Disable ▾
g22	Disable ▾
g23	Disable ▾
v24	Disable ▾

Apply Changes

Configuration de la fonction de contrôle des tempêtes informatiques à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration de la fonction de contrôle des tempêtes informatiques comme indiqué à la page [Storm Control](#) (Contrôle des tempêtes informatiques).

Tableau 7-55. Commandes CLI de la fonction de contrôle des tempêtes informatiques

Commande CLI	Description
<code>port storm-control include-multicast</code>	Permet au périphérique de compter les paquets multidiffusion et les paquets diffusion.
<code>port storm-control broadcast enable</code>	Active la fonction de contrôle des tempêtes informatiques de diffusion.
<code>port storm-control broadcast rate <i>fréquence</i></code>	Configure la fréquence de diffusion maximale.
<code>show ports storm-control [ethernet <i>interface</i>]</code>	Affiche la configuration de la fonction de contrôle des tempêtes informatiques.

Vous trouverez ci-dessous un exemple de commande CLI :

```

console> enable

console# configure

Console(config)# port storm-control include-multicast

Console(config)# port storm-control broadcast rate 8000

Console(config)# interface ethernet g1

Console(config-if)# port storm-control broadcast enable

Console(config-if)# end

Console# show ports storm-control

```

Port	Contrôle des tempêtes informatiques de diffusion [Paquets/s]
-----	-----
g1	8 000
g2	Désactivé
g4	Désactivé

Définition des sessions de 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 jusqu'à un port de contrôle.

La mise en miroir des ports 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 Port Mirroring (Mise en miroir des ports), notez bien ce qui suit :

- 1 Les ports contrôlés ne peuvent pas fonctionner plus rapidement que les ports de contrôle.

- 1 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 :

- 1 Les ports ne peuvent pas être configurés comme ports source.
- 1 Les ports ne peuvent pas être membres d'un LAG.
- 1 Des interfaces IP ne sont pas configurées sur le port.
- 1 GVRP n'est pas activé sur le port.
- 1 Le port n'est pas membre d'un VLAN.
- 1 Un seul port de destination peut être défini.

Les restrictions suivantes s'appliquent aux ports configurés comme ports source :

- 1 Les ports source ne peuvent pas être membres d'un LAG.
- 1 Les ports ne peuvent pas être configurés comme ports de destination.
- 1 Tous les paquets sont marqués lorsqu'ils sont transmis depuis le port de destination.
- 1 Tous les paquets RX/TX doivent être contrôlés sur le même port.

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.


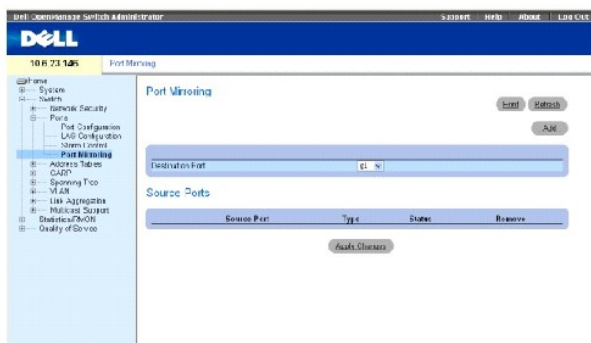
 **REMARQUE** : Lorsqu'un port est défini pour être un port cible pour une session de mise en miroir des ports, toutes les opérations courantes sont interrompues sur ce port. Ces opérations comprennent Spanning Tree et LACP.

Figure 7-94. Mise en miroir des ports



Destination Port (Port de destination) — Numéro du port vers lequel le trafic de ports est dupliqué.

Source Port (Port source) — Numéro du port depuis lequel le trafic de ports est dupliqué.

Type — Indique si le port source est RX, TX ou les deux.

Status (État) — Indique si le port est surveillé (**Active** (Actif)) ou non (**Ready** (Prêt)).

Remove (Supprimer) — Supprime la session de mise en miroir des ports.

Ajout d'une session de mise en miroir des ports

1. Ouvrez la page [Port Mirroring](#) (Mise en miroir des ports).

2. Cliquez sur **Ajouter**.

La page **Add Source Port** (Ajouter un port source) s'ouvre.

3. Sélectionnez le port de destination dans le menu déroulant **Destination Port** (Port de destination).
4. Sélectionnez un port source dans le menu déroulant **Source Port** (Port source).
5. Définissez le champ **Type**.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau port source est défini et le périphérique est mis à jour.

Suppression d'un port de duplication d'une session de mise en miroir des ports

1. Ouvrez 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 est modifiée et le périphérique est mis à jour.

Configuration d'une session de mise en miroir des ports à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration d'une session de mise en miroir des ports comme sur la page [Port Mirroring](#) (Mise en miroir des ports).

Tableau 7-56. Commandes CLI de mise en miroir des ports

Commande CLI	Description
<code>port monitor src-interface [rx tx]</code>	Démarre une session de surveillance des ports.

Vous trouverez ci-dessous un exemple de commande CLI :

```

Console(config)# interface ethernet g1

Console(config-if)# port monitor g8

Console# show ports monitor

```

Port source	Port de destination	Type	État	Marquage VLAN
-----	-----	-----	-----	-----
g8	g1	RX, TX	Actif	Non
g2	g8	RX, TX	Actif	Non
g18	g8	Rx	Actif	Non

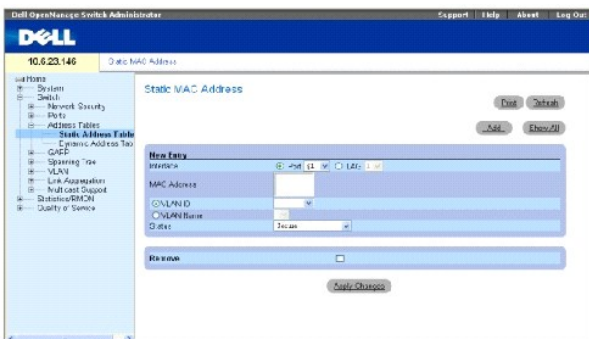
Configuration des tables d'adresses

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. Les tables d'adresses statiques et dynamiques peuvent être triées par interface, par VLAN et par type d'interface. Les adresses MAC sont apprises de façon dynamique au fur et à mesure que les paquets provenant des sources arrivent au commutateur. Les adresses sont associées aux ports grâce à l'apprentissage des ports à partir de l'adresse source de la trame. Les trames adressées à une adresse MAC de destination qui n'est associée à aucun port vont inonder tous les ports du VLAN approprié. Les adresses statiques sont configurées manuellement. Pour empêcher la table de pontage de déborder, 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 Table** (Tables d'adresses) dans l'arborescence.

Définition d'adresses statiques

La page [Static MAC Address](#) (Adresse MAC statique) contient une liste des adresses MAC statiques. Les adresses statiques peuvent être ajoutées et supprimées à partir de la page [Static MAC Address](#) (Adresse MAC statique). Par ailleurs, différentes adresses MAC peuvent être définies pour un seul port. Pour ouvrir la page [Static MAC Address](#) (Adresse MAC statique), cliquez sur **Switch** (Commutateur) → **Address Table** (Table des adresses) → **Static Address** (Adresse statique) dans l'arborescence.

Figure 7-95. Adresse MAC statique



Interface — Indique le port ou le LAG pour lequel une adresse MAC statique est ajoutée.

MAC Address (Adresse MAC) — Adresse MAC répertoriée dans la liste des adresses statiques actuelles.

VLAN ID (ID VLAN) — ID VLAN associé à l'adresse MAC.

VLAN Name (Nom du VLAN) — Nom du VLAN défini par l'utilisateur.

Status (État) — État de l'adresse MAC. Ce champ peut prendre les valeurs suivantes :

Secure (Sécurisé) — Garantit qu'une adresse MAC de Locked Port (Port verrouillé) n'est pas supprimée.

Permanent — Indique que l'adresse MAC est permanente.

Delete on Reset (Effacer à la réinitialisation) — Indique que l'adresse MAC est supprimée lors de la réinitialisation du périphérique.

Delete on Timeout (Effacer au délai d'expiration) — Indique que l'adresse MAC est supprimée si le délai d'attente du périphérique arrive à expiration.

Remove (Supprimer) — Supprime l'adresse MAC de la table des adresses MAC.

Ajout d'une adresse MAC statique

1. Ouvrez la page [Static MAC Address](#) (Adresse MAC statique).
2. Cliquez sur **Ajouter**.

La page **Add Static MAC Address** (Ajouter une adresse MAC statique) s'ouvre.

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

La nouvelle adresse statique est ajoutée à la **table des adresses MAC statiques** et le périphérique est mis à jour.

Modification d'une adresse de la table des adresses MAC statiques

1. Ouvrez la page [Static MAC Address](#) (Adresse MAC statique).
2. Modifiez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse MAC statique est modifiée et le périphérique est mis à jour.

Suppression d'une adresse de la table des adresses statiques

1. Ouvrez la page [Static MAC Address](#) (Adresse MAC statique).
2. Cliquez sur **Show All** (Afficher tout).

La **table des adresses statiques** s'ouvre.

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

L'adresse statique sélectionnée est supprimée et le périphérique est mis à jour.

Configuration des paramètres des adresses statiques à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des paramètres des adresses statiques comme sur la page [Static MAC Address](#) (Adresse MAC statique).

Tableau 7-57. Commandes CLI des adresses statiques

Commande CLI	Description
<code>bridge address mac-address {ethernet interface port-channel numéro-canal-port} [permanent delete-on-reset delete-on-timeout secure]</code>	Ajoute une adresse source de station de couche MAC statique à la table de pontage.
<code>show bridge address-table [vlan vlan] [ethernet interface port-channel numéro-canal-port]</code>	Affiche les entrées dans la base de données de transmission de pont.

Voici un exemple de commandes CLI :

```
Console# show bridge address-table
```

Délai d'expiration : 300 s			
vlan	adresse mac	port	type
----	-----	----	-----
1	00:60:70:4C:73:FF	g8	dynamique
1	00:60:70:8C:73:FF	g8	dynamique
200	00:10:0D:48:37:FF	g9	statique
g8	00:10:0D:98:37:88	g8	dynamique

Affichage des adresses dynamiques

La page [Dynamic Address Table](#) (Table des adresses dynamiques) contient des informations sur 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 transmis directement à ces ports. La [table des adresses dynamiques](#) contient également des informations sur le délai d'expiration avant qu'une adresse MAC dynamique soit effacée et inclut des paramètres d'interrogation et d'affichage de la liste des adresses dynamiques. La table des adresses actuelles contient les paramètres d'adresse dynamique en fonction desquels les paquets sont directement transmis aux ports.

Pour ouvrir la page [Dynamic Address Table](#) (Table des adresses dynamiques), cliquez sur **Switch** (Commutateur) → **Address Table** (Table des adresses) → **Dynamic Addresses Table** (Table des adresses dynamiques) dans l'arborescence.

Figure 7-96. Table des adresses dynamiques

The screenshot shows the 'Dynamic Addresses Table' configuration page in the Dell OpenManage Switch Administrator. The page includes a navigation tree on the left, a main configuration area with fields for 'Address Aging (10-360)', 'Interface', 'MAC Address', and 'VLAN ID', and a 'Current Address Table' section displaying a table of dynamic addresses.

VLAN ID	MAC	Port
1	00:30:30:70:1	17
2	00:30:40:00:00:00	17
3	00:30:40:00:00:00	17
4	00:30:40:70:20	17
5	00:30:40:70:20	17
6	00:30:40:70:20	17
7	00:30:40:70:20	17
8	00:30:40:70:20	17
9	00:30:40:70:20	17
10	00:30:40:70:20	17
11	00:30:40:70:20	17

Address Aging (10-360) (Expiration de l'adresse [10-360])— Indique la durée pendant laquelle l'adresse MAC reste dans la [table des adresses dynamiques](#) avant qu'elle n'arrive à expiration si aucun trafic provenant de la source n'est détecté. La valeur par défaut est 300 secondes.

Interface — Indique l'interface pour laquelle la table est interrogée. Il existe deux types d'interface.

Port — Indique les numéros de port pour lesquels la table est interrogée.

LAG — Indique le LAG pour lequel la table est interrogée.

MAC Address (Adresse MAC) — Indique l'adresse MAC pour laquelle la table est interrogée.

VLAN ID (ID 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.

Redéfinition du délai d'expiration

1. Ouvrez la page [Dynamic Address Table](#) (Table des adresses dynamiques).
2. Définissez le champ **Aging Time** (Délai d'expiration).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le délai d'expiration est modifié et le périphérique est mis à jour.

Interrogation de la table des adresses dynamiques

1. Ouvrez la page [Dynamic Address Table](#) (Table des adresses dynamiques).
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 des adresses dynamiques](#) est interrogée.

Tri de la table des adresses dynamiques

1. Ouvrez la page [Dynamic Address Table](#) (Table des adresses dynamiques).
2. Dans le menu déroulant **Address Table Sort Key** (Clé de tri de la table d'adresses), choisissez de trier les adresses par adresse, par ID VLAN ou par interface.
3. Cliquez sur **Query** (Interroger).

La [table des adresses dynamiques](#) est triée.

Interrogation et tri des adresses dynamiques à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'interrogation et le tri des adresses dynamiques comme sur la page [Dynamic Address Table](#) (Table des adresses dynamiques).

Tableau 7-58. Commandes CLI d'interrogation et de tri

Commande CLI	Description
<code>bridge aging-time secondes</code>	Définit le délai d'expiration de la table d'adresses.
<code>show bridge address-table [vlan vlan] [ethernet interface port-channel numéro-canal-port]</code>	Affiche les classes des entrées créées de façon dynamique dans la base de données de transmission de pont.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# bridge aging-time 250

Console (config)# exit
```

```
Console# show bridge address-table
```

Délai d'expiration : 250 s			
vlan	adresse MAC	port	type
1	00:60:70:4C:73:FF	g8	dynamique
1	00:60:70:8C:73:FF	g8	dynamique
200	00:10:0D:48:37:FF	g8	statique

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. Le protocole GARP définit un ensemble de périphériques intéressés par un attribut de réseau donné, tel qu'un VLAN ou une adresse de multidiffusion.

Avant de configurer le protocole GARP, vérifiez ce qui suit :

- 1 Le délai de sortie (Leave) doit être supérieur ou égal à trois fois le délai de jointure (Join).
- 1 Le délai général de sortie (Leave all) doit être supérieur au délai de sortie (Leave).

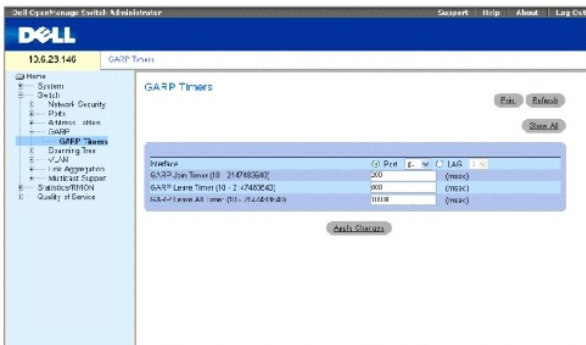
Définissez les mêmes valeurs de temporisateur GARP pour tous les périphériques connectés de couche 2. Si les temporisateurs GARP sont définis différemment sur les périphériques connectés de couche 2, l'application GARP ne peut pas fonctionner.

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 le protocole GARP sur le périphérique. Pour ouvrir la page [GARP Timers](#) (Temporisateurs GARP), cliquez sur **Switch** (Commutateur) → **GARP** → **GARP Timers** (Temporisateurs GARP) dans l'arborescence.

Figure 7-97. Temporisateurs GARP



Interface — Indique si les temporisateurs sont activés sur un port ou sur un LAG.

GARP Join Timer (10 - 2147483640) (Temporisateur Join GARP [10 - 2147483640]) — Durée en millisecondes pendant laquelle des PDU sont transmises. Ce champ peut prendre la valeur 10-2147483640. La valeur par défaut est de 200 ms.

GARP Leave Timer (10 - 2147483640) (Temporisateur Leave GARP [10 - 2147483640]) — Durée en millisecondes pendant laquelle le périphérique attend avant de sortir de son état GARP. Le délai de sortie 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 jointure (Join). Ce champ peut prendre la valeur 0-2147483640. La valeur par défaut est de 600 ms.

GARP Leave All Timer (10 - 2147483640) (Temporisateur Leave All GARP [10 - 2147483640]) — Durée en millisecondes pendant laquelle tous les périphériques attendent avant de sortir de leur état GARP. Le délai général de sortie (Leave all) doit être supérieur au délai de sortie (Leave). Ce champ peut prendre la valeur 0-2147483640. La valeur par défaut est de 10 000 ms.

Définition des temporisateurs GARP

1. Ouvrez la page [GARP Timers](#) (Temporisateurs GARP).
2. Renseignez les autres champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres GARP sont sauvegardés sur le périphérique.

Copie des paramètres dans la table des temporisateurs GARP

1. Ouvrez la page [GARP Timers](#) (Temporisateurs GARP).
2. Cliquez sur **Show All** (Afficher tout).

La **table des temporisateurs GARP** s'ouvre.

3. Sélectionnez une interface dans le champ **Copy Parameters from** (Copier paramètres à partir de).
4. Sélectionnez une interface dans le menu déroulant **Port** ou **LAG**.
5. Les définitions de cette interface sont copiées dans les interfaces sélectionnées. Reportez-vous à l'étape 6.
6. Cochez la case **Copy to** (Copier vers) pour définir les interfaces où les définitions de temporisateurs GARP seront copiées ou bien cliquez sur **Select All** (Tout sélectionner) pour copier les définitions dans tous les ports ou tous les LAG.
7. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont copiés vers les ports ou les LAG sélectionnés dans la **table des temporisateurs GARP** et le périphérique est mis à jour.

Définition des temporisateurs GARP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des temporisateurs GARP comme sur la page [GARP Timers](#) (Temporisateurs GARP).

Tableau 7-59. Commandes CLI des temporisateurs GARP

Commande CLI	Description
<code>garp timer {join leave leaveall} valeurs_temporisateurs</code>	Définit les valeurs des temporisateurs Join, Leave et Leave All de l'application GARP.

Vous trouverez ci-dessous un exemple de commande CLI :

```
console(config)# interface ethernet g1
```

```
console(config-if)# garp timer leave 900
```

```
console(config-if)# end
```

```
console# show gvrp configuration ethernet g1
```

La fonctionnalité GVRP est actuellement désactivée sur le périphérique.

Nombre max. de VLAN : 223

Port(s)	GVRP	Enregistrement	VLAN dynamique	Temporisateurs	(millisecondes)	
	État		Création	Join	Leave	Leave All
-----	-----	-----	-----	-----	-----	-----
g1	Désactivé	Normal (Standard)	Activée	200	900	10 000
console#						

Configuration du protocole Spanning Tree

Le STP (Protocole Spanning Tree) fournit une topographie en arborescence de la présentation des ponts. Le protocole STP fournit également 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 chemins secondaires entre les hôtes. Dans un réseau étendu, les boucles peuvent générer des ponts qui transmettent le trafic indéfiniment, ce qui entraîne une augmentation du trafic et une réduction des performances du réseau.

Les périphériques prennent en charge les protocoles Spanning Tree suivants :

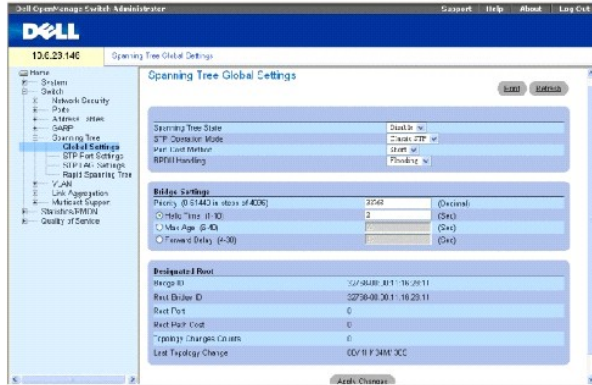
- 1 Classic STP — Fournit un chemin unique entre les stations terminales en évitant et en éliminant les boucles. Pour plus d'informations sur la configuration de Classic STP, reportez-vous à la section [«Définition des paramètres globaux STP»](#).
- 1 Rapid STP — Détecte et utilise des topologies de réseau qui permettent une convergence plus rapide du Spanning Tree sans création de boucles de transmission. Pour plus d'informations sur la configuration de Rapid STP, reportez-vous à la section [«Configuration du protocole Rapid Spanning Tree»](#).

Pour ouvrir la page **Spanning Tree** (Arbre maximal), cliquez sur **Switch** (Commutateur) → **Spanning Tree** (Arbre maximal) dans l'arborescence.

Définition des paramètres globaux STP

La page [STP Global Settings](#) (Paramètres globaux STP) contient des paramètres permettant d'activer et de configurer le fonctionnement du protocole STP sur le périphérique. Pour ouvrir la page [STP Global Settings](#) (Paramètres globaux STP), cliquez sur Switch (Commutateur) → Spanning Tree (Arbre maximal) → Global Settings (Paramètres globaux) dans l'arborescence.

Figure 7-98. Paramètres globaux STP



Spanning Tree State (État de l'arbre maximal) — Active ou désactive le protocole Spanning Tree sur le périphérique. Ce champ peut prendre les valeurs suivantes :

- o **Enable** (Activer) — Active le protocole Spanning Tree.
- o **Disable** (Désactiver) — Désactive le protocole Spanning Tree.

STP Operation Mode (Mode de fonctionnement STP) — Mode STP pour lequel STP est activé sur l'unité. Ce champ peut prendre les valeurs suivantes :

Classic STP — Active Classic STP sur le périphérique. Il s'agit de la valeur par défaut.

Rapid STP — Active Rapid STP sur le périphérique.

Path Cost Method (Méthode du coût de résolution) — Détermine la méthode du coût de résolution par défaut du protocole Spanning Tree. Ce champ peut prendre les valeurs suivantes :

Short (Court) — Indique une plage 1 à 65535 pour les coûts de résolution du port. Il s'agit de la valeur par défaut.

Long — Indique une plage de 1 à 200000000 pour les coûts de résolution du port.

BPDUs Handling (Gestion BPDU) — Détermine la façon dont les paquets BPDU sont gérés lorsque le STP est désactivé sur le port/périphérique. Les paquets BPDU sont utilisés pour transmettre des informations Spanning Tree. Ce champ peut prendre les valeurs suivantes :

Filtering (Filtrage) — Filtre les paquets BPDU lorsque le Spanning Tree est désactivé sur une interface.

Flooding (Inondation) — Inonde les paquets BPDU lorsque le Spanning Tree est désactivé sur une interface. Il s'agit de la valeur par défaut.

Priority (0-61440, in steps of 4096) (Priorité [0-61440, par étapes de 4096]) — Indique la valeur de priorité des ponts. Lorsque des commutateurs ou des ponts exécutent STP, une priorité est affectée à chacun d'eux. Après avoir échangé des BPDU, le commutateur possédant la valeur de priorité la plus basse devient le pont racine. La valeur par défaut est 32768. La valeur de priorité du pont est incrémentée en fonction de multiples de 4096 (incrément de 4 K). Par exemple 0, 4096, 8192, etc.

Hello Time (1-10) — Indique le délai Hello Time du périphérique. Le délai Hello Time indique la durée, en secondes, pendant laquelle un pont racine attend entre deux messages de configuration. La valeur par défaut est 2 secondes.

Max Age (6-40) (Délai d'attente maximal [6-40]) — Indique le délai d'attente maximal du périphérique. Le délai d'attente maximal indique la durée en secondes pendant laquelle un pont attend avant d'envoyer des messages de configuration. La valeur par défaut est 20 secondes.

Forward Delay (4-30) (Délai avant transfert [4-30])— Indique le délai avant transfert du périphérique. 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 15 secondes.

Bridge ID (ID pont) — Identifie la priorité et l'adresse MAC du pont.

Root Bridge ID (ID pont racine) — Identifie la priorité et l'adresse MAC du pont racine.

Root Port (Port racine) — 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. La valeur par défaut est zéro.

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 depuis le dernier redémarrage.

Last Topology Change (Dernière modification de topologie) — Durée qui s'est écoulée depuis l'initialisation ou réinitialisation du pont ou depuis la dernière modification topographique. Cette durée s'affiche selon un format jour heure minutes secondes ; par exemple, 0 jours 1 heure 34 minutes et 38 secondes.

Définition des paramètres globaux STP

1. Ouvrez la page [STP Global Settings](#) (Paramètres globaux STP).
2. Sélectionnez le port qui doit être activé dans le menu déroulant **Select a Port** (Sélectionner un port).
3. Sélectionnez **Enable** (Activer) dans le champ **Spanning Tree State** (État Spanning Tree).
4. Sélectionnez le mode **STP** dans le champ **STP Operation Mode** (Mode de fonctionnement STP) et définissez les paramètres du pont.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le protocole STP est activé sur le périphérique.

Modification des paramètres globaux STP

1. Ouvrez la page [STP Global Settings](#) (Paramètres globaux STP).
2. Renseignez les champs de la fenêtre.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

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

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des paramètres globaux STP comme indiqué dans la page [STP Global Settings](#) (Paramètres globaux STP).

Tableau 7-60. Commandes CLI des paramètres globaux STP

Commande CLI	Description
<code>spanning-tree</code>	Active la fonctionnalité Spanning Tree.
<code>spanning-tree mode { stp rstp }</code>	Configure le protocole STP.

<code>spanning-tree priority <i>priorité</i></code>	Configure la priorité Spanning Tree.
<code>spanning-tree hello-time <i>secondes</i></code>	Configure le délai Hello Time du pont Spanning Tree qui correspond à la fréquence à laquelle le périphérique diffuse des messages Hello aux autres commutateurs.
<code>spanning-tree max-age <i>secondes</i></code>	Configure le délai d'attente maximal du pont Spanning Tree.
<code>spanning-tree forward-time <i>secondes</i></code>	Configure le délai avant transmission du pont Spanning Tree 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 transmission.
<code>show spanning-tree [<i>ethernet interface</i> <i>port-channel numéro-canal-port</i>]</code>	Affiche l'identifiant de configuration de Spanning Tree.
<code>show spanning-tree [<i>detail</i>] [<i>active</i> <i>blockedports</i>]</code>	Affiche des informations de configuration de Spanning Tree - informations détaillées, ports actifs ou ports bloqués.

Vous trouverez ci-dessous un exemple de commande CLI :

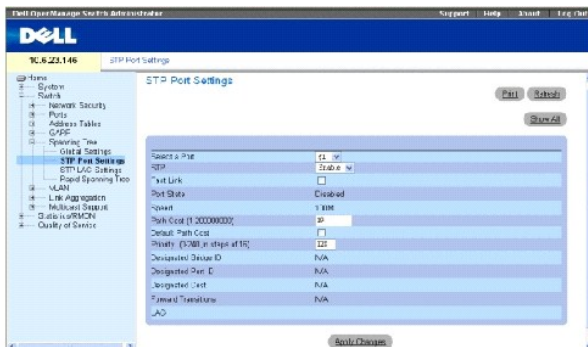
<pre> console(config)# spanning-tree console(config)# spanning-tree mode rstp console(config)# spanning-tree priority 12288 console(config)# spanning-tree hello-time 5 console(config)# spanning-tree max-age 15 console(config)# spanning-tree forward-time 25 console(config)# exit console# show spanning-tree Spanning Tree a activé le mode RSTP Méthode de coût du port par défaut : short (court) </pre>																																															
<table border="1"> <tr> <td>ID racine</td> <td>Priorité</td> <td>12288</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td>Adresse</td> <td>00:e8:00:b4:c0:00</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td colspan="3">Ce commutateur est la racine</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td colspan="7">Hello Time 5 s Délai d'attente maximal 15 s Délai avant transmission 25 s</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>								ID racine	Priorité	12288							Adresse	00:e8:00:b4:c0:00							Ce commutateur est la racine								Hello Time 5 s Délai d'attente maximal 15 s Délai avant transmission 25 s														
ID racine	Priorité	12288																																													
	Adresse	00:e8:00:b4:c0:00																																													
	Ce commutateur est la racine																																														
	Hello Time 5 s Délai d'attente maximal 15 s Délai avant transmission 25 s																																														
<p>Nombre de modifications de topologie 5 dernière modification il y a 00:05:28</p>																																															

Fréquences : mise en garde 1, modification de topologie 40, notification 5							
hello 5, délai d'attente maximal 15, délai avant transmission 25							
Interfaces							
Nom	État	ID port	Coût	Sts	Rôle	PortFast	Type
----	-----	-----	----	-----	-----	-----	-----
-							
g1	activé	128.1	100	DÉSACT	Désact	Non	P2p (STP)
g2	activé	128.2	100	DÉSACT	Désact	Non	P2p (STP)
g3	activé	128.3	100	DÉSACT	Désact	Non	P2p (STP)

Définition des paramètres des ports STP

La page [STP Port Settings](#) (Paramètres des ports STP) contient des champs permettant d'affecter des propriétés STP aux ports individuels. Pour ouvrir la page [STP Port Settings](#) (Paramètres des ports STP), cliquez sur **Switch** (Commutateur) → **Spanning Tree** (Arbre maximal) → **Port Settings** (Paramètres des ports) dans l'arborescence.

Figure 7-99. Paramètres des ports STP



Select a Port (Sélectionner un port) — Port pour lequel le protocole STP est activé.

STP — Active ou désactive le protocole STP sur le port.

Fast Link — Active le mode Fast Link pour le port. Si le mode Fast Link est activé pour un port, la valeur **Port State** (État du port) passe automatiquement à **Forwarding** (Transmission) lorsque la liaison du port est activée. Le mode Fast Link optimise le temps nécessaire à la convergence du protocole STP. La convergence STP peut nécessiter 30 à 60 secondes dans les réseaux de grande envergure.

Port State (État du port) — État STP actuel d'un port. Si cette option est activée, l'état du port détermine quelle action de transmission est effectuée sur le

trafic. Ce champ peut prendre les valeurs suivantes :

Disabled (Désactivé) — La liaison du port est actuellement désactivée.

Blocking (Blocage) — Le port est actuellement bloqué et ne peut pas être utilisé pour transmettre du trafic ou pour apprendre des adresses MAC. Le blocage s'affiche lorsque le 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.

Speed (Vitesse) — Indique la vitesse de fonctionnement du port.

Path Cost (1-200000000) (Coût de résolution [1-200000000]) — Contribution du port au coût de résolution racine. Le coût de résolution peut être ajusté sur une valeur supérieure ou inférieure et peut transmettre du trafic lorsqu'un chemin est en cours de reroutage.

Default Path Cost (Coût de résolution par défaut) — Le coût de résolution par défaut du port est défini automatiquement par la vitesse du port et la méthode du coût de résolution par défaut.

Les valeurs par défaut des coûts de résolution longs sont :

Ethernet - 2000000

Fast Ethernet - 200000

Gigabit Ethernet - 20000

Les valeurs par défaut des coûts de résolution courts (les coûts de résolution sont courts par défaut) sont :

Ethernet - 100

Fast Ethernet - 19

Gigabit Ethernet - 4

Priority (0-240, in steps of 16) (Priorité [0-240, par étapes de 16]) — Valeur de priorité du port. La valeur de priorité peut être utilisée pour influencer le choix du port lorsqu'un pont comprend deux ports connectés en boucle. La valeur de priorité est comprise entre 0 et 240. Elle est incrémentée en fonction de multiples de 16.

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 sélectionné.

Designated Cost (Coût désigné) — Coût du port participant à la topologie STP. Les ports à moindre coût risquent moins d'être bloqués si le STP détecte des

boucles.

Forward Transitions (Transitions vers transfert) — Nombre de fois où le port est passé de l'état **Blocking** (Blocage) à l'état **Forwarding** (Transfert).

LAG — Indique le LAG auquel le port est rattaché.

Activation du protocole STP sur un port

1. Ouvrez la page [STP Port Settings](#) (Paramètres des ports STP).
2. Sélectionnez **Enabled** (Activé) dans le champ **STP Port Status** (État port STP).
3. Définissez les champs **Fast Link** (Liaison rapide), **Path Cost** (Coût de résolution) et **Priority** (Priorité).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le protocole STP est activé sur le port.

Modification des propriétés des ports STP

1. Ouvrez la page [STP Port Settings](#) (Paramètres des ports STP).
2. Modifiez les champs **Priority** (Priorité), **Fast Link** (Liaison rapide) et **Path Cost** (Coût de résolution).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Affichage de la table des ports STP

1. Ouvrez la page [STP Port Settings](#) (Paramètres des ports STP).
2. Cliquez sur **Show All** (Afficher tout).

La page **STP Port Table** (Table des ports STP) s'ouvre.

Définition des paramètres des ports STP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des paramètres des ports STP comme sur la page [STP Port Settings](#) (Paramètres des ports STP).

Tableau 7-61. Commandes CLI des paramètres des ports STP

Commande CLI	Description
<code>spanning-tree disable</code>	Désactive Spanning Tree sur un port spécifique.
<code>spanning-tree cost coût</code>	Configure le coût de résolution de l'arbre maximal pour un port.
<code>spanning-tree port-priority priorité</code>	Configure la priorité du port.
<code>spanning-tree portfast</code>	Active le mode PortFast.
<code>show spanning-tree [ethernet interface port-channel numéro-canal-port]</code>	Affiche la configuration de Spanning Tree.

Vous trouverez ci-dessous un exemple de commande CLI :

```
console(config)# interface ethernet g5
```



```
console(config-if)# spanning-tree disable
```

```
console(config-if)# spanning-tree cost 35000
```

```
console(config-if)# spanning-tree port-priority 96
```

```
console(config-if)# exit
```

```
console(config)# exit
```

```
console# show spanning-tree ethernet g5
```

```
Port g5 désactivé
```

```
État : désactivé
```

```
ID port : 96.5
```

```
Type : P2p (configuré : Auto) STP
```

```
Priorité pont désigné : 32768
```

```
ID port désigné : 96.5
```

```
Nombre de transitions vers état  
transmission : 0
```

```
BPDU : envoyé 0, reçu 0
```

```
console#
```

```
Rôle : désactivé
```

```
Coût port : 35 000
```

```
Port Fast : Non (configuré : Non)
```

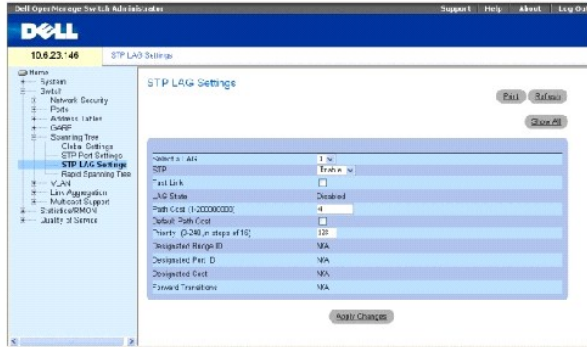
```
Adresse : 00:e8:00:b4:c0:00
```

```
Coût de résolution désigné : 19
```

Définition des paramètres des LAG STP

La page [STP LAG Settings](#) (Paramètres des LAG STP) contient des champs permettant d'affecter des paramètres STP aux LAG. Pour ouvrir la page [STP LAG Settings](#) (Paramètres des LAG STP), cliquez sur **Switch** (Commutateur) → **Spanning Tree** (Arbre maximal) → **LAG Settings** (Paramètres des LAG) dans l'arborescence.

Figure 7-100. Paramètres des LAG STP



Select a LAG (Sélectionner un LAG) — Indique le LAG défini par l'utilisateur. Pour plus d'informations, reportez-vous à la section [«Définition de l'appartenance à un LAG»](#).

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, la valeur **LAG State** (État du LAG) passe automatiquement à **Forwarding** (Transmission) lorsque le LAG est activé. Le mode Fast Link optimise le temps nécessaire à la convergence du protocole STP. La convergence STP peut nécessiter 30 à 60 secondes dans les réseaux de grande envergure.

LAG State (État du LAG) — État STP actuel d'un LAG. Si cette option est activée, l'état du LAG détermine quelle action de transmission est effectuée sur le trafic. Si le pont découvre un LAG défectueux, le LAG passe à l'état **Broken** (Défectueux). Ce champ peut prendre les valeurs suivantes :

Disabled (Désactivé) — La liaison du LAG est actuellement désactivée.

Blocking (Blocage) — Le LAG est actuellement bloqué et ne peut pas être utilisé pour transmettre du trafic ou pour apprendre des adresses MAC.

Listening (Écoute) — Le LAG est actuellement en mode d'écoute. Il ne peut ni transférer du trafic, ni apprendre d'adresses MAC.

Learning (Apprentissage) — Le LAG est en mode d'apprentissage et ne peut pas transmettre de trafic, mais il peut apprendre de nouvelles adresses MAC.

Forwarding (Transfert) — Le LAG est actuellement en mode de transfert. Il peut transmettre du trafic et apprendre de nouvelles adresses MAC.

Broken (Défectueux) — Le LAG présente un dysfonctionnement et ne peut pas être utilisé pour transmettre du trafic.

Path Cost (1-200000000) (Coût de résolution [1-200000000]) — Contribution du LAG au coût de résolution racine. Le coût de résolution peut être ajusté sur une valeur supérieure ou inférieure et peut transmettre du trafic lorsqu'un chemin est en cours de reroutage. La valeur du coût de résolution est comprise entre 1 et 200000000. Si la méthode du coût de résolution est courte, la valeur par défaut du coût du LAG est 4. Si la méthode du coût de résolution est longue, la valeur par défaut du coût du LAG est 20000.

Default Path Cost (Coût de résolution par défaut) — Le coût de résolution du LAG reprend sa valeur par défaut.

Priority (0-240, in steps of 16) (Priorité [0-240, par étapes de 16]) — Valeur de priorité du LAG. La valeur de priorité peut être utilisée pour influencer le choix du LAG lorsqu'un pont comprend deux ports connectés en boucle. La valeur de priorité est comprise entre 0 et 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) — Priorité et numéro d'interface du port désigné.

Designated Cost (Coût désigné) — Coût du pont désigné.

Forward Transitions (Transitions vers transfert) — Nombre de fois où le **LAG est passé** de l'état **Blocking** (Blocage) à l'état **Forwarding** (Transfert).

Modification des paramètres des LAG STP

1. Ouvrez la page [STP LAG Settings](#) (Paramètres des LAG STP).
2. Sélectionnez un LAG dans le menu déroulant **Select a LAG** (Sélectionner un LAG).
3. Modifiez les champs comme vous le désirez.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Définition des paramètres des LAG STP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des paramètres des LAG STP.

Tableau 7-62. Commandes CLI des paramètres des LAG STP

Commande CLI	Description
<code>spanning-tree</code>	Active la fonctionnalité Spanning Tree.
<code>spanning-tree disable</code>	Désactive le protocole Spanning Tree sur un LAG spécifique.
<code>spanning-tree cost coût</code>	Configure le coût de résolution de l'arbre maximal pour un LAG.
<code>spanning-tree port-priority priorité</code>	Configure la priorité du port.
<code>show spanning-tree [ethernet interface port-channel numéro-canal-port]</code>	Affiche la configuration de Spanning Tree.
<code>show spanning-tree [detail] [active blockedports]</code>	Affiche des informations Spanning Tree détaillées sur les ports actifs ou bloqués.

Vous trouverez ci-dessous un exemple de commande CLI :

```
console(config)# interface port-channel 1

console(config-if)# spanning-tree port-priority 16
```

Configuration du protocole Rapid Spanning Tree (RSTP)

Le protocole Classic Spanning Tree empêche les boucles de transmission de type L2 dans une topologie de réseau générale. Toutefois, la convergence peut nécessiter 30 à 60 secondes. La durée de convergence est considérée comme excessive pour de nombreuses applications. Lorsque la topologie de réseau le permet, il peut être possible d'avoir une convergence plus rapide. Le protocole RSTP (Protocole Rapid Spanning) détecte et utilise des topologies de réseau qui permettent une convergence plus rapide du Spanning Tree sans création de boucles de transmission.

Le protocole STP comprend les différents états de port suivants :

- 1 Disabled (Désactivé)
- 1 Learning (Apprentissage)
- 1 Discarding (Refus)
- 1 Forwarding (Transfert)

Utilisez la page [STP Global Settings](#) (Paramètres globaux STP) pour activer le protocole RSTP. Pour ouvrir la page [Rapid Spanning Tree \(RSTP\)](#) (Protocole RSTP), cliquez sur **Switch** (Commutateur) → **Spanning Tree** → **Rapid Spanning Tree** dans l'arborescence.

Figure 7-101. Rapid Spanning Tree (RSTP)



Interface — Port ou LAG sur lequel Rapid STP est activé.

Rôle (Rôle) — Rôle du port assigné par l'algorithme STP, à fournir aux chemins STP. Ce champ peut prendre les valeurs suivantes :

Root (Racine) — Fournit le coût de résolution le plus bas pour transmettre des paquets au périphérique racine.

Designated (Désigné) — Port ou LAG à travers lequel le périphérique désigné est rattaché au LAN.

Alternate (Autre) — Fournit un autre chemin vers le périphérique racine à partir de l'interface racine.

Backup (Sauvegarde) — Fournit un chemin de sauvegarde vers le chemin du port désigné en direction des feuilles de l'arbre maximal (Spanning Tree). Les ports de sauvegarde ne sont créés que lorsque deux ports sont connectés en boucle. Les ports de sauvegarde sont également créés lorsqu'un LAN possède au moins deux connexions à un segment partagé.

Disabled (Désactivé) — Le port ne participe pas au Spanning Tree (la liaison du port est désactivée).

Fast Link Operational Status (État opérationnel Fast Link) — Indique si le mode Fast Link (Liaison rapide) est activé ou désactivé pour le port ou le LAG. Si le mode Fast Link est activé pour un port, celui-ci passe automatiquement à l'état transmission.

Point-to-Point Admin Status (État admin point à point) — Active ou désactive l'établissement d'une liaison point à point ou permet au périphérique d'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 LCP (protocole de contrôle de liaison) pour configurer et tester la liaison de données. Après avoir établi une liaison et négocié des options en fonction des besoins du protocole LCP, le protocole PPP d'origine envoie des paquets NCP (protocole de contrôle de réseau) pour sélectionner et configurer un ou plusieurs protocoles de couche réseau. Lorsque tous les protocoles de couche réseau choisis ont été configurés, leurs paquets peuvent être envoyés sur la liaison. La liaison reste configurée pour des communications jusqu'à ce que des paquets LCP ou NCP explicites la fermeture ou jusqu'à ce qu'un événement extérieur survienne. Il s'agit du type de liaison de port de périphérique réel. Il peut être différent de l'état administratif.

Point-to-Point Operational Status (État opérationnel point à point) — État de fonctionnement du mode Point à point.

Activate Protocol Migrational Test (Activer le test de la migration de protocole) — Permet au protocole PPP d'envoyer des paquets LCP pour configurer et tester la liaison de données.

Activation du protocole RSTP

1. Ouvrez la page [Rapid Spanning Tree](#) (Protocole RSTP).
2. Définissez les champs **Point-to-Point Admin** (Admin point à point), **Point-to-Point Oper** (Fonctionnement point à point) et **Activate Protocol Migration** (Activer la migration de protocole).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le protocole RSTP est activé et le périphérique est mis à jour.

Définition des paramètres Rapid STP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des paramètres Rapid STP comme sur la page [Rapid Spanning Tree \(RSTP\)](#) (Protocole RSTP).

Tableau 7-63. Commandes CLI des paramètres RSTP

Commande CLI	Description
<code>spanning-tree link-type { point-to-point shared }</code>	Remplace le paramètre du type de liaison par défaut.
<code>spanning tree mode { stp rstp }</code>	Configure le protocole RSTP en cours d'exécution.
<code>clear spanning-tree detected-protocols [ethernet interface port-channel numéro-canal-port]</code>	Relance le processus de migration de protocole.
<code>show spanning-tree [ethernet interface port-channel numéro-canal-port]</code>	Affiche la configuration de Spanning Tree.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console(config)# interface ethernet g5

Console(config-if)# spanning-tree link-type
shared
```

Configuration des VLAN

Les VLAN sont des sous-groupes logiques d'un réseau local (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 un seul domaine, 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 par logiciel permettent de réduire le délai d'implémentation des modifications du réseau.

