Guide d'utilisation

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.

Janvier 2005

Retour à la page du sommaire

Informations sur les câbles, les ports et le brochage

Systèmes Dell™ PowerConnect™ 6024/6024F

Cette section décrit les interfaces physiques du commutateur et fournit des informations sur les raccordements par câbles.

Les stations sont connectées aux ports du commutateur via les ports de l'interface physique situés sur le panneau avant. Le mode approprié (Semi-duplex/Duplex intégral, Auto) est défini pour chaque station.

Connexion des broches de l'interface Ethernet 10/100/1000

Le port de commutation peut être connecté à des stations câblées en mode station Ethernet RJ-45 standard à l'aide de câbles droits. Les périphériques de transmission reliés entre eux utilisent des câbles croisés.

La Figure 3-1 illustre les broches RJ-45 et le Tableau 3-1 indique les affections des broches RJ-45.

Figure 3-1. Connecteur RJ-45

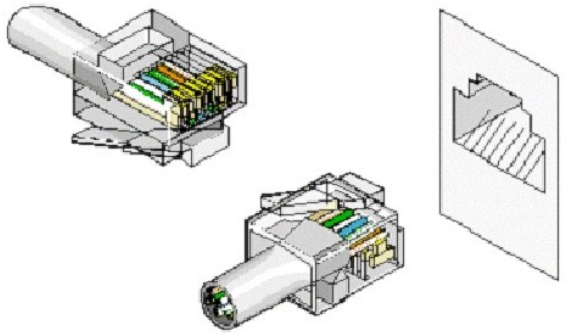


Tableau 3-1. Connexion des broches RJ-45 pour 10/100/1000 Base T

Broche	Utiliser
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+
4	TxRx 2-
5	TxRx 3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

Connexion des broches des interfaces SFP

La Figure 3-2 illustre un connecteur SFP et le Tableau 3-2 indique les affectations des broches d'un connecteur SFP optionnel.

Figure 3-2. Connecteur SFP

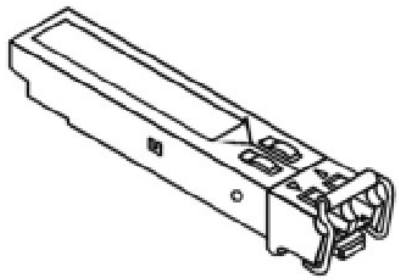


Tableau 3-2. Connexion des broches SFP

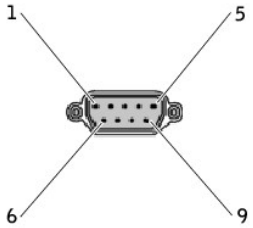
Broche	Utiliser
1	Terre émetteur - transmetteur (idem terre récepteur)
2	Défaillance émetteur - transmetteur
3	Désactivation émetteur - transmetteur ; sortie laser désactivée sur haut ou ouvert.
4	Définition de module 2 ; ligne de données pour ID série.
5	Définition de module 1 ; ligne d'horloge pour ID série.
6	Définition de module 0 ; mis à la terre à l'intérieur du module
7	Sélection du débit ; aucune connexion requise.
8	Perte de l'indication du signal ; la logique 0 indique un fonctionnement normal.
9	Terre récepteur (idem terre émetteur - transmetteur)
10	Terre récepteur (idem terre émetteur - transmetteur)
11	Terre récepteur (idem terre émetteur - transmetteur)
12	Données inversées en sortie récepteur ; CA couplé.
13	Données non inversées en sortie récepteur ; CA couplé.
14	Terre récepteur (idem terre émetteur - transmetteur)
15	Bloc d'alimentation récepteur
16	Bloc d'alimentation émetteur - transmetteur
17	Terre émetteur - transmetteur (idem terre récepteur)
18	Données non inversées en entrée émetteur - transmetteur
19	Données inversées en entrée émetteur - transmetteur
20	Terre émetteur - transmetteur (idem terre récepteur)

Connexion des câbles série

Vous pouvez utiliser des câbles série (simulateur de modem) pour relier le commutateur à un terminal lors de l'installation et de la configuration initiales (vous pouvez également utiliser un PC exécutant un logiciel d'émulation de terminal). Le câble série du commutateur est un câble de jonction DB-9 avec connecteurs femelle-femelle (reportez-vous à la Figure 3-3).

La Figure 3-3 illustre un câble série et le Tableau 3-3 indique les affectations des broches du connecteur série.

Figure 3-3. Connecteur série



Le Tableau 3-3 indique les affectations des broches du câble série.

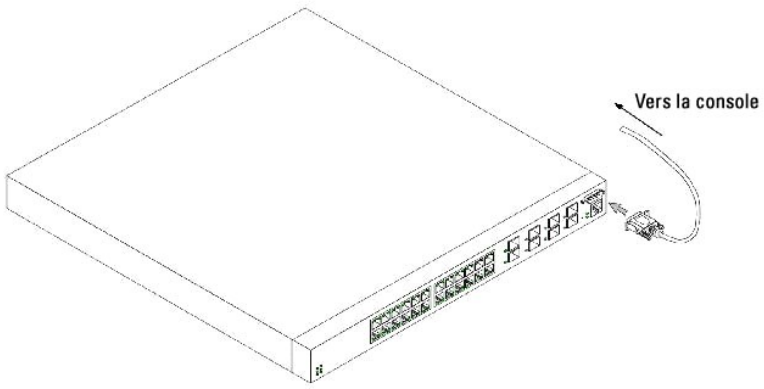
Tableau 3-3. Affectations des broches du connecteur série

Signal	Broche	Signal du port de la Console de gestion
Inutilisé	1	Inutilisé
TXD	2	TXD
RXD	3