Les VLAN possèdent un nombre illimité de ports et peuvent être créés en fonction d'un périphérique ou de toute autre combinaison de connexions logiques, car ils sont gérés par logiciel au lieu d'être définis par des attributs physiques.

Les VLAN fonctionnent au niveau Couche 2. Du fait que les VLAN isolent le trafic à l'intérieur du VLAN, un routeur fonctionnant au niveau Couche 3 est nécessaire pour permettre l'acheminement du trafic entre les VLAN. Les routeurs de type 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.

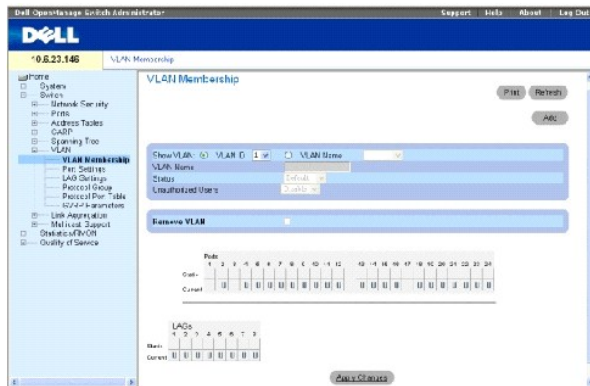
L'étiquetage de VLAN constitue une méthode de transmission des informations VLAN entre les groupes de VLAN. Il attache une étiquette aux en-têtes de paquets. L'étiquette VLAN indique le VLAN auquel le paquet appartient. Les étiquettes VLAN sont attachées au paquet soit par la station terminale, soit par le périphérique réseau. Elles contiennent également les informations de priorité réseau du VLAN. La combinaison des VLAN et du protocole GVRP permet de transmettre automatiquement les informations VLAN. Pour ouvrir la page **VLAN**, cliquez sur **Switch** (Commutateur) → **VLAN** dans l'arborescence.

Définition des membres d'un VLAN

La page VLAN Membership (Appartenance à un VLAN) contient des champs permettant de définir des groupes de VLAN. Le périphérique prend en charge

l'adresse de 4094 ID de VLAN à 256 VLAN. Tous les ports doivent posséder un PVID défini. Si aucune autre valeur n'est configurée, le PVID du VLAN par défaut est utilisé. Le VLAN numéro 1 est le VLAN par défaut et 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 7-102. Page Appartenance à un VLAN



Show VLAN (Afficher le VLAN) — Répertorie et affiche des informations VLAN spécifiques en fonction de l'ID ou du nom du VLAN.

VLAN Name (Nom du VLAN) — Nom du VLAN défini par l'utilisateur.

Status (État)— Indique le type de VLAN. Ce champ peut prendre les valeurs suivantes :

Dynamic (Dynamique) — Le VLAN a été créé de façon dynamique par le biais du protocole GVRP.

Static (Statique) — Le VLAN est défini par l'utilisateur.

Default (Par défaut) — Le VLAN est le VLAN par défaut.

Unauthorized Users (Utilisateurs non autorisés) — Permet ou non aux utilisateurs non autorisés d'accéder à un VLAN.

Remove VLAN (Supprimer le VLAN) — Supprime le VLAN de la table d'appartenance à un VLAN.

Ajout de nouveaux VLAN

1. Ouvrez la page VLAN Membership (Appartenance à un VLAN).
2. Cliquez sur **Ajouter**.

La page **Create New VLAN** (Créer un VLAN) s'ouvre.

3. Entrez un ID et un nom pour le VLAN.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau VLAN est ajouté et le périphérique est mis à jour.

Modification des groupes d'appartenance à un VLAN

1. Ouvrez 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 comme vous le désirez.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les informations relatives à l'appartenance à un VLAN sont modifiées et le périphérique est mis à jour.

Suppression des groupes d'appartenance à un VLAN

1. Ouvrez 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 le périphérique est mis à jour.

Définition des groupes d'appartenance à un VLAN à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des groupes d'appartenance à un VLAN comme indiqué dans la page VLAN Membership (Appartenance à un VLAN).

Tableau 7-64. Commandes CLI des groupes d'appartenance à un VLAN

Commande CLI	Description
<code>vlan database</code>	Passe en mode (VLAN) de configuration de l'interface.
<code>vlan {plage-vlan}</code>	Crée un VLAN.
<code>name chaîne</code>	Ajoute un nom à un VLAN.

Vous trouverez ci-dessous un exemple de commande CLI :

```
console(config)#vlan database

console(config-vlan)#vlan 1972

console(config-vlan)#exit

console(config)#interface vlan 1972

console(config-if)#name Marketing

console(config-if)#exit


console(config)#
```

Table d'appartenance des ports à un VLAN

La VLAN Port Membership Table (Table d'appartenance des ports à un VLAN) contient une table des ports permettant d'affecter des ports à des VLAN. Pour affecter à un port l'appartenance à un VLAN, vous devez basculer entre les différentes valeurs de Port Control (Contrôle des ports). Les ports peuvent avoir les valeurs suivantes :

Tableau 7-65. Table d'appartenance des ports à un VLAN

Contrôle du port	Définition
T	L'interface est membre d'un VLAN. Tous les paquets transmis par l'interface sont marqués. Les paquets contiennent des informations VLAN.
V	L'interface est membre d'un VLAN. Les paquets transmis par l'interface ne sont pas marqués.
F	L'appartenance à un VLAN n'est pas accordée à l'interface.
Blanc	L'interface n'est pas membre d'un VLAN. Les paquets associés à l'interface ne sont pas transmis.

 **REMARQUE** : Les ports qui sont membres d'un LAG ne s'affichent pas dans la table d'appartenance des ports à un VLAN.

La 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. Ouvrez la page VLAN Membership (Appartenance à un VLAN).
2. Cliquez sur le bouton **VLAN ID** (ID 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 une valeur au port.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port est affecté au groupe de VLAN et le périphérique est mis à jour.

Suppression d'un VLAN

1. Ouvrez la page VLAN Membership (Appartenance à un VLAN).
2. Cliquez sur le bouton **VLAN ID** (ID VLAN) ou **VLAN Name** (Nom du VLAN) et sélectionnez un VLAN dans le menu déroulant.
3. Cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le VLAN sélectionné est supprimé et le périphérique est mis à jour.

Affectation de ports à des groupes de VLAN à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affectation de ports à des groupes de VLAN.

Tableau 7-66. Commandes CLI d'affectation de ports à des groupes de VLAN

Commande CLI	Description
<code>switchport general acceptable-frame-types tagged-only</code>	Ignore les trames non marquées en entrée.
<code>switchport forbidden vlan {add liste-vlan remove liste-vlan}</code>	Interdit l'ajout de VLAN spécifiques au port.
<code>switchport mode { access trunk general }</code>	Configure le mode d'appartenance à un VLAN d'un port.
<code>switchport access vlan id-vlan</code>	Configure l'ID du VLAN lorsque l'interface est en mode d'accès.
<code>switchport trunk allowed vlan { add vlan-list remove vlan-list }</code>	Ajoute ou supprime des VLAN d'un port de segment.
<code>switchport trunk native vlan id-vlan</code>	Configure le port en tant que membre du VLAN et l'ID VLAN en tant que «PVID (ID VLAN par défaut du port)».

<code>switchport general allowed vlan add <i>liste-vlan</i> [tagged untagged]</code>	Ajoute ou supprime des VLAN d'un port général.
<code>switchport general pvid <i>id-vlan</i></code>	Configure le PVID lorsque l'interface est en mode Général.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# vlan database

Console (config-vlan)# vlan 23-25

Console (config-vlan)# exit

Console(config)# interface vlan 23

Console (config-if)# name Marketing

Console (config-if)# exit

Console (config)# interface ethernet g8

Console (config-if)# switchport mode access

Console (config-if)# switchport access vlan 23

Console (config-if)# exit

Console (config)# interface ethernet g9

Console (config-if)# switchport mode trunk

Console (config-if)# swithport mode trunk allowed vlan add 23-25

Console (config-if)# exit

Console (config)# interface ethernet g10

Console (config-if)# switchport mode general

Console (config-if)# switchport general allowed vlan add 23,25 tagged
```

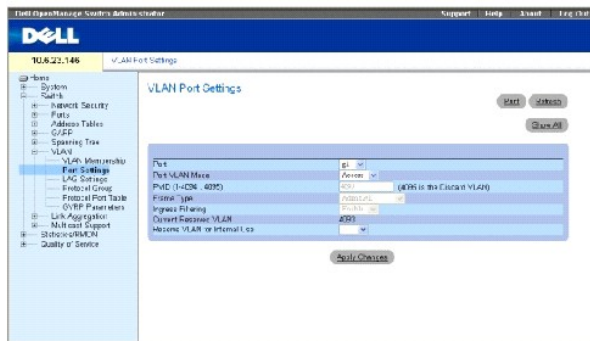
```
Console (config-if)# switchport general pvid 25
```

Définition des paramètres des ports VLAN

La page [VLAN Port Settings](#) (Paramètres des ports VLAN) contient des champs permettant de gérer les ports qui font partie d'un VLAN. L'ID VLAN par défaut du port (PVID) est configuré sur la page [VLAN Port Settings](#) (Paramètres des ports VLAN). Tous les paquets non marqués arrivant au périphérique sont marqués par le PVID du port.

Pour ouvrir la page [VLAN Port Settings](#) (Paramètres des ports VLAN), cliquez sur **Switch** (Commutateur) → **VLAN** → **Port Settings** (Paramètres des ports) dans l'arborescence.

Figure 7-103. Paramètres des ports VLAN



Port — Numéro de 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 un ou plusieurs VLAN et chaque VLAN est défini par l'utilisateur comme étant marqué ou non marqué (Full 802.1Q mode).

Access (Accès) — Le port appartient à un seul VLAN non marqué. Lorsqu'un port est en mode Access, les types de paquets acceptés sur ce port ne peuvent pas être désignés. Le filtrage d'entrée ne peut pas être activé/désactivé sur un port d'accès.

Trunk (Segment) — Le port appartient à des VLAN dans lesquels tous les ports sont marqués (sauf pour un port qui ne peut pas être non marqué).

PVID — Affecte un ID VLAN aux paquets non marqués. Les valeurs possibles pour ce champ sont 1 à 4094. Le VLAN 4095 est considéré par la norme comme un VLAN de mise au rebut. Les paquets dirigés vers ce VLAN sont ignorés.

Frame Type (Type de trames) — Type de paquets accepté sur le port. Ce champ peut prendre les valeurs suivantes :

Admit Tag Only (Admettre uniquement les paquets marqués) — Seuls les paquets marqués sont acceptés par le port.

Admit All (Admettre tout) — Les paquets marqués et non marqués sont acceptés sur le port.

Ingress Filtering (Filtrage d'entrée) — Active ou désactive le filtrage d'entrée sur le port. Le filtrage d'entrée rejette les paquets associés à des VLAN qui ne contiennent pas le LAG spécifique.

Current Reserve VLAN (VLAN de réserve actuel) — VLAN actuellement désigné par le système comme VLAN réservé.

Reserve VLAN for Internal Use (VLAN de réserve à usage interne) — VLAN sélectionné par l'utilisateur pour être le VLAN réservé, s'il n'est pas utilisé par le système.

Affectation des paramètres de port

1. Ouvrez la page [VLAN Port Settings](#) (Paramètres des ports VLAN).
2. Sélectionnez le port à paramétrer dans le menu déroulant **Port**.
3. Renseignez les autres champs de la page.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des ports VLAN sont définis et le périphérique est mis à jour.

Affichage de la table des ports VLAN

1. Ouvrez la page [VLAN Port Settings](#) (Paramètres des ports VLAN).
2. Cliquez sur **Show All** (Afficher tout).

La **table des ports VLAN** s'ouvre.

Affectation de ports à des groupes de VLAN à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affectation de ports à des groupes de VLAN.

Tableau 7-67. Commandes CLI des ports VLAN

Commande CLI	Description
<code>switchport mode { access trunk general }</code>	Configure le mode d'appartenance VLAN d'un port.
<code>switchport trunk native vlan <i>id-vlan</i></code>	Configure le port en tant que membre du VLAN et l'ID VLAN en tant que «PVID (ID VLAN par défaut du port)».
<code>switchport general pvid <i>id-vlan</i></code>	Configure l'ID VLAN du port (PVID) lorsque l'interface est en mode Général.
<code>switchport general allowed vlan add <i>liste-vlan</i> [tagged untagged]</code>	Ajoute ou supprime des VLAN d'un port général.
<code>switchport general acceptable-frame-types tagged-only</code>	Ignore les paquets non marqués en entrée.
<code>switchport general ingress-filtering disable</code>	Désactive le filtrage d'entrée d'un port.
<code>shutdown</code>	Désactive les interfaces.
<code>set interface active { ethernet <i>interface</i> port-channel <i>numéro-canal-port</i> }</code>	Réactive une interface qui a été arrêtée pour des raisons de sécurité.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface range ethernet g18-20

Console (config-if)# switchport mode access

Console (config-if)# switchport general pvid 234
```

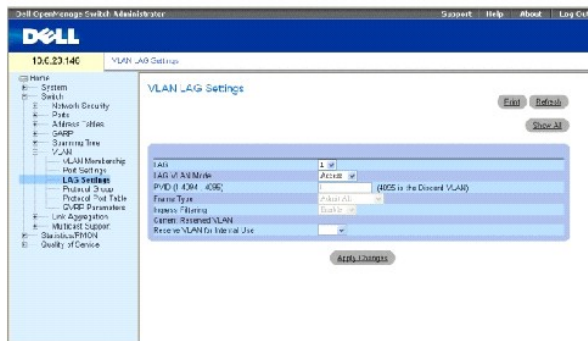
```
Console (config-if)# switchport general allowed vlan add 1,2,5,6 tagged
```

```
Console (config-if)# switchport general ingress-filtering disable
```

Définition des paramètres des LAG VLAN

La page [VLAN LAG Setting](#) (Paramètres des LAG VLAN) fournit des paramètres permettant de gérer les LAG qui font partie d'un VLAN. Les VLAN sont composés de ports ou de LAG individuels. Les paquets non marqués intégrant le périphérique sont marqués de l'ID des LAG spécifié par le PVID. Pour ouvrir la page [VLAN LAG Setting](#) (Paramètres des LAG VLAN), cliquez sur **Switch** (Commutateur) → **VLAN** → **LAG Settings** (Paramètres des LAG) dans l'arborescence.

Figure 7-104. Paramètres des LAG VLAN



LAG — Numéro de LAG inclus dans le VLAN.

LAG VLAN Mode (Mode VLAN du LAG) — Mode du VLAN du LAG. Ce champ peut prendre les valeurs suivantes :

General (Général) — Le LAG appartient à un ou plusieurs VLAN et chaque VLAN est défini par l'utilisateur comme étant marqué ou non marqué (Full 802.1Q mode).

Access (Accès) — Le LAG appartient à un seul VLAN non marqué.

Trunk (Segment) — Le LAG appartient à des VLAN dans lesquels tous les ports sont marqués (sauf pour un VLAN natif unique facultatif).

PVID — Affecte un ID VLAN aux paquets non marqués. Les valeurs possibles pour ce champ sont 1 à 4095. Le VLAN 4095 est considéré par la norme comme un VLAN de mise au rebut. Les paquets dirigés vers ce VLAN sont ignorés.

Frame Type (Type de trames) — Type de paquets accepté sur le LAG. Ce champ peut prendre les valeurs suivantes :

Admit Tag Only (Admettre uniquement les paquets marqués) — Seuls les paquets marqués sont acceptés par le LAG.

Admit All (Admettre tout) — Les paquets marqués et non marqués sont acceptés sur le LAG.

Ingress Filtering (Filtrage d'entrée) — Active ou désactive le filtrage d'entrée par le LAG. Le filtrage d'entrée rejette les paquets associés à des VLAN qui ne contiennent pas le port spécifique.

Current Reserve VLAN (VLAN de réserve actuel) — VLAN actuellement désigné comme VLAN réservé.

Reserve VLAN for Internal Use (VLAN de réserve à usage interne) — VLAN désigné comme le VLAN réservé après une réinitialisation du périphérique.

Affectation des paramètres LAG VLAN :

1. Ouvrez la page [VLAN LAG Setting](#) (Paramètres des LAG VLAN).
2. Sélectionnez un LAG dans le menu déroulant **LAG** et renseignez les champs de la page.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres des LAG VLAN sont définis et le périphérique est mis à jour.

Affichage de la table des LAG VLAN

1. Ouvrez la page [VLAN LAG Setting](#) (Paramètres des LAG VLAN).
2. Cliquez sur **Show All** (Afficher tout).

La table des LAG VLAN s'ouvre.

Affectation de LAG à des groupes de VLAN à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affectation de LAG à des groupes de VLAN comme sur la page [VLAN LAG Setting](#) (Paramètres des LAG VLAN).

Tableau 7-68. Commandes CLI d'affectation de LAG à des VLAN

Commande CLI	Description
<code>switchport mode { access trunk general }</code>	Configure le mode d'appartenance VLAN d'un port.
<code>switchport trunk native vlan <i>id-vlan</i></code>	Configure le port en tant que membre du VLAN et l'ID VLAN en tant que PVID (ID VLAN par défaut du port).
<code>switchport general pvid <i>id-vlan</i></code>	Configure l'ID VLAN du port (PVID) lorsque l'interface est en mode Général.
<code>switchport general allowed vlan add <i>liste-vlan</i> [tagged untagged]</code>	Ajoute ou supprime des VLAN d'un port général.
<code>switchport general acceptable-frame-type tagged-only</code>	Ignore les paquets non marqués en entrée.
<code>switchport general ingress-filtering disable</code>	Désactive le filtrage d'entrée d'un port.

Vous trouverez ci-dessous un exemple de commande 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

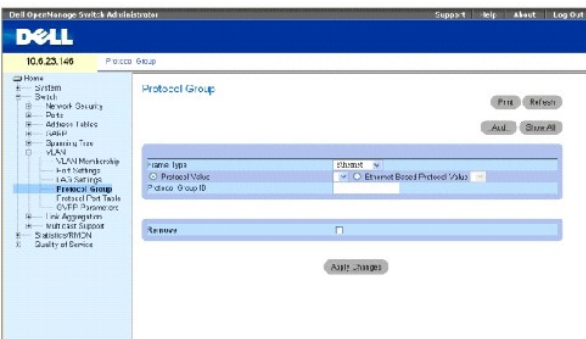
console(config-if)#exit

```

Définitions des groupes de protocoles VLAN

La page [Protocol Group](#) (Groupe de protocoles) fournit des paramètres permettant de configurer des types de trames dans des groupes de protocoles spécifiques. Pour ouvrir la page [Protocol Group](#) (Groupe de protocoles), cliquez sur **Switch** (Commutateur) → **VLAN** → **Protocol Group** (Groupe de protocoles) dans l'arborescence.

Figure 7-105. Groupe de protocoles



Frame Type (Type de trames) — Type du paquets. Ce champ peut prendre les valeurs **Ethernet**, **RFC1042** et **LLC Other** (LLC autre).

Protocol Value (Valeur du protocole) — Nom du protocole défini par l'utilisateur.

Ethernet-Based Protocol Value (Valeur du protocole basé sur Ethernet) — Type de groupe de protocoles Ethernet. Ce champ peut prendre les valeurs IP, IPX et **IPv6**.

Protocol Group ID (ID du groupe de protocoles) — Numéro ID du groupe VLAN.

Remove (Supprimer) — Supprime l'adressage de groupes trame-protocole, si le groupe de protocoles à supprimer n'est pas configuré sur ce port de protocoles.

Ajout d'un groupe de protocoles

1. Ouvrez la page [Protocol Group](#) (Groupe de protocoles).
2. Cliquez sur **Ajouter**.

La page **Add Protocol to Group** (Ajouter un protocole au groupe) s'ouvre.

3. Renseignez les champs de cette page.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le groupe de protocoles est affecté et le périphérique est mis à jour.

Affectation des paramètres de groupe de protocoles VLAN

1. Ouvrez la page [Protocol Group](#) (Groupe de protocoles).
2. Renseignez les champs de cette page.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres du groupe de protocoles VLAN sont définis et le périphérique est mis à jour.

Suppression de protocoles dans la table des groupes de protocoles

1. Ouvrez la page [Protocol Group](#) (Groupe de protocoles).
2. Cliquez sur **Show All** (Afficher tout).

La **table des groupes de protocoles** s'ouvre.

3. Sélectionnez **Remove** (Supprimer) pour les groupes de protocoles à supprimer.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Définition des groupes de protocoles VLAN à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration de groupes de protocoles.

Tableau 7-69. Commandes CLI des groupes de protocoles VLAN

Commande CLI	Description
<code>map protocol <i>protocole</i> [<i>encapsulation</i>] protocols-group <i>groupe</i></code>	Adresse un protocole à un groupe de protocoles. Les groupes de protocoles sont utilisés pour l'affectation des VLAN basée sur le protocole.

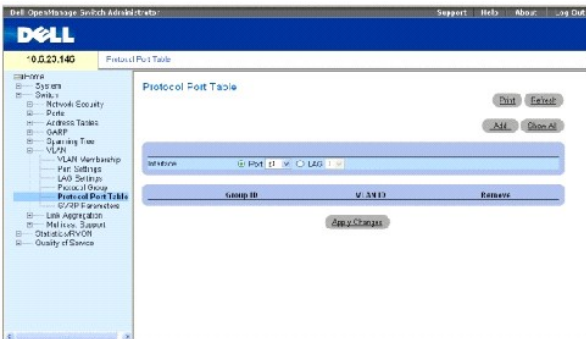
Vous trouverez ci-dessous un exemple de mise en correspondance du protocole IP-ARP avec le groupe «213» :

```
Console (config)# vlan database
Console (config-vlan)# map protocol ip-arp protocols-group 213
```

Ajout de ports de protocole

La page [Protocol Port](#) (Port de protocole) permet d'ajouter des interfaces aux groupes de protocoles. Pour ouvrir la page [Protocol Port](#) (Port de protocole), cliquez sur **Switch** (Commutateur) → **VLAN** → **Protocol Port** (Port de protocole) dans l'arborescence.

Figure 7-106. Port de protocole



Interface — Numéro du port ou du LAG ajouté à un groupe de protocoles.

Group ID (ID du groupe) — ID du groupe de protocoles auquel l'interface est ajoutée. Les ID des groupes de protocoles sont définis dans la table des groupes de protocoles.

VLAN ID (1-4095) (ID VLAN [1-4095]) — Lie l'interface à un ID VLAN défini par l'utilisateur. L'ID VLAN est défini sur la page [Create a New VLAN](#) (Créer un VLAN). Les ports de protocoles peuvent être rattachés à un ID VLAN ou à un nom de VLAN.

REMARQUE : Le VLAN 4095 est le VLAN de mise au rebut.

Ajout d'un port de protocole

REMARQUE : Les ports de protocoles peuvent être définis uniquement sur des ports définis comme General (Général) sur la page [VLAN Port Settings](#) (Paramètres des ports VLAN).

1. Ouvrez la page [Protocol Port](#) (Port de protocoles).
2. Cliquez sur **Ajouter**.

La page **Add Protocol Port** (Ajouter un port de protocoles) s'ouvre.

3. Renseignez les champs de la fenêtre.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau groupe de protocoles VLAN est ajouté à la **Protocol Port Table** (Table des ports de protocole) et le périphérique est mis à jour.

Définition des ports de protocole à l'aide de commandes CLI

Le tableau suivant récapitule la commande CLI équivalente pour la définition de ports de protocoles.

Tableau 7-70. Commandes CLI des ports de protocoles

Commande CLI	Description
<code>switchport general map protocols-group groupe vlan id-vlan</code>	Configure une règle de classification basée sur un protocole.

Vous trouverez ci-dessous un exemple de règle de classification basée sur un protocole pour le groupe de protocoles 1 du VLAN 8 :

```
Console (config-if)# switchport general map protocols-group 1 vlan 8
```

Configuration du protocole GVRP

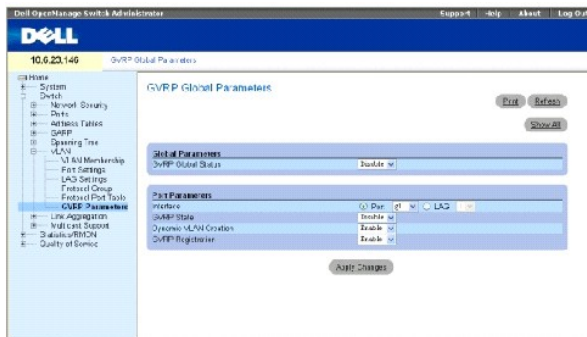
Le protocole GVRP (GARP VLAN Registration Protocol) est fourni spécifiquement pour la diffusion automatique des informations relatives à l'appartenance aux VLAN entre les ponts compatibles VLAN. Le protocole GVRP permet aux ponts compatibles VLAN d'apprendre automatiquement l'adressage des ports VLAN sans avoir à configurer individuellement chaque pont et à enregistrer l'appartenance à un VLAN.

Pour assurer le bon fonctionnement du protocole GVRP, définissez le nombre maximal de VLAN GVRP sur une valeur dépassant de façon significative la somme des deux valeurs suivantes :

- 1 Le nombre de tous les VLAN statiques à la fois actuellement configurés et en voie d'être configurés.
- 1 Le nombre de tous les VLAN dynamiques participant au protocole GVRP à la fois actuellement configurés (le nombre initial de VLAN GVRP dynamiques est de 128) et en voie d'être configurés.

La page **GVRP Global Parameters** (Paramètres globaux GVRP) permet d'activer le protocole GVRP globalement. Vous pouvez également activer le protocole GVRP par interface. Pour ouvrir la page [GVRP Parameters](#) (Paramètres GVRP), cliquez sur **Switch** (Commutateur) → **VLAN** → **GVRP Parameters** (Paramètres GVRP) dans l'arborescence.

Figure 7-107. Paramètres GVRP



GVRP Global Status (État global GVRP) — Active ou désactive le protocole GVRP sur le périphérique. Par défaut, le protocole GVRP est désactivé.

Interface — Port ou LAG sur lequel GVRP est activé.

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.

GVRP Registration (Enregistrement GVRP) — État de l'enregistrement GVRP.

Activation du protocole GVRP sur le périphérique

1. Ouvrez la page GVRP Global Parameters (Paramètres globaux GVRP).
2. Sélectionnez **Enable** (Activer) dans le champ **GVRP Global Status** (État global GVRP).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le protocole GVRP est activé sur le périphérique.

Activation de l'enregistrement de VLAN par le biais de GVRP

1. Ouvrez la page GVRP Global Parameters (Paramètres globaux GVRP).
2. Sélectionnez **Enable** (Activer) dans le champ **GVRP Global Status** (État global GVRP) de l'interface concernée.
3. Sélectionnez **Enable** (Activer) dans le champ **GVRP Registration** (Enregistrement GVRP).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'enregistrement de VLAN par le biais de GVRP est activé sur le port et le périphérique est mis à jour.

Configuration du protocole GVRP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration du protocole GVRP comme indiqué dans la page GVRP Global Parameters (Paramètres globaux GVRP).

Tableau 7-71. Commandes CLI des paramètres globaux GVRP

Commande CLI	Description
<code>gvrp enable</code> (global)	Active le protocole GVRP de façon globale.
<code>gvrp enable</code> (interface)	Active le protocole GVRP sur une interface.
<code>gvrp vlan-creation-forbid</code>	Active ou désactive la création dynamique de VLAN.
<code>gvrp registration-forbid</code>	Désenregistre tous les VLAN dynamiques et empêche l'enregistrement dynamique de VLAN sur le port.
<code>show gvrp configuration</code> [ethernet interface] [port-channel numéro-canal-port]	Affiche les informations de configuration GVRP, y compris les valeurs des temporisateurs, si le protocole GVRP et la création dynamique de VLAN sont activés et quels ports exécutent le protocole GVRP.
<code>show gvrp error-statistics</code> [ethernet interface] [port-channel numéro-canal-port]	Affiche les statistiques des erreurs du protocole GVRP.
<code>show gvrp statistics</code> [ethernet interface] [port-channel numéro-canal-port]	Affiche les statistiques du protocole GVRP.
<code>clear gvrp statistics</code> [ethernet interface] [port-channel numéro-canal-port]	Efface toutes les statistiques du protocole GVRP.

Vous trouverez ci-dessous un exemple de commande CLI :

```
console(config)# gvrp enable

console(config)# interface ethernet g1

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

La fonctionnalité GVRP est actuellement activée sur le périphérique.

Nombre max. de VLAN : 223

```

Port (s)	État GVRP	Enregistrement	Création de VLAN dynamique	Temporisateurs (millisecondes) Join	Leave	Leave All
---	-----	-----	-----	-----	-----	-----
g1	Activé	Interdit	Désactivée	200	900	10 000
g2	Désactivé	Normal (Standard)	Activée	200	600	10 000

Agrégation des ports

La fonction d'agrégation des ports optimise l'utilisation des ports en reliant des ports de façon à former un LAG (Link Aggregated Group) unique. L'agrégation des ports multiplie la bande passante entre les périphériques, augmente la flexibilité des ports et assure la redondance des liaisons. Le périphérique prend en charge jusqu'à huit LAG par système et huit ports par LAG par périphérique.

Chaque LAG est composé de ports ayant la même vitesse, configurés en mode Duplex intégral. Les ports d'un LAG peuvent être composés de différents types de supports (UTP/Fiber ou différents types de fibres) à condition qu'ils fonctionnent à la même vitesse.

Les liaisons agrégées peuvent être affectées manuellement ou automatiquement à travers l'activation du protocole LACP (Link Aggregation Control Protocol) sur les liaisons appropriées. Le périphérique assure une fonction d'équilibrage des charges entre les LAG (LAG Load Balancing) basée à la fois sur les adresses MAC source et les adresses MAC de destination.

Les liaisons agrégées sont considérées comme un seul et unique port logique par le système. Plus précisément, la liaison agrégée possède des attributs de port similaires à ceux d'un port non agrégé, notamment la négociation automatique, la vitesse, le réglage du mode Duplex, etc.

Le périphérique prend en charge à la fois les LAG statiques et les LAG LACP (Link Aggregation Control Protocol). Les LAG LACP négocient les liaisons de ports agrégées avec d'autres ports LACP situés sur un périphérique différent. Si les autres ports du périphérique sont également des ports LACP, les périphériques établissent un groupe de liaisons agrégées (LAG) entre elles.

Utilisez les consignes suivantes lorsque vous ajoutez des ports à un LAG :

- 1 Aucune interface de type Couche 3 n'est définie sur le port.
- 1 Le port n'appartient à aucun VLAN.
- 1 Le port n'appartient à aucun autre LAG.
- 1 Le port n'est pas un port miroir.
- 1 La priorité 802.1p du port est égale à la priorité 802.1p du LAG.
- 1 Le mode Confiance QoS n'est pas désactivé sur le port.
- 1 Le protocole GVRP n'est pas activé.

 **REMARQUE** : Les ports peuvent être configurés comme des ports LACP uniquement s'ils ne font pas partie d'un LAG configuré précédemment.

Le périphérique utilise une fonction de hachage pour déterminer quelles trames sont transmises sur quel membre d'un LAG. La fonction de hachage effectue un équilibrage de charge à base de statistiques entre les membres des liaisons agrégées. Le périphérique considère une liaison agrégée comme un seul et même port logique.

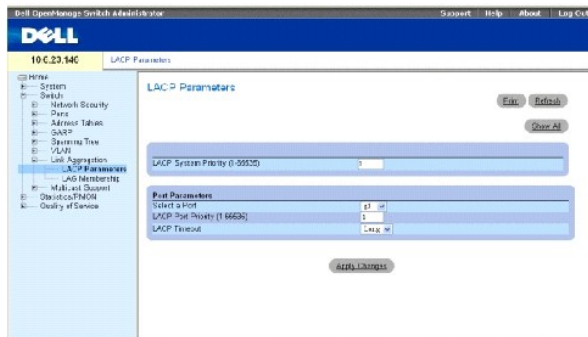
Chaque liaison agrégée a un type de port de liaison agrégée, notamment les types de port Gigabit Ethernet. Des ports ne peuvent être ajoutés à une liaison agrégée que s'ils sont du même type. Lorsque des ports sont supprimés d'une liaison agrégée, leurs paramètres d'origine sont rétablis. Pour ouvrir la page **Link Aggregation** (Agrégation de liaisons), cliquez sur **Switch** (Commutateur) → **Link Aggregation** (Agrégation de liaisons) dans l'arborescence.

Définition des paramètres LACP

La page **LACP Parameters** (Paramètres LACP) contient des champs permettant de configurer des LAG LACP. Les ports agrégés peuvent être reliés en groupes de ports à agrégation de liaisons. Chaque groupe est composé de ports ayant la même vitesse.

Les liaisons agrégées peuvent être définies manuellement ou établies automatiquement à travers l'activation du protocole LACP (Link Aggregation Control Protocol) sur les liaisons appropriées. 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 7-108. Paramètres LACP



LACP System Priority (Priorité LACP du système) — Indique la valeur de priorité LACP pour les 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 délai et priorité sont affectées.

LACP Port Priority (1-65535) (Priorité LACP du port [1-65535]) — Indique la valeur de priorité LACP pour le port.

LACP Timeout (Délai d'expiration LACP) — Délai d'expiration LACP administratif. 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 des liaisons

1. Ouvrez la page [LACP Parameters](#) (Paramètres LACP).
2. Renseignez le champ **LACP System Priority** (Priorité LACP du système).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Définition des paramètres des ports d'agrégation des liaisons

1. Ouvrez la page [LACP Parameters](#) (Paramètres LACP).
2. Renseignez les champs de la zone **Port Parameters** (Paramètres des ports).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Affichage de la table des paramètres LACP

1. Ouvrez la page [LACP Parameters](#) (Paramètres LACP).
2. Cliquez sur **Show All** (Afficher tout).

La **table des paramètres LACP** s'ouvre.

Configuration des paramètres LACP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des paramètres LACP comme sur la page [LACP Parameters](#) (Paramètres LACP).

Tableau 7-72. Commandes CLI des paramètres LACP

Commande CLI	Description
<code>lACP system-priority <i>valeur</i></code>	Configure la priorité du système.
<code>lACP port-priority <i>valeur</i></code>	Configure la valeur de priorité des ports physiques.
<code>lACP timeout {long short}</code>	Affecte un délai d'expiration LACP administratif.
<code>show lACP ethernet <i>interface</i> [<i>parameters</i> <i>statistics</i> <i>protocol-state</i>]</code>	Affiche des informations LACP pour les ports ethernet.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# lACP system-priority 120

Console (config)# interface ethernet g1

Console (config-if)# lACP port-priority 247

Console (config-if)# lACP timeout long
```

```

Console (config-if)# end

Console# show lacp ethernet gi statistics

Statistiques LACP du port gi :

PDU LACP envoyés : 2

PDU LACP reçus : 2

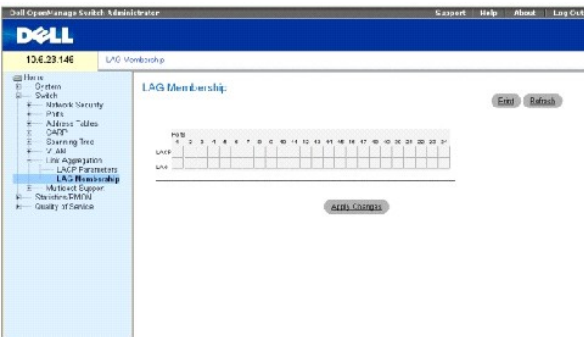
```

Définition de l'appartenance à un LAG

La page [LAG Membership](#) (Appartenance à un LAG) contient des champs permettant d'affecter des ports à des LAG. Les LAG peuvent contenir jusqu'à 8 ports. Lorsqu'un port est ajouté à un LAG, il acquiert les propriétés du LAG. Si le port ne peut pas être configuré avec les propriétés du LAG, une interruption est générée et le port fonctionne avec ses paramètres par défaut.

La page [LAG Membership](#) (Appartenance à un LAG) contient des champs permettant d'affecter des ports à des LAG. Pour ouvrir la page [LAG Membership](#) (Appartenance à un LAG), cliquez sur **Switch** (Commutateur) → **Link Aggregation** (Agréation de liaisons) → **LAG Membership** (Appartenance à un LAG) dans l'arborescence.

Figure 7-109. Appartenance à un LAG



LACP — Ajoute le port à un LAG par le biais du protocole LACP.

LAG — Ajoute un port à un LAG et indique le LAG spécifique auquel le port appartient.

Configuration d'un port sur LAG ou LACP

1. Ouvrez la page [LAG Membership](#) (Appartenance à un LAG).
2. Sur la ligne des LAG (deuxième ligne), basculez le bouton sur un numéro spécifique pour ajouter ou supprimer le port de ce numéro de LAG.
3. Sur la ligne des LACP (première ligne), basculez le bouton sous le numéro du port pour assigner le LACP ou le LAG statique.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port est ajouté au LAG ou au LACP et le périphérique est mis à jour.

Affectation de ports à des LAG à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affectation de ports à des LAG comme sur la page [LAG Membership](#) (Appartenance à un LAG).

Tableau 7-73. Commandes CLI d'appartenance à un LAG

Commande CLI	Description
<code>interface port-channel numéro-canal-port</code>	Passer en mode de configuration de l'interface d'un canal de port spécifique.
<code>channel-group numéro-canal-port mode {on auto}</code>	Associer un port à un canal de port. Utilisez la forme «no» de cette commande pour supprimer la configuration du groupe de canal de l'interface.
<code>show interfaces port-channel [numéro-canal-port]</code>	Afficher des informations sur le canal de port.

Vous trouverez ci-dessous un exemple de commande CLI :

```
console# config
console(config)# interface ethernet g1
console(config-if)# channel-group 1 mode on
console(config-if)# 01-Jan-2000 01:47:18 %LINK-W-Down: canal1


console(config-if)#
```

Prise en charge du transfert multidiffusion

La transmission multidiffusion permet la diffusion d'un même paquet à plusieurs destinations. Le service de multidiffusion de couche 2 est basé sur un commutateur de couche 2 qui reçoit un seul paquet destiné à une adresse de multidiffusion spécifique. La transmission multidiffusion crée des copies de ce paquet et transmet les paquets aux ports appropriés.

Le périphérique prend en charge les fonctions suivantes :

- 1 **Forwarding L2 Multicast Packets** (Transmission de paquets multidiffusion de couche 2) — Activée par défaut et non configurable.

 **REMARQUE** : Le système prend en charge le filtrage multidiffusion pour 63 groupes de multidiffusion.

- 1 **Filtering L2 Multicast Packets** (Filtrage des paquets multidiffusion de couche 2) — Active le transfert de paquets de couche 2 vers des interfaces. Si le filtrage multidiffusion est désactivé, les paquets multidiffusion vont inonder tous les ports appropriés.

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

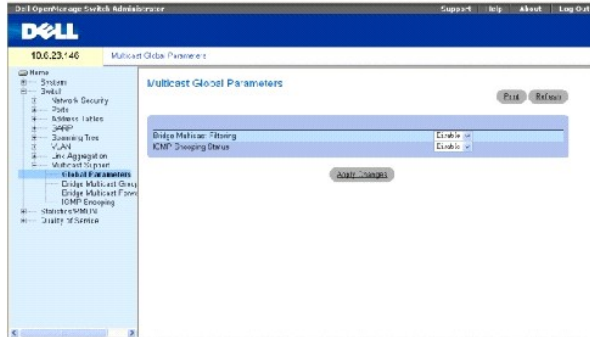
La commutation de type Couche 2 transmet des paquets multidiffusion vers tous les ports du VLAN approprié par défaut et traite le paquet comme une transmission de multidiffusion. Ce type de transfert de trafic est opérationnel, dans le sens où tous les ports/noeuds appropriés reçoivent une copie de la trame ; toutefois, les ports/noeuds reçoivent également des trames non appropriées nécessaires uniquement pour un sous-ensemble de ports de ce VLAN. Les filtres de transmission multidiffusion permettent de transmettre des paquets de type Couche 2 à des sous-ensembles de ports définis dans la base de données de filtrage multidiffusion.

Lorsque la surveillance IGMP est activée de façon globale, le circuit intégré ASIC de commutation est programmé pour transmettre tous les paquets IGMP à 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 et 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 ce groupe de multidiffusion. D'où la création de la base de données de filtrage

multidiffusion.

La page [Multicast Global Parameters](#) (Paramètres globaux de multidiffusion) contient des champs permettant d'activer la surveillance IGMP sur le périphérique. Pour ouvrir la page [Multicast Global Parameters](#) (Paramètres globaux de multidiffusion), cliquez sur **Switch** (Commutateur) → **Multicast Support** (Prise en charge de la multidiffusion) → **Global Parameters** (Paramètres globaux) dans l'arborescence.

Figure 7-110. Paramètres globaux de multidiffusion



Bridge Multicast Filtering (Filtrage multidiffusion par ponts) — Active ou désactive le filtrage multidiffusion par ponts. Cette option est désactivée par défaut. La surveillance IGMP ne peut être activée que si le filtrage multidiffusion par ponts est activé.

IGMP Snooping Status (État de la surveillance IGMP) — Active ou désactive la surveillance IGMP sur le périphérique. Cette option est désactivée par défaut.

Activation du filtrage multidiffusion par ponts sur le périphérique

1. Ouvrez la page [Multicast Global Parameters](#) (Paramètres globaux de multidiffusion).
2. Sélectionnez **Enable** (Activer) dans le champ **Bridge Multicast Filtering** (Filtrage multidiffusion par ponts).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La multidiffusion par ponts est activée sur le périphérique.

Activation de la surveillance IGMP sur le périphérique

1. Ouvrez la page [Multicast Global Parameters](#) (Paramètres globaux de multidiffusion).
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 le périphérique.

Activation de la transmission multidiffusion et de la surveillance IGMP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'activation du transfert multidiffusion et de la surveillance IGMP comme sur la page [Multicast Global Parameters](#) (Paramètres globaux de multidiffusion).

Tableau 7-74. Commandes CLI du transfert multidiffusion et de la surveillance

Commande CLI	Description
<code>bridge multicast filtering</code>	Active le filtrage des adresses de multidiffusion.
<code>ip igmp snooping</code>	Active la surveillance IGMP (Internet Group Management Protocol).

Vous trouverez ci-dessous un exemple de commande CLI :

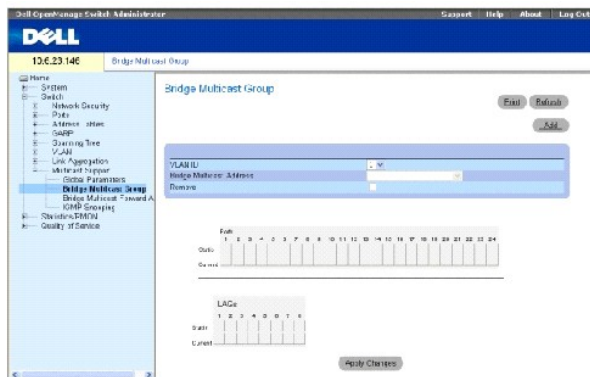
```
Console (config)# bridge multicast filtering
Console (config)# ip igmp snooping
```

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 rattachés au groupe de service de multidiffusion dans les tables **Ports** et **LAG**. Les tables **Port** et **LAG** 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 aux groupes de services de multidiffusion d'être créés. La page [Bridge Multicast Group](#) (Groupe de multidiffusion par ponts) permet également d'affecter des ports à un groupe spécifique d'adresses de service de multidiffusion.

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 Address** (Adresse de multidiffusion par ponts) dans l'arborescence.

Figure 7-111. Groupe de multidiffusion par ponts



VLAN ID (ID 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 IP/adresse MAC du groupe de multidiffusion.

Remove (Supprimer) — Supprime une adresse de multidiffusion par ponts.

Ports — Ports qui peuvent être ajoutés à un service de multidiffusion.

LAG — LAG qui peuvent être ajoutés à un service de multidiffusion.

Le tableau suivant récapitule les paramètres de gestion des membres des ports et des LAG IGMP :

Tableau 7-75. Paramètres de contrôle de la table des membres des ports/LAG IGMP

Contrôle du port	Définition
D	Indique que le port/LAG a rejoint le groupe de multidiffusion de façon dynamique à la ligne <i>Current</i> (Actuel).
S	Rattache le port au groupe de multidiffusion en tant que membre statique à la ligne <i>Static</i> (Statique).

	Indique que le port/LAG a rejoint le groupe de multidiffusion de façon statique à la ligne <i>Current</i> (Actuel).
F	Interdit.
Blanc	Indique que le port n'est pas rattaché à ce groupe de multidiffusion.

Ajout d'adresses de multidiffusion par ponts

1. Ouvrez la page [Bridge Multicast Group](#) (Groupe de multidiffusion par ponts).
2. Cliquez sur **Ajouter**.

La page [Add Bridge Multicast Group](#) (Ajouter un groupe de multidiffusion par ponts) s'ouvre :

Figure 7-112. Ajouter un groupe de multidiffusion par ponts

3. Définissez les champs **VLAN ID** (ID VLAN) et **New Bridge Multicast Address** (Nouvelle adresse de multidiffusion par ponts).
4. Faites basculer un port vers la valeur **S** pour rattacher ce port à un groupe de multidiffusion sélectionné.
5. Faites basculer un port vers la valeur **F** pour l'empêcher de se joindre à ce groupe de multidiffusion.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse de multidiffusion par ponts est affectée au groupe de multidiffusion et le périphérique est mis à jour.

Définition des ports pour qu'ils reçoivent un service de multidiffusion

1. Ouvrez la page [Bridge Multicast Group](#) (Groupe de multidiffusion par ponts).
2. Définissez les champs **VLAN ID** (ID VLAN) et **Bridge Multicast Address** (Adresse de multidiffusion par ponts).
3. Faites basculer un port vers la valeur **S** pour rattacher ce port à un groupe de multidiffusion sélectionné.
4. Faites basculer un port vers la valeur **F** pour l'empêcher de se joindre à ce groupe de multidiffusion.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port est affecté au groupe de multidiffusion et le périphérique est mis à jour.

Affectation des LAG pour qu'ils reçoivent un service de multidiffusion

1. Ouvrez la page [Bridge Multicast Group](#) (Groupe de multidiffusion par ponts).
2. Définissez les champs **VLAN ID** (ID VLAN) et **Bridge Multicast Address** (Adresse de multidiffusion par ponts).
3. Faites basculer le LAG vers la valeur **S** pour rattacher ce LAG au groupe de multidiffusion sélectionné.
4. Faites basculer le LAG vers la valeur **F** pour empêcher ce LAG de se joindre à un groupe de multidiffusion.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le LAG est affecté au groupe de multidiffusion et le périphérique est mis à jour.

Gestion des membres du service de multidiffusion à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la gestion des membres du service de multidiffusion comme indiqué dans la page [Bridge Multicast Group](#) (Groupe de multidiffusion par ponts).

Tableau 7-76. Commandes CLI des membres du service de multidiffusion

Commande CLI	Description
bridge multicast address { <i>adresse-multidiffusion-mac</i> <i>adresse-multidiffusion-ip</i> }	Enregistre les adresses de multidiffusion de couche MAC dans la table des ponts et ajoute des ports statiques au groupe.
bridge multicast forbidden address { <i>adresse-multidiffusion-mac</i> <i>adresse-multidiffusion-ip</i> } [add remove] { ethernet <i>liste-interfaces</i> port-channel <i>liste-numéros-canaux-ports</i> }	Interdit d'ajouter une adresse de multidiffusion spécifique à des ports spécifiques. Utilisez la forme «no» de cette commande pour récupérer la valeur par défaut.
show bridge multicast address-table [vlan <i>id-vlan</i>] [address <i>adresse-multidiffusion-mac</i> <i>adresse-multidiffusion-ip</i>] [format ip mac]	Affiche des informations sur la table des adresses MAC de multidiffusion.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console> enable

console#config

console(config)#vlan database

console(config-if)#vlan 8

console(config-if)#exit

console(config)#interface range ethernet g1-9

console(config-if)# switchport mode general

console(config-if)# switchport general allow vlan add 8

console(config)#interface vlan 8

console(config-if)#exit

Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1,g2

Console(config-if)# exit

Console(config)# exit
```

Console# show bridge multicast address-table

VLAN	Adresse MAC	Type	Ports
----	-----	----	-----
1	0100.5e02.0203	statique	g1, g2
19	0100.5e02.0208	statique	g1-8
19	0100.5e02.0208	dynamique	g9-11

Ports interdits pour les adresses de multidiffusion :

VLAN	Adresse MAC	Ports
----	-----	-----
1	0100.5e02.0203	g8
19	0100.5e02.0208	g8

Console # show bridge multicast address-table format ip

VLAN	Adresse IP	Type	Ports
----	-----	----	-----
1	224-239.130 2.2.3	statique	g1, g2
19	224-239.130 2.2.8	statique	g1-8
19	224-239.130 2.2.8	dynamique	g9-11

Ports interdits pour les adresses de multidiffusion :

VLAN	Adresse IP	Ports
----	-----	-----

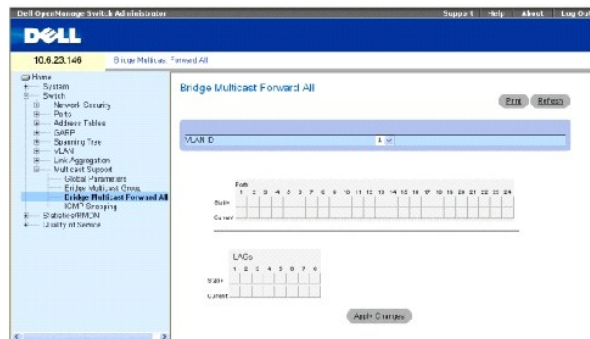
---	-----	-----	
1	224-239.130 2.2.3	g8	
19	224-239.130 2.2.8	g8	

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 un périphérique lui-même rattaché à un routeur/commutateur multidiffusion voisin. Une fois la surveillance IGMP activée, les paquets multidiffusion sont transmis 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** (Multidiffusion par ponts) → [Bridge Multicast Forward All](#) (Transfert multidiffusion total par ponts) dans l'arborescence.

Figure 7-113. Transfert multidiffusion total par ponts



VLAN ID (ID VLAN) — Identifie un VLAN.

Ports — Ports qui peuvent être ajoutés à un service de multidiffusion.

LAG — LAG qui peuvent être ajoutés à un service de multidiffusion.

La [table des paramètres de contrôle des ports/routeurs de transfert multidiffusion total par ponts](#) contient les paramètres permettant de gérer les paramètres des routeurs et des ports.

Tableau 7-77. Table des paramètres de contrôle des ports/routeurs de transfert multidiffusion total par ponts

Contrôle du port	Définition
D	Rattache le port au routeur ou commutateur multidiffusion en tant que port dynamique.
S	Rattache le port au routeur ou commutateur multidiffusion en tant que port statique.
F	Interdit.
Blanc	Indique que le port n'est pas rattaché à ce routeur ou commutateur multidiffusion.

Rattachement d'un port à un routeur ou commutateur multidiffusion

- Ouvrez la page [Bridge Multicast Forward All](#) (Transfert multidiffusion total par ponts).

2. Définissez le champ **VLAN ID** (ID VLAN).
3. Sélectionnez un port dans la table **Ports** et affectez-lui une valeur.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port est rattaché au routeur ou commutateur multidiffusion.

Rattachement d'un LAG à un routeur ou commutateur multidiffusion

1. Ouvrez la page [Bridge Multicast Forward All](#) (Transfert multidiffusion total par ponts).
2. Définissez le champ **VLAN ID** (ID VLAN).
3. Sélectionnez un LAG dans la table **LAG** et affectez-lui une valeur.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le LAG est rattaché au 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 pour la gestion des LAG et des ports rattachés aux routeurs multidiffusion comme indiqué dans la page [Bridge Multicast Forward All](#) (Transfert multidiffusion total par ponts).

Tableau 7-78. Commandes CLI de gestion des LAG et des ports rattachés aux routeurs multidiffusion

Commande CLI	Description
<code>show bridge multicast filtering id-vlan</code>	Affiche la configuration de filtrage multidiffusion.
<code>no bridge multicast forbidden forward-all</code>	Désactive le transfert des paquets multidiffusion sur un port.
<code>bridge multicast forward-all {add remove} {ethernet liste-interfaces port-channel liste-numéros-canaux-ports}</code>	Active le transfert de tous les paquets multidiffusion sur un port. Utilisez la forme «no» de cette commande pour récupérer la valeur par défaut.

Vous trouverez ci-dessous un exemple de commande CLI :

```

console(config)#vlan database

console(config-if)#vlan 8

console(config-vlan)#exit

console(config)#interface range ethernet g1-9

console(config-if)# switchport mode general

console(config-if)# switchport general allow vlan add 8

Console(config-if)# exit

console(config)#interface vlan 8

```

```

Console(config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console(config-if)# exit

Console (config)# interface vlan 1

Console (config-if)# bridge multicast forward-all add ethernet g8

Console(config-if)# end

Console# show bridge multicast filtering 1

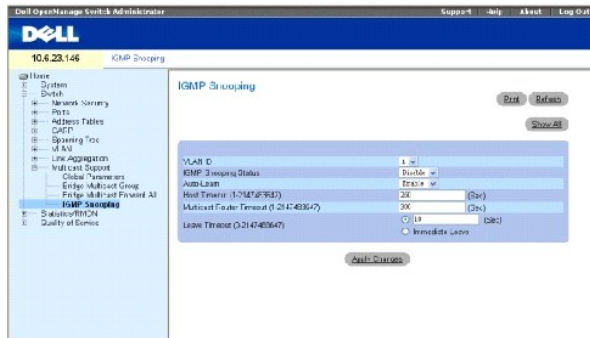
```

Filtrage : Activé		
VLAN :	Transmission totale	
Port	Statique	État
-----	-----	-----
g1	Interdit	Filtre
g2	Transmettre	Transmettre(s)
g3	-	Transmettre(d)

Surveillance IGMP

La page [IGMP Snooping](#) (Surveillance IGMP) contient des champs permettant d'ajouter des membres IGMP. 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 7-114. Surveillance IGMP



VLAN ID (ID VLAN) — Indique l'ID du VLAN.

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 le périphérique.

Host Timeout (1-2147483647) (Délai d'expiration de l'hôte [1-2147483647]) — Délai avant qu'une entrée de surveillance IGMP n'arrive à expiration. La valeur par défaut est 260 secondes.

Multicast Router Timeout (1-2147483647) (Délai d'expiration du routeur multidiffusion [1-2147483647]) — Durée avant qu'une entrée du routeur multidiffusion n'arrive à expiration. La valeur par défaut est 300 secondes.

Leave Timeout (0-2147483647) (Délai de sortie [0-2147483647]) — Délai en secondes après réception d'un message de sortie du port avant que l'entrée n'arrive à expiration. **User-defined (Défini par l'utilisateur)** active une période de délai définie par l'utilisateur et **Immediate Leave (Sortie immédiate)** indique une période de délai immédiate. La valeur par défaut est 10 secondes.

Activation de la surveillance IGMP sur le périphérique

1. Ouvrez la page [IGMP Snooping](#) (Surveillance IGMP).
2. Sélectionnez l'ID VLAN du périphérique sur lequel la surveillance IGMP doit être activée.
3. Sélectionnez **Enable** (Activer) dans le champ **IGMP Snooping Status** (État de la surveillance IGMP).
4. Renseignez les champs de cette page.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La surveillance IGMP est activée sur le périphérique.

Affichage de la table de surveillance IGMP

1. Ouvrez la page [IGMP Snooping](#) (Surveillance IGMP).
2. Cliquez sur **Show All** (Afficher tout).

La table de surveillance IGMP s'ouvre.

Configuration de la surveillance IGMP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration de la [surveillance IGMP](#) sur le périphérique :

Tableau 7-79. Commandes CLI de la surveillance IGMP

Commande CLI	Description
ip igmp snooping	Active la surveillance IGMP (Internet Group Management 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 <i>délai-expiration</i>	Configure le délai d'expiration de l'hôte.
ip igmp snooping mrouter-time-out <i>délai-expiration</i>	Configure le délai d'expiration du routeur multidiffusion.
ip igmp snooping leave-time-out {<i>délai-expiration</i> <i>sortie-immédiate</i>}	Configure le délai d'expiration de sortie.
show ip igmp snooping groups [vlan <i>id-vlan</i>] [address <i>adresse-multidiffusion-ip</i>]	Affiche les groupes de multidiffusion appris par la surveillance IGMP.
show ip igmp snooping interface <i>id-vlan</i>	Affiche la configuration de la surveillance IGMP.
show ip igmp snooping mrouter [interface <i>id-vlan</i>]	Affiche des informations sur les interfaces du routeur multidiffusion apprises de façon dynamique.

Vous trouverez ci-dessous un exemple de commande 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)# exit

Console (config)# interface vlan 1

Console (config-if)# ip igmp snooping leave-time-out 60

Console (config-if)# exit

Console (config)# exit

Console # show ip igmp snooping groups

Vlan Adresse IP Querier Ports
-----

```

1 224-239.130|2.2.3 Oui g1, g2

19 224-239.130|2.2.8 Oui g9-11

Console # show ip igmp snooping interface 1

La surveillance IGMP est activée de façon globale

La surveillance IGMP est activée sur le VLAN 1

Le délai d'expiration de l'hôte IGMP est de 300 s

La sortie immédiate IGMP est désactivée. Le délai d'expiration de sortie IGMP est de 60 s

Le délai d'expiration du routeur multidiffusion IGMP est de 200 s

L'apprentissage automatique des ports des routeurs multidiffusion est activé

Console # show ip igmp snooping mrouter

VLAN	Ports
----	-----
1	g1

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Configuration des informations système

Guide d'utilisation du système Dell™ PowerConnect™ 5324

- [Définition des informations générales relatives au périphérique](#)
- [Configuration des paramètres du SNMP](#)
- [Gestion des journaux](#)
- [Définition d'adresses IP pour le périphérique](#)
- [Exécution de diagnostics sur les câbles](#)
- [Gestion de la sécurité du périphérique](#)
- [Définition des paramètres SNMP](#)
- [Gestion des fichiers](#)
- [Définition de paramètres avancés](#)

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 du périphérique. Pour ouvrir la page System (Système), cliquez sur System (Système) dans l'arborescence.

Figure 6-15. Système



Définition des informations générales relatives au périphérique

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

Affichage de la page Asset (Inventaire)

La page **Asset** (Inventaire) contient les paramètres qui permettent de configurer des informations générales sur le périphérique : 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**, cliquez sur System (Système) → General → Asset (Inventaire) dans l'arborescence.

Figure 6-16. Inventaire



System Name (0-160 Characters) (Nom du système [0 à 160 caractères])— Indique le nom attribué au périphérique par l'utilisateur.

System Contact(Contact système [0 à 160 caractères]) — Indique le nom du contact.

System Location (0-160 Characters) (Emplacement du système [0 à 160 caractères]) — Indique l'emplacement sur lequel le système est actuellement exécuté.

MAC Address (Adresse MAC) — Indique l'adresse MAC du périphérique.

Sys Object ID (ID objet sys) — Indique l'identification par voie d'autorité du fournisseur du sous-système de gestion de réseau contenu dans l'entité.

Service Tag (Numéro de service) — Numéro de référence à communiquer pour la maintenance du périphérique.

Asset Tag (0-16 Characters) (Numéro d'inventaire [0 à 16 caractères]) — Indique la référence attribuée au périphérique par l'utilisateur.

Serial No. (N° de série) — Indique le numéro de série du périphérique.

Date (DD/MM/YY) (Date [JJ/MM/AA]) — Date du jour du système, au format mois, jour, année. Exemple : 11/10/02 correspond au 10 novembre 2002.

Time (HH:MM:SS) (Heure, HH/MM/SS) — Indique l'heure, au format heure, minute, seconde. 20:12:03 correspond à vingt heures, douze minutes et trois secondes, par exemple.

System Up Time (Durée de fonctionnement du système) — Indique la durée qui s'est écoulée depuis la dernière réinitialisation du périphérique. Elle s'affiche au format : jours, heures, minutes, secondes. Exemple : 41 jours 2 heures 22 minutes 15 secondes.

Définition des informations système :

1. Ouvrez la page [Asset](#) (Inventaire).
2. Définissez les champs concernés.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres du système sont définis et le périphérique est mis à jour.

Ouverture d'une session Telnet :

1. Ouvrez la page [Asset](#) (Inventaire).
2. Cliquez sur **Telnet**.

Une session Telnet s'ouvre.

Configuration des informations relatives au périphérique à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage et la configuration des champs de la page [Asset](#) (Inventaire).

Tableau 6-11. Commandes CLI de l'inventaire

Commande CLI	Description
<code>hostname nom</code>	Définit ou modifie le nom d'hôte du périphérique.
<code>snmp-server contact texte</code>	Définit un contact pour le système.
<code>snmp-server location texte</code>	Précise l'emplacement du périphérique.
<code>show clock [détails]</code>	Affiche la date et l'heure de l'horloge système.
<code>show system id</code>	Affiche le numéro de service.
<code>show system</code>	Affiche les informations système.
<code>asset-tag</code>	Affiche le numéro d'inventaire attribué au périphérique.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# hostname dell

Console (config)# snmp-server contact Supp_Tech_Dell

Console (config)# snmp-server location New_York

Console (config)# exit

Console# exit

Console (config)# asset-tag lqwepot

Console> clock set 13:32:00 7 Déc. 2004

Console> show clock

13:32:00 (UTC+0) Déc. 7 2004

No time source
```

DELL Switch# show system	
Description du système :	Commutateur de routage Ethernet

Durée de fonctionnement du système (jours,heures:mm:s) :		0,00:04:17
Contact système :		spk
Nom système :		Commutateur DELL
Emplacement système :		R&D
Adresse MAC système :		00:10:b5:f4:00:01
ID objet sys :		1.3.6.1.4.1.674.10895.3000
Type : PowerConnect 5324		
Bloc d'alimentation	État	
-----	-----	
Principale	OK	
Module d'alimentation redondant	OK	
Ventilateur	État	
-----	-----	
1	OK	
2	OK	
DELL Switch#		

Définition des paramètres d'heure du système

La page [Time Synchronization](#) (Synchronisation de l'heure) contient des champs permettant de définir des paramètres d'heure du système pour l'horloge matérielle locale et pour l'horloge SNTP externe. Si le système est maintenu en utilisant une horloge SNTP externe et que cette horloge tombe en panne, l'heure du système revient à celle de l'horloge matérielle locale. Vous pouvez activer les changements relatifs à l'heure d'été sur le périphérique. Voici une liste des dates de l'heure d'été de certains pays :

- 1 Afrique du Sud — L'Afrique du Sud n'applique pas le changement d'heure.
- 1 Albanie — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Allemagne — Du dernier week-end de mars au dernier week-end d'octobre.

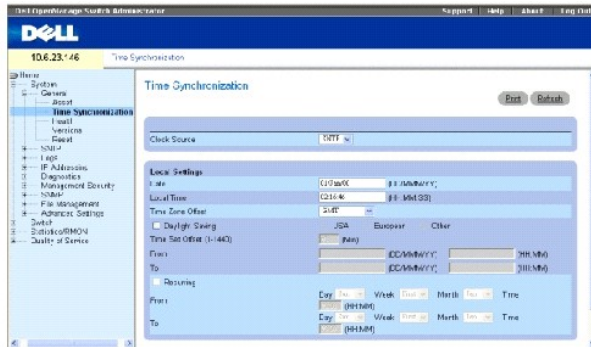
- 1 Australie — De la fin octobre à la fin mars.
- 1 Australie - Tasmanie — Du début octobre à la fin mars.
- 1 Arménie — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Autriche — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Bahamas — D'avril à octobre, aligné sur l'heure d'été aux États-Unis.
- 1 Bélarus — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Belgique — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Brésil — Du troisième dimanche d'octobre au troisième dimanche de mars. Pendant l'heure d'hiver, presque tout le sud-est du Brésil avance sa montre d'une heure.
- 1 Chili - Ile de Pâques — Du 9 mars au 12 octobre. Le premier dimanche de mars ou le premier dimanche après le 9 mars.
- 1 Chine — La Chine n'applique pas le changement d'heure.
- 1 Canada — Du premier dimanche d'avril au dernier dimanche d'octobre. Le changement d'heure est décidé par les gouvernements provinciaux et territoriaux. Il existe des exceptions dans certaines municipalités.
- 1 Cuba — Du dernier dimanche de mars au dernier dimanche d'octobre.
- 1 Chypre — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Danemark — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Égypte — Du dernier vendredi d'avril au dernier jeudi de septembre.
- 1 Espagne — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Estonie — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 États-Unis d'Amérique — Du premier dimanche d'avril à 02:00 au dernier dimanche d'octobre à 02:00.
- 1 Finlande — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 France — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Grèce — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Hongrie — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Inde — L'Inde n'applique pas le changement d'heure.
- 1 Iran — Du 1er Farvardin au 1er Mehr.
- 1 Iraq — Du 1er avril au 1er octobre.
- 1 Irlande — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Israël — Varie d'année en année.
- 1 Italie — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Japon — Le Japon n'applique pas le changement d'heure.
- 1 Jordanie — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Lettonie — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Liban — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Lituanie — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Luxembourg — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Macédoine — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Mexique — Du premier dimanche d'avril à 02:00 au dernier dimanche d'octobre à 02:00.
- 1 Moldavie — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Monténégro — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Pays-Bas — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Nouvelle Zélande — Du premier dimanche d'octobre au premier dimanche de mars ou après le 15 mars.
- 1 Norvège — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Paraguay — Du 6 avril au 7 septembre.
- 1 Pologne — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Portugal — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Roumanie — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Royaume-Uni — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Russie — Du 29 mars au 25 octobre.
- 1 Serbie — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Slovaquie — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Suède — Du dernier week-end de mars au dernier week-end d'octobre.

- 1 Suisse — Du dernier week-end de mars au dernier week-end d'octobre.
- 1 Syrie — Du 31 mars au 30 octobre.
- 1 Taiwan — Taiwan n'applique pas le changement d'heure.
- 1 Turquie — Du dernier week-end de mars au dernier week-end d'octobre.

Pour plus d'informations sur le SNTP, reportez-vous à la section [«Configuration des paramètres du SNTP»](#).

Pour ouvrir la page [Time Synchronization](#) (Synchronisation de l'heure), cliquez sur **System (Système)** → **General** → **Time Synchronization** (Synchronisation de l'heure) dans l'arborescence.

Figure 6-17. Synchronisation de l'heure



Source de l'horloge

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

SNTP — Indique que l'heure du système est configurée via un serveur SNTP. Pour plus d'informations, reportez-vous à la section [«Configuration des paramètres du SNTP»](#).

None (Aucune) — Indique que l'heure du système n'est configurée par aucune source externe.

Paramètres locaux

Date — Définit la date du système. Le format de ce champ est Jour:Mois:Année, 04 mai 2050 par exemple.

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

Time Zone Offset (Décalage fuseau horaire) — Différence en l'heure GMT (Greenwich Mean Time) et l'heure locale. Par exemple, le décalage fuseau horaire pour Paris est GMT +1, alors que l'heure locale à New York est GMT -5.

Vous pouvez paramétrer les changements de l'heure d'été de deux façons : à une date spécifique suivant l'année ou à la même date chaque année. Pour paramétrer une date spécifique suivant l'année, complétez la zone **Daylight Savings** (Changement heure d'été) et pour paramétrer à la même date chaque année, complétez la zone **Recurring** (Périodique).

Daylight Savings (Changement heure d'été) — Active le changement heure d'été (DST) sur le périphérique en fonction de sa localisation. Ce champ peut prendre les valeurs suivantes :

USA — Le périphérique change d'heure à 2h du matin le premier dimanche d'avril et revient à l'heure normale à 2h du matin le dernier dimanche d'octobre.

European (Europe) — Le périphérique change d'heure à 1h du matin le dernier dimanche de mars et revient à l'heure normale à 1h du matin le dernier dimanche d'octobre. L'option European concerne les membres de l'Union Européenne et les autres pays européens qui observent la norme de l'UE.

Other (Autre) — Le DST est défini par l'utilisateur en fonction de la localisation du périphérique. Lorsque cette option est sélectionnée, les champs **From** (Du) et **To** (Au) doivent être définis.

From (Du) — Définit l'heure à laquelle le changement se fait dans les pays qui n'appliquent pas le DST des États-Unis ou de l'Europe. Le format de ce champ est JourMoisAnnée dans un seul champ et heure dans un autre. Par exemple, pour un DST commençant le 25 octobre 2007 à 5h du matin, les deux champs seront 25Oct07 et 5:00. Les valeurs possibles de ce champ sont :

Date — Date de début du DST. La plage est comprise entre 1 et 31.

Month (Mois) — Mois de début du DST. La plage est comprise entre Jan et Déc.

Year (Année) — Année au cours de laquelle le DST configuré commence.

Time (Heure) — Heure de début du DST. Le format de ce champ est Heure:Minute, 05:30 par exemple.

To (Au) — Définit l'heure à laquelle le changement se termine dans les pays qui n'appliquent pas le DST des États-Unis ou de l'Europe. Le format de ce champ est JourMoisAnnée dans un champ et heure dans un autre. Par exemple, pour un DST se terminant le 23 mars 2008 à 12h, les deux champs seront 23Mar08 et 12:00. Les valeurs possibles de ce champ sont :

Date — Date de fin du DST. La plage est comprise entre 1 et 31.

Month (Mois) — Mois de fin du DST. La plage est comprise entre Jan et Déc.

Year (Année) — Année au cours de laquelle le DST configuré se termine.

Time (Heure) — Heure de fin du DST. Le format de ce champ est Heure:Minute, 05:30 par exemple.

Recurring (Périodique) — Définit l'heure à laquelle le DST commence dans les pays qui n'appliquent pas le DST des États-Unis ou de l'Europe, et où le DST est constant d'année en année. Ce champ peut prendre les valeurs suivantes :

From (Du) — Définit l'heure de début du DST chaque année. Par exemple, le DST commence localement chaque deuxième dimanche d'avril à 5h du matin. Ce champ peut prendre les valeurs suivantes :

Day (Jour) — Jour de la semaine à partir duquel commence le DST chaque année. La plage est comprise entre dimanche et samedi.

Week (Semaine) — Semaine d'un mois à partir de laquelle commence le DST chaque année. La plage est comprise entre 1 et 5.

Month (Mois) — Mois de l'année à partir duquel le DST commence chaque année. La plage est comprise entre Jan. et Déc.

Time (Heure) — Heure à laquelle le DST commence chaque année. Le format de ce champ est Heure:Minute, 02:10 par exemple.

To (Au) — Définit l'heure récurrente à laquelle le DST se termine chaque année. Par exemple, le DST se termine localement chaque quatrième vendredi d'octobre à 5h du matin. Ce champ peut prendre les valeurs suivantes :

Day (Jour) — Jour de la semaine auquel se termine le DST chaque année. La plage est comprise entre dimanche et samedi.

Week (Semaine) — Semaine dans le mois à laquelle se termine le DST chaque année. La plage est comprise entre 1 et 5.

Month (Mois) — Mois de l'année auquel se termine le DST chaque année. La plage est comprise entre Jan. et Déc.

Time (Heure) — Heure à laquelle le DST se termine chaque année. Le format de ce champ est Heure:Minute, 05:30 par exemple.

Sélection d'une source de l'horloge

1. Ouvrez la page [Time Synchronization](#) (Synchronisation de l'heure).
2. Définissez le champ **Clock Source** (Source de l'horloge).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La source de l'horloge est sélectionnée et le périphérique est mis à jour.

Définition des paramètres de l'horloge locale

1. Ouvrez la page [Time Synchronization](#) (Synchronisation de l'heure).
2. Définissez les champs **Recurring** (Périodique).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de l'horloge locale sont appliqués.

Définition des paramètres d'horloge externe SNTP

1. Ouvrez la page [Time Synchronization](#) (Synchronisation de l'heure).
2. Renseignez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de l'horloge externe sont appliqués.

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

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [Time Synchronization](#) (Synchronisation de l'heure).

Tableau 6-12. Commandes CLI de paramétrage de l'horloge

CLI	Description
<code>clock source {sntp}</code>	Configure une source d'heure externe pour l'horloge du système.
<code>clock timezone heures-décalage [minutes minutes-décalage][zone acronyme]</code>	Configure la zone horaire à des fins d'affichage.
<code>clock summer-time</code>	Configure le système pour qu'il bascule automatiquement à l'heure d'été (changement heure d'été).
<code>clock summer-time recurring {usa eu { semaine jour mois hh:mm semaine jour mois hh:mm } [offset décalage] [zone acronyme]}</code>	Configure le système pour qu'il bascule automatiquement à l'heure d'été (conformément aux normes américaines et européennes).
<code>clock summer-time date date mois année hh:mm date mois année hh:mm [offset décalage] [zone acronyme]</code>	Configure le système pour qu'il bascule automatiquement à l'heure d'été (changement heure été) pendant une période spécifique (format date/mois/année).

Vous trouverez ci-dessous un exemple de commande CLI :

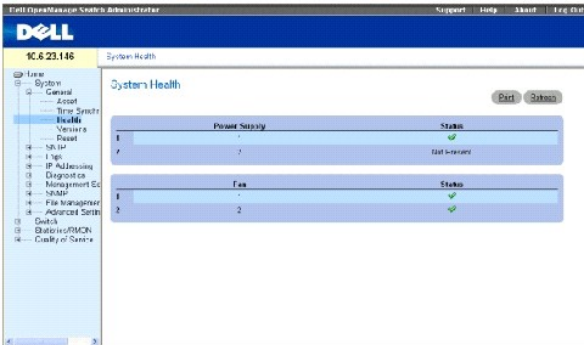
```
Console(config)# clock timezone -6 zone CST
```

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


Affichage d'informations sur l'intégrité du système


La page [System Health](#) (Intégrité du système) fournit des informations sur les périphériques matériels. Pour ouvrir la page [System Health](#), cliquez sur System (Système) → General → Health (Intégrité) dans l'arborescence.

Figure 6-18. Intégrité du système




Power Supply Status (État du bloc d'alimentation) — Indique l'état du bloc d'alimentation principal. Ce champ peut prendre les valeurs suivantes :


 — Le bloc d'alimentation principal de l'unité spécifiée fonctionne normalement.

 — Le bloc d'alimentation principal de l'unité spécifiée ne fonctionne pas normalement.

Not Present (Absent) — Indique que le bloc d'alimentation de l'unité spécifiée est absent.

Fan (Ventilateur) — Indique l'état des ventilateurs du périphérique. Ce champ peut prendre les valeurs suivantes :

 — Les ventilateurs de l'unité spécifiée fonctionnent normalement.

 — Les ventilateurs de l'unité spécifiée ne fonctionnent pas normalement.

Not Present (Absent) — Indique que les ventilateurs de l'unité spécifiée sont absents.

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

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage des champs de la page [System Health](#) (Intégrité du système).

Table 6-13. Commandes CLI de l'intégrité du système

Commande CLI	Description
show system	Affiche les informations système.

DELL Switch# show system		
Description du système :		Commutateur de routage Ethernet
Durée de fonctionnement du système (jours,heures:mn:s) :		0,00:04:17
Contact système :		spk
Nom système :		Commutateur DELL
Emplacement système :		R&D
Adresse MAC système :		00:10:b5:f4:00:01
ID objet sys :		1.3.6.1.4.1.674.10895.3000
Type : PowerConnect 5324		
Bloc d'alimentation	État	
-----	-----	
Principale	OK	
Module d'alimentation redondant	OK	
Ventilateur	État	
-----	-----	
1	OK	
2	OK	
DELL Switch#		

Affichage de la page Versions

La page [Versions](#) contient des informations sur les versions logicielle et matérielle actuellement exécutées. Pour ouvrir la page [Versions](#), cliquez sur System (Système) → General → Versions dans l'arborescence.

Figure 6-19. Versions



Software Version (Version du logiciel) — Indique le numéro de version du logiciel exécuté sur le périphérique.

Boot Version (Version de démarrage) — Indique le numéro de version du programme de démarrage exécuté sur le périphérique.

Hardware Version (Version du matériel) — Indique le numéro de version du matériel du périphérique.

Affichage des versions du périphérique à l'aide de l'interface de ligne de commande

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage des champs de la page [Versions](#).

Tableau 6-14. Commandes CLI des versions

Commande CLI	Description
show version	Affiche les informations de version du système.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console> show version

Version logiciel x.xxx (date 23-Juil-xxxx heure 17:34:19)

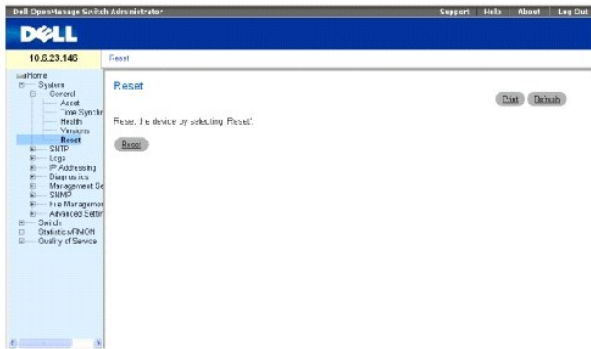
Version démarrage x.xxx (date 17-Jan-xxxx heure 11:48:21)

Version matériel x.x.x
```

Réinitialisation du périphérique

La page [Reset](#) (Réinitialisation) permet de réinitialiser le périphérique à partir d'un site distant. Pour ouvrir la page [Reset](#), cliquez sur System (Système) → General → Reset (Réinitialisation) dans l'arborescence.

Figure 6-20. Réinitialisation



REMARQUE : Enregistrez toutes les modifications dans le fichier de configuration en cours avant de réinitialiser le périphérique pour éviter de perdre la configuration matérielle existante. Pour plus d'informations sur l'enregistrement des fichiers de configuration, reportez-vous à la section [«Gestion des fichiers»](#).

Réinitialisation du périphérique

1. Ouvrez la page [Reset](#) (Réinitialisation).
2. Cliquez sur **Reset**.

Un message de confirmation s'affiche.

3. Cliquez sur **OK**.

Le périphérique est réinitialisé. La réinitialisation effectuée, l'utilisateur est invité à saisir un nom et un mot de passe.

4. Saisissez un nom d'utilisateur et un mot de passe pour vous reconnecter à l'interface Web.

Réinitialisation du périphérique à l'aide de l'interface de ligne de commande

Le tableau suivant récapitule les commandes CLI équivalentes pour effectuer une réinitialisation du périphérique via la CLI.

Tableau 6-15. Commandes CLI de réinitialisation

Commande CLI	Description
reload	Recharge le système d'exploitation.

Vous trouverez ci-dessous un exemple de commande CLI :

```

Console >reload

Cette commande réinitialise tout le système et déconnecte votre session

en cours. Êtes-vous certain de vouloir continuer (y/n) [n] ?

```

Configuration des paramètres du SNTP

Le périphérique prend en charge le protocole SNTP (Protocole de temps de réseau simple). Le protocole SNTP assure une synchronisation de l'heure de l'horloge du périphérique réseau avec une précision d'une milliseconde. La synchronisation de l'heure se fait via un serveur réseau SNTP. Le périphérique ne fonctionne que comme client SNTP et ne peut pas proposer de services liés à l'heure aux autres systèmes.

Le périphérique peut interroger les serveurs suivant concernant l'heure :

- 1 Monodiffusion
- 1 Multidiffusion
- 1 Diffusion

Les sources de temps sont établies par des Stratum. Les Stratum définissent la précision de l'horloge de référence. Plus le Stratum est haut (zéro représente le plus haut), plus l'horloge est précise. Le périphérique reçoit l'heure du Stratum 1 ou supérieur.

Vous trouverez ci-dessous des exemples de stratum :

- 1 **Stratum 0** — Une horloge temps réel, comme un système GPS, est utilisée comme source d'heure.
- 1 **Stratum 1** — Un serveur directement lié à une source d'heure de Stratum 0 est utilisé. Des serveurs d'heure de Stratum 1 définissent les normes d'heure du réseau principal.
- 1 **Stratum 2** — La source d'heure est éloignée du serveur de Stratum 1 par un chemin du réseau. Par exemple, un serveur de Stratum 2 reçoit l'heure envoyée par un serveur de Stratum 1 sur une liaison de réseau via NTP.

Les informations reçues des serveurs SNTP sont évaluées en fonction du niveau de l'heure et du type de serveur.

Les définitions d'heure SNTP sont calculées et déterminées par les niveaux d'heure suivants :

- 1 **T1** — Heure à laquelle la demande originale a été envoyée par le client.
- 1 **T2** — Heure à laquelle la demande originale a été reçue par le serveur.
- 1 **T3** — Heure à laquelle le serveur a envoyé une réponse au client.
- 1 **T4** — Heure à laquelle le client a reçu la réponse du serveur.

Demande d'informations sur l'heure monodiffusion

Ce type de demande est utilisé pour interroger un serveur dont on ne connaît pas l'adresse IP. Les valeurs T1 à T4 sont utilisées pour déterminer l'heure du serveur. Il s'agit de la méthode utilisée prioritairement pour synchroniser l'heure du commutateur.

Demande d'informations sur l'heure multidiffusion

Ce type de demande est utilisé lorsqu'on ne connaît pas l'adresse IP du serveur. Le premier serveur multidiffusion à répondre sert pour configurer la valeur de l'heure. Les niveaux d'heure T3 et T4 sont utilisés pour déterminer l'heure du serveur. Il est préférable d'utiliser les informations sur l'heure multidiffusion pour synchroniser l'heure du commutateur plutôt que les informations sur l'heure diffusion.

Informations sur l'heure multidiffusion

Ce type d'information est utilisé lorsqu'on ne connaît pas l'adresse IP du serveur. Lorsqu'un message de diffusion est envoyé d'un serveur SNTP, le client SNTP écoute la réponse. Il n'y a pas d'échange de question-réponse entre le client SNTP et le serveur de diffusion.

L'authentification MD5 (condensé de message 5) sauvegarde les chemins de synchronisation du commutateur dans les serveurs SNTP. MD5 est un algorithme qui permet un hachage à 128 bits. MD5 est une variante de MD4 avec plus de sécurité. MD5 vérifie l'intégrité de la communication et identifie son origine.

Cliquez sur **System** (Système) → **Sntp** dans l'arborescence pour ouvrir la page **Sntp**.

Définition des paramètres globaux SNTP

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

Figure 6-21. Paramètres globaux SNTP



Poll Interval (60-86400) (Intervalle d'interrogation [60-86400]) — Définit l'intervalle (en secondes) pendant lequel le serveur SNTP est interrogé pour des informations de monodiffusion.

Receive Broadcast Servers Updates (Mises à jour de serveurs de diffusion reçues) — Demande aux serveurs SNTP des informations sur l'heure du serveur de diffusion sur les interfaces sélectionnées.

Receive Anycast Servers Updates (Mises à jour de serveurs de multidiffusion reçues) — Demande au serveur SNTP des informations sur l'heure du serveur de multidiffusion. Si les champs **Receive Anycast Servers Update** et **Receive Broadcast Servers Update** sont activés, l'heure du système est configurée suivant les informations d'heure du serveur de multidiffusion.

Receive Unicast Servers Updates (Mises à jour de serveurs de monodiffusion reçues) — Demande au serveur SNTP des informations sur l'heure du serveur de monodiffusion. Si les champs **Receive Broadcast Servers Updates**, **Receive Anycast Servers Updates** et **Receive Unicast Servers Updates** sont tous activés, l'heure du système est configurée suivant les informations d'heure du serveur de monodiffusion.

Poll Unicast Servers (Interrogation serveurs monodiffusion) — Envoie des informations de transmission monodiffusion SNTP au serveur SNTP.

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

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs affichés dans la page **SNTP Global Settings** (Paramètres globaux SNTP).

Tableau 6-16. Commandes CLI des paramètres globaux SNTP

Commande CLI	Description
<code>sntp broadcast client enable</code>	Active les clients de diffusion SNTP.
<code>sntp unicast client enable</code>	Active les clients de monodiffusion SNTP prédéfinis.

Vous trouverez ci-dessous un exemple de commande CLI :

```
console> enable

console# configure

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

Définition des méthodes d'authentification du 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 choisie sur cette page. Cliquez sur **System** (Système) → **SNTP** → **Authentication** dans l'arborescence pour ouvrir la page **SNTP Authentication** (Authentification SNTP).

Figure 6-22. Authentification SNTP



SNTP Authentication (Authentification SNTP) — Active l'authentification d'une session SNTP entre le périphérique et un serveur SNTP.

Encryption Key ID (ID de la clé de cryptage) — Identifie la clé utilisée pour authentifier le serveur SNTP et le périphérique. Ce champ peut contenir jusqu'à 4 294 967 295 caractères.

Authentication Key (1 à 8 caractères) (Clé d'authentification [1 à 8 caractères]) — Clé utilisée pour l'authentification.

Trusted Key (Clé de confiance) — Clé de cryptage utilisée pour authentifier le serveur SNTP.

Remove (Supprimer) — Supprime la clé sélectionnée.

Ajout d'une clé d'authentification SNTP

1. Ouvrez la page [SNTP Authentication](#) (Authentification SNTP).
2. Cliquez sur **Add** (Ajouter).

La page [Add Authentication Key](#) (Ajouter une clé d'authentification) s'ouvre :

Figure 6-23. Ajouter une clé d'authentification



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

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

Affichage de la table des clés d'authentification

1. Ouvrez la page [SNTP Authentication](#) (Authentication SNMP).
2. Cliquez sur **Show All** (Afficher tout).

La page [Authentication Key Table](#) (Table des clés d'authentification) s'ouvre :

Figure 6-24. Table des clés d'authentification

Encryption Key ID	Authentication Key	Trusted Key	Remove
1	pass	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Suppression de la clé d'authentification

1. Ouvrez la page [SNTP Authentication](#) (Authentication SNMP).
2. Cliquez sur **Show All** (Afficher tout).

La page [Authentication Key Table](#) (Table des clés d'authentification) s'ouvre :

3. Sélectionnez une entrée de 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 le périphérique est mis à jour.

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

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [SNTP Authentication](#) (Authentication SNMP).

Tableau 6-17. Commandes CLI d'authentification du SNMP

Commande CLI	Description
<code>sntp authenticate</code>	Définit l'authentification du trafic SNMP provenant des serveurs.
<code>sntp authentication-key numéro md5 valeur</code>	Définit une clé d'authentification pour le SNMP.

Vous trouverez ci-dessous un exemple de commande CLI :

```

console> enable

console# configure

Console(config)# sntp authentication-key 8 md5 ClkKey

Console(config)# sntp trusted-key 8

Console(config)# sntp authenticate

```

Définition des serveurs SNMP

La page [SNTP Servers](#) (Serveurs SNTP) contient des informations permettant d'ajouter et d'activer des serveurs SNTP. De plus, la page [SNTP Servers](#) permet au périphérique de demander et d'accepter du trafic SNTP provenant d'un serveur. Pour ouvrir la page [SNTP Servers](#), cliquez sur **System (Système)** → **SNTP** → **SNTP Servers (Serveurs SNTP)** dans l'arborescence.

Figure 6-25. Serveurs SNTP



SNTP Server (Serveur SNTP) — Saisissez une adresse IP de serveur SNTP ou un nom d'hôte définis par l'utilisateur. Vous pouvez définir jusqu'à huit serveurs SNTP. Ce champ peut contenir de 1 à 158 caractères.

Poll Interval (Intervalle d'interrogation) — Active l'interrogation du serveur SNTP concernant des informations sur l'heure du système.

Encryption Key ID (ID de la clé de cryptage) — Identifie la clé utilisée pour communiquer entre le serveur SNTP et le périphérique. La plage est comprise entre 1 et 4 294 967 295.

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

Primary (Principal) — Le serveur principal fournit des informations SNTP.

Secondary (Secondaire) — Ce serveur de sauvegarde fournit des informations SNTP.

Status Up (État d'activation) — État de fonctionnement du serveur SNTP. Ce champ peut prendre les valeurs suivantes :

Up (Opérationnel) — Le serveur SNTP fonctionne normalement.

Down (Désactivé) — Le serveur SNTP ne fonctionne pas normalement.

Unknown (Inconnu) — L'état du serveur SNTP n'est pas connu.

Last Response (Dernière réponse) — Heure de la dernière réponse reçue du serveur SNTP.

Offset (Décalage) — Décalage entre l'horloge locale du périphérique et l'heure reçue du serveur SNTP.

Delay (Retard) — Temps nécessaire pour atteindre le serveur SNTP.

Remove (Supprimer) — Supprime un serveur SNTP de la liste des **serveurs SNTP**.

Ajout d'un serveur SNTP

1. Ouvrez la page [SNTP Servers](#) (Serveurs SNTP).
2. Cliquez sur **Add** (Ajouter).

La page [Add SNTP Server](#) (Ajouter un serveur SNTP) s'ouvre :

Figure 6-26. Ajouter un serveur SNTP

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

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

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs affichés dans la page [Add SNTP Server](#) (Ajouter un serveur SNTP).

Tableau 6-18.

Commande CLI	Description
<code>sntp server <i>adresse-ip</i>/<i>nom d'hôte</i> [<i>poll</i>] [<i>key id</i>]</code>	Configure le périphérique pour qu'il utilise le SNTP pour demander et accepter du trafic NTP depuis un serveur.

Commandes CLI du serveur SNTP

Vous trouverez ci-dessous un exemple de commande CLI :

```
console> enable

console# configure

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

Affichage de la table des serveurs SNTP

1. Ouvrez la page [SNTP Servers](#) (Serveurs SNTP).
2. Cliquez sur **Show All** (Afficher tout).

La page [SNTP Servers Table](#) (Table des serveurs SNTP) s'ouvre :

Figure 6-27. Table des serveurs SNTP

Modification d'un serveur SNTP

1. Ouvrez la page [SNTP Servers](#) (Serveurs SNTP).
2. Cliquez sur **Show All** (Afficher tout).

La page [SNTP Servers Table](#) (Table des serveurs SNTP) s'ouvre.

3. Sélectionnez un serveur SNTP.
4. Modifiez les champs concernés.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les informations sur le serveur SNTP sont mises à jour.

Suppression du serveur SNTP

1. Ouvrez la page [SNTP Servers](#) (Serveurs SNTP).
2. Cliquez sur **Show All** (Afficher tout).

La page [SNTP Servers Table](#) (Table des serveurs SNTP) s'ouvre.

3. Sélectionnez une entrée **SNTP Server** (Serveur SNTP).
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

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

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [SNTP Servers](#) (Serveurs SNTP).

Tableau 6-19. Commandes CLI des serveurs SNTP

Commande CLI	Description
<code>sntp server <i>adresse-ip</i> <i>nom d'hôte</i> [<i>poll</i>] [<i>key idcdé</i>]</code>	Configure le périphérique pour qu'il utilise le SNTP pour demander et accepter du trafic NTP provenant d'un serveur.

Vous trouverez ci-dessous un exemple de commande CLI :

```

console> enable

console# configure

Console(config)# sntp server 100.1.1.1 poll key 10

Console# show sntp status

L'horloge est synchronisée, le stratum est 4, la référence est
176.1.1.8

L'heure de référence est AFE2525E.70597B34 (00:10:22.438 PDT 5 juil
1993)

```

Serveurs monodiffusion :					
Serveur	Préférence	État	Dernière réponse	Décalage [mSec]	Retard [mSec]
-----	-----	-----	-----	-----	-----
176.1.1.8	Principal	Opérationnel	AFE252C1.6DBDDFF2	7.33	117.79
176.1.8.179	Secondaire	Inconnu	AFE21789.643287C9	8.98	189.19
Serveur multidiffusion :					
Serveur	Préférence	État	Dernière réponse	Décalage [mSec]	Retard [mSec]
-----	-----	-----	-----	-----	-----
VLAN 119	Secondaire	Opérationnel	19:53:21.789 PDT 19 fév 2002	7.19	119.89
Diffusion :					
Interface	Adresse IP	Dernière réponse			
-----	-----	-----			
176.1.1.8	Principal	AFE252C1.6DBDDFF2			
176.1.8.179	Secondaire	AFE21789.643287C9			

Définition des interfaces SNTP

La **SNTP Broadcast Interface Table** (Table des interfaces de diffusion SNTP) contient des champs permettant de configurer le SNTP sur différentes interfaces. Pour ouvrir la **SNTP Broadcast Interface Table** (Table des interfaces de diffusion SNTP), cliquez sur System (Système) → SNTP → Interfaces Settings (Paramètres d'interface).

La **SNTP Broadcast Interface Table** (Table des interfaces de diffusion SNTP) contient les champs suivants :

Interface — Contient une liste d'interfaces sur lesquelles le SNTP peut être activé.

Receive Server Updates (Mises à jour de serveur reçues) — Active ou désactive l'interface spécifique.

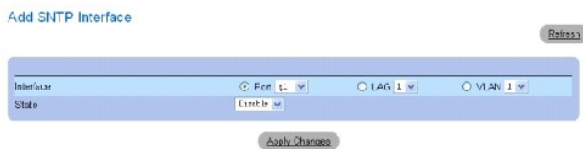
Remove (Supprimer) — Supprime le SNTP d'une interface spécifique.

Ajout d'une interface SNTP

1. Ouvrez la page **SNTP Broadcast Interface Table** (Table des interfaces de diffusion SNTP).
2. Cliquez sur **Add** (Ajouter).

La page **Add SNTP Interface** (Ajouter une interface SNTP) s'ouvre :

Figure 6-28. Ajouter une interface SNTP



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

L'interface SNTP est ajoutée et le périphérique est mis à jour.

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

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs affichés dans la **SNTP Broadcast Interface Table** (Table des interfaces de diffusion SNTP).

Tableau 6-20. Commandes CLI de diffusion SNTP

Commande CLI	Description
<code>sntp client enable</code>	Active le client protocole de temps de réseau simple (SNTP) sur une interface.
<code>show sntp configuration</code>	Affiche la configuration du protocole de temps de réseau simple (SNTP).

Vous trouverez ci-dessous un exemple de commande CLI :

Console# show sntp configuration
Intervalle d'interrogation : 7200 secondes.
Clés d'authentification MD5 : 8, 9
Une authentification est requise pour la synchronisation.
Clés de confiance : 8,9
Interrogation de clients de monodiffusion : Activé.

Serveur	Interrogation	Clé de cryptage
-----	-----	-----
176.1.1.8	Activée	9
176.1.8.179	Désactivée	Désactivée
Clients de diffusion : Activée		
Interrogation de clients de diffusion : Activée		
Interfaces de diffusion : g1, g3		

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.

La page **Logs (Journaux)** contient des liens vers différentes pages de journalisation.

Définition des paramètres globaux de journalisation

Les journaux système vous permettent d'afficher des événements du périphérique en temps réel et de les enregistrer en vue d'une utilisation ultérieure. Les journaux du système consignent et gèrent des événements et génèrent des rapports d'erreurs ou des messages d'information.

Les messages relatifs aux événements se présentent sous un format unique, conforme au format SYSLOG RFC recommandé pour les rapports d'erreurs. Par exemple, un code de gravité ainsi qu'une notation mnémonique permettant d'identifier l'application source du message sont associés aux messages Syslog et aux rapports sur les périphériques locaux. Ainsi, les messages sont filtrés en fonction de leur urgence ou de leur pertinence. La gravité de chaque message détermine le groupe de périphériques de consignation d'événements auquel des messages sont envoyés.

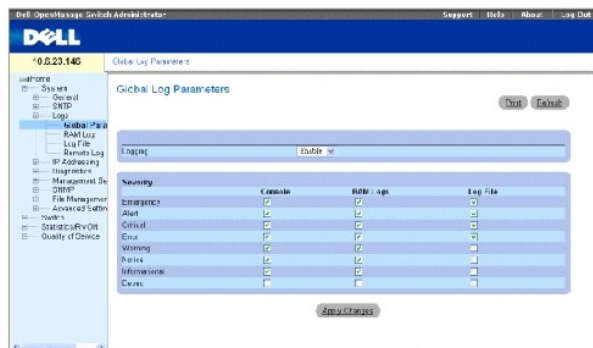
Le tableau ci-après récapitule les différents niveaux de gravité des journaux :

Tableau 6-21. Niveaux de gravité des journaux

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

La page [Global Log Parameters](#) (Paramètres globaux de journalisation) contient des champs qui permettent de définir les événements à enregistrer dans les journaux. Elle contient des champs qui permettent d'activer les journaux de façon globale et des paramètres qui permettent de définir des options de journalisation. Les messages de journalisation Severity (Gravité) sont classés par ordre décroissant de gravité. Pour ouvrir la page [Global Log Parameters](#), cliquez sur **System (Système)** → **Logs (Journaux)** → **Global Parameters (Paramètres globaux)** dans l'arborescence.

Figure 6-29. Paramètres globaux de journalisation



Logging (Journalisation) — Active la journalisation générale pour les journaux en mémoire cache, dans un fichier et sur serveur. La journalisation de la console est activée par défaut.

Severity (Gravité) — Il existe différents niveaux de gravité de journalisation des événements :

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

Alert (Alerte) — Deuxième plus haut niveau d'avertissement. Un journal d'alerte est enregistré en cas de dysfonctionnement grave du périphérique, lorsque les fonctions ne répondent plus, par exemple.

Critical (Critique) — Troisième plus haut niveau d'avertissement. Un journal critique est enregistré en cas de dysfonctionnement critique du périphérique ; lorsque deux ports ne fonctionnent plus alors que tous les autres restent parfaitement opérationnels, par exemple.


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

Warning (Avertissement) — Niveau d'avertissement le plus faible. Le périphérique fonctionne, mais un problème est survenu.

Notice (Mise en garde) — Fournit des informations relatives au périphérique.

Informational (Informations) — Fournit des informations sur le périphérique.

Debug (Débogage) — Fournit des messages de débogage.

 **REMARQUE** : Lorsqu'un niveau de gravité est sélectionné, les options correspondantes sont automatiquement activées.

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

Console — Indique le niveau de gravité minimum à partir duquel les journaux sont envoyés à la console.

RAM Logs (Journaux RAM) — Indique le niveau de gravité minimum à partir duquel les journaux sont envoyés au fichier journal stocké en RAM (mémoire cache).

Log File (Fichier journal) — Indique le niveau de gravité minimum à partir duquel les journaux sont envoyés au fichier journal stocké en mémoire FLASH.

Activation des journaux :

1. Ouvrez 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 gravité 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 le périphérique est mis à jour.

Activation des journaux à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [Global Log Parameters](#) (Paramètres globaux de journalisation).

Tableau 6-22. Commandes CLI des paramètres globaux de journalisation

Commande CLI	Description
logging on	Active la journalisation des messages d'erreur.
logging { <i>adresse-ip</i> } <i>nom d'hôte</i> [<i>port port</i>] [<i>severity niveau</i>] [<i>facility voie de transmission</i>] [<i>description texte</i>]	Consigne les messages sur un serveur syslog. Pour connaître la liste des niveaux de gravité, reportez-vous à la section «Niveaux de gravité des journaux» .
logging console <i>niveau</i>	Limite les messages consignés sur la console en fonction de leur gravité.
logging buffered <i>niveau</i>	Limite les messages syslog affichés à partir d'un tampon interne (RAM) en fonction de leur gravité.
logging file level	Limite les messages syslog envoyés au fichier de journalisation en fonction de leur gravité.
clear logging	Efface les journaux.
clear logging file	Efface les messages du fichier de journalisation.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# logging on

Console (config)# logging console errors

Console (config)# logging buffered debugging

Console (config)# logging file alerts

Console (config)# clear logging

Console (config)# exit

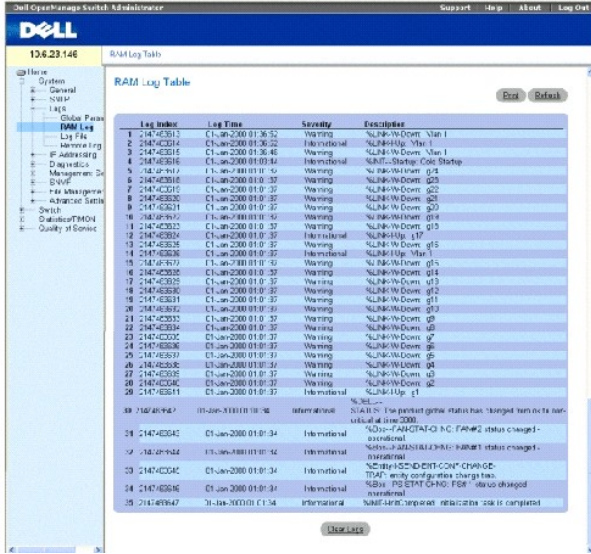
Console# clear logging file

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

Affichage de la table des journaux en RAM

La page [RAM Log Table](#) (Table des journaux en RAM) contient des informations relatives aux entrées de journaux stockées en RAM, notamment l'heure de création du journal, sa gravité ou encore sa description. Pour ouvrir la page [RAM Log Table](#), cliquez sur System (Système) → Logs (Journaux) → RAM Log (Journal en RAM) dans l'arborescence.

Figure 6-30. Table des journaux en RAM



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 (Gravité) — Indique la gravité du journal.

Description — Description définie par l'utilisateur pour le journal.

Suppression d'informations de journalisation :

- Ouvrez la page [RAM Log Table](#) (Table des journaux en RAM).
- Cliquez sur **Clear Log** (Effacer le journal).

Les informations de journalisation sont supprimés de la [table des journaux en RAM](#) et le périphérique est mis à jour.

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

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage et l'effacement des champs de la page [RAM Log Table](#) (Table des journaux en RAM).

Tableau 6-23. 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.

Vous trouverez ci-dessous un exemple de commande CLI :

```


```

```
console# show logging
```

```
La journalisation est activée.
```

```
Journalisation console : Niveau info. Messages console : 0 rejetés.
```

```
Journalisation tampon : Niveau info. Messages tampon : 26 consignés, 26 affichés, 200 maxi.
```

```
Journalisation fichiers : Niveau erreur. Messages fichiers : 157 consigné, 26 rejetés.
```

```
1 message n'a pas été consigné
```

```
01-Jan-2000 01:03:42 :%INIT-I-Startup: Démarrage à froid
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g24
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g23
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g22
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g21
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g20
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g19
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g18
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g17
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g13
```

```
1-Jan-2000 01:01:36 :%LINK-W-Down: g2
```

```
01-Jan-2000 01:01:36 :%LINK-W-Down: g1
```

```
01-Jan-2000 01:01:32 :%INIT-I-InitCompleted: Initialisation terminée
```

```
Console # clear logging
```

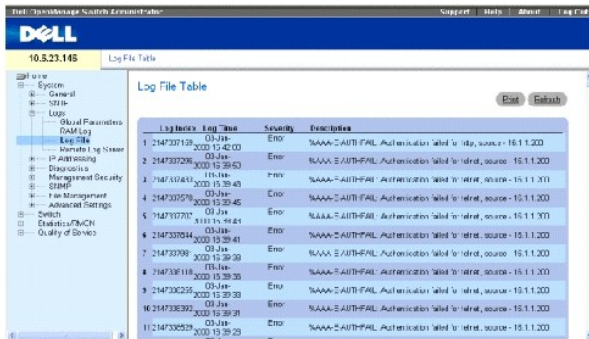
```
clear logging buffer [y/n]?
```

```
console#
```

Affichage de la table des fichiers journaux

La page [Log File Table](#) (Table des fichiers journaux) contient des informations sur les entrées de journaux enregistrées dans le fichier journal stocké en mémoire FLASH, notamment l'heure de création du journal, sa gravité et une description du message de journalisation. Pour ouvrir la page [Log File Table](#), cliquez sur System (Système) → Logs (Journaux) → Log File (Fichier journal) dans l'arborescence.

Figure 6-31. Table des fichiers journaux



The screenshot shows the 'Log File Table' interface. The table has the following columns: Log Index, Log Time, Severity, and Description. The data rows are as follows:

Log Index	Log Time	Severity	Description
1	2147327132 03:14:03	Error	%AAA-AUTH-FAIL: Authentication failed to http, source - 15.1.1.200
2	2147327226 03:14:03	Error	%AAA-AUTH-FAIL: Authentication failed to http, source - 15.1.1.200
3	2147327319 03:14:03	Warn	%AAA-AUTH-FAIL: Authentication failed to http, source - 15.1.1.200
4	2147327359 03:14:03	Error	%AAA-AUTH-FAIL: Authentication failed to http, source - 15.1.1.200
5	2147327371 03:14:03	Error	%AAA-AUTH-FAIL: Authentication failed to http, source - 15.1.1.200
6	2147327384 03:14:03	Error	%AAA-AUTH-FAIL: Authentication failed to http, source - 15.1.1.200
7	2147327398 03:14:03	Error	%AAA-AUTH-FAIL: Authentication failed to http, source - 15.1.1.200
8	2147327418 03:14:03	Warn	%AAA-AUTH-FAIL: Authentication failed to http, source - 15.1.1.200
9	2147327435 03:14:03	Warn	%AAA-AUTH-FAIL: Authentication failed to http, source - 15.1.1.200
10	2147327450 03:14:03	Error	%AAA-AUTH-FAIL: Authentication failed to http, source - 15.1.1.200
11	2147327457 03:14:03	Error	%AAA-AUTH-FAIL: Authentication failed to http, source - 15.1.1.200

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 (Gravité) — Indique la gravité du journal.

Description — Texte du message de journalisation.

Affichage de la table des fichiers journaux à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage et la configuration des champs de la page [Log File Table](#) (Table des fichiers journaux).

Tableau 6-24. Commandes CLI de la table des fichiers journaux

Commande CLI	Description
show logging file	Affiche l'état de la consignation et les messages syslog stockés dans le fichier de journalisation.
clear logging file	Efface les messages du fichier journal.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console # show logging file
```

```
La journalisation est activée.
```

```
Journalisation console : Niveau info. Messages console : 0 rejetés.
```

Journalisation tampon : Niveau info. Messages tampon : 62 consignés, 62 affichés, 200 maxi.

Journalisation fichiers : Débogage niveau. Messages fichiers : 11 consignés, 51 rejetés.

Journalisation serveur SysLog 12.1.1.2 : avertissement. Messages : 14 rejetés.

Journalisation serveur SysLog 1.1.1.1 : info. Messages : 0 rejetés.

1 message n'a pas été consigné

01-Jan-2000 01:12:01 :%COPY-W-TRAP: L'opération de copie s'est terminée avec succès

01-Jan-2000 01:11:49 :%LINK-I-Up: g21

01-Jan-2000 01:11:49 :%2SWPHY-I-CHNGCOMBOMEDIA: Support cuivre modifié

en support fibre (1000BASE-SX) sur le port g21.

01-Jan-2000 01:11:48 :%2SWPHY-I-CHNGCOMBOMEDIA: Support fibre modifié en support cuivre sur le port g21.

01-Jan-2000 01:11:48 :%LINK-W-Down: g21

01-Jan-2000 01:11:46 :%LINK-I-Up: g19

01-Jan-2000 01:11:42 :%LINK-W-Down: g14

01-Jan-2000 01:11:41 :%LINK-I-Up: g14

01-Jan-2000 01:11:36 :%LINK-W-Down: g9

01-Jan-2000 01:11:35 :%LINK-I-Up: g1

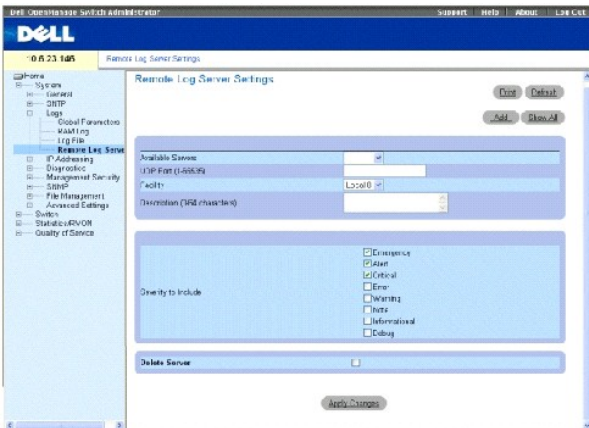
01-Jan-2000 01:11:34 :%LINK-W-Down: g1

console#

Configuration de la page 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 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 gravité des journaux à chaque serveur. Pour ouvrir la page [Remote Log Server Settings](#), cliquez sur System (Système) → Logs (Journaux) → Remote Log Server (Serveur de journalisation à distance) dans l'arborescence.

Figure 6-32. Paramètres des serveurs de journalisation à distance



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) — Application, définie par l'utilisateur, à partir de laquelle les journaux système sont envoyés au serveur distant. Une seule voie de transmission peut être affectée à un même serveur. Si une deuxième voie de transmission est affectée, la première voie est annulée. Toutes les applications définies pour un périphérique utilisent la même voie de transmission sur un serveur. Ce champ peut prendre les valeurs suivantes :

Local 0 - Local 7.

Description (0-64 Characters) Description (0-64 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) contient également une liste de niveaux de gravité. Les définitions de niveaux de gravité sont identiques à celles de la page [Global Log Parameters](#) (Paramètres globaux de journalisation).

Envoi de journaux à un serveur :

1. Ouvrez 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. Renseignez les champs.
4. Sélectionnez la gravité du journal à l'aide des cases à cocher **Severity to Include** (Gravité à inclure).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Définition d'un nouveau serveur :

1. Ouvrez 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'ouvre :

Figure 6-33. Ajouter un serveur de journalisation

Add a Log Server

Refresh

New Log Server IP Address [] [Refresh]

UDP Port (1-65535) 514

Facility Local7

Description (0-64 characters) []

Severity to include

- Emergency
- Alert
- Critical
- Error
- Warning
- Note
- Informational
- Debug

Apply Changes

New Log Server IP Address (Adresse IP du nouveau serveur de journalisation) — Indique l'adresse IP du nouveau serveur de journalisation.

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

Le serveur est défini et ajouté à la liste des serveurs disponibles.

Affichage de la table des serveurs de journalisation à distance :

1. Ouvrez la page [Remote Log Server Settings](#) (Paramètres des serveurs de journalisation à distance).
2. Cliquez sur **Show All** (Afficher tout).

La page [Remote Log Servers Table](#) (Table des serveurs de journalisation à distance) s'ouvre :

Figure 6-34. Table des serveurs de journalisation à distance

Remote Log Servers Table

Refresh

Server	UDP Port	Facility	Description	Minimum Severity	Remove
--------	----------	----------	-------------	------------------	--------

Apply Changes

Suppression d'un serveur de la page Log Server Table (Table des serveurs de journalisation) :

1. Ouvrez la page [Remote Log Server Settings](#) (Paramètres des serveurs de journalisation à distance).
2. Cliquez sur **Show All** (Afficher tout).

La page [Remote Log Servers Table](#) (Table des serveurs de journalisation à distance) s'ouvre :

3. Sélectionnez une entrée dans la [table des serveurs de journalisation à distance](#).
4. Cochez la case **Remove** (Supprimer) pour supprimer le(s) serveur(s).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée de la [table des serveurs de journalisation à distance](#) est supprimée et le périphérique est mis à jour.

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

Le tableau suivant récapitule les commandes CLI équivalentes pour l'utilisation de serveurs de journalisation à distance.

Tableau 6-25. Commandes CLI des serveurs de journalisation à distance

Commande CLI	Description
logging (<i>adresse ip nom d'hôte</i>) [<i>port port</i>] [<i>severity niveau</i>] [<i>facility voie de transmission</i>] description <i>texte</i>	Consigne les messages sur un serveur distant.
no logging	Supprime un serveur syslog.
show logging	Affiche l'état de la consignation et les messages syslog.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console> enable

console#configure

console (config) # logging 10.1.1.1 severity critical

Console # show logging

La journalisation est activée.

Journalisation console : Débogage niveau. Messages console : 5 rejetés.

Journalisation tampon : Débogage niveau. Messages tampon : 16 consignés, 16 affichés, 200 maxi.

Journalisation fichiers : Niveau erreur. Messages fichiers : 0 consigné, 209 rejetés.

Journalisation serveur SysLog 31.1.1.2 : erreur. Messages : 22 rejetés.

Journalisation serveur SysLog 5.2.2.2 : info. Messages : 0 rejeté.

Journalisation serveur SysLog 10.2.2.2 : critique. Messages : 21 rejetés.

Journalisation serveur SysLog 10.1.1.1 : critique. Messages : 0 rejetés.

1 message n'a pas été consigné

03-Mar-2004 12:02:03 :%LINK-I-Up: g1

03-Mar-2004 12:02:01 :%LINK-W-Down: g2
```

Définition d'adresses IP pour le périphérique

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'assigner des périphériques de type passerelle. Les paquets sont transmis à l'IP par défaut lors de l'envoi des 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 :

Default Gateway (Passerelle par défaut) — Adresse IP du périphérique faisant office de passerelle.

Remove (Supprimer) — Supprime des périphériques de la liste déroulante **Default Gateway** (Passerelle par défaut).

Sélection d'un périphérique passerelle :

1. Ouvrez 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 est sélectionnée et le périphérique est mis à jour.

Suppression d'une passerelle par défaut :

1. Ouvrez la page **Default Gateway** (Passerelle par défaut).
2. Cochez la case **Remove** (Supprimer) pour supprimer la passerelle par défaut.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée de passerelle par défaut est supprimée et le périphérique est mis à jour.

Définition de passerelles à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs affichés dans la page **Default Gateway** (Passerelle par défaut).

Tableau 6-26. Commandes CLI des passerelles par défaut

Commande CLI	Description
<code>ip default-gateway adresse-ip</code>	Définit une passerelle par défaut.
<code>no ip default-gateway</code>	Supprime une passerelle par défaut.

Vous trouverez ci-dessous un exemple de commande CLI :

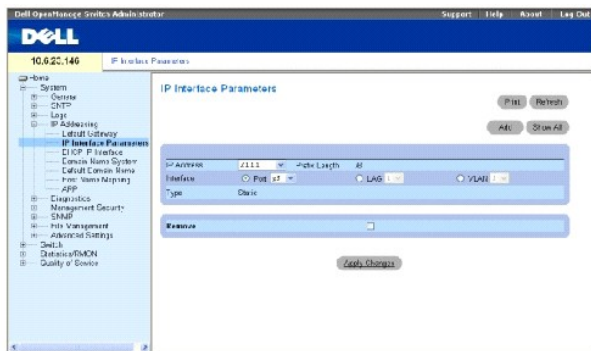
```
Console(config)# ip default-gateway 196.210.10.1
```

```
Console (config)# no ip default-gateway
```

Définition d'interfaces IP

La page [IP Interface Parameters](#) (Paramètres d'interface IP) contient des champs permettant d'affecter des adresses IP aux interfaces. Pour ouvrir la page [IP Interface Parameters](#), cliquez sur **System** (Système) → **IP Addressing** (Adressage IP) → **Interface Parameters** (Paramètres d'interface) dans l'arborescence.

Figure 6-35. Paramètres d'interface IP



IP Address (Adresse IP) — Adresse IP de l'interface.

Prefix Length (Longueur du préfixe) — Nombre de bits qui comprennent le préfixe de l'adresse IP source ou le masque de réseau de l'adresse IP source.

Interface — Type d'interface pour lequel l'adresse IP sélectionnée est définie. Sélectionnez **Port**, **LAG** ou **VLAN**.

Pour plus d'informations, reportez-vous à la section [«Configuration des VLAN»](#).

Type — Indique si l'adresse IP a été définie en tant qu'adresse IP statique ou non.

Forward Directed IP Broadcasts (Transmettre des diffusions IP dirigées) — Active la traduction d'une diffusion dirigée en diffusions physiques. Si vous désactivez ce paramètre, les diffusions dirigées IP sont rejetées et ne sont pas transmises.

Broadcast Type (Type de diffusion) — Définit une adresse de diffusion de l'interface.

One Fill — L'adresse de diffusion de l'interface est One Fill (255.255.255.255).

Zero Fill — L'adresse de diffusion de l'interface est Zero Fill (0.0.0.0).

Remove (Supprimer) — Supprime l'interface sélectionnée de la liste déroulante **IP Address** (Adresse IP).

Ajout d'une interface IP

1. Ouvrez la page [IP Interface Parameters](#) (Paramètres d'interface IP).
2. Cliquez sur **Ajouter**.

La page [Add a Static Interface](#) (Ajouter une interface statique) s'ouvre :

Figure 6-36. Ajouter une interface statique

The screenshot shows a configuration window titled "Add a Static IP Interface". It contains the following fields and controls:

- Source IP Address:** A text input field with a placeholder "(X.X.X.X)".
- Network Mask:** A text input field with a placeholder "(X.X.X.X)".
- Prefix Length:** A dropdown menu with "1/24" selected.
- Interface:** Radio buttons for "Gigabit Ethernet" (selected), "LAG", and "VLAN".
- Buttons:** "Refresh" (top right) and "Apply Changes" (bottom center).

3. Renseignez les champs de cette page.

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

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

La nouvelle interface est ajoutée et le périphérique est mis à jour.

Modifications des paramètres d'adresse IP

1. Ouvrez la page [IP Interface Parameters](#) (Paramètres d'interface IP).
2. Sélectionnez une adresse IP dans le menu déroulant **IP Address** (Adresse IP).
3. Modifiez les champs souhaités.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Suppression d'adresses IP

1. Ouvrez la page [IP Interface Parameters](#) (Paramètres d'interface IP).
2. Cliquez sur **Show All** (Afficher tout).

La **table des paramètres d'interface** s'ouvre :

Figure 6-37. Table des paramètres d'interface IP

The screenshot shows a table titled "IP Interface Parameter Table" with the following data:

	IP Address	Prefix Length	Interface	Type	Remove
1	2.1.1	/8	g3	Static	<input type="checkbox"/>
2	10.1.254.48	/24	g1/2	DHCP	<input type="checkbox"/>
3	16.1.1.3	/8	g1	Static	<input type="checkbox"/>

Buttons: "Refresh" (top right) and "Apply Changes" (bottom center).

3. Sélectionnez une adresse IP et cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse IP sélectionnée est supprimée et le périphérique est mis à jour.

Définition des interfaces IP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [IP Interface Parameters](#) (Paramètres d'interface IP).

Tableau 6-27. Commandes CLI des paramètres d'interface IP

Commande CLI	Description
<code>ip address adresse-ip {masque longueur de préfixe}</code>	Définit une adresse IP.
<code>no ip address [adresse-ip]</code>	Supprime une adresse IP.
<code>show ip interface [ethernet interface-numéro vlan id-vlan port-channel numéro]</code>	Affiche l'état d'utilisabilité des interfaces IP.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console(config)# interface vlan 1

Console(config-if)# ip address 131.108.1.27 255.255.255.0

Console (config-if)# no ip address 131.108.1.27

Console (config-if)# exitconsole# show ip interface vlan 1

Output

État Activité Adresse IP Passerelle
-----
192.168.1.1 Active

Type interface adresse-IP
-----

192.168.1.123 /24 VLAN 1 Statique
```

Définition de paramètres d'interface IP DHCP

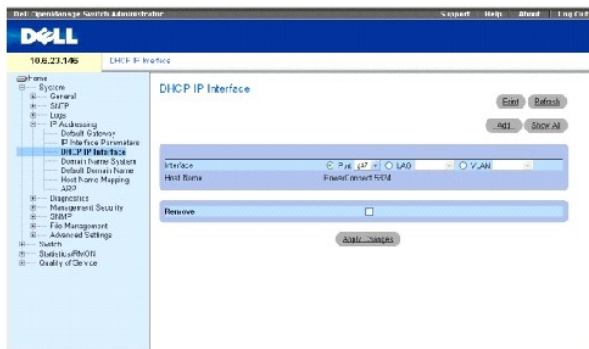
```
console# show ip interface vlan 1
```

Sortie

Adresse IP de la passerelle	État activité	
-----	-----	
192.168.1.1	Actif	
Adresse IP	Interface	Type
-----	-----	-----
192.168.1.123 /24	VLAN 1	Statique

La page [DHCP IP Interface](#) (Interface IP DHCP) contient des champs permettant de définir les clients DHCP connectés au périphérique. Cliquez sur **System** (Système) → **IP Addressing** (Adressage IP) → **DHCP IP Interface** (Interface IP DHCP) dans l'arborescence pour ouvrir la page [DHCP IP Interface](#).

Figure 6-38. Interface IP DHCP



Interface — Interface spécifique connectée au périphérique. Cliquez sur le bouton d'option en regard des champs **Port**, **LAG** ou **VLAN** et sélectionnez l'interface connectée au périphérique.

Host Name (Nom d'hôte) — Nom du système. Ce champ peut contenir 20 caractères.

Remove (Supprimer) — Supprime les clients DHCP.

Ajout de clients DHCP

1. Ouvrez la page [DHCP IP Interface](#) (Interface IP DHCP).
2. Cliquez sur **Add** Ajouter.

La page **Add DHCP IP Interface** (Ajouter une interface IP DHCP) s'ouvre.

3. Renseignez les champs de la page.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'interface DHCP est ajoutée et le périphérique est mis à jour.

Modification d'une interface IP DHCP

1. Ouvrez la page [DHCP IP Interface](#) (Interface IP DHCP).
2. Modifiez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Suppression d'une interface IP DHCP DHCP IP

1. Ouvrez la page [DHCP IP Interface](#) (Interface IP DHCP).
2. Cliquez sur **Show All** (Afficher tout).

La **table des clients DHCP** s'ouvre.

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 le périphérique est mis à jour.

Définition d'interfaces IP DHCP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des clients DHCP.

Tableau 6-28. Commandes CLI de l'interface IP DHCP

Commande CLI	Description
<code>ip address dhcp [hostname nom d'hôte]</code>	Permet d'acquérir une adresse IP sur une interface Ethernet à partir du protocole DHCP (Protocole de configuration dynamique de l'hôte).

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console> enable

console#config

console (config#) interface ethernet g1

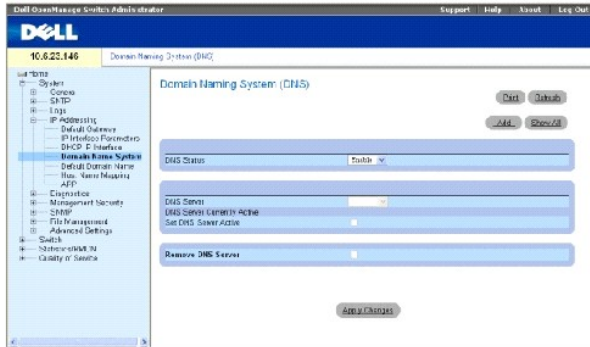
console (config-if)# ip address dhcp 10.0.0.1 /8
```

Configuration de systèmes de noms de domaine

Le DNS (système de noms de domaine) convertit les noms de domaine définis par l'utilisateur en adresses IP. Chaque fois qu'un nom de domaine est assigné, le service DNS le traduit en adresse IP numérique. Par exemple, `www.ipexample.com` est traduit en `192.87.56.2`. Les serveurs DNS gèrent les bases de données de noms de domaine et les adresses IP correspondantes.

La page **Domain Naming System (DNS)** (Système de noms de domaine (DNS)) contient des champs permettant d'activer des serveurs DNS spécifiques. Pour ouvrir la page **Domain Naming System (DNS)**, cliquez sur **System** (Système) → **IP Addressing** (Adressage IP) → **Domain Name System** (Système de nom de domaine) dans *l'arborescence*.

Figure 6-39. Système de noms de domaine (DNS)



DNS Status (État DNS) — Active ou désactive la traduction de noms DNS en adresses IP.

DNS Server (Serveur DNS) — Dresse la liste des serveurs DNS. Les serveurs DNS sont ajoutés sur la page **Add DNS Server** (Ajouter un serveur DNS).

DNS Server Currently Active (Serveur DNS actif) — Serveur DNS désigné comme serveur DNS actif.

Set DNS Server Active (Configurer le serveur DNS actif) — Active le serveur DNS sélectionné dans le champ **DNS Server** (Serveur DNS).

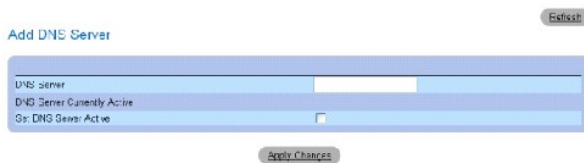
Remove DNS Server (Supprimer le serveur DNS) — Supprime les serveurs DNS.

Ajout d'un serveur DNS

1. Ouvrez la page **Domain Naming System (DNS)** (Système de noms de domaine (DNS)).
2. Cliquez sur **Add** Ajouter.

La page **Add DNS Server** (Ajouter un serveur DNS) s'ouvre :

Figure 6-40. Ajouter un serveur DNS



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

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

Affichage de la table des serveurs DNS

1. Ouvrez la page **Domain Naming System (DNS)** (Système de noms de domaine (DNS)).
2. Cliquez sur **Show All** (Afficher tout).

La **table des serveurs DNS** s'ouvre :

Figure 6-41. Table des serveurs DNS

DNS Server Table



Suppression de serveurs DNS

1. Ouvrez la page **Domain Naming System (DNS)** (Système de noms de domaine (DNS)).
2. Cliquez sur **Show All** (Afficher tout).
3. La **table des serveurs DNS** s'ouvre.
4. Sélectionnez une entrée de la **table des serveurs DNS**.
5. Cochez la case **Remove** (Supprimer).
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Configuration de serveurs DNS à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI pour la configuration des informations système du périphérique.

Tableau 6-29. Commandes CLI des serveurs DNS

Commande CLI	Description
<code>ip name-server adresse-serveur</code>	Configure les serveurs de noms disponibles. Vous pouvez définir jusqu'à huit serveurs de noms.
<code>no ip name-server adresse-serveur</code>	Supprime un serveur de noms.
<code>ip domain-name nom</code>	Définit un nom de domaine par défaut que le logiciel utilise pour compléter les noms d'hôtes non qualifiés.
<code>clear host { nom * }</code>	Supprime les entrées de la mémoire cache nom d'hôte-à-adresse.
<code>show hosts [nom]</code>	Affiche le nom de domaine par défaut, une liste des hôtes du serveur de noms, la liste statique et mise en mémoire cache des noms d'hôtes et des adresses.

Vous trouverez ci-dessous un exemple de commande CLI :

```
console> enable

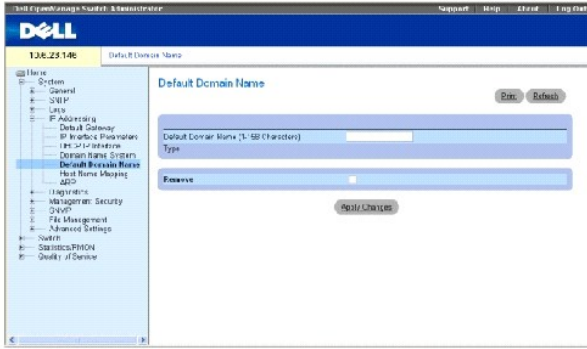
Console# configure

console (config)# ip name-server 176.16.1.18
```

Définition de domaines par défaut

La page **Default Domain Name** (Nom de domaine par défaut) fournit des informations permettant de définir des noms de domaine DNS par défaut. Pour ouvrir la page **Default Domain Name**, cliquez sur **System** (Système) → **IP Addressing** (Adressage IP) → **Default Domain Name** (Nom de domaine par défaut) dans l'arborescence.

Figure 6-42. Nom de domaine par défaut



Default Domain Name (1-158 Characters) (Nom de domaine par défaut [1 à 158 caractères]) — Contient un serveur de noms de domaine DNS défini par l'utilisateur. Le nom de domaine DNS est le domaine par défaut.

Type — Type du domaine si celui-ci a été créé de façon statique ou dynamique.

Remove (Supprimer) — Supprime un domaine sélectionné.

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

Le tableau suivant récapitule les commandes CLI pour la configuration des noms de domaine DNS.

Tableau 6-30. Commandes CLI des noms de domaine DNS

Commande CLI	Description
ip domain-name <i>nom</i>	Définit un nom de domaine par défaut que le logiciel utilise pour compléter les noms d'hôtes non qualifiés.
no ip domain-name	Désactive l'utilisation du DNS (système de noms de domaine).
show hosts [<i>nom</i>]	Affiche le nom de domaine par défaut, une liste des hôtes du serveur de noms, la liste statique et mise en mémoire cache des noms d'hôtes et des adresses.

Vous trouverez ci-dessous un exemple de commande CLI :

```

console> enable

console# configure

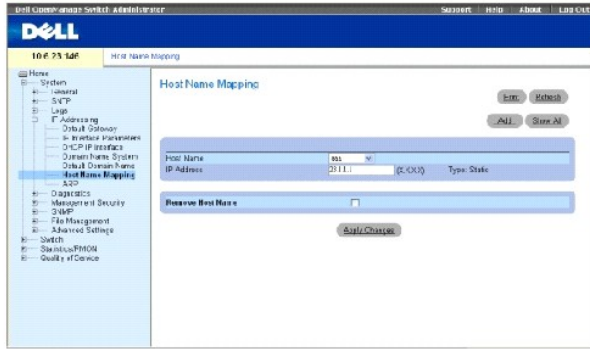
console (config)# ip domain-name www.dell.com

```

Adressage d'hôtes de domaine

La page **Host Name Mapping** (Adressage de noms d'hôtes) fournit des paramètres permettant d'assigner des adresses IP de noms d'hôtes statiques. La page **Host Name Mapping** fournit jusqu'à huit adresses IP par hôte. Pour ouvrir la page **Host Name Mapping**, cliquez sur **System** (Système) → **IP Addressing** (Adressage IP) → **Host Name Mapping** (Adressage de noms d'hôtes).

Figure 6-43. Adressage de noms d'hôtes



Host Name (Nom d'hôte) — Dresse une liste des noms d'hôtes. Les noms d'hôtes sont définis sur la page **Add Host Name Mapping** (Ajouter un adressage de nom d'hôte). Chaque hôte fournit jusqu'à huit adresses IP. Les valeurs admises pour le champ Host Name (Nom d'hôte) sont les suivantes :

IP Address (Adresse IP) (X.X.X.X) — Fournit jusqu'à huit adresses IP assignées au nom d'hôte spécifié.

Type — Type de l'adresse IP. Ce champ peut prendre les valeurs suivantes :

Dynamic (Dynamique) — L'adresse IP a été créée en mode Dynamique.

Static (Statique) — L'adresse IP est une adresse IP statique.

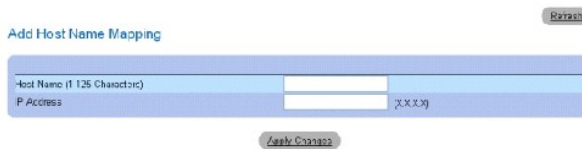
Remove Host Name Mapping (Supprimer l'adressage de nom d'hôte) — Supprime l'adressage d'hôte DNS.

Ajout de noms de domaine d'hôte

1. Ouvrez la page **Host Name Mapping** (Adressage de noms d'hôtes).
2. Cliquez sur **Add** Ajouter.

La page **Add Host Name Mapping** (Ajouter un adressage de nom d'hôte) s'ouvre :

Figure 6-44. Ajouter un adressage de nom d'hôte



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

L'adresse IP est adressée au nom d'hôte et le périphérique est mis à jour.

Affichage de la table d'adressage des noms d'hôtes

1. Ouvrez la page **Host Name Mapping** (Adressage de noms d'hôtes).
2. Cliquez sur **Show All** (Afficher tout).

La **table d'adressage des noms d'hôtes** s'ouvre :

Figure 6-45. Table d'adressage des noms d'hôtes

Hosts Name Mapping Table

Refresh

Host Name	IP Address	Remove Select All
1 aaa	192.1.1	<input type="checkbox"/>
2 www.com	231.1.1	<input type="checkbox"/>

Apply Changes

Suppression d'un nom d'hôte de l'adressage des adresses IP

1. Ouvrez la page **Host Name Mapping** (Adressage de noms d'hôtes).
2. Cliquez sur **Show All** (Afficher tout).
3. La **table d'adressage des hôtes** s'ouvre.
4. Sélectionnez une entrée de la **table d'adressage des hôtes**.
5. Cochez la case **Remove** (Supprimer).
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Adressage d'une adresse IP à des noms d'hôtes de domaine à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'adressage de noms d'hôtes de domaine à des adresses IP.

Tableau 6-31. Commandes CLI des noms d'hôtes de domaine

Commande CLI	Description
ip host name <i>adresse1</i> [<i>adresse2</i> ... <i>adresse8</i>]	Définit l'adressage statique nom d'hôte-à-adresse dans la mémoire cache de l'hôte.
no ip host name	Supprime l'adressage nom-à-adresse.
clear host { <i>nom</i> * }	Efface les entrées de la mémoire cache nom d'hôte-à-adresse.
show hosts [<i>nom</i>]	Affiche le nom de domaine par défaut, une liste des hôtes du serveur de noms, la liste statique et mise en mémoire cache des noms d'hôtes et des adresses.

Vous trouverez ci-dessous un exemple de commande CLI :

```
console# enable
```

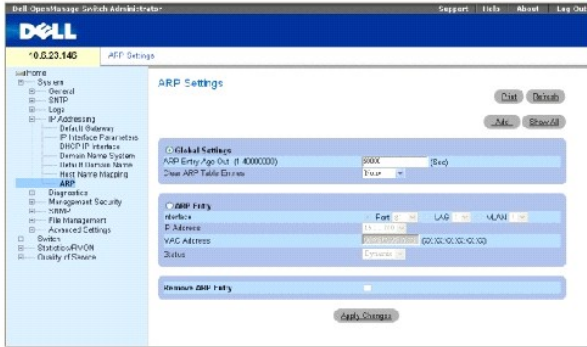
```
console# configure
```

```
console (config)# ip host accounting.abc.com 176.10.23.1
```

Configuration du protocole ARP

Le protocole ARP (Protocole de résolution d'adresse) est un protocole TCP/IP qui convertit les adresses IP en adresses physiques. Les entrées statiques peuvent être définies dans la **table ARP**. Lors de la définition des entrées statiques, une entrée permanente est créée et elle est ensuite utilisée pour convertir les adresses IP en adresses MAC. Pour ouvrir la page [ARP Settings](#) (Paramètres ARP), cliquez sur System (Système) → IP Addressing (Adressage IP) → ARP dans l'arborescence.

Figure 6-46. Paramètres ARP



Global Settings (Paramètres globaux) — Sélectionnez cette option pour activer les champs des paramètres globaux ARP.

ARP Entry Age Out (1-4000000) (Délai d'expiration de l'entrée ARP [1-4000000]) — Pour tous les périphériques, délai qui peut s'écouler (en secondes) entre les demandes ARP relatives à une entrée de la table ARP. Ce délai écoulé, l'entrée est supprimée de la table. La plage est comprise entre 1 et 4000 000, zéro indiquant que les entrées ne sont jamais effacées de la mémoire cache. La valeur par défaut est 60 000 secondes.

Clear ARP Table Entries (Effacer les entrées de la table ARP) — Type des entrées ARP à effacer sur tous les périphériques. Les valeurs possibles sont les suivantes :

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 un seul périphérique.

Interface — Numéro d'interface du port, du LAG ou du VLAN connecté au périphérique.

IP Address (Adresse IP) — Adresse IP de la station associée à l'adresse MAC renseignée 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. Ce champ peut prendre les valeurs suivantes :

Dynamic (Dynamique) — L'entrée ARP a été obtenue de façon dynamique.

Static (Statique) — L'entrée ARP est une entrée statique.

Remove ARP Entry (Supprimer l'entrée ARP) — Supprime une entrée ARP.

Ajout d'une entrée statique dans la table ARP :

1. Ouvrez la page [ARP Settings](#) (Paramètres ARP).
2. Cliquez sur **Add** Ajouter.

La page **Add ARP Entry** (Ajouter une entrée ARP) s'ouvre :

Figure 6-47. Ajouter une entrée ARP

The screenshot shows the 'Add ARP Entry' configuration page. At the top right is a 'Refresh' button. Below it is a form with three main fields: 'Interface' (with a dropdown menu), 'IP Address' (with a text input containing '0.0.0.0' and a '[?] [X]' icon), and 'MAC Address' (with a text input containing '000000000000' and a '[?] [X]' icon). At the bottom center is an 'Apply Changes' button.

3. Sélectionnez une interface.
4. Renseignez les champs.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée de la **table ARP** est ajoutée et le périphérique est mis à jour.

Affichage de la table ARP

1. Ouvrez la page [ARP Settings](#) (Paramètres ARP).
2. Cliquez sur **Show All** (Afficher tout).

La **table ARP** s'ouvre :

Figure 6-48. Table ARP

The screenshot shows the 'ARP Table' configuration page. At the top right is a 'Refresh' button. Below it is a table with the following data:

	Interface	IP Address	MAC Address	Status	Remove
1	g1	15.1.1.200	0003c3951793	Dynamic	<input type="checkbox"/>
2	g-7	10.6.23.129	0003e00010d	Dynamic	<input type="checkbox"/>

At the bottom center is an 'Apply Changes' button.

Suppression d'une entrée de la table ARP

1. Ouvrez la page [ARP Settings](#) (Paramètres ARP).
2. Cliquez sur **Show All** (Afficher tout).

La page **ARP Table** (Table ARP) s'ouvre.

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

L'entrée de la **table ARP** est supprimée et le périphérique est mis à jour.

Configuration d'ARP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [ARP Settings](#) (Paramètres ARP).

Tableau 6-32. Commandes CLI des paramètres ARP

Commande CLI	Description
<code>arp adr_ip adr_hw { ethernet interface-numéro vlan id-vlan port-channel numéro }</code>	Ajoute une entrée permanente dans la mémoire cache ARP.
<code>arp timeout secondes</code>	Indique la durée pendant laquelle une entrée est conservée dans la mémoire cache ARP.
<code>clear arp-cache</code>	Supprime toutes les entrées dynamiques de la mémoire cache ARP.
<code>show arp</code>	Affiche les entrées de la table ARP.
<code>no arp</code>	Supprime une entrée de la table ARP.

Vous trouverez ci-dessous un exemple de commande CLI :

```

Console(config)# arp 198.133.219.232 00-00-0c-40-0f-bc

Console (config)# exit

Console# arp timeout 12000

Console# show arp

Délai ARP : 80 000 secondes

```

Interface	Adresse IP	Adresse matérielle	État
-----	-----	-----	-----
g1	10.7.1.102	00:10:B5:04:DB:4B	Dynamique
g2	10.7.1.135	00:50:22:00:2A:A4	Statique

Exécution de diagnostics sur les câbles

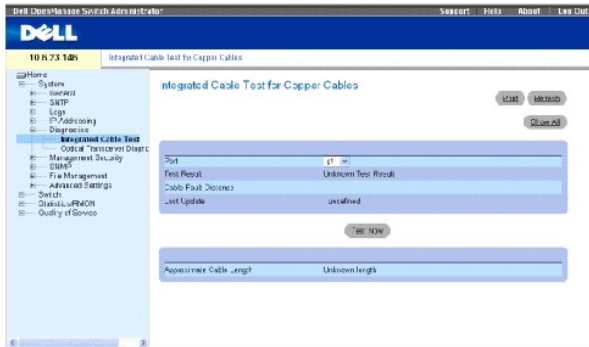
La page **Diagnostics** contient des liens vers des pages permettant d'effectuer des tests de câbles virtuels sur les câbles en cuivre et en fibres optiques. Pour ouvrir la page **Diagnostics**, cliquez sur **System (Système)** → **Diagnostics** dans l'arborescence.

Affichage des diagnostics sur les câbles en cuivre

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

Pour ouvrir la page [Integrated Cable Test for Copper Cables](#) (Test de câble intégré pour câbles en cuivre), cliquez sur **System (Système)** → **Diagnostics** → **Integrated Cable Test** (Test de câble intégré) dans l'arborescence.

Figure 6-49. Test de câble intégré pour câbles en cuivre



Port — Port auquel le câble est raccordé.

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

No Cable (Pas de câble) — Aucun câble n'est raccordé au port.

Open Cable (Câble ouvert) — Le câble n'est raccordé que d'un seul côté.

Short Cable (Câble en court-circuit) — Un court-circuit est survenu sur le câble.

OK — Le câble a réussi le test.

Fiber Cable (Câble en fibres) — Un câble en fibres est raccordé au port.

Cable Fault Distance (Distance de défaut du câble) — Distance depuis le port où l'erreur de câble est survenue.

Last Update (Dernière mise à jour) — Dernière fois que le port a été testé.

Approximate Cable Length (Longueur approximative des câbles) — Longueur approximative des câbles. Ce test ne peut être effectué que lorsque le port est actif et qu'il fonctionne à 1 Gbps.

Réalisation d'un test de câble

1. Assurez-vous que les deux extrémités du câble en cuivre sont raccordées à un périphérique.
2. Ouvrez la page [Integrated Cable Test for Copper Cables](#) (Test de câble intégré pour câbles en cuivre).
3. Cliquez sur **Test Now** (Tester maintenant).

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

Affichage de la table des résultats des tests de câbles virtuels

1. Ouvrez la page [Integrated Cable Test for Copper Cables](#) (Test de câble intégré pour câbles en cuivre).
2. Cliquez sur **Show All** (Afficher tout).

La **table des résultats des tests de câbles virtuels** s'ouvre.

Réalisation de tests de câbles en cuivre à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la réalisation de tests de câbles en cuivre.

Tableau 6-33. Commandes CLI des tests de câbles en cuivre

Commande CLI	Description
<code>test copper-port tdr <i>interface</i></code>	Effectue les tests VCT.
<code>show copper-port tdr [<i>interface</i>]</code>	Affiche les résultats des derniers tests VCT effectués sur les ports.
<code>show copper-port cable-length [<i>interface</i>]</code>	Affiche une estimation de la longueur du câble en cuivre raccordé à un port.

Vous trouverez ci-dessous un exemple de commande CLI :


```
console> enable

Console# test copper-port tdr g3

Le câble est ouvert à 100 mètres.

Console> show copper-ports tdr
```

Port	Résultat	Longueur [mètres]	Date
----	-----	-----	----
g1	OK		
g2	Court-circuit	50	13:32:00 15 janvier 2004
g3	Aucun test n'a été réalisé		
g4	Ouvrir	64	13:32:00 15 janvier 2004
g5	Fibre	-	-

 **REMARQUE** : La longueur de câble renvoyée est une approximation dans les plages de 50 mètres, 50 m à 80 m, 80 m à 110 m, 110 m à 120 m ou plus de 120 m. La déviation peut se faire sur 20 mètres.

Affichage des diagnostics d'émetteurs-récepteurs optiques

La page [Optical Transceiver Diagnostics](#) (Diagnostic d'émetteurs-récepteurs optiques) contient des champs permettant de réaliser des tests sur des câbles en fibres optiques. Pour ouvrir la page [Optical Transceiver Diagnostics](#) (Diagnostics d'émetteurs-récepteurs optiques), cliquez sur **System** (Système) → **Diagnostics** → **Optical Transceiver Diagnostics** (Diagnostic d'émetteur-récepteurs optiques) dans l'arborescence.


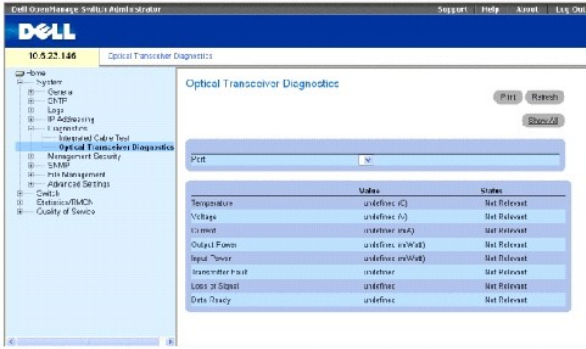
 **REMARQUE** : Les diagnostics d'émetteurs-récepteurs optiques ne peuvent être réalisés que si la liaison est présente.

Figure 6-50. Diagnostics d'émetteurs-récepteurs optiques



Port — Port auquel le câble en fibres est raccordé.

Temperature (Température) — Température (C) de fonctionnement du câble.

Voltage (Tension) — Tension de fonctionnement du câble.

Current (Courant) — Courant de fonctionnement du câble.

Output Power (Puissance de sortie) — Niveau auquel la puissance de sortie est transmise.

Input Power (Puissance d'entrée) — Niveau auquel la puissance d'entrée est transmise.

Transmitter Fault (Défaillance d'émetteur-transmetteur) — Indique si une défaillance est survenue pendant la transmission.

Loss of Signal (Perte de signal) — Indique si le câble a perdu le signal.

Data Ready (Données prêtes) — L'émetteur-récepteur est sous tension et les données sont prêtes.

Affichage de la table des résultats des diagnostics d'émetteurs-récepteurs optiques

1. Ouvrez la page [Optical Transceiver Diagnostics](#) (Diagnostics d'émetteurs-récepteurs optiques).
2. Cliquez sur **Show All** (Afficher tout).

Le test est exécuté et la **table des résultats des tests de câbles virtuels** s'ouvre.

Réalisation de tests de câbles à fibres optiques à l'aide de commandes CLI

Le tableau suivant récapitule la commande CLI équivalente pour la réalisation de tests de câbles en fibres optiques.

Tableau 6-34. Commandes CLI des tests de câbles en fibres optiques

Commande CLI	Description
<code>show fiber-ports optical-transceiver [interface] [détaillée]</code>	Affiche les diagnostics d'émetteurs-récepteurs optiques.

Vous trouverez ci-dessous un exemple de commande CLI :

```

console> enable

Console# show fiber-ports optical-transceiver

```

Port	Temp	Tension	Courant	Puissance		Émetteur-transmetteur	LOS
				Sortie	Entrée		
	(C)	(Volt)	(mA)	(mWatt)	(mWatt)	Défaillance	
g1	W	OK	E	OK	OK	OK	OK
g2	OK	OK	OK	OK	OK	E	OK
g3	Cuivre						

Temp - Température de l'émetteur-récepteur mesurée en interne.

Voltage (Tension) - Tension d'alimentation mesurée en interne.

Current (Courant) - Courant de polarisation mesuré de l'émetteur-transmetteur.

Output Power (Puissance de sortie) - Puissance de sortie mesurée de l'émetteur-transmetteur.


Input Power (Puissance d'entrée) - Puissance reçue mesurée de l'émetteur-récepteur.

Tx Fault (Défaillance d'émetteur-transmetteur) - Défaillance de l'émetteur-transmetteur

LOS/Loss of Signal - Perte de signal


La **table des diagnostics de l'émetteur-récepteur optique** contient les colonnes suivantes :

- 1 **Temp** — Température de l'émetteur-récepteur mesurée en interne.
- 1 **Voltage** (Tension) — Tension d'alimentation mesurée en interne.
- 1 **Current** (Courant) — Courant de polarisation mesuré de l'émetteur-transmetteur.
- 1 **Output Power** (Puissance de sortie) — Puissance de sortie de l'émetteur-transmetteur mesurée en milliwatts.
- 1 **Input Power** (Puissance d'entrée) — Puissance reçue de l'émetteur-transmetteur mesurée en milliwatts.
- 1 **TX Fault** (Défaillance d'émetteur-transmetteur) — Défaillance de l'émetteur-transmetteur.

 **REMARQUE** : Les émetteurs-récepteurs Finisair ne prennent pas en charge le diagnostic de défaillance de l'émetteur-transmetteur.

- 1 **LOS/Loss of Signal** — Perte de signal.

- 1 **Data Ready** (Données prêtes) — L'émetteur-récepteur est sous tension et les données sont prêtes.
- 1 **N/A** - Non disponible, N/S - Non pris en charge, W - Avertissement, E - Erreur.

 **REMARQUE** : Les fonctions d'analyse des fibres optiques ne fonctionnent que sur des SFP qui prennent en charge la norme de diagnostic numérique SFF 4872.

Gestion de la sécurité du périphérique

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 de périphérique, 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 au périphérique. L'accès aux fonctions de gestion peut être limité à un groupe d'utilisateurs, défini par les interfaces d'entrée, l'adresse IP source et/ou les sous-réseaux IP sources.

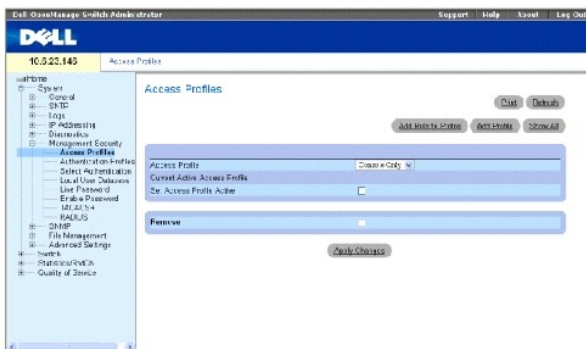
Un accès de gestion distinct peut être défini pour chaque type de méthode d'accès de gestion : accès Web (HTTP), Web sécurisés (HTTPS), Telnet, Secure Telnet et SNMP.

Les méthodes d'accès de gestion varient d'un groupe d'utilisateurs à un autre. Par exemple, le groupe d'utilisateurs 1 ne peut accéder au périphérique que via une session HTTP alors que le groupe 2 peut y accéder par le biais de sessions HTTP et Telnet.

Les listes d'accès de gestion contiennent les règles qui déterminent les modalités de gestion du périphérique et les utilisateurs auxquels cette gestion incombe. Des utilisateurs peuvent également ne pas être autorisés à accéder au périphérique.

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**, cliquez sur **System** (Système) → **Management Security** (Sécurité de gestion) → **Access Profiles** (Profils d'accès) dans l'arborescence.

Figure 6-51. Profils d'accès



Access Profile (Profil d'accès) — Listes des profils d'accès définis par l'utilisateur. La liste **Access Profile** contient une valeur par défaut de la liste **console**, à laquelle les profils d'accès définis par l'utilisateur sont ajoutés. La sélection de l'option **Console Only** (Console uniquement) comme nom de **profil d'accès** déconnecte la session et active l'accès au périphérique par l'intermédiaire de la console uniquement.

Current Active Access Profile (Profil d'accès actif) — Profil d'accès actuellement actif.

Set Access Profile Active (Définir le profil d'accès comme actif) — Active un profil d'accès.

Remove (Supprimer) — Supprime le profil d'accès sélectionné de la liste **Access Profile Name** (Noms de profils d'accès).

Activation d'un profil

1. Ouvrez 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 certaines priorités : la méthode de gestion du périphérique, le type d'interface, l'adresse IP source et le masque de réseau ou l'action d'accès de gestion du périphérique. Les utilisateurs peuvent se voir autoriser ou refuser un accès de gestion. La priorité définit l'ordre dans lequel les règles sont appliquées au sein d'un profil.

Définition de règles pour un profil d'accès :

1. Ouvrez la page **Access Profiles** (Profils d'accès).
2. Cliquez sur **Add an Access Profile** (Ajouter un profil d'accès).

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

Figure 6-52. Ajouter un profil d'accès


The screenshot shows the 'Add an Access Profile' configuration page. At the top right is a 'Refresh' button. Below it is a text input field for 'Access Profile Name'. The main configuration area includes: 'Rule Priority (1-65535)' text input; 'Management Method' dropdown menu with 'AI' selected; 'Interface' checkbox; 'Source IP Address' text input; 'VLAN Mask' text input; 'VLAN Length' text input; and 'Action' dropdown menu with 'Permit' selected. At the bottom center is an 'Apply Changes' button.

Access Profile Name (1-32 Characters) (Nom du profil d'accès [1 à 32 caractères])— Nom défini par l'utilisateur pour le profil d'accès.

Rule Priority (1-65535) (Priorité de la règle [1-65535])— Priorité de la règle. Lorsque le paquet correspond à une règle, les groupes d'utilisateurs sont autorisés ou non à accéder à la gestion du périphérique. L'ordre de la règle est établi en définissant un numéro de règle dans la **table des règles de profil**. Le numéro de règle est primordial pour la correspondance paquets-règles, les paquets étant mis en correspondance selon une base «first-fit» (premier convenant). Les priorités de la règle sont affectées à la table **Profile Rules** (Règles de profil).

Management Method (Méthode de gestion) — Méthode de gestion pour laquelle le profil d'accès est défini. Les utilisateurs bénéficiant de ce profil d'accès peuvent accéder au périphérique à l'aide de la méthode de gestion sélectionnée.

Interface — Type d'interface à laquelle la règle s'applique. Ce champ est facultatif. Vous pouvez appliquer cette règle à un port, un LAG ou un VLAN sélectionné en cochant cette case et en sélectionnant le bouton d'option et l'interface appropriés.

 **REMARQUE** : L'affectation d'un profil d'accès à une interface implique que l'accès via d'autres interfaces est interdit. Si un profil d'accès n'est pas affecté à une interface, le périphérique est accessible via toutes les interfaces.

Source IP Address (Adresse IP source) — Adresse IP source de l'interface à laquelle la règle s'applique. Ce champ est facultatif. Il indique que la règle s'applique à un sous-réseau.

Network Mask (Masque de réseau) — Masque de sous-réseau IP.


Prefix Length (Longueur du préfixe) — Nombre de bits qui comprennent le préfixe de l'adresse IP source ou le masque de réseau de l'adresse IP source.

Action — Indique si l'accès de gestion à l'interface définie est autorisé ou interdit.

3. Complétez le champ **Access Profile Name** (Nom du profil d'accès).
4. Définissez les champs concernés.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau profil d'accès est ajouté et le périphérique est mis 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. Ouvrez la page **Access Profiles** (Profils d'accès).
2. Cliquez sur **Add Profile to Rule** (Ajouter un profil à la règle).

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


Figure 6-53. Ajouter une règle à un profil d'accès



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

La règle est ajoutée au profil d'accès et le périphérique est mis 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 mis en correspondance avec la première règle qui répond aux critères.

1. Ouvrez 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'ouvre :

Figure 6-54. Table des règles de profil



Suppression d'une règle

1. Ouvrez la page **Access Profiles** (Profils d'accès).
2. Cliquez sur **Show All** (Afficher tout).

La **table des règles de profil** s'ouvre.

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

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

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

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [Access Profiles](#) (Profils d'accès).

Tableau 6-35. Commandes CLI des profils d'accès

Commande CLI	Description
<code>management access-list nom</code>	Définit une liste d'accès de gestion et crée le contexte de la liste d'accès pour la configuration.
<code>permit [ethernet interface-numéro vlan id-vlan port-channel numéro] [service service]</code>	Définit des conditions d'autorisation de port pour la liste d'accès de gestion.
<code>permit ip-source adresse-ip [mask masque longueur-préfixe] [ethernet interface-numéro vlan id-vlan port-channel numéro] [service service]</code>	Définit des conditions d'autorisation de port pour la liste d'accès de gestion et la méthode de gestion sélectionnée.
<code>deny [ethernet interface-numéro] vlan id-vlan port-channel numéro] [service service]</code>	Définit des conditions de refus de port pour la liste d'accès de gestion et la méthode de gestion sélectionnée.
<code>deny ip-source adresse-ip [mask masque longueur-préfixe] [ethernet interface-numéro vlan id-vlan port-channel numéro] [service service]</code>	Définit des conditions de refus de port pour la liste d'accès de gestion et la méthode de gestion sélectionnée.
<code>management access-class { console-only nom }</code>	Définit la liste d'accès utilisée pour les connexions de gestion actives.
<code>show management access-list [nom]</code>	Affiche les listes d'accès de gestion actives.
<code>show management access-class</code>	Affiche des informations sur la classe d'accès de gestion.

Vous trouverez ci-dessous un exemple de commande CLI :

```

Console (config)# management access-list mlist

Console (config-macl)# permit ethernet g1

Console (config-macl)# permit ethernet g9

```

```
Console (config-macl)# deny ethernet g2

Console (config-macl)# deny ethernet g10

Console (config-macl)# exit

Console (config)# management access-class mlist

Console (config)# exit

Console# show management access-list

mlist
-----

permit ethernet g1

permit ethernet g9

! (Remarque : Tous les autres accès sont implicitement refusés)

Console> show management access-class

La classe d'accès de gestion est activée à l'aide de la liste d'accès mlist
```

Définition de profils d'authentification

La page [Authentication Profiles](#) (Profils d'authentification) contient des champs permettant de sélectionner une méthode d'authentification des utilisateurs sur le périphérique. L'authentification des utilisateurs est effectuée :

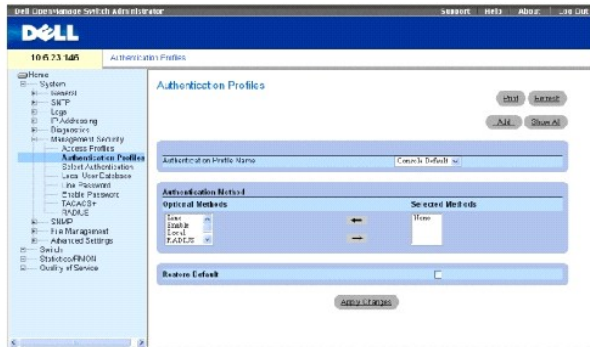
- 1 Localement
- 1 Par le biais d'un serveur externe

Vous pouvez également sélectionner None (Aucune) pour désactiver l'authentification des utilisateurs.

L'authentification des utilisateurs est effectuée selon l'ordre des méthodes sélectionnées. Par exemple, si les options Local et RADIUS sont sélectionnées, l'utilisateur est d'abord authentifié localement. Si la base de données d'utilisateurs locaux est vide, l'utilisateur est alors authentifié via le serveur RADIUS.

Si une erreur survient au cours de l'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 6-55. Profils d'authentification



Authentication Profile Name (Nom du profil d'authentification) — Listes de profils d'authentification auxquelles les profils d'authentification définis par l'utilisateur seront ajoutés. Les valeurs par défaut sont **Network Default** (Valeur par défaut pour le réseau) et **Console Default** (Valeur par défaut pour la console).

Optional Methods (Méthodes facultatives) — Méthodes d'authentification des utilisateurs. Les options possibles sont :

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

Local (Locale) — L'authentification des utilisateurs est effectuée au niveau du périphérique. Le périphérique vérifie le nom d'utilisateur et le mot de passe pour procéder à l'authentification.

RADIUS — L'authentification des utilisateurs est effectuée sur le serveur RADIUS. Pour plus d'informations, reportez-vous à la section [«Configuration de paramètres RADIUS globaux»](#).

Line (Ligne) — Le mot de passe de ligne est utilisé pour l'authentification.

Enable — Le mot de passe d'activation est utilisé pour l'authentification.

TACACS+ — L'authentification utilisateur est effectuée sur le serveur TACACS+.

Restore Default (Restaurer les valeurs par défaut) — Restaure la méthode d'authentification des utilisateurs par défaut sur le périphérique.

Sélection d'un profil d'authentification :

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

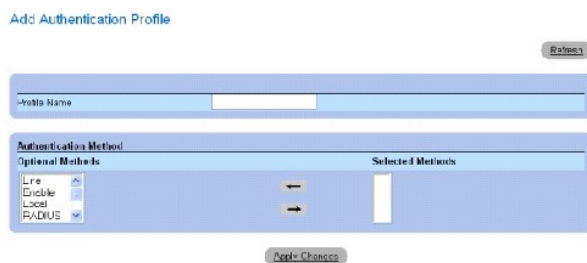
Le profil d'authentification des utilisateurs est mis à jour sur le périphérique.

Ajout d'un profil d'authentification :

1. Ouvrez la page [Authentication Profiles](#) (Profils d'authentification).
2. Cliquez sur **Add** (Ajouter).

La page **Add Authentication Method Profile Name** (Ajouter un nom de profil de méthode d'authentification) s'ouvre :

Figure 6-56.



Ajouter un profil d'authentification

3. Configurez le profil.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

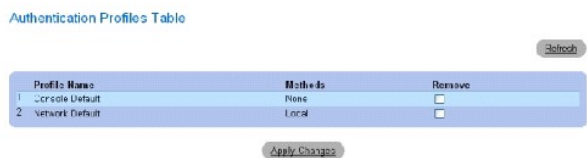
Le profil d'authentification est mis à jour sur le périphérique.

Affichage de la page Afficher tous les profils d'authentification :

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

La page **Authentication Profile** (Profil d'authentification) s'ouvre :

Figure 6-57. Profils d'authentification



Suppression d'un profil d'authentification :

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

La page **Authentication Profile** (Profil d'authentification) s'ouvre.

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 de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [Authentication Profiles](#) (Profils d'authentification).

Tableau 6-36. Commandes CLI des profils d'authentification

Commande CLI	Description
--------------	-------------

<code>aaa authentication login { default liste-nom} méthode1 [méthode2]</code>	Configure l'authentification des connexions.
<code>no aaa authentication login { default liste-nom}</code>	Supprime un profil d'authentification des connexions.

Vous trouverez ci-dessous un exemple de commande CLI :

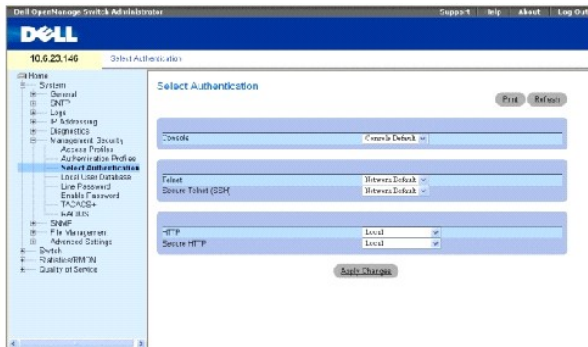
```
Console (config)# aaa authentication login default radius local enable none

Console (config)# no aaa authentication login default
```

Attribution de profils d'authentification

Après avoir été définis, les profils d'authentification peuvent être appliqués à des méthodes d'accès de gestion. Les utilisateurs de la console peuvent être authentifiés par la liste de méthodes d'authentification 1, par exemple, et les utilisateurs Telnet par 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 6-58. Sélectionner une authentification



Console — Profils d'authentification utilisés pour authentifier les utilisateurs de la console.

Telnet — Profils d'authentification utilisés pour authentifier les utilisateurs Telnet.

Secure Telnet (SSH) (Telnet sécurisé) — Profils d'authentification utilisés pour authentifier les utilisateurs SSH. Le protocole SSH permet aux clients SSH d'établir une connexion sécurisée et cryptée avec un périphérique.

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

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

Local (Locale) — L'authentification est effectuée au niveau local.

RADIUS — L'authentification est effectuée sur le serveur RADIUS.

TACACS+ — L'authentification est effectuée sur le serveur TACACS+.

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

1. Ouvrez la page [Select Authentication](#) (Sélection d'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 affectée à des sessions de console.

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

1. Ouvrez la page [Select Authentication](#) (Sélection d'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 affectée à des sessions Telnet.

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

1. Ouvrez la page [Select Authentication](#) (Sélection d'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).

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

1. Ouvrez la page [Select Authentication](#) (Sélection d'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 affectée à des sessions HTTP.

Affectation de sessions HTTP sécurisées à une séquence d'authentification

1. Ouvrez la page [Select Authentication](#) (Sélection d'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 affectée à des sessions HTTP sécurisées.

Attribution de profils ou de séquences d'authentification des accès à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [Select Authentication](#) (Sélection d'une authentification).

Tableau 6-37. Commandes CLI de la sélection de l'authentification

Commande CLI	Description
<code>enable authentication [default liste-nom]</code>	Spécifie 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 à distance.
<code>login authentication [default liste-nom]</code>	Spécifie la liste de méthodes d'authentification des connexions pour une console ou une session Telnet à distance.
<code>ip http authentication méthode1</code>	Spécifie les méthodes d'authentification pour les serveurs HTTP.

[méthode2]	
ip https authentication méthode1 [méthode2]	Spécifie les méthodes d'authentification pour les serveurs HTTPS.
show authentication methods	Affiche des informations sur les méthodes d'authentification.

Vous trouverez ci-dessous un exemple de commande 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

Listes de méthodes d'authentification des connexions
-----

Valeur par défaut : Radius, Local, Ligne

Console_Login : Ligne, Aucune

Listes de méthodes d'authentification d'activation
-----

Valeur par défaut : Radius, Enable

Console_Enable : Enable, Aucune

Ligne Liste de méthodes de connexion Liste de méthodes Enable

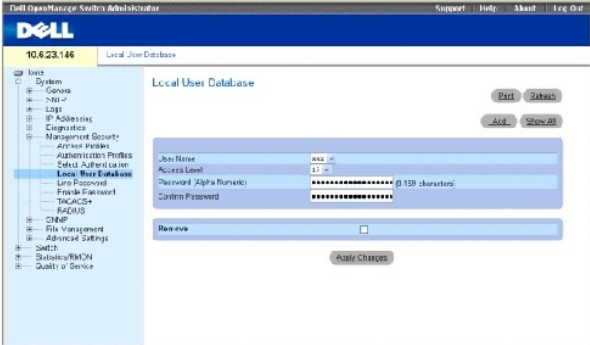
```

```
-----  
Console Console_Login Console_Enable  
  
Telnet Valeur par défaut Valeur par défaut  
  
SSH Valeur par défaut Valeur par défaut  
  
HTTP : Radius, local  
  
HTTPS : Radius, local  
  
Dot1x : Radius
```

Définition des bases de données d'utilisateurs locales

La page [Local User Database](#) (Base de données d'utilisateurs locaux) contient des champs permettant de définir des utilisateurs, des mots de passe et des niveaux d'accès. Pour ouvrir la page [Local User Database](#), cliquez sur System (Système) > Management Security (Sécurité de gestion) > Local User Database (Base de données d'utilisateurs locaux) dans l'arborescence.

Figure 6-59. Base de données d'utilisateurs locaux



User Name (Nom d'utilisateur) — Liste d'utilisateurs.

Access Level (Niveau d'accès) — Niveau d'accès des utilisateurs. Le niveau le plus faible est 1 et le plus élevé est 15.

Password (0-159 Characters) (Mot de passe [0 à 159 caractères]) — Mot de passe défini par l'utilisateur. Les mots de passe des bases de données d'utilisateurs locaux peuvent avoir jusqu'à 159 caractères.

Confirm Password (Confirmer le mot de passe) — Confirme le mot de passe défini par l'utilisateur.

Remove (Supprimer) — Supprime des utilisateurs de la liste des **User Name** (Noms d'utilisateur).

Attribution de droits d'accès à un utilisateur :

1. Ouvrez la page [Local User Database](#) (Base de données d'utilisateurs locaux).
2. Sélectionnez un utilisateur dans le champ **User Name** (Nom d'utilisateur).
3. Renseignez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Définition d'un nouvel utilisateur :

1. Ouvrez la page [Local User Database](#) (Base de données d'utilisateurs locaux).
2. Cliquez sur **Add** (Ajouter).

La page **Add User** (Ajouter un utilisateur) s'ouvre :

Figure 6-60. Ajouter un utilisateur

Attribute	Value
User Name (Alpha Numeric)	<input type="text"/> (0-23 characters)
Access Level (1-16)	1
Password (Alpha Numeric)	<input type="text"/> (0-165 characters)
Confirm Password	<input type="text"/>

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

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

Affichage de la table d'utilisateurs locaux :

1. Ouvrez la page [Local User Database](#) (Base de données d'utilisateurs locaux).
2. Cliquez sur **Show All** (Afficher tout).

La table d'utilisateurs locaux s'ouvre :

Figure 6-61. Table d'utilisateurs locaux

User Name	Access Level	Remove	
1	xxxx	15	-

Suppression d'utilisateurs :

1. Ouvrez la page [Local User Database](#) (Base de données d'utilisateurs locaux).
2. Cliquez sur **Show All** (Afficher tout).

La **table d'utilisateurs locaux** s'ouvre.

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 le périphérique est mis à jour.

Affectation d'utilisateurs à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [Local User Database](#) (Base de données d'utilisateurs locaux).

Tableau 6-38. Commandes CLI de la base de données d'utilisateurs locaux

Commande CLI	Description
<code>username nom [password mot de passe] [level niveau] [encrypted]</code>	Définit un système d'authentification reposant sur le nom des utilisateurs.

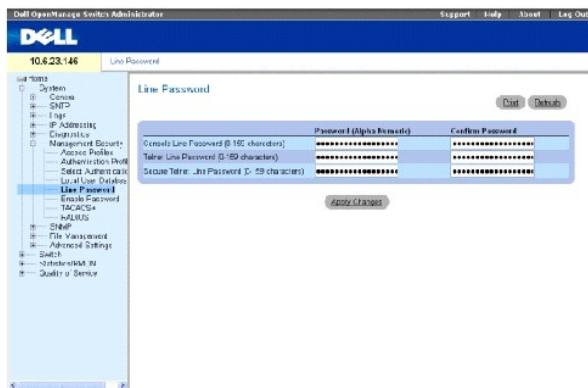
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# username jules password vincent level 15
```

Définition de mots de passe de ligne

La page [Line Password](#) (Mots de passe de ligne) contient des champs permettant de définir des mots de passe de ligne pour les méthodes de gestion. Pour ouvrir la page [Line Password](#), cliquez sur System (Système) → Management Security (Sécurité de gestion) → Line Passwords (Mots de passe de ligne) dans l'arborescence.

Figure 6-62. Mots de passe de ligne



Line Password for Console/Telnet/Secure Telnet (0-159 Characters) (Mot de passe de ligne pour la console/Telnet/Telnet sécurisé [0 à 159 caractères]) — Mot de passe de ligne permettant d'accéder au périphérique par le biais d'une session de console, Telnet ou Telnet sécurisé. Les mots de passe peuvent comprendre jusqu'à 159 caractères.

Confirm Password (Confirmer le mot de passe) — Confirme le nouveau mot de passe de ligne. Le mot de passe s'affiche sous forme d'astérisques : *****.

Définition de mots de passe de ligne pour les sessions de console

1. Ouvrez la page [Line Password](#) (Mot de passe de ligne).
2. Définissez le champ **Line Password for Console** (Mot de passe de ligne pour la console).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mot de passe de ligne à utiliser pour les sessions de console est défini et le périphérique est mis à jour.

Définition de mots de passe de ligne pour les sessions Telnet

1. Ouvrez la page [Line Password](#) (Mot de passe de ligne).
2. Complétez le champ **Line Password for Telnet** (Mot de passe de ligne pour Telnet).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mot de passe de ligne à utiliser pour les sessions Telnet est défini et le périphérique est mis à jour.

Définition de mots de passe de ligne pour les sessions Telnet sécurisées

1. Ouvrez la page [Line Password](#) (Mot de passe de ligne).
2. Définissez le champ **Line Password for Secure Telnet** (Mot de passe pour Telnet sécurisé).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mot de passe de ligne à utiliser pour les sessions Telnet sécurisées est défini et le périphérique est mis à jour.

Affectation de mots de passe de ligne à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [Line Password](#) (Mot de passe de ligne).

Tableau 6-39. Commandes CLI des mots de passe de ligne

Commande CLI	Description
<code>password <i>mot de passe</i> [encrypted]</code>	Définit un mot de passe de ligne.

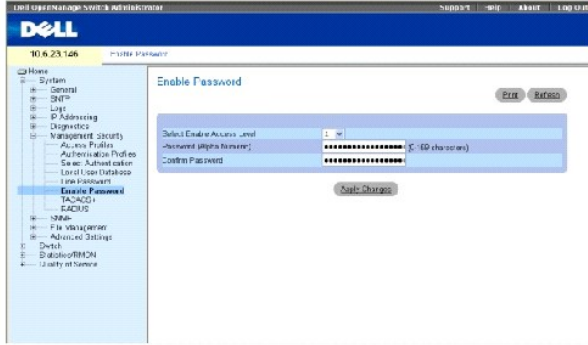
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config-line)# password dell
```

Définition du mot de passe d'activation

La page [Modify Enable Password](#) (Modifier le mot de passe d'activation) définit le mot de passe local permettant de contrôler l'accès aux configurations normale, mode Privilégié et globale. Pour ouvrir la page [Modify Enable Password](#), cliquez sur System (Système) → Management Security (Sécurité de gestion) → Enable Passwords (Mots de passe d'activation) dans l'arborescence.

Figure 6-63. Modifier le mot de passe d'activation



Select **Enable Access Level** (Sélectionner le niveau d'accès d'activation) — Niveau d'accès associé au mot de passe d'activation. La plage est comprise entre 1 et 15.

Password (0-159 Characters) (Mot de passe [0 à 159 caractères]) — Mot de passe enable actuellement configuré. Les mots de passe d'activation peuvent comprendre jusqu'à 159 caractères.

Confirm Password (Confirmer le mot de passe) — Confirmez le nouveau mot de passe d'activation. Le mot de passe s'affiche sous forme d'astérisques : * * * * *

Définition d'un nouveau mot de passe d'activation :

1. Ouvrez la page [Modify Enable Password](#) (Modifier le mot de passe d'activation).
2. Définissez les champs concernés.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau mot de passe d'activation est défini et le périphérique est mis à jour.

Affectation de mots de passe d'activation à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [Modify Enable Password](#) (Modifier le mot de passe d'activation).

Tableau 6-40. Commandes CLI de modification du mot de passe d'activation

Commande CLI	Description
<code>enable password [level niveau] mot de passe [encrypted]</code>	Définit un mot de passe local pour contrôler l'accès aux utilisateurs et niveaux de privilèges.
<code>show users accounts</code>	Affiche des informations sur la base de données d'utilisateurs locaux.

Vous trouverez ci-dessous un exemple de commande CLI :

```

Console (config)# enable password level 15 secret

Console# show users accounts

Nom d'utilisateur Privilège
-----
secret 15

```

Définition de paramètres TACACS+

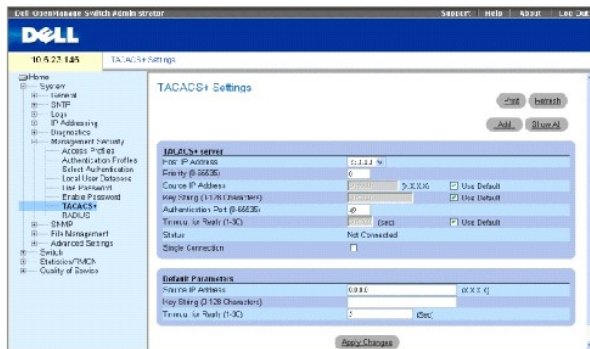
Les périphériques offrent un support client TACACS+ (Terminal Access Controller Access Control System). TACACS+ offre une sécurité centralisée pour la vérification des utilisateurs qui accèdent au périphérique.

TACACS+ permet d'avoir un système de gestion centralisée des utilisateurs, tout en conservant le RADIUS et les autres processus d'authentification. TACACS+ offre les services suivants :

- 1 Authentification — Permet une authentification pendant la connexion par le biais des noms d'utilisateur et des mots de passe définis par les utilisateurs.
- 1 Autorisation — Réalisée à la connexion. Une fois l'authentification terminée, une session d'autorisation démarre en utilisant le nom d'utilisateur authentifié. Le serveur TACACS vérifie les droits d'accès de l'utilisateur.

Le protocole TACACS+ assure l'intégrité du réseau grâce à des échanges en protocole crypté entre le périphérique 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 6-64. Paramètres TACACS+



Host IP Address (Adresse IP hôte) — Adresse IP du serveur TACACS+.

Priority (0-65535) (Priorité [0 à 65535])— Ordre d'utilisation des serveurs TACACS+. La valeur par défaut est 0.

Source IP Address (Adresse IP source) — Adresse IP source du périphérique utilisée pour la session TACACS+ entre le périphérique et le serveur TACACS+.

Key String (0-128 Characters) (Clé de codage [0 à 128 caractères])— Définit la clé d'authentification et de cryptage des communications TACACS+ entre le périphérique et le serveur TACACS+. Cette clé doit correspondre à la clé de cryptage utilisée sur le serveur TACACS+.

Authentication Port (0-65535) (Port d'authentification [0 à 65535])— Numéro du port par où passe la session TACACS+. Le port 49 est le port par défaut.

Reply Timeout (1-30 Seconds) (Délai de réponse [1 à 30 secondes]) — Délai qui s'écoule avant l'expiration de la connexion entre le périphérique et le serveur TACACS+. La plage est comprise entre 1 et 30 secondes.

Status (État) — État de la connexion entre le périphérique et le serveur TACACS+. Ce champ peut prendre les valeurs suivantes :

Connected (Connexion) — Une connexion existe entre le périphérique et le serveur TACACS+.

Not Connected (Pas de connexion) — Il n'y a pas de connexion actuellement entre le périphérique et le serveur TACACS+.

Single Connection (Une seule connexion) — Conserve une seule connexion ouverte entre le périphérique 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 aucune valeur par défaut n'est définie, les valeurs par défaut du système sont appliquées aux nouveaux serveurs TACACS+. Voici les paramètres par défauts des serveurs TACACS+ :

Source IP Address (Adresse IP source) — Adresse IP source par défaut du périphérique utilisée pour la session TACACS+ entre le périphérique et le serveur TACACS+.

Key String (0-128 Characters) (Clé de codage [0 à 128 caractères]) — Clé d'authentification et de cryptage par défaut des communications TACACS+ entre le périphérique et le serveur TACACS+.

Timeout for Reply (1-30 Seconds) (Délai de réponse [1 à 30 secondes]) — Délai par défaut qui s'écoule avant l'expiration de la connexion entre le périphérique et le serveur TACACS+.

Ajout d'un serveur TACACS+

1. Ouvrez la page [TACACS+ Settings](#) (Paramètres TACACS+).
2. Cliquez sur **Add** (Ajouter).

La page [Add TACACS+ Host](#) (Ajouter un hôte TACACS+) s'ouvre :

Figure 6-65. Ajouter un hôte TACACS+

Host IP Address	<input type="text"/>	[X.X.X.X]
Priority (0-255)	<input type="text"/>	
Source IP Address	<input type="text"/>	[X.X.X.X] <input type="checkbox"/> Use Default
Key String (0-128 Characters)	<input type="text"/>	<input type="checkbox"/> Use Default
Authentication (0-255)	<input type="text"/>	<input type="checkbox"/> Use Default
Timeout for Reply (1-30)	<input type="text"/>	(sec) <input type="checkbox"/> Use Default
Single Connection	<input type="checkbox"/>	

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

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

Affichage de la [table TACACS+](#)

1. Ouvrez la page [TACACS+ Settings](#) (Paramètres TACACS+).
2. Cliquez sur **Show All** (Afficher tout).

La page [TACACS+ Table](#) (Table TACACS+) s'ouvre :

Figure 6-66. Table TACACS+

TACACS+ Table

Host IP Address	Priority	Source IP Address	Authentication Port	Timeout for Reply	Single Connection	Status	Remove
1 23.1.1.1	0	Default	40	Default	<input type="checkbox"/>	Not Connected	<input type="checkbox"/>

[Apply Changes](#)

Suppression d'un serveur TACACS+

- Ouvrez la page [TACACS+ Settings](#) (Paramètres TACACS+).
- Cliquez sur **Show All** (Afficher tout).

La page [TACACS+ Table](#) (Table TACACS+) s'ouvre.

- Sélectionnez une entrée de la [table TACACS+](#).
- Cochez la case **Remove** (Supprimer).
- Cliquez sur **Apply Changes** (Appliquer les modifications).

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

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

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [TACACS+ Settings](#) (Paramètres TACACS+).

Tableau 6-41. Commandes CLI TACACS+

Commande CLI	Description
TACACS-server host (<i>adresse-ip</i> <i>nom-hôte</i>) [single-connection] [port <i>numéro-port</i>] [timeout <i>délai</i>] [key <i>clé-codage</i>] [source <i>source</i>] [priority <i>priorité</i>]	Indique un hôte TACACS+.
no TACACS-server host (<i>adresse-ip</i> <i>nom-hôte</i>)	Supprime un hôte TACACS+.
tacacs-server key <i>clé-codage</i>	Désigne la clé d'authentification et de cryptage de toutes les communications TACACS+ entre le périphérique et le serveur TACACS+. Cette clé doit correspondre à la clé de cryptage utilisée sur le serveur TACACS+ démon. (Plage : 0 à 128 caractères.)
tacacs-server timeout <i>délai</i>	Spécifie la valeur de délai en secondes. (Plage : 1 à 30.)
tacacs-server source-ip <i>source</i>	Spécifie l'adresse IP source. (Plage : Adresse IP valide.)
show TACACS [<i>adresse-ip</i>]	Affiche la configuration et les statistiques d'un serveur TACACS+.

Vous trouverez ci-dessous un exemple de commande CLI :

Console# show tacacs						
Configuration du routeur						

Adresse IP	État	Port	Unique Connexion	Délai	IP source	Priorité

-----	-----	-----	-----	-----	-----	-----
12.1.1.1.2	Pas connecté	49	Oui	1	12.1.1.1	1
Valeurs globales						

Délai : 5						
Configuration du routeur						

IP source : 0.0.0.0						
console#						

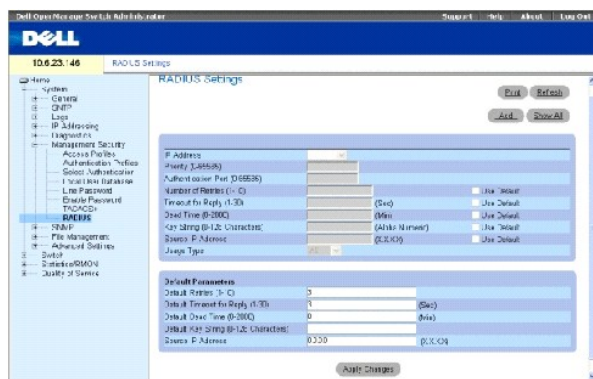
Configuration de paramètres RADIUS globaux

Les serveurs RADIUS (Remote Authorization Dial-In User Service) permettent d'augmenter la sécurité des réseaux. Les serveurs RADIUS assurent une méthode d'authentification centralisée pour :

- 1 les accès Telnet
- 1 les accès Web
- 1 les accès console à périphérique

Pour ouvrir la page [RADIUS Settings](#) (Paramètres RADIUS), cliquez sur System (Système) → Management Security (Sécurité de gestion) → RADIUS dans l'arborescence.

Figure 6-67. Paramètres RADIUS



IP Address (Adresse IP) — Liste des adresses IP de serveurs d'authentification.

Priority (1-65535) (Priorité [1 à 65535])— Indique la priorité du serveur. La plage est comprise entre 1 et 65535. 1 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. Le port d'authentification est utilisé pour vérifier l'authentification du serveur RADIUS.

Number of Retries (1-10) (Nombre de tentatives [1 à 10])— Nombre de demandes de transmission envoyées au serveur RADIUS avant la survenue d'un échec. La plage est comprise entre 1 et 10. La valeur par défaut est trois.

Timeout for Reply (1-30) (Délai de réponse [1 à 30])— Délai en secondes pendant lequel le périphérique attend une réponse du serveur RADIUS avant de tenter une nouvelle requête ou de basculer sur le serveur suivant. La plage est comprise entre 1 et 30. La valeur par défaut est 3.

Dead Time (0-2000) (Délai d'inactivité [0 à 2000])— Définit le délai (en secondes) pendant lequel un serveur RADIUS est écarté 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 le périphérique et le serveur RADIUS. Cette clé est cryptée.

Source IP Address (Adresse IP source) — Définit l'adresse IP source utilisée pour communiquer avec les serveurs RADIUS.

Les valeurs RADIUS par défaut sont définies à l'aide des champs suivants :

Default Timeout for Reply (1-30) (Délai de réponse par défaut [1 à 30])— Délai par défaut (en secondes) pendant lequel le périphérique attend une réponse du serveur RADIUS avant expiration.

REMARQUE : En l'absence de délai d'attente pour l'hôte, de retransmission, de délai d'inactivité, ou de refus, les valeurs globales (par défaut) sont appliquées à chaque hôte.

Default Retries (1-10) (Tentatives par défaut [1 à 10])— Nombre de demandes de transmission par défaut envoyées au serveur RADIUS avant la survenue d'un échec.

Default Dead time (0-2000) (Délai d'inactivité par défaut [0 à 2000])— Définit le délai par défaut (en secondes) pendant lequel un serveur RADIUS est écarté 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 utilisée par défaut pour authentifier et crypter toutes les communications RADIUS entre le périphérique et le serveur RADIUS. Cette clé est cryptée.

Source IP Address (Adresse IP source) — Définit l'adresse IP source utilisée pour communiquer avec les serveurs RADIUS.

Usage Type (Type d'utilisation) — Indique le type d'utilisation du serveur. Ce champ peut prendre les valeurs suivantes : login (connexion), 802.1x ou all (tout). La valeur par défaut est all.

Définition des paramètres RADIUS :

1. Ouvrez la page [RADIUS Settings](#) (Paramètres RADIUS).
2. Renseignez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres RADIUS sont mis à jour sur le périphérique.

Ajout d'un serveur RADIUS :

1. Ouvrez la page [RADIUS Settings](#) (Paramètres RADIUS).
2. Cliquez sur **Add** (Ajouter).

La page **Add RADIUS Server** (Ajouter un serveur RADIUS) s'ouvre :

Figure 6-68. Ajouter un serveur RADIUS

IP Address	<input type="text"/>	(X.X.X)
Priority ID (5535)	<input type="text"/>	0
Authentication Port (0-65535)	<input type="text"/>	1812
Number of Retries (1-10)	<input type="text"/>	3 <input checked="" type="checkbox"/> Use Default
Timeout for Reply (1-30)	<input type="text"/>	30 (Sec) <input checked="" type="checkbox"/> Use Default
Dead time (0-300)	<input type="text"/>	30 (Min) <input checked="" type="checkbox"/> Use Default
Key string (0-120 characters)	<input type="text"/>	(Alpha numeric) <input type="checkbox"/> Use Default
Source IP Address	<input type="text"/>	(X.X.X) <input checked="" type="checkbox"/> Use Default
Usage Type	<input type="text"/>	All

Apply Changes

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

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

Affichage de la liste de serveurs RADIUS :

1. Ouvrez la page [RADIUS Settings](#) (Paramètres RADIUS).
2. Cliquez sur **Show All** (Afficher tout).

La page [Show all RADIUS Servers](#) (Afficher tous les serveurs RADIUS) s'ouvre :

Figure 6-69. Afficher tous les serveurs RADIUS

IP Address	Priority	Authentication Port	Number of Retries	Timeout for Reply	Dead Time	Source IP Address	Usage Type	Remove
------------	----------	---------------------	-------------------	-------------------	-----------	-------------------	------------	--------

Apply Changes

Modification des paramètres des serveurs RADIUS :

1. Ouvrez la page [RADIUS Settings](#) (Paramètres RADIUS).
2. Cliquez sur **Show All** (Afficher tout).

La page **RADIUS Servers List** (Liste des serveurs RADIUS) s'ouvre.

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

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

Suppression d'un serveur RADIUS de la liste des serveurs RADIUS :

1. Ouvrez la page [RADIUS Settings](#) (Paramètres RADIUS).
2. Cliquez sur **Show All** (Afficher tout).

La page **RADIUS Servers List** (Liste des serveurs RADIUS) s'ouvre.

3. Sélectionnez un serveur RADIUS dans la **Liste de serveurs RADIUS**.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le serveur RADIUS est supprimé de la liste Serveurs RADIUS.

Définition des serveurs RADIUS à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [RADIUS Settings](#) (Paramètres RADIUS).

Tableau 6-42. Commandes CLI des paramètres RADIUS

Commande CLI	Description
<code>radius-server timeout <i>délai</i></code>	Définit la durée par défaut pendant laquelle un périphérique attend une réponse d'un serveur hôte.
<code>radius-server retransmit <i>tentatives</i></code>	Définit le nombre de tentatives par défaut de recherche de la liste de serveurs RADIUS hôtes.
<code>radius-server deadtime <i>délai-inactivité</i></code>	Définit les serveurs par défaut non disponibles à ignorer.
<code>radius-server key [<i>clé-codage</i>]</code>	Définit la clé de codage d'authentification et de cryptage par défaut utilisée pour toutes les communications RADIUS entre le périphérique et le serveur RADIUS.
<code>radius-server host { <i>adresse-ip</i> <i>nom-hôte</i> } [<i>auth-port</i> <i>port-auth-numéro</i>] [<i>timeout</i> <i>délai</i>] [<i>retransmit</i> <i>tentatives</i>] [<i>deadtime</i> <i>délai-inactivité</i>] [<i>key</i> <i>clé-codage</i>] [<i>source</i> <i>source</i>] [<i>priority</i> <i>priorité</i>] [<i>usage</i> <i>type</i>]</code>	Définit un serveur RADIUS hôte et tous les paramètres autres que les valeurs par défaut.
<code>show radius-servers</code>	Affiche les paramètres des serveurs RADIUS.

Vous trouverez ci-dessous un exemple de commande 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 1645
timeout 20

```

```

Console# show radius-servers

```

Port								
Adresse IP	Auth	Cpte	Délai	Retransm.	Délai d'inactiv.	IP source	Priorité	Utilisation
-----	----	----	-----	-----	-----	-----	-----	-----
33.1.1.1	1812	1813	6	4	10	0.0.0.0	0	All (Tous)
172.16.1.2	1645	1646	11	8	paramètres	paramètres	2	All (Tous)


```

Valeurs globales

-----

Délai :5

Retransm. : 5

Délai d'inactiv. :10

IP source :0.0.0.0

```

Définition des paramètres SNMP

Le protocole SNMP (Simple Network Management Protocol - protocole de gestion de réseau simple) fournit une méthode de gestion des périphériques réseau. Les périphériques SNMP exécutent un logiciel local, appelé «agent».

Les agents SNMP gèrent une liste de variables qui sont utilisées pour gérer le périphérique. Ces variables sont définies dans la MIB (base d'informations de gestion). La MIB contient les variables gérées par l'agent. Le protocole SNMP définit un format de spécifications MIB ainsi que le format utilisé pour accéder aux informations sur le réseau.

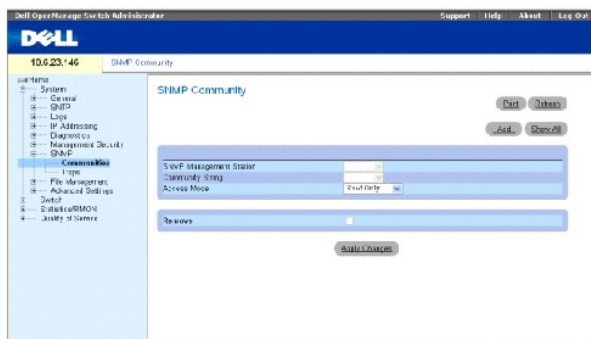
Les droits d'accès aux agents SNMP sont contrôlés par des chaînes d'accès. Pour communiquer avec le périphérique, le serveur Web intégré soumet une chaîne de communauté valide en vue de son authentification. Pour ouvrir la page SNMP, cliquez sur System (Système) → SNMP dans l'arborescence.

Cette section contient des informations permettant de gérer la configuration du protocole SNMP.

Définition de communautés

Les droits d'accès sont gérés en définissant des communautés dans la **Community Table** (Table des communautés). Lorsqu'un nom de communauté est modifié, les droits d'accès qui lui sont associés le sont également. Pour ouvrir la page [SNMP Community](#) (Communauté SNMP), cliquez sur System (Système) → SNMP → Communities (Communautés) dans l'arborescence.

Figure 6-70. Communauté SNMP



SNMP Management Station (Station de gestion SNMP) — Liste d'adresses IP de stations de gestion.

Community String (Chaîne de communauté) — Fonctionne comme un mot de passe et permet d'authentifier la station de gestion sélectionnée sur le périphérique.

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, pour toutes les MIB sauf la table des communautés, pour laquelle il n'y a pas d'accès.

Read Write (Lecture/écriture) — L'accès à la station de gestion s'effectue en lecture/écriture, pour toutes les MIB sauf la table des communautés, pour laquelle il n'y a pas d'accès.

SNMP Admin (Admin SNMP) — L'accès à la station de gestion se fait en lecture/écriture pour toutes les MIB, y compris la table des communautés.

Remove (Supprimer) — Lorsqu'elle est cochée, cette option supprime une communauté.

Définition d'une nouvelle communauté

1. Ouvrez la page [SNMP Community](#) (Communauté SNMP).
2. Cliquez sur **Add** (Ajouter).

La page **Add SNMP Community** (Ajouter une communauté SNMP) s'ouvre :

Figure 6-71. Ajouter une communauté SNMP

Add SNMP Community



3. Sélectionnez une option parmi les suivantes :

Management Station (Station de gestion) — Définit une communauté SNMP pour une station de gestion spécifique. (La valeur 0.0.0.0 définit toutes les stations de gestion.)

All (Toutes) — Indique que la communauté SNMP est définie pour toutes les stations de gestion.

4. Définissez les autres champs.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle communauté est enregistrée et le périphérique est mis à jour.

Affichage de toutes les communautés

1. Ouvrez la page [SNMP Community](#) (Communauté SNMP).
2. Cliquez sur **Show All** (Afficher tout).

La page [Community Table](#) (Table des communautés) s'ouvre :

Figure 6-72. **Table des communautés**



Suppression de communautés

1. Ouvrez la page [SNMP Community](#) (Communauté SNMP).
2. Cliquez sur **Show All** (Afficher tout).

La page [Community Table](#) (Table des communautés) s'ouvre.

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

L'entrée de la communauté sélectionnée est supprimée et le périphérique est mis à jour.

Configuration de communautés à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage des champs de la page [SNMP Community](#) (Communauté SNMP).

Tableau 6-43. **Commandes CLI des communautés SNMP**

Commande CLI	Description
--------------	-------------

<code>snmp-server community chaîne [ro rw su] [adresse-ip]</code>	Configure la chaîne d'accès à la communauté afin d'autoriser l'accès au protocole SNMP.
<code>snmp-server host {adresse-ip nom-hôte} chaîne de communauté [1 2]</code>	Détermine le type d'interruption envoyée au destinataire sélectionné.
<code>show snmp</code>	Vérifie l'état des communications SNMP.

Vous trouverez ci-dessous un exemple de commande CLI :

console(config)# snmp-server community public_1 su 1.1.1.1		
console(config)# snmp-server community public_2 rw 2.2.2.2		
console(config)# snmp-server community public_3 ro 3.3.3.3		
console(config)# snmp-server host 1.1.1.1 public_1 1		
console(config)# snmp-server host 2.2.2.2 public_2 2		
console(config)#		
console# show snmp		

Chaîne de communauté	Accès de communauté	Adresse IP
public_1	super	1.1.1.1
public_2	lecture/écriture	2.2.2.2
public_3	lecture seule	3.3.3.3
Interruptions activées.		
Interruption authentication-échec activées.		

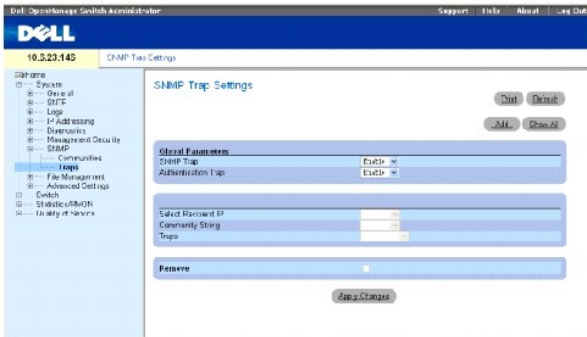
Adresse dest. interruption	Communauté dest. interruption	Version
-----	-----	-----
1.1.1.1	public_1	1
2.2.2.2	public_2	2
Contact système : 345 6789		
Emplacement système : 1234 5678		

console#

Définition d'interruptions

La page [SNMP Trap Settings](#) (Paramètres d'interruption SNMP) permet d'activer ou de désactiver l'envoi de notifications ou d'interruptions SNMP par le périphérique. Pour ouvrir la page [SNMP Trap Settings](#), cliquez sur System (Système) → SNMP → Traps (Interruptions) dans l'arborescence.

Figure 6-73. Paramètres d'interruption SNMP



SNMP Trap (Interruption SNMP) — Active l'envoi d'interruptions ou de notifications SNMP à partir du périphérique vers des destinataires d'interruption.

Authentication Trap (Interruption d'authentification) — Active l'envoi d'interruptions SNMP à des destinataires définis en cas d'échec d'authentification.

Select Recipient IP (Sélectionner IP destinataire) — Adresse IP à laquelle les interruptions sont envoyées.

Community String (Chaîne de communauté) — Identifie la chaîne de communauté du gestionnaire d'interruption.

Traps (Interruptions) — Détermine le type d'interruption envoyée au destinataire. Ce champ peut prendre les valeurs suivantes :

SNMP V1 — Des interruptions de type SNMP version 1 sont envoyées.

SNMP V2c — Des interruptions de type SNMP version 2 sont envoyées.

Remove (Supprimer) — Supprime des entrées de la table du gestionnaire d'interruption.

Activation des interruptions SNMP sur le périphérique

1. Ouvrez la page [SNMP Trap Settings](#) (Paramètres d'interruption SNMP).
2. Sélectionnez **Enable** (Activer) dans la liste déroulante **SNMP Trap** (Interruption SNMP).
3. Renseignez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les interruptions SNMP sont activées sur le périphérique.

Activation des interruptions d'authentification sur le périphérique

1. Ouvrez la page [SNMP Trap Settings](#) (Paramètres d'interruption SNMP).
2. Sélectionnez **Enable** (Activer) dans la liste déroulante **Authentication Trap** (Interruption d'authentification).
3. Renseignez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les interruptions d'authentification sont activées sur le périphérique.

Ajout d'un nouveau destinataire d'interruption

1. Ouvrez la page [SNMP Trap Settings](#) (Paramètres d'interruption SNMP).
2. Cliquez sur **Add** (Ajouter).

La page [Add Trap Receiver/Manager](#) (Ajouter un récepteur/gestionnaire d'interruption) s'ouvre :

Figure 6-74. Ajouter un récepteur/gestionnaire d'interruption

3. Renseignez les champs. La valeur 0.0.0.0 correspond à «All» (Toutes) et signifie que toutes les interruptions sont diffusées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le destinataire/gestionnaire d'interruptions est ajouté et le périphérique est mis à jour.

Affichage de la table des gestionnaires d'interruption

La **table des gestionnaires d'interruption** contient les champs qui permettent de configurer différents types d'interruption.

1. Ouvrez la page [SNMP Trap Settings](#) (Paramètres d'interruption SNMP).
2. Cliquez sur **Show All** (Afficher tout).

La page [Trap Managers Table](#) (Table des gestionnaires d'interruption) s'ouvre :

Figure 6-75. Table des gestionnaires d'interruption

Recipient IP	Trap	Community String	Remove

Suppression d'une entrée de la table des gestionnaires d'interruption

1. Ouvrez la page [SNMP Trap Settings](#) (Paramètres d'interruption SNMP).
2. Cliquez sur **Show All** (Afficher tout).

La page [Trap Managers Table](#) (Table des gestionnaires d'interruption) s'ouvre.

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

Le gestionnaire d'interruption sélectionné est supprimé et le périphérique est mis à jour.

Configuration d'interruptions à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [SNMP Trap Settings](#) (Paramètres d'interruption SNMP).

Tableau 6-44. Commandes CLI des paramètres d'interruption SNMP

Commande CLI	Description
<code>snmp-server enable traps</code>	Autorise le périphérique à envoyer des interruptions ou notifications SNMP.
<code>snmp-server trap authentication</code>	Autorise le périphérique à envoyer des interruptions SNMP en cas d'échec d'authentification.
<code>snmp-server host <i>adr-hôte chaîne de communauté</i> [1 2]</code>	Détermine le type d'interruption envoyé au destinataire sélectionné.
<code>show snmp</code>	Affiche l'état des communications SNMP.

Vous trouverez ci-dessous un exemple de commande CLI :

<code>console(config)# snmp-server community public_1 su 1.1.1.1</code>		
<code>console(config)# snmp-server community public_2 rw 2.2.2.2</code>		
<code>console(config)# snmp-server community public_3 ro 3.3.3.3</code>		
<code>console(config)# snmp-server host 1.1.1.1 public_1 1</code>		
<code>console(config)# snmp-server host 2.2.2.2 public_2 2</code>		
<code>console(config)# snmp-server enable traps</code>		
<code>console(config)# snmp-server trap authentication</code>		
<code>console(config)#</code>		
<code>console# show snmp</code>		
Chaîne de communauté	Accès de communauté	Adresse IP

public_1	super	1.1.1.1
public_2	lecture/écriture	2.2.2.2
public_3	lecture seule	3.3.3.3

Interruptions activées.		
Interruption authentification-échec activée.		
Adresse dest. interruption	Communauté dest. interruption	Version
-----	-----	-----
1.1.1.1	public_1	1
2.2.2.2	public_2	2
Contact système : 345 6789		
Emplacement système : 1234 5678		
console#		

Gestion des fichiers

La page File Management (Gestion de fichiers) contient des champs permettant de gérer les logiciels du périphérique, les fichiers image et les fichiers de configuration. Des fichiers peuvent être téléchargés via un serveur TFTP.

Présentation de la gestion des fichiers

La structure des fichiers de configuration s'établit comme suit :

- 1 Fichier de configuration de démarrage — Contient les commandes nécessaires pour reconfigurer le périphérique avec les mêmes paramètres que lors de sa mise hors tension ou de son redémarrage. Le fichier de démarrage est créé en copiant les commandes de configuration du fichier de configuration en cours d'exécution ou du fichier de configuration de sauvegarde.
- 1 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 hors tension ou au redémarrage du périphérique, toutes les commandes stockées dans le fichier de configuration d'exécution sont perdues. Pendant le processus de démarrage, toutes les commandes du fichier de démarrage sont copiées dans le fichier de configuration d'exécution et appliquées au périphérique. Pendant la session, toutes les nouvelles commandes saisies sont ajoutées aux commandes existantes du fichier de configuration d'exécution. Les commandes ne sont pas remplacées. Pour mettre à jour le fichier de démarrage, le fichier de configuration d'exécution doit être copié dans le fichier de configuration de démarrage avant la mise hors tension du périphérique. Au prochain redémarrage du périphérique, les commandes sont recopiées dans le fichier de configuration d'exécution à partir du fichier de configuration de démarrage.
- 1 Fichier de configuration de sauvegarde — Contient une copie de sauvegarde de la configuration du périphérique. Le fichier de sauvegarde est généré lors de la copie du fichier de configuration d'exécution ou du fichier de démarrage dans le fichier de sauvegarde. Les commandes copiées dans le fichier remplacent les commandes existantes enregistrées dans le fichier de sauvegarde. Le contenu du fichier de sauvegarde peut aussi bien être copié dans le fichier de configuration d'exécution que dans le fichier de configuration de démarrage.
- 1 Fichiers image — Des images du système sont enregistrées dans deux fichiers FLASH appelés fichiers image (Image 1 et Image 2). L'image active stocke la copie active pendant que l'autre image stocke une deuxième copie. Le périphérique démarre et s'exécute à partir de l'image active. Si l'image active est corrompue, le système démarre automatiquement à partir de l'image non active. Ce mécanisme de sécurité permet de remédier aux défaillances susceptibles de survenir lors du processus de mise à niveau du logiciel.

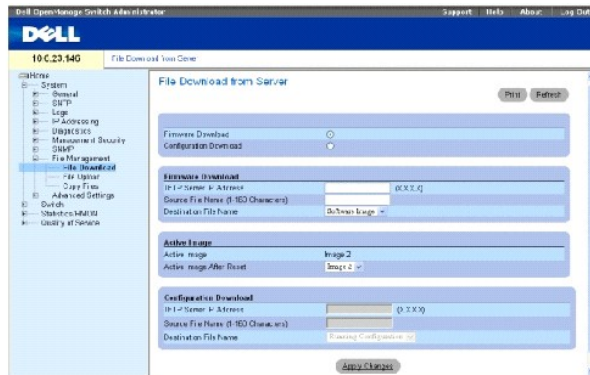
Pour ouvrir la page File Management (Gestion de fichiers), cliquez sur System (Système) → File Management (Gestion de fichiers) dans l'arborescence. La page File Management (Gestion des fichiers) contient les liens suivants :

- 1 File Download (Téléchargement de fichier)
- 1 File Upload (Chargement de fichiers)
- 1 Copy Files (Copie de fichiers)

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 et des fichiers de configuration du serveur TFTP au périphérique. Pour ouvrir la page [File Download From Server](#), cliquez sur System (Système) → File Management (Gestion des fichiers) → File Download (Téléchargement de fichiers) dans l'arborescence.

Figure 6-76. Téléchargement de fichiers à partir du serveur



Firmware Download (Téléchargement de micrologiciel) — Indique que le fichier de micrologiciel est téléchargé. Lorsque l'option **Firmware Download** est sélectionnée, les champs de **Configuration Download** (Téléchargement de configuration) sont estompés.

Configuration Download (Téléchargement de configuration) — Indique que le fichier de configuration est téléchargé. Si l'option **Configuration Download** est sélectionnée, les champs de **Firmware Download** (Téléchargement du micrologiciel) sont estompés.

Firmware Download TFTP Server IP Address (Adresse IP du serveur TFTP de téléchargement de micrologiciel) — Adresse IP du serveur TFTP à partir duquel les fichiers sont téléchargés.

Firmware Download Source File Name (Nom du fichier source de téléchargement de micrologiciel) — Indique le fichier à télécharger.

Firmware Download Destination File (Fichier de destination de téléchargement de micrologiciel) — Type de fichier de destination vers lequel le micrologiciel est téléchargé. Ce champ peut prendre les valeurs suivantes :

Software Image (Image du logiciel) — Télécharge le fichier image.

Boot Code (Code de démarrage) — Télécharge le fichier de démarrage.

Active Image (Image active) — Fichier image actuellement actif.

Active Image After Reset (Image active après réinitialisation) — Fichier image actif après la réinitialisation du périphérique.

Configuration Download File TFTP Server IP Address (Adresse IP du serveur TFTP de téléchargement du fichier de configuration) — Adresse IP du serveur TFTP par l'intermédiaire duquel le fichier de configuration est téléchargé.

Configuration Download File Source File Name (Nom du fichier source de téléchargement de configuration) — Identifie le fichier de configuration à télécharger.

Configuration Download File Destination (Destination du fichier de téléchargement de configuration) — Fichier de destination vers lequel télécharger le fichier

de configuration. 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 en écrasant le fichier existant.

Téléchargement de fichiers :

1. Ouvrez la page [File Download From Server](#) (Téléchargement de fichiers à partir du serveur).
2. Définissez le type de fichier à télécharger.
3. Renseignez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le logiciel est téléchargé sur le périphérique.

 **REMARQUE** : Pour activer le fichier image sélectionné, réinitialisez le périphérique. Pour plus d'informations sur la réinitialisation du périphérique, reportez-vous à la section [«Réinitialisation du périphérique»](#).

Téléchargement de fichiers à l'aide de commandes CLI


Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [File Download From Server](#) (Téléchargement de fichiers à partir du serveur).

Tableau 6-45. Commandes CLI de téléchargement de fichiers

Commande CLI	Description
<code>copy url-source url-destination [snmp]</code>	Copie un fichier d'une source vers une destination.

Vous trouverez ci-dessous un exemple de commande CLI :

```
console# copy running-config tftp://11.1.1.2/pp.txt

 REMARQUE : Chaque symbole ! indique que dix paquets ont été correctement transférés.

Accès au fichier 'file1' sur 172.16.101.101.

Chargement du fichier file1 depuis
172.16.101.101 : !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK]

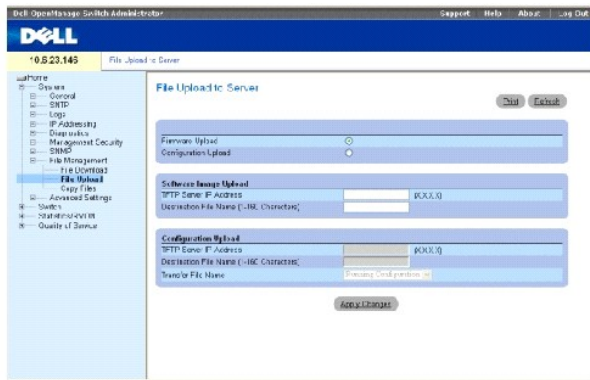
La copie s'est effectuée en 0:01:11 [hh:mm:ss]
```

Chargement de fichiers

La page [File Upload to Server](#) (Chargement de fichiers sur le serveur) contient des champs permettant de charger des logiciels du serveur TFTP vers le

périphérique. 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](#), cliquez sur System (Système) → File Management (Gestion de fichiers) → File Upload (Téléchargement de fichiers) dans l'arborescence.

Figure 6-77. Chargement de fichiers sur le serveur



Firmware Upload (Chargement de micrologiciel) — Le fichier de micrologiciel est chargé. Si l'option **Firmware Upload** est sélectionnée, les champs de **Configuration Upload** (Chargement de la configuration) sont estompés.

Configuration Upload (Chargement de configuration) — Le fichier de configuration est chargé. Lorsque l'option **Configuration Upload** (Chargement de configuration) est sélectionnée, les champs de **Software Image Upload** (Chargement d'image du logiciel) sont estompés.

Software Image Upload TFTP Server IP Address (Adresse IP du serveur TFTP de chargement d'image du logiciel) — Adresse IP du serveur TFTP sur lequel l'image du logiciel est chargée.

Software Image Upload Destination (Destination du chargement d'image du logiciel) — Indique le chemin d'accès au fichier image du logiciel vers lequel le fichier est chargé.

Configuration Upload TFTP Server IP Address (Adresse IP du serveur TFTP de chargement de configuration) — Adresse IP du serveur TFTP sur lequel le fichier de configuration est chargé.

Configuration Upload Destination (Destination du chargement de configuration) — Indique le chemin d'accès au fichier de configuration vers lequel le fichier est chargé.

Configuration Upload Transfer file name (Nom du fichier de transfert de chargement de configuration) — Fichier logiciel dans 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

Backup Configuration (Configuration de sauvegarde) — Charge le fichier de configuration de sauvegarde

Chargement de fichiers

1. Ouvrez la page [File Upload to Server](#) (Chargement de fichiers sur le serveur).
2. Définissez le type de fichier à charger.
3. Renseignez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le logiciel est chargé sur le périphérique.

Chargement de fichiers à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [File Upload to Server](#) (Chargement de fichiers sur le serveur).

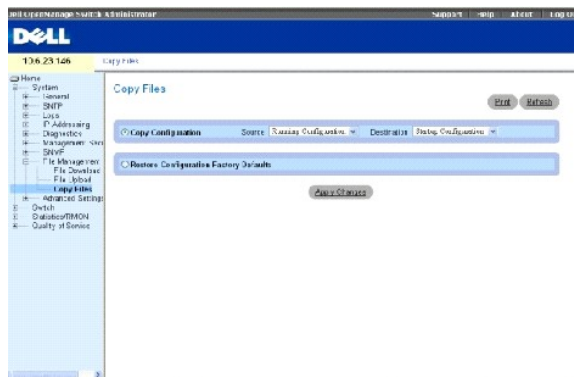
Tableau 6-46. Commandes CLI de chargement de fichiers

Commande CLI	Description
<code>copy url-source url-destination [snmp]</code>	Copie un fichier d'une source vers une destination.

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](#), cliquez sur System (Système) → File Management (Gestion de fichiers) → Copy Files (Copier des fichiers) dans l'arborescence.

Figure 6-78. Copier des fichiers



Copy Configuration (Copier la configuration) — Copie les fichiers de configuration en cours d'exécution, de configuration de démarrage ou de configuration de sauvegarde. Ce champ peut prendre les valeurs suivantes :

Source — Identifie les fichiers de configuration en cours d'exécution, de configuration de démarrage ou de configuration de sauvegarde.

Destination — Identifie le fichier où la configuration en cours d'exécution, la configuration de démarrage ou la configuration de sauvegarde est copiée.

Restore Configuration Factory Defaults (Restaurer la configuration d'origine) — Indique que les fichiers de configuration d'origine doivent être réinitialisés. Lorsque cette option n'est pas sélectionnée, les paramètres de configuration en cours sont conservés.

Copie de fichiers

1. Ouvrez la page [Copy Files](#) (Copier des fichiers).
2. Définissez les champs **Source** et **Destination**.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le fichier est copié et le périphérique est mis à jour.

Restauration de la configuration d'origine

1. Ouvrez la page [Copy Files](#) (Copier des fichiers).
2. Cliquez sur **Restore Company Factory Defaults** (Restaurer la configuration d'origine).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres d'origine par défaut sont rétablis et le périphérique est mis à jour.

Copie et suppression de fichiers à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage des champs de la page [Copy Files](#) (Copier des fichiers).

Tableau 6-47. Commandes CLI de copie de fichiers

Commande CLI	Description
<code>copy url-source url-destination [snmp]</code>	Copie un fichier d'une source vers une destination.
<code>delete startup-config</code>	Supprime le fichier de configuration de démarrage.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console # copy tftp://172.16.101.101/file1 image

Accès au fichier 'file1' sur 172.16.101.101.

Chargement du fichier file1 depuis
172.16.101.101 : !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK]

La copie s'est effectuée en 0:01:11 [hh:mm:ss]

Console# delete startup-config

Console# copy running-config startup-config

01-Jan-2000 01:55:03 %COPY-W-TRAP: L'opération de copie s'est terminée avec succès

Copie réussie
```

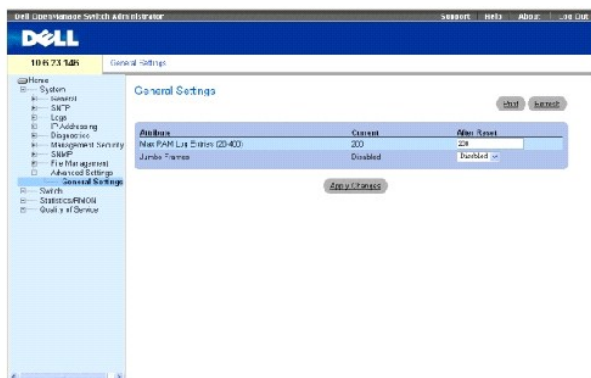
Définition de paramètres avancés

La page **Advanced Settings** (Paramètres avancés) contient un lien permettant de configurer des paramètres généraux. Utilisez les paramètres avancés si vous voulez définir divers attributs globaux du périphérique. Les modifications apportées à ces attributs n'entrent en vigueur qu'après la réinitialisation du périphérique. Pour ouvrir la page **Advanced Settings** (Paramètres avancés), cliquez sur System (Système) → Advanced Settings (Paramètres avancés) dans l'arborescence.

Configuration des paramètres de réglage généraux du périphérique

La page [General Settings](#) (Paramètres globaux) fournit des informations permettant de définir les paramètres globaux du périphérique. Pour ouvrir la page [General Settings](#), cliquez sur System (Système) → Advanced Settings (Paramètres avancés) → General (Général) dans l'arborescence.

Figure 6-79. Paramètres globaux



Attribute (Attribut) — Attribut du paramètre général.

Current (En cours) — Valeur en cours.

After Reset (Après réinitialisation) — Future valeur après réinitialisation. Lorsqu'une valeur est saisie dans la colonne After Reset (Après réinitialisation), la mémoire est allouée à la table des champs.

Max RAM Log Entries(20-400) (Nombre max. d'entrées de journal en RAM [20 à 400]) — Nombre maximum d'entrées de journal en RAM. Lorsque le maximum est atteint, le journal est effacé et le fichier journal réinitialisé.

Jumbo Frames (Trames Jumbo) — Active ou désactive la fonction de trame Jumbo. Les trames Jumbo permettent de transporter les données identiques sur un nombre réduit de trames. Elles permettent d'éviter la surcharge, de réduire le temps de traitement et de diminuer les interruptions.

Affichage du compteur d'entrées de journal en RAM à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page [General Settings](#) (Paramètres globaux).

Tableau 6-48. Commandes CLI des paramètres globaux

Commande CLI	Description
logging buffered size <i>nombre</i>	Définit le nombre de messages syslog stockés dans la mémoire tampon interne (RAM).
port jumbo-frame	Active les trames Jumbo sur le périphérique.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# logging buffered size 300
```

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Guide d'utilisation du système Dell™ PowerConnect™ 5324



REMARQUE : Une REMARQUE indique une information importante qui peut vous aider à mieux utiliser votre ordinateur.



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



PRÉCAUTION : Une PRÉCAUTION indique un risque potentiel de dommages matériels ou corporels, ou de mort.

Les informations contenues dans ce document sont sujettes à modification sans préavis.

© 2003 - 2004 Dell Inc. Tous droits réservés.

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

Marques utilisées dans ce document : *Dell, Dell OpenManage, le logo DELL, Inspiron, Dell Precision, Dimension, OptiPlex, PowerConnect, PowerApp, PowerVault, Axim, DellNet et Latitude* sont des marques de Dell Inc. *Microsoft et Windows* sont des marques déposées de Microsoft Corporation.

D'autres marques et noms commerciaux peuvent être utilisés dans ce document pour faire référence aux entités se réclamant de ces marques et de ces noms ou à leurs produits. Dell Inc. rejette tout intérêt propriétaire dans les marques et les noms commerciaux autres que les siens.

Avril 2004 Rév. A00

[Retour à la page du sommaire](#)

[Retour à la page du sommaire](#)

Utilisation de Dell OpenManage Switch Administrator

Guide d'utilisation du système Dell™ PowerConnect™ 5324

- [Comprendre l'interface](#)
- [Utilisation des boutons de Switch Administrator](#)
- [Démarrage de l'application](#)
- [Accès au périphérique via l'interface de ligne de commande \(CLI\)](#)
- [Utilisation de la CLI](#)

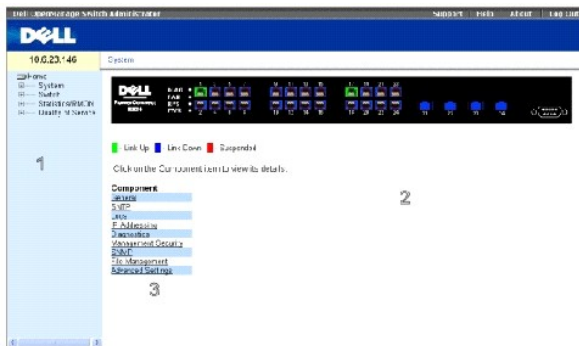
Cette section présente l'interface utilisateur.

Comprendre l'interface

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

- 1 Vue Arborescence — Affichée dans le volet gauche de la page d'accueil, l'arborescence fournit une représentation hiérarchisée des différentes fonctionnalités et de leurs composants.
- 1 Vue du périphérique — Située dans le volet droit de la page d'accueil, la vue du périphérique fournit une représentation graphique du périphérique, une zone d'informations ou un tableau et des instructions de configuration.

Figure 5-13. Composants de Switch Administrator



Le [Tableau 5-7](#) répertorie les composants de l'interface et les numéros qui leur sont associés.

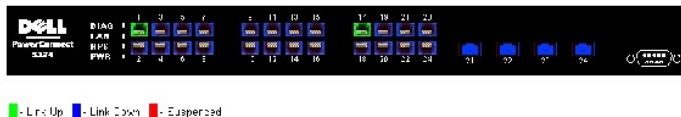
Tableau 5-7. Composants de l'interface

Composant	Nom
1	L'arborescence dresse la liste des différentes fonctionnalités du périphérique. Vous pouvez développer les branches de l'arborescence de façon à afficher tous les composants rattachés à une fonctionnalité spécifique ou les réduire pour masquer les composants. 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 du périphérique fournit des informations sur les ports, la configuration et l'état en cours, les tableaux et les composants. En fonction des options sélectionnées, la zone au bas de la vue du périphérique affiche d'autres informations et/ou des fenêtres de dialogue pour la configuration des paramètres.
3	La liste des composants dresse une liste de ceux-ci. Vous pouvez également afficher des composants en développant une fonctionnalité dans l'arborescence.
4	Les boutons d'information permettent d'accéder à des informations relatives au périphérique et aux services Dell. Pour plus d'informations, reportez-vous à la section «Boutons d'information» .

Représentation du périphérique

La page d'accueil PowerConnect contient une représentation graphique du panneau avant du périphérique.

Figure 5-14. Voyants des ports



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

Tableau 5-8. Voyants

Composant	Nom
Voyants des ports	
Vert	Le port est connecté.
Rouge	Une erreur est survenue sur le port.
Bleu	Le port est déconnecté.

REMARQUE : Dans le module OpenManage Switch Administrator, les DEL des ports ne sont pas représentées sur le panneau avant des PowerConnect. L'état des DEL ne peut être déterminé qu'en observant les voyants directement sur le périphérique. Pour plus d'informations sur les DEL, reportez-vous à la section [«Signification des DEL»](#).

Utilisation des boutons de Switch Administrator

Cette section décrit les boutons de l'interface OpenManage Switch Administrator.

Boutons d'information

Les boutons d'information donnent accès au support et à l'aide en ligne et fournissent des informations sur les interfaces d'OpenManage Switch Administrator.

Tableau 5-9. Boutons d'information

Bouton	Description
Support (Assistance technique)	Ouvre la page de support technique de Dell à l'adresse support.dell.com .
Help (Aide)	Aide en ligne contenant des informations qui vous aideront à configurer et à gérer le périphérique. Les pages de l'aide en ligne sont directement liées à la page courante. Par exemple, si la page IP Addressing (Adressage IP) est ouverte, la rubrique d'aide de cette page s'ouvre lorsque vous cliquez sur Help (Aide).
About (À propos de)	Indique le numéro de version et les informations de copyright Dell.
Log Out (Déconnexion)	Vous déconnecte de l'application et ferme la fenêtre du navigateur.

Boutons de gestion du périphérique

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

Tableau 5-10. Boutons de gestion du périphérique

Bouton	Description
Apply Changes (Appliquer les modifications)	Applique les modifications définies au périphérique.
Add (Ajouter)	Ajoute des informations dans des tableaux ou des fenêtres.
Telnet	Ouvre une session Telnet.


Query (Interroger)	Interroge des tableaux.
Show All (Afficher tout)	Affiche les tableaux du périphérique.
Left arrow/Right arrow (Flèche gauche/droite)	Fait passer des informations d'une liste à une autre.
Refresh (Actualiser)	Actualise les informations relatives au périphérique.
Reset All Counters (Réinitialiser tous les compteurs)	Réinitialise les compteurs de statistiques.
Print (Imprimer)	Imprime les informations qui figurent dans les pages ou les tableaux du système de gestion du réseau .
Show Neighbors Info (Afficher infos voisins)	Affiche la liste de voisins à partir de la page Neighbors Table (Tableau des voisins).
Draw (Dessiner)	Crée des graphiques de statistiques en temps réel.


Démarrage de l'application

1. Ouvrez un navigateur Web.
2. Saisissez l'adresse IP du périphérique (telle que définie dans la CLI) dans la barre d'adresses et appuyez sur <Entrée>.

Pour plus d'informations sur l'affectation d'une adresse IP à un périphérique, reportez-vous à la section «Adresse IP statique et masque de sous-réseau».

3. Lorsque la fenêtre **Enter Network Password** (Saisie du mot de passe réseau) s'affiche, entrez un nom d'utilisateur et un mot de passe.

 **REMARQUE** : Le périphérique n'est pas configuré avec un mot de passe par défaut ; vous pouvez le configurer sans mot de passe. Pour plus d'informations sur la récupération d'un mot de passe perdu, reportez-vous à la section «Récupération d'un mot de passe».

 **REMARQUE** : Les mots de passe font la distinction entre majuscules et minuscules et ils doivent obligatoirement être alphanumériques.


4. Cliquez sur **OK**.

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

Accès au périphérique via l'interface de ligne de commande (CLI)


Le périphérique peut être géré par le biais d'une connexion directe avec le port de la console ou par l'intermédiaire d'une connexion Telnet. L'utilisation de l'interface de ligne de commande s'apparente à la saisie de commandes sur un système Linux. Si l'accès est effectué par l'intermédiaire d'une connexion Telnet, assurez-vous qu'une adresse IP est définie pour le périphérique et que la station de travail utilisée pour accéder au périphérique est connectée avant d'utiliser les commandes de l'interface de ligne de commande.

Pour plus d'informations sur la configuration d'une adresse IP initiale, reportez-vous à la section «Adresse IP statique et masque de sous-réseau».

 **REMARQUE** : Vérifiez que le client est chargé avant d'utiliser l'interface de ligne de commande.

Connexion par l'intermédiaire de la console

1. Mettez le périphérique sous tension et attendez la fin du démarrage.
2. À l'affichage de l'invite `Console>`, tapez `enable` et appuyez sur <Entrée>.
3. Configurez le périphérique et entrez les commandes nécessaires à l'exécution des tâches requises.
4. Lorsque vous avez terminé, refermez la session en tapant la commande `quit` ou `exit`.

 **REMARQUE** : Lorsqu'un utilisateur se connecte au système en mode de commande Privileged EXEC (EXEC privilégié), l'utilisateur en cours est déconnecté et remplacé par le nouvel utilisateur.

Connexion Telnet

Telnet est un protocole TCP/IP d'émulation de terminal. Les terminaux ASCII peuvent être virtuellement connectés au périphérique local par le biais d'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.

Le périphérique peut gérer jusqu'à quatre sessions Telnet simultanées. Toutes les commandes de l'interface de ligne de commande peuvent être utilisées au cours d'une session Telnet.

Pour ouvrir une session Telnet :

1. Sélectionnez Démarrer > Exécuter.

La fenêtre **Exécuter** s'ouvre.

2. Dans la fenêtre **Exécuter**, tapez Telnet <adresse IP> dans le champ **Ouvrir**.
3. Cliquez sur **OK** pour démarrer la session Telnet.

Utilisation de la CLI

Cette section contient des informations sur l'utilisation de la 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 de la console.

Au sein de chaque mode, une commande particulière permet de passer d'une commande à une autre.

Lors de l'initialisation de la session CLI, le mode User EXEC (EXEC utilisateur) est activé par défaut. Seul un sous-ensemble partiel de commandes est disponible dans ce mode. Ce niveau est réservé aux tâches qui ne modifient pas la configuration de la console et s'utilise pour accéder à des sous-systèmes de configuration tels que l'interface de ligne de commande. Le passage au niveau suivant (mode Privileged EXEC (EXEC privilégié)) exige la saisie d'un mot de passe (à configurer).

Le mode Privileged EXEC (EXEC privilégié) permet d'accéder à la configuration générale du périphérique. Pour procéder à des configurations globales sur le périphérique, vous devez passer au niveau suivant, autrement dit, le mode Global Configuration (Configuration globale). La saisie d'un mot de passe n'est pas obligatoire.


Le mode Global Configuration (Configuration globale) gère la configuration du périphérique sur un niveau global.

Le mode Interface Configuration (Configuration de l'interface) permet de configurer le périphérique au niveau de l'interface physique. Les commandes de l'interface qui exigent des sous-commandes sont accessibles à un autre niveau : le mode Subinterface Configuration (Configuration de la sous-interface). La saisie d'un mot de passe n'est pas obligatoire.

Mode User EXEC (EXEC utilisateur)

Après la connexion au périphérique, le mode de commande User EXEC (EXEC utilisateur) est activé. L'invite utilisateur se compose d'un nom d'hôte suivi d'un crochet (>). Par exemple :

```
console>
```

 **REMARQUE** : À moins qu'il n'ait été modifié lors de la configuration initiale, le nom d'hôte par défaut est console.

Les commandes accessibles dans ce mode permettent d'établir une connexion avec des périphériques distants, de modifier provisoirement les paramètres des terminaux, d'effectuer des tests de base et de répertorier des informations système.

Pour afficher la liste des commandes du mode User EXEC (EXEC utilisateur), tapez un point d'interrogation (?) à l'invite.

Mode Privileged EXEC (EXEC privilégié)

Ce mode permet de s'assurer que l'accès privilégié est protégé par mot de passe de façon à éviter toute utilisation non autorisée. Les mots de passe s'affichent sous la forme ***** à l'écran et ils font la distinction entre majuscules et minuscules.

Pour accéder aux commandes du mode Privileged EXEC (EXEC privilégié) et les répertorier :

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

L'invite du mode Privileged EXEC (EXEC privilégié) se compose du nom d'hôte du périphérique suivi du symbole dièse (#). Par exemple :

```
console#
```

Pour afficher la liste des commandes du mode Privileged EXEC (EXEC privilégié), tapez un point d'interrogation (?) à l'invite et appuyez sur <Entrée>.

Pour revenir du mode Privileged EXEC (EXEC privilégié) au mode User EXEC (EXEC utilisateur), tapez l'une des commandes suivantes : `disable`, `exit/end`, ou <Ctrl><Z>.

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

```
console>enable
```

```
Enter Password: *****
```

```
console#
```

```
console#disable
```

```
console>
```

La commande `exit` permet de passer du mode en cours au mode du niveau inférieur. Par exemple, vous pouvez passer du mode Interface Configuration (Configuration de l'interface) au mode Global Configuration (Configuration globale) ou du mode Global Configuration (Configuration globale) au mode Privileged EXEC (EXEC privilégié).

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 Global Configuration (Configuration globale), à l'invite du mode Privileged EXEC (EXEC privilégié), tapez `configure` et appuyez sur <Entrée>. L'invite du mode Global Configuration (Configuration globale) se compose du nom d'hôte du périphérique suivi de `(config)` et du symbole #.

```
console(config)#
```

Pour afficher la liste des commandes du mode Global Configuration (Configuration globale), tapez un point d'interrogation (?) à l'invite.

Pour revenir du mode Global Configuration (Configuration globale) au mode Privileged EXEC (EXEC privilégié), tapez la commande `exit` ou utilisez la commande `<Ctrl><Z>`.

L'exemple ci-dessous illustre la procédure d'accès au mode Global Configuration (Configuration globale) et de retour au mode Privileged EXEC (EXEC privilégié) :

```
console#  
  
console# configure  
  
console(config)# exit  
  
console#
```

Mode Interface Configuration (Configuration de l'interface)

Les commandes de configuration de l'interface permettent de modifier certains paramètres des interfaces IP, tels que pont-groupe, description, etc.

Mode VLAN Database

Le mode VLAN contient les commandes qui permettent de créer et configurer un VLAN dans son ensemble, créer un VLAN et lui appliquer une adresse IP, par exemple. Vous trouverez ci-dessous un exemple d'invite en mode VLAN :

```
Console # vlan database  
  
Console (config-vlan)#
```

Mode Port Channel

Le mode Port Channel (Canal de port) contient les commandes qui permettent de configurer des LAG (groupes de liaisons agrégées). Vous trouverez ci-dessous un exemple d'invite en mode Port Channel :

```
Console(config)# interface port-channel 1  
  
Console (config-if)#
```

Mode Interface

Le mode Interface contient des commandes permettant de configurer l'interface. La commande du mode Global Configuration `interface ethernet` permet de passer en mode de configuration Interface. Vous trouverez ci-dessous un exemple d'invite en mode Interface :

```
console> enable
```

```
console#configure
```

```
console(config)# interface ethernet g18
```

```
console(config-if)#
```

Mode Management Access List

Le mode Management Access List (Liste d'accès de gestion) contient des commandes permettant de définir des listes d'accès de gestion. La commande du mode Global Configuration `management access-list` permet de passer en mode de configuration Management Access List.

L'exemple qui suit montre comment créer une liste d'accès appelée «m1ist», comment configurer deux interfaces de gestion Ethernet g1 et Ethernet g9 et comment faire de la liste d'accès une liste active :

```
Console (config)# management access-list m1ist
```

```
Console (config-macl)# permit ethernet g1
```

```
Console (config-macl)# permit ethernet g9
```

```
Console (config-macl)# exit
```

```
Console (config)# management access-class m1ist
```

Mode SSH Public Key

Le mode SSH Public Key (Clé publique SSH) contient des commandes permettant de définir manuellement d'autres clés publiques SSH de périphériques.

La commande du mode Global Configuration `crypto key pubkey-chain ssh` permet de passer en mode de configuration SSH Public Key-chain.

Voici un exemple de commandes permettant de passer en mode de configuration SSH Public Key-chain :

```
Console(config)# crypto key pubkey-chain ssh
```

```
Console(config-pubkey-chain)#
```

Exemples de commandes CLI

Les commandes de l'interface de ligne de commande sont fournies en tant qu'exemples de configuration. Pour obtenir une description complète des commandes de l'interface de ligne de commande avec des exemples, reportez-vous au «Guide de référence CLI» inclus sur le CD de documentation.

[Retour à la page du sommaire](#)


[Retour à la page du sommaire](#)

Affichage des statistiques

Guide d'utilisation du système Dell PowerConnect 5324

- [Affichage des tables](#)
- [Affichage des statistiques RMON](#)
- [Affichage des graphiques](#)

La page **Statistic** (Statistiques) contient des informations relatives aux interfaces, aux réseaux virtuels dynamiques (GVRP), à Etherlike, à la télésurveillance (RMON) et à l'utilisation du périphérique. Pour ouvrir la page **Statistics** (Statistiques), cliquez sur **Statistics** (Statistiques) dans l'arborescence.

 **REMARQUE** : Il n'existe aucune commande CLI pour les pages de statistiques.

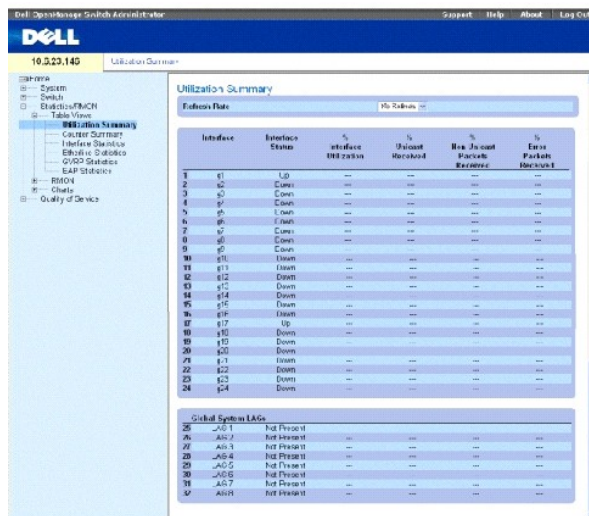
Affichage des tables

La page **Table Views** (Vues Tables) contient des liens qui permettent d'afficher les statistiques sous forme de table. Pour ouvrir la page, cliquez sur **Statistics** (Statistiques) → **Table** dans l'arborescence.

Affichage du récapitulatif de l'utilisation

La page [Utilization Summary](#) (Récapitulatif de l'utilisation) fournit des statistiques sur l'utilisation de l'interface. Pour ouvrir cette page, cliquez sur **Statistics** (Statistiques) → **Table Views** (Vues Tables) → **Utilization Summary** (Récapitulatif de l'utilisation) dans l'arborescence.

Figure 8-115. Récapitulatif de l'utilisation



The screenshot shows the Dell OpenManage Switch Administrator interface. The main window displays the 'Utilization Summary' page. The table below is a reproduction of the data shown in the screenshot.

Interface	Interface Status	% Interface Utilization	% Packet Received	% Bus Percent Received	% Error Packet Received
1	ET	LD	---	---	---
2	E2	Down	---	---	---
3	E3	Down	---	---	---
4	E4	Down	---	---	---
5	E5	Down	---	---	---
6	E6	Down	---	---	---
7	E7	Down	---	---	---
8	E8	Down	---	---	---
9	E9	Down	---	---	---
10	E10	Down	---	---	---
11	E11	Down	---	---	---
12	E12	Down	---	---	---
13	E13	Down	---	---	---
14	E14	Down	---	---	---
15	E15	Down	---	---	---
16	E16	Down	---	---	---
17	E17	Up	---	---	---
18	E18	Down	---	---	---
19	E19	Down	---	---	---
20	E20	Down	---	---	---
21	E21	Down	---	---	---
22	E22	Down	---	---	---
23	E23	Down	---	---	---
24	E24	Down	---	---	---

Global System LAGs	LAG Status	LAG Name	LAG Type
25	Not Present	JAG.1	LAG
26	Not Present	JAG.2	LAG
27	Not Present	JAG.3	LAG
28	Not Present	JAG.4	LAG
29	Not Present	JAG.5	LAG
30	Not Present	JAG.6	LAG
31	Not Present	JAG.7	LAG
32	Not Present	AG.H	LAG

Refresh Rate (Taux d'actualisation) 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 en 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 passe par l'interface. La valeur maximale pour une connexion en mode Semi-duplex est 100 %.

% Unicast Received (% monodiffusion reçus) Pourcentage de paquets monodiffusion reçus sur l'interface.

% Non Unicast Packets Received (% paquets non monodiffusion reçus) Pourcentage de paquets non monodiffusion reçus sur l'interface.

% Error Packets Received (% paquets avec erreurs reçus) Pourcentage de paquets contenant des erreurs, qui ont été reçus sur l'interface.

Global System LAG (LAG système global) Performances du LAG/faisceau en cours.

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 8-116. Récapitulatif des compteurs

Interface	Status	Received Unicast Packets	Received Non Unicast Packets	Transmit Unicast Packets	Received Errors
1	Up	1279	262	23	130
2	Down	0	0	0	0
3	Down	0	0	0	0
4	Down	0	0	0	0
5	Down	0	0	0	0
6	Down	0	0	0	0
7	Down	0	0	0	0
8	Down	0	0	0	0
9	Down	0	0	0	0
10	Down	0	0	0	0
11	Down	0	0	0	0
12	Down	0	0	0	0
13	Down	0	0	0	0
14	Down	0	0	0	0
15	Down	0	0	0	0
16	Down	0	0	0	0
17	Up	2520	626	159	60
18	Down	0	0	0	0
19	Down	0	0	0	0
20	Down	0	0	0	0
21	Down	0	0	0	0
22	Down	0	0	0	0
23	Down	0	0	0	0
24	Down	0	0	0	0

LAG ID	Name	Status	Received Unicast Packets	Received Non Unicast Packets	Transmit Unicast Packets	Received Errors
25	LAG1	Up	0	0	0	0
26	LAG2	Up	0	0	0	0
27	LAG3	Up	0	0	0	0
28	LAG4	Up	0	0	0	0
29	LAG5	Up	0	0	0	0
30	LAG6	Up	0	0	0	0
31	LAG7	Up	0	0	0	0
32	LAG8	Up	0	0	0	0

Refresh Rate (Taux d'actualisation) 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) Nombre de paquets monodiffusion reçus sur l'interface.

Received Non Unicast Packets (Paquets non monodiffusion reçus) Nombre de paquets non monodiffusion reçus sur l'interface.

Transmit Unicast Packets (Paquets monodiffusion transmis) Nombre de paquets monodiffusion transmis depuis l'interface.

Transmit Non Unicast Packets (Paquets non monodiffusion transmis) Nombre de paquets non monodiffusion transmis depuis l'interface.

Received Errors (Erreurs reçues) Nombre de paquets contenant des erreurs, qui ont été reçus sur l'interface.

Global System LAG (LAG système global) Performances du LAG/faisceau en cours.

Affichage des statistiques relatives aux interfaces

La page [Interface Statistics](#) (Statistiques sur les interfaces) contient des statistiques sur les paquets reçus et transmis. Les champs sont les mêmes pour ces deux types de paquets. 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 8-117. Statistiques sur les interfaces



Interface Indique si des statistiques sont affichées pour un port ou un LAG.

Refresh Rate (Taux d'actualisation) Délai qui s'écoule entre deux actualisations des statistiques sur les interfaces.

Statistiques des paquets reçus

Total Bytes (Octets totaux) Nombre d'octets reçus sur l'interface sélectionnée.

Unicast Packets (Paquets monodiffusion) Nombre de paquets monodiffusion reçus sur l'interface sélectionnée.

Multicast Packets (Paquets multidiffusion) Nombre de paquets multidiffusion reçus sur l'interface sélectionnée.

Broadcast Packets (Paquets diffusion) Nombre de paquets diffusion reçus sur l'interface sélectionnée.

Packets with Errors (Paquets avec erreurs) Nombre de paquets contenant des erreurs, qui ont été reçus sur l'interface sélectionnée.

Statistiques des paquets transmis

Total Bytes (Octets totaux) Nombre d'octets transmis sur l'interface sélectionnée.

Unicast Packets (Paquets monodiffusion) Nombre de paquets monodiffusion transmis sur l'interface sélectionnée.

Multicast Packets (Paquets multidiffusion) Nombre de paquets multidiffusion transmis sur l'interface sélectionnée.

Broadcast Packets (Paquets diffusion) Nombre de paquets diffusion transmis sur l'interface sélectionnée.

Packets with Errors (Paquets avec erreurs) Nombre de paquets contenant des erreurs, qui ont été transmis sur l'interface sélectionnée.

Affichage des statistiques relatives aux interfaces

1. Ouvrez la page [Interface Statistics](#) (Statistiques sur les interfaces).
2. Sélectionnez une interface dans le champ **Interface**.

Les statistiques de l'interface s'affichent.

Réinitialisation des compteurs de statistiques sur les interfaces

1. Ouvrez la page [Interface Statistics](#) (Statistiques sur les interfaces).
2. Cliquez sur **Reset All Counters** (Réinitialiser tous les compteurs).

Les compteurs de statistiques sur les interfaces sont réinitialisés.

Affichage des statistiques relatives aux interfaces à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage des statistiques relatives aux interfaces.

Tableau 8-80. Commandes CLI des statistiques relatives aux interfaces

Commande CLI	Description
<code>show interfaces counters [ethernet interface port-channel numéro-canal-port]</code>	Affiche le trafic enregistré par l'interface physique.

Vous trouverez ci-dessous un exemple de commande CLI.

```
Console> enable
Console# show interfaces counters
```

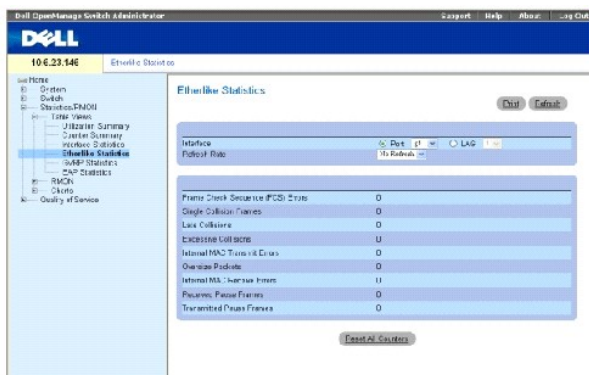
Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
-----	-----	-----	-----	-----
g1	183892	1289	987	8
g2	0	0	0	0
g3	123899	1788	373	19

Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
-----	-----	-----	-----	-----
g4	9188	9	8	0
g5	0	0	0	0
g6	8789	27	8	0
Canal	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
-----	-----	-----	-----	-----
1	27889	928	0	78
Canal	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
-----	-----	-----	-----	-----
1	23739	882	0	122

Affichage des statistiques relatives à Etherlike

La page [Etherlike Statistics](#) (Statistiques Etherlike) fournit des statistiques relatives 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 8-118. Statistiques Etherlike



Interface Indique si des statistiques sont affichées pour un port ou un LAG.

Refresh Rate (Taux d'actualisation) Délai qui s'écoule entre deux actualisations des statistiques sur les interfaces.

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) Nombre d'erreurs de trames monocollision reçues sur l'interface sélectionnée.

Multiple Collision Frames (Trames multicollisions) Nombre d'erreurs de trames multicollision reçues sur l'interface sélectionnée.

Single Quality Error (SQE) Test Errors (Erreurs du test de détection des erreurs de qualité simples) Nombre d'erreurs du test SQE reçues sur l'interface sélectionnée.

Deferred Transmissions (Transmissions différées) Nombre de transmissions différées sur l'interface sélectionnée.

Late Collisions (Collisions tardives) Nombre de trames de collision tardive reçues sur l'interface sélectionnée.

Excessive Collisions (Collisions excessives) Nombre de collisions excessives reçues sur l'interface sélectionnée.

Internal MAC Transmit Errors (Erreurs de transmission MAC internes) Nombre d'erreurs de transmission MAC internes reçues sur l'interface sélectionnée.

Carrier Sense Errors (Erreurs de détection de porteuse) Nombre d'erreurs de détection de porteuse reçues sur l'interface sélectionnée.

Oversize Packets (Paquets de taille excessive) Nombre d'erreurs dues à des paquets de taille excessive reçues sur l'interface sélectionnée.

Internal MAC Receive Errors (Erreurs de réception MAC internes) Nombre d'erreurs de réception MAC internes reçues sur l'interface sélectionnée.

Single Quality Errors (SQE) Test Errors (Erreurs du test de détection des erreurs de qualité simples) Nombre d'erreurs du test SQE reçues sur l'interface sélectionnée.

Receive Pause Frames (Trames de pause reçues) Nombre de trames de pause reçues sur l'interface sélectionnée.

Transmitted Paused Frames (Trames de pause transmises) Nombre de trames de pause transmises depuis l'interface sélectionnée.

Affichage des statistiques Etherlike pour une interface

1. Ouvrez la page [Etherlike Statistics](#) (Statistiques Etherlike).
2. Sélectionnez une interface dans le champ **Interface**.

Les statistiques Etherlike relatives à l'interface s'affichent.

Réinitialisation des statistiques Etherlike

1. Ouvrez la page [Etherlike Statistics](#) (Statistiques Etherlike).
2. Cliquez sur **Reset All Counters** (Réinitialiser tous les compteurs).

Les statistiques Etherlike sont réinitialisées.

Affichage des statistiques Etherlike à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage des statistiques Etherlike.

Tableau 8-81. Commandes CLI des statistiques Etherlike

Commande CLI	Description
<code>show interfaces counters [ethernet <i>interface</i> port-channel <i>numéro-canal-port</i>]</code>	Affiche le trafic enregistré par l'interface physique.

Vous trouverez ci-dessous un exemple de commande CLI.

Console> enable				
Console# show interfaces counters ethernet g1				
Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
-----	-----	-----	-----	-----
g1	183892	1289	987	8
Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
-----	-----	-----	-----	-----
g1	9188	9	8	0
Erreurs FCS : 8				
Trames monocollision : 0				
Trames multicollision : 0				
Erreurs du test SQE : 0				
Transmissions différées : 0				
Collisions tardives : 0				
Collisions excessives : 0				
Erreurs de transmission MAC internes : 0				
Erreurs de détection de porteuse : 0				

Pqts de taille excessive : 0

Erreurs de réception MAC internes : 0

Trames en pause reçues : 0

Trames en pause transmises : 0

Affichage des statistiques GVRP

La page [GVRP Statistics](#) (Statistiques GVRP) contient des statistiques du périphérique relatives aux réseaux virtuels dynamiques (GVRP). Pour ouvrir la page, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **Table Views** (Vues Tables) → **GVRP Statistics** (Statistiques GVRP) dans l'arborescence.

Figure 8-119. Statistiques GVRP



Interface Indique si des statistiques sont affichées pour un port ou un LAG.

Refresh Rate (Taux d'actualisation) Délai qui s'écoule entre deux actualisations des statistiques sur les interfaces.

Join Empty Affiche les statistiques Join Empty GVRP du périphérique.

Empty Affiche les statistiques Empty GVRP du périphérique.

Leave Empty Affiche les statistiques Leave Empty GVRP du périphérique.

Join In Affiche les statistiques Join In GVRP du périphérique.

Leave In Affiche les statistiques Leave In GVRP du périphérique.

Leave All Affiche les statistiques Leave all GVRP du périphérique.

Invalid Protocol ID (ID de protocole incorrect) Statistiques relatives aux ID de protocole GVRP incorrects sur le périphérique.

Invalid Attribute Type (Type d'attribut incorrect) Statistiques relatives aux ID d'attributs GVRP incorrects sur le périphérique.

Invalid Attribute Value (Valeur d'attribut incorrecte) Statistiques relatives aux valeurs d'attributs GVRP incorrectes sur le périphérique.

Invalid Attribute Length (Longueur d'attribut incorrecte) Statistiques relatives aux longueurs d'attributs GVRP incorrectes sur le périphérique.

Invalid Events (Événements incorrects) Statistiques relatives aux événements GVRP incorrects sur le périphérique.

Affichage des statistiques GVRP pour un port

1. Ouvrez la page [GVRP Statistics](#) (Statistiques GVRP).
2. Sélectionnez une interface dans le champ **Interface**.

Les statistiques GVRP relatives à l'interface s'affichent.

Réinitialisation des statistiques GVRP

1. Ouvrez la page [GVRP Statistics](#) (Statistiques GVRP).
2. Cliquez sur **Reset All Counters** (Réinitialiser tous les compteurs).

Les compteurs GVRP sont réinitialisés.

Affichage des statistiques GVRP à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage des statistiques GVRP.

Tableau 8-82. Commandes CLI des statistiques GVRP

Commande CLI	Description
<code>show gvrp statistics [ethernet interface port-channel numéro-canal-port]</code>	Affiche les statistiques du protocole GVRP.
<code>show gvrp error-statistics [ethernet interface port-channel numéro-canal-port]</code>	Affiche les statistiques des erreurs du protocole GVRP.

Vous trouverez ci-dessous un exemple de commande CLI :

Console# show gvrp statistics	
Statistiques du protocole GVRP :	

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
----	---	----	----	----	---	----	---	----	----	----	---	----
g1	0	0	0	0	0	0	0	0	0	0	0	0
g2	0	0	0	0	0	0	0	0	0	0	0	0
g3	0	0	0	0	0	0	0	0	0	0	0	0
g4	0	0	0	0	0	0	0	0	0	0	0	0
g5	0	0	0	0	0	0	0	0	0	0	0	0
g6	0	0	0	0	0	0	0	0	0	0	0	0
g7	0	0	0	0	0	0	0	0	0	0	0	0
g8	0	0	0	0	0	0	0	0	0	0	0	0

Console# show gvrp error-statistics	
Statistiques des erreurs GVRP :	

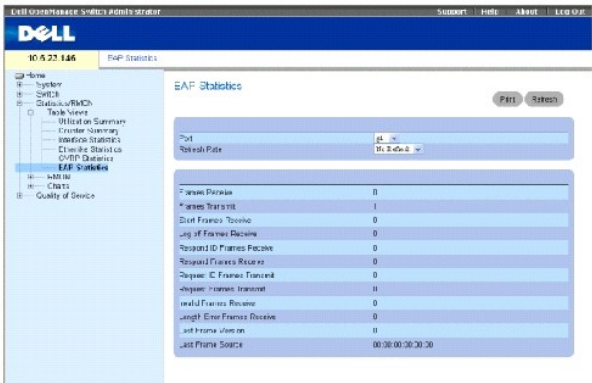
Légende :	
INVPROT : ID de protocole incorrect	INVPLEN : longueur de PDU incorrecte
INVATYP : type d'attribut incorrect	INVALEN : longueur d'attribut incorrecte
INVAVAL : valeur d'attribut incorrecte	INVEVENT : événement incorrect

Port	INVPROT	INVATYP	INVAVAL	INVALEN	INVEVENT
---	---	---	---	---	---
g1	0	0	0	0	0
g2	0	0	0	0	0
g3	0	0	0	0	0
g4	0	0	0	0	0
g5	0	0	0	0	0
g6	0	0	0	0	0
g7	0	0	0	0	0
g8	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 l'EAP, reportez-vous à la section «[Authentification basée sur le port \(802.1x\)](#)». 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 8-120. Statistiques EAP



Port Port dont on recherche les statistiques.

Refresh Rate (Taux d'actualisation) Délai qui s'écoule entre deux actualisations des statistiques sur les interfaces.

Frames Receive (Trames reçues) Nombre de trames EAPOL valides reçues sur le port.

Frames Transmit (Trames transmises) Nombre de trames EAPOL transmises via le port.

Start Frames Receive (Trames de démarrage reçues) Nombre de trames de démarrage EAPOL reçues sur le port.

Log off Frames Receive (Trames de déconnexion reçues) Nombre de trames de déconnexion EAPOL reçues sur le port.

Respond ID Frames Receive (Trames d'ID de réponse reçues) Nombre de trames ID/réponse EAP reçues sur le port.

Respond Frames Receive (Trames de réponse reçues) Nombre de trames de réponse EAP valides reçues sur le port.

Request ID Frames Transmit (Trames d'ID de demande transmises) Nombre de trames d'ID de demande EAP transmises via le port.

Request Frames Transmit (Trames de demande transmises) Nombre de trames de demande EAP transmises via le port.

Invalid Frames Receive (Trames non valides reçues) Nombre de trames EAPOL non reconnues reçues sur ce port.

Length Error Frames Receive (Trames avec erreurs de longueur reçues) Nombre de trames EAPOL avec une longueur de paquet non valide reçues sur ce port.

Last Frame Version (Version de la dernière trame) Numéro de version du protocole rattaché à la dernière trame EAPOL reçue.

Last Frame Source (Source de la dernière trame) Adresse MAC source rattachée à la dernière trame EAPOL reçue.

Affichage des statistiques EAP pour un port

1. Ouvrez la page [EAP Statistics](#) (Statistiques EAP).
2. Sélectionnez une interface dans le champ **Interface**.

Les statistiques EAP de l'interface s'affichent.

Réinitialisation des statistiques EAP

1. Ouvrez la page [EAP Statistics](#) (Statistiques EAP).
2. Cliquez sur **Reset All Counters** (Réinitialiser tous les compteurs) pour réinitialiser le compteur.

Les statistiques EAP sont réinitialisées.

Affichage des statistiques EAP à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage des statistiques EAP.

Tableau 8-83. Commandes CLI des statistiques EAP

Commande CLI	Description
<code>show dot1x statistics ethernet <i>interface</i></code>	Affiche les statistiques 802.1X pour l'interface spécifiée.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Switch# show dot1x statistics ethernet g1

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 (RMON) est composée de liaisons permettant d'afficher à distance des informations relatives au réseau. Pour ouvrir la page **RMON**, cliquez sur **Statistics/RMON** (Statistiques/RMON) → **RMON** dans l'arborescence.

Affichage de groupes de statistiques RMON

La page [RMON Statistics](#) (Statistiques RMON) contient des champs permettant d'obtenir des informations sur l'utilisation du périphérique et sur les erreurs survenues sur le périphérique. Pour ouvrir la page [RMON Statistics](#) (Statistiques RMON), cliquez sur **Statistics/RMON** (Statistiques/RMON) → **RMON** → **Statistics** (Statistiques) dans l'arborescence.

Figure 8-121. Statistiques RMON

RMON Statistics	
Interface	10.0.20.140
Refresh Rate	10 Seconds
Drop Events	0
Received Bytes (Octets)	27751
Received Packets	1318
Broadcast Packets Received	65
Multicast Packets Received	0
CRC/Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	11
Frames of 64 Bytes	1159
Frames of 65 to 127 Bytes	361
Frames of 128 to 255 Bytes	24
Frames of 256 to 511 Bytes	14
Frames of 512 to 1023 Bytes	230
Frames of 1024 to 1518 Bytes	0

Interface Indique le port ou le LAG pour lequel les statistiques sont affichées.

Refresh Rate (Taux d'actualisation) Délai qui s'écoule entre deux actualisations des statistiques.

Drop Events (Événements rejetés) Nombre d'événements qui ont été rejetés sur l'interface depuis la dernière actualisation.

Received Bytes (Octets reçus) Nombre d'octets reçus sur l'interface depuis la dernière actualisation du périphérique. Ce chiffre tient compte des paquets défectueux et des octets FCS mais exclut les bits de verrouillage de trame.

Received Packets (Paquets reçus) Nombre de paquets reçus sur l'interface depuis la dernière actualisation du périphérique, paquets défectueux et paquets multidiffusion et diffusion inclus.

Broadcast Packets Received (Paquets diffusion reçus) Nombre de paquets diffusion sans erreur reçus sur l'interface depuis la dernière actualisation du périphérique. Ce chiffre ne tient pas compte des paquets multidiffusion.

Multicast Packets Received (Paquets multidiffusion reçus) Nombre de paquets multidiffusion sans erreur reçus sur l'interface depuis la dernière actualisation du périphérique.

CRC & Align Errors (Erreurs de CRC et d'alignement) Nombre d'erreurs de CRC et d'alignement qui se sont produites sur l'interface depuis la dernière actualisation du périphérique.

Undersize Packets (Paquets de taille insuffisante) Nombre de paquets de taille insuffisante (moins de 64 octets) reçus sur l'interface depuis la dernière actualisation du périphérique.

Oversize Packets (Paquets de taille excessive) Nombre de paquets de taille excessive (plus de 1518 octets) reçus sur l'interface depuis la dernière actualisation du périphérique.

Fragments Nombre de fragments (paquets de moins de 64 octets, comprenant les octets FCS et excluant les bits de verrouillage de trame) reçus sur l'interface depuis la dernière actualisation du périphérique.

Jabbers (Jabotages) Nombre de jabotages (paquets de plus de 1518 octets de long) reçus sur l'interface depuis la dernière actualisation du périphérique.

Collisions Nombre de collisions reçues sur l'interface depuis la dernière actualisation du périphérique.

Frames of xx Bytes (Trames de xx octets) Nombre de trames de xx octets reçues sur l'interface depuis la dernière actualisation du périphérique.

Affichage des statistiques relatives aux interfaces

1. Ouvrez la page [RMON Statistics](#) (Statistiques RMON).
2. Sélectionnez un type et un numéro d'interface dans le champ **Interface**.

Les statistiques relatives à l'interface s'affichent.

Affichage des statistiques RMON à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage des statistiques RMON.

Tableau 8-84. Commandes CLI des statistiques RMON

Commande CLI	Description
<code>show rmon statistics {ethernet <i>interface</i> port-channel <i>numéro-canal-port</i>}</code>	Affiche les statistiques Ethernet RMON.

Vous trouverez ci-dessous un exemple de commande CLI :

```
console> enable
```

```
console> enable

Console# show rmon statistics ethernet g1

Port g1

Rejeté : 8

Octets : 878 128 Paquets : 978

Diffusion : 7 Multidiffusion : 1

Erreurs CRC et alignement : 0 Collisions : 0

Pqts de taille insuff : 0 Pqts de taille excessive : 0

Fragments : 0 Jabotages : 0

64 Octets : 98 65 à 127 Octets : 0
```

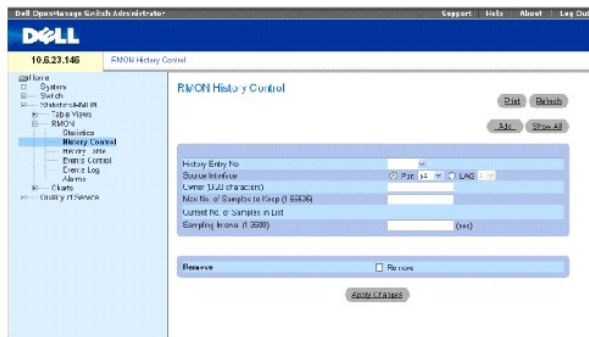
128 à 255 Octets : 0 256 à 511 Octets : 0

512 à 1 023 Octets : 491 1 024 à 1 518 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 des échantillons de données prélevés sur les ports. Par exemple, les échantillons peuvent être des définitions d'interface ou des périodes de scrutation. Pour ouvrir la page [RMON History Control](#) (Contrôle de l'historique RMON), cliquez sur **Statistics/RMON** (Statistiques/RMON) → **History Control** (Contrôle de l'historique) dans l'arborescence.

Figure 8-122. Contrôle de l'historique RMON



History Entry No. Numéro d'entrée de la page History Control Table (Table de contrôle de l'historique).

Source Interface (Interface source) Port ou LAG à partir duquel les échantillons d'historique ont été prélevés.

Owner (0-20 Characters) (Propriétaire [0 à 20 caractères]) Utilisateur ou station RMON qui a demandé les informations RMON.

Max No. of Samples to Keep (1-65535) (Nombre max. d'échantillons à conserver [1 à 65535]) Nombre d'échantillons à enregistrer. La valeur par défaut est 50.

Current No. of Samples in List (Nombre d'échantillons en cours dans la liste) Nombre d'échantillons existants.

Sampling Interval (1-3600) (Intervalle d'échantillonnage [1 à 65535]) Indique, en secondes, la fréquence à laquelle des échantillons sont prélevés 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. Ouvrez la page [RMON History Control](#) (Contrôle de l'historique RMON).
2. Cliquez sur **Ajouter**.

La page **Add History Entry** (Ajouter une entrée à l'historique) s'ouvre.

3. Renseignez les champs de la fenêtre.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est ajoutée à la **table de contrôle de l'historique**.

Modification d'une entrée dans la table de contrôle d'historique

1. Ouvrez la page [RMON History Control](#) (Contrôle de l'historique RMON).
2. Sélectionnez une entrée dans le champ **History Entry No.** (Numéro d'entrée d'historique).
3. Modifiez les champs comme vous le désirez.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée de la table est modifiée et le périphérique est mis à jour.

Suppression d'une entrée de la table de contrôle d'historique

1. Ouvrez la page [RMON History Control](#) (Contrôle de l'historique RMON).
2. Sélectionnez une entrée dans le champ **History Entry No.** (Numéro d'entrée d'historique).
3. Cliquez sur **Remove** (Retirer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée de la table sélectionnée est supprimée et le périphérique est mis à jour.

Affichage de l'historique RMON à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage des statistiques GVRP.

Tableau 8-85. Commandes CLI de l'historique RMON

Commande CLI	Description
<code>rmon collection history</code> <i>index</i> [<i>owner nom-propiétaire</i> <i>buckets numéro-groupe de blocs</i>] [<i>interval secondes</i>]	Active et définit la surveillance RMON sur une interface.
<code>show rmon collection history</code> [<i>ethernet interface</i> <i>port-channel numéro-canal-port</i>]	Affiche les statistiques de l'historique RMON.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface ethernet g8

Console (config-if)# rmon collection history 1 interval 2400

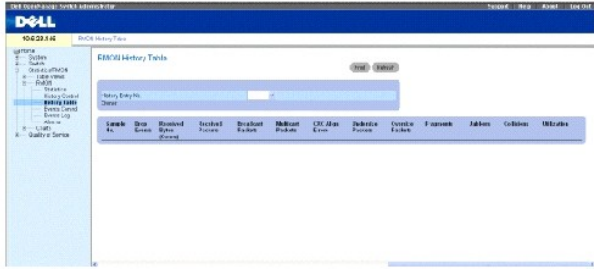
Console (config-if)# exit

Console (config)# exit
```

Affichage de la table d'historique RMON

La page [RMON History Table](#) (Table d'historique RMON) contient des échantillons de statistiques réseau spécifiques à l'interface. Chaque entrée de la table représente toutes les valeurs des compteurs compilés 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 8-123. Table d'historique RMON



Sample No. (N° d'échantillon) Échantillon auquel se rapportent les informations affichées dans la table.

Drop Events (Événements rejetés) 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 reçus) Nombre d'octets de données, paquets défectueux inclus, reçus sur le réseau.

Received Packets (Paquets reçus) Nombre de paquets reçus durant l'intervalle d'échantillonnage.

Broadcast Packets (Paquets diffusion) Nombre de paquets diffusion corrects reçus durant l'intervalle d'échantillonnage.

Multicast Packets (Paquets multidiffusion) Nombre de paquets multidiffusion corrects reçus durant l'intervalle d'échantillonnage.

CRC Align Errors (Erreurs d'alignement CRC) Nombre de paquets de 64 à 1518 octets reçus durant la session d'échantillonnage possédant une séquence de contrôle de trame (FCS) erronée et un nombre entier d'octets ou une séquence FCS erronée et un nombre non entier d'octets.

Undersize Packets (Paquets de taille insuffisante) Nombre de paquets de taille inférieure à 64 octets reçus pendant la session d'échantillonnage.

Oversize Packets (Paquets de taille excessive) Nombre de paquets de taille supérieure à 1518 octets reçus pendant la session d'échantillonnage.

Fragments Nombre de paquets de taille inférieure à 64 octets et possédant un FCS reçus pendant la session d'échantillonnage.

Jabbers (Jabotages) Nombre de paquets de taille supérieure à 1518 octets et possédant un FCS 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 deux ou 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 avec deux chiffres après la virgule.

Affichage des statistiques relatives à une entrée spécifique de l'historique

1. Ouvrez la page [RMON History Table](#) (Table d'historique RMON).
2. Sélectionnez une entrée dans le champ **History Table No.**.

Les statistiques relatives à l'entrée s'affichent dans la table d'historique RMON.

Affichage de l'historique RMON à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage de l'historique RMON.

Tableau 8-86. Commandes CLI de contrôle de l'historique RMON

Commande CLI	Description
<code>show rmon history index { throughput errors other } [period secondes]</code>	Affiche l'historique des statistiques Ethernet RMON.

Voici un exemple de commandes CLI permettant d'afficher des statistiques Ethernet RMON pour le débit à l'index 1 :

```

console> enable

Console# show rmon history 1 throughput

```

Échantillons : 1		Propriétaire : CLI			
Interface : gl		Intervalle : 1800			
Échantillons demandés : 50		Échantillons accordés : 50			
Taille max. de la table : 500					
Date et heure	Octets	Paquets	Diffusion	Multidiffusion	%
-----	-----	-----	-----	-----	-----
18 jan 2004 21:57:00	303595962	357568	3289	7287	19,98 %
18 jan 2004 21:57:30	287696304	275686	2789	2789	20,17 %

Définition d'événements RMON sur le périphérique

La page [RMON Events Control](#) (Contrôle des événements RMON) contient des champs permettant 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 8-124. Contrôle des événements RMON



Event Entry (Entrée événement) Identifie l'événement.

Community (Communauté) Communauté à laquelle l'événement appartient.

Description Description de l'événement définie par l'utilisateur.

Type Précise le type de l'événement. Ce champ peut prendre les valeurs suivantes :

Log (Journal) L'événement est une entrée de journal.

Trap (Interruption) L'événement est une interruption.

Log and Trap (Journal et Interruption) L'événement est à la fois une entrée de journal et une interruption.

None (Aucun) Il n'y a pas d'événement.

Time (Heure) Indique l'heure à laquelle l'événement est survenu. Par exemple, le 29 mars 2004 à 11h00 du matin s'affichera sous la forme 29/03/2004 11:00:00.

Owner (Propriétaire) Périphérique ou utilisateur qui a défini l'événement.

Remove (Supprimer) Supprime l'événement de la table des événements RMON.

Ajout d'un événement RMON

1. Ouvrez la page [RMON Events Control](#) (Contrôle des événements RMON) .
2. Cliquez sur **Ajouter**.

La page **Add an Event Entry** (Ajouter une entrée d'événement) s'ouvre.

3. Renseignez les informations de la fenêtre de dialogue et cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée de la **table des événements** est ajoutée et le périphérique est mis à jour.

Modification d'un événement RMON

1. Ouvrez la page [RMON Events Control](#) (Contrôle des événements RMON).
2. Sélectionnez une entrée dans la **table des événements**.
3. Modifiez les champs de la fenêtre de dialogue et cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée de la **table des événements** est modifiée et le périphérique est mis à jour.


Suppression d'entrées d'événements RMON

1. Ouvrez la page [RMON Events Control](#) (Contrôle des événements RMON).
2. Cliquez sur **Show All** (Afficher tout).

La page **Events Table** (Table des événements) s'ouvre.

3. Sélectionnez **Remove** (Supprimer) pour le/les événement(s) à supprimer, puis cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée de la table sélectionnée est supprimée et le périphérique est mis à jour.

 **REMARQUE** : Il est possible de supprimer une seule entrée d'événement de la page **RMON Events Control** (Contrôle des événements RMON) en cochant la case **Remove** (Supprimer) de cette page.

Définition des événements du périphérique à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des événements du périphérique.

Tableau 8-87. Commandes CLI de définition des événements du périphérique

Commande CLI	Description
<code>rmon event type d'index [community texte] [description texte] [owner nom]</code>	Configure des événements RMON.
<code>show rmon events</code>	Affiche la table des événements RMON.

Vous trouverez ci-dessous un exemple de commande CLI :

```

console> enable

console# config

console (config)# rmon event 1 log

console(config)# exit

Console# show rmon events

```

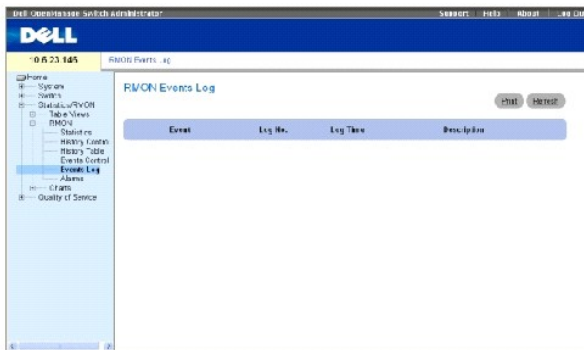
Index	Description	Type	Communauté	Propriétaire	Dernier envoi
-----	-----	-----	-----	-----	-----
1	Erreurs	Journal		CLI	18 jan 2002 23:58:17

2	Diffusion importante	Journal- Interruption	routeur	Gestionnaire	18 jan 2002 23:59:48
---	----------------------	-----------------------	---------	--------------	-------------------------

Affichage du journal des événements RMON

La page [RMON Events Log](#) (Journal des événements RMON) dresse la liste des événements RMON. Pour ouvrir la page [RMON Events Log](#) (Journal des événements RMON), cliquez sur [Statistics/RMON](#) (Statistiques/RMON) → [RMON](#) → [Events](#) (Événements) dans l'arborescence.

Figure 8-125. Journal des événements RMON



Event (Événement) Numéro de l'entrée dans le journal des événements RMON.

Log No. Numéro du journal.

Log Time (Heure du journal) Heure à laquelle l'entrée a été créée dans le journal.

Description Décrit l'entrée de journal.

Définition des événements du périphérique à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des événements du périphérique.

Tableau 8-88. Commandes CLI de définition des événements du périphérique

Commande CLI	Description
<code>show rmon log [événement]</code>	Affiche la table de journalisation RMON.

Vous trouverez ci-dessous un exemple de commande CLI :

```
console> enable

console# config
```

```

console (config)# rmon event 1 log

console(config)# exit

Console# show rmon log

```

Taille max. de la table : 500		
Événement	Description	Date et heure
-----	-----	-----
1	Erreurs	18 jan 2002 23:48:19
1	Erreurs	18 jan 2002 23:58:17
2	Diffusion importante	18 jan 2002 23:59:48

```

Console# show rmon log

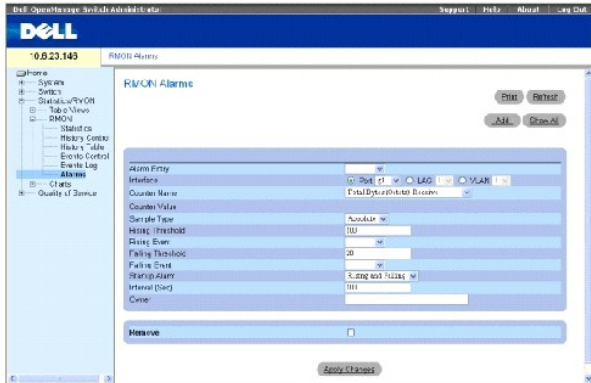
```

Taille max. de la table : 500 (800 après réinitialisation)		
Événement	Description	Date et heure
-----	-----	-----
1	Erreurs	18 jan 2002 23:48:19
1	Erreurs	18 jan 2002 23:58:17
2	Diffusion importante	18 jan 2002 23:59:48

Définition d'alarmes RMON sur le périphérique

La page [RMON Alarms](#) (Alarmes RMON) contient des champs permettant de configurer des alarmes réseau. Ces alarmes sont émises en cas de détection d'un problème ou d'un événement sur le réseau. La hausse et la baisse des seuils génèrent des événements. Pour ouvrir la page [RMON Alarms](#) (Alarmes RMON), cliquez sur **Statistics/RMON** (Statistiques/RMON) → **RMON** → **Alarms** (Alarmes) dans l'arborescence.

Figure 8-126. Alarmes RMON



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) Valeur de la variable MIB sélectionnée.

Sample Type (Type d'échantillon) Indique la méthode d'échantillonnage utilisée pour la variable sélectionnée et compare la valeur par rapport aux seuils. Ce champ peut prendre les valeurs suivantes :

Delta (Différence) Retire la valeur du dernier échantillon de la valeur en cours. La différence obtenue est comparée au seuil.

Absolute (Absolue) Compare directement les valeurs aux seuils au terme de l'intervalle d'échantillonnage.

Rising Threshold (Seuil en hausse) Hausse de valeur du compteur qui déclenche l'alarme de seuil en hausse. Le seuil en hausse est représenté dans la partie supérieure des histogrammes. Une couleur spécifique est associée à chaque variable contrôlée.

Rising /Falling Event (Événement hausse/baisse) Mécanisme qui reporte les alarmes LOG, TRAP ou les deux. Lorsque l'option LOG est sélectionnée, aucun mécanisme d'enregistrement n'est activé sur le périphérique ni dans le système de gestion. Toutefois, si le périphérique n'est pas réinitialisé, il est conservé dans la table LOG du périphérique. Si l'option TRAP est sélectionnée, une interruption est générée via SNMP et reportée par l'intermédiaire du mécanisme général des interruptions. L'interruption peut être enregistrée à l'aide de ce même mécanisme.

Falling Threshold (Seuil en baisse) Baisse de valeur du compteur qui déclenche l'alarme de seuil en baisse. Le seuil en baisse est représenté sous forme graphique dans la partie inférieure des histogrammes. Une couleur spécifique est associée à chaque variable contrôlée.

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 (Sec) (Intervalle [s]) Intervalle qui sépare deux alarmes.

Owner (Propriétaire) Périphérique ou utilisateur qui a défini l'alarme.

Remove (Supprimer) Supprime une alarme RMON.

Ajout d'une entrée dans la table des alarmes

1. Ouvrez la page [RMON Alarms](#) (Alarmes RMON).
2. Cliquez sur **Ajouter**.

La page **Add an Alarm Entry** (Ajouter une entrée d'alarme) s'ouvre :

Figure 8-127. Page **Ajouter une entrée d'alarme**

Alarm Entry	1
Interface	Port 1
Counter Name	Total Bytes (C)ets Received
Sample Type	Absolute
Rising Threshold	100
Rising Event	
Falling Threshold	20
Falling Event	
Startup Alarm	Rising and Falling
Interval	100
Overcr	

3. Sélectionnez une interface.
4. Renseignez les champs de la fenêtre.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'alarme RMON est ajoutée et le périphérique est mis à jour.

Modification d'une entrée de la table des alarmes

1. Ouvrez la page [RMON Alarms](#) (Alarmes RMON).
2. Sélectionnez une entrée dans le menu déroulant **Alarm Entry** (Entrée d'alarme).
3. Modifiez les champs comme vous le désirez.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Affichage de la table des alarmes

1. Ouvrez la page [RMON Alarms](#) (Alarmes RMON).
2. Cliquez sur **Show All** (Afficher tout).

La page **Alarms Table** (Table des alarmes) s'ouvre.

Suppression d'une entrée de la table des alarmes

1. Ouvrez 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 sélectionnée est supprimée et le périphérique est mis à jour.

Définition des alarmes du périphérique à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des alarmes du périphérique.

Tableau 8-89. Commandes CLI des alarmes du périphérique

Commande CLI	Description
<code>rmon alarm index variable interval rthreshold fthreshold revent fevent [type type] [startup direction] [owner nom]</code>	Configure des conditions d'alarme RMON.
<code>show rmon alarm-table</code>	Affiche un résumé de la table des alarmes.
<code>show rmon alarm</code>	Affiche la configuration des alarmes RMON.

Vous trouverez ci-dessous un exemple de commande CLI :

```

console> enable

console# config

Console (config)# rmon alarm 1000 dell 360000 1000000 1000000 10 20

Console# show rmon alarm-table

```

Index	OID	Propriétaire
-----	-----	-----
1	1.3.6.1.2.1.2.2.1.1 0.1	CLI
2	1.3.6.1.2.1.2.2.1.1 0.1	Gestionnaire
3	1.3.6.1.2.1.2.2.1.1 0.9	CLI

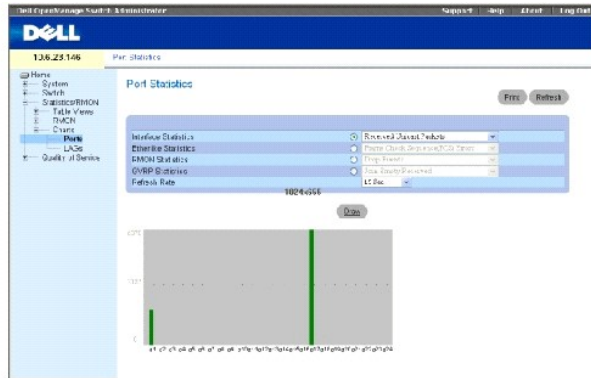
Affichage des graphiques

La page **Charts** (Graphiques) contient des liens qui permettent d'afficher les statistiques sous forme graphique. Pour ouvrir la page, cliquez sur **Statistics** (Statistiques) → **Charts** (Graphiques) dans l'arborescence.

Affichage des statistiques relatives aux ports

La page **Port Statistics** (Statistiques sur les ports) contient des champs permettant d'ouvrir des statistiques sous forme graphique pour des éléments de port. Pour ouvrir la page **Port Statistics** (Statistiques sur les ports), cliquez sur **Statistics** (Statistiques) → **Charts** (Graphiques) → **Ports** dans l'arborescence.

Figure 8-128. Statistiques sur les ports



Interface Statistics (Statistiques d'interface) Sélectionne le type de statistiques d'interface à ouvrir.

Etherlike Statistics (Statistiques Etherlike) Sélectionne le type de statistiques Etherlike à ouvrir.

RMON Statistics (Statistiques RMON) Sélectionne le type de statistiques RMON à ouvrir.

GVRP Statistics (Statistiques GVRP) Sélectionne le type de statistiques GVRP à ouvrir.

Refresh Rate (Taux d'actualisation) Délai qui s'écoule entre deux actualisations des statistiques.

Affichage des statistiques relatives aux ports

1. Ouvrez la page [Port Statistics](#) (Statistiques sur les ports).
2. Sélectionnez la catégorie de statistique à ouvrir.
3. Sélectionnez un taux d'actualisation dans le menu **Refresh Rate** (Taux d'actualisation).
4. Cliquez sur **Draw** (Dessiner).

Le graphique des statistiques sélectionnées s'affiche.

Affichage des statistiques relatives aux ports à l'aide des commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage des statistiques des ports.

Tableau 8-90. Commandes CLI des statistiques relatives aux ports

Commande CLI	Description
<code>show interfaces counters [ethernet interface port-channel numéro-canal-port]</code>	Affiche le trafic enregistré par l'interface physique.
<code>show rmon statistics { ethernet interface port-channel numéro-canal-port }</code>	Affiche les statistiques Ethernet RMON.
<code>show gvrp statistics { ethernet interface port-channel numéro-canal-port }</code>	Affiche les statistiques du protocole GVRP.
<code>show gvrp error-statistics { ethernet interface port-channel numéro-canal-port }</code>	Affiche les statistiques des erreurs du protocole GVRP.

```
Console# show interfaces description ethernet g1
```

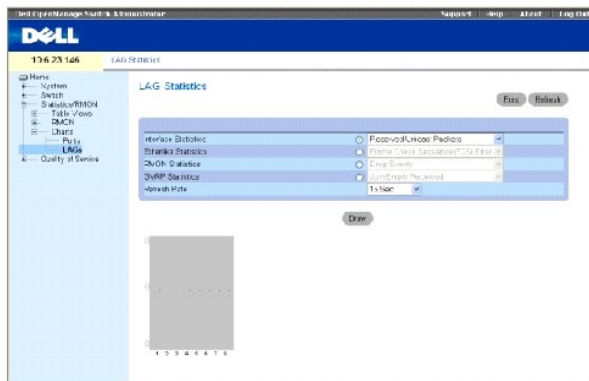
Port	Description
---	-----

g1	Management_port
g2	R&D_port
g3	Finance_port
Canal	Description
----	-----
1	Output

Affichage des statistiques relatives aux LAG

La page [LAG Statistics](#) (Statistiques sur les LAG) contient des champs permettant d'ouvrir des statistiques sous forme graphique pour des LAG. Pour ouvrir la page [LAG Statistics](#) (Statistiques LAG), cliquez sur **Statistics** (Statistiques) → **Charts** (Graphiques) → **LAG** dans l'arborescence.

Figure 8-129. Statistiques sur les LAG



Interface Statistics (Statistiques d'interface) Sélectionne le type de statistiques d'interface à ouvrir.

Etherlike Statistics (Statistiques Etherlike) Sélectionne le type de statistiques Etherlike à ouvrir.

RMON Statistics (Statistiques RMON) Sélectionne le type de statistiques RMON à ouvrir.

GVRP Statistics (Statistiques GVRP) Sélectionne le type de statistiques GVRP à ouvrir.

Refresh Rate (Taux d'actualisation) Délai qui s'écoule entre deux actualisations des statistiques.

Affichage des statistiques relatives aux LAG

- Ouvrez la page [LAG Statistics](#) (Statistiques sur les LAG).

g4	0	0	0	0	0	0	0	0	0	0	0	0	0
g5	0	0	0	0	0	0	0	0	0	0	0	0	0
g6	0	0	0	0	0	0	0	0	0	0	0	0	0
g7	0	0	0	0	0	0	0	0	0	0	0	0	0
g8	0	0	0	0	0	0	0	0	0	0	0	0	0

[Retour à la page du sommaire](#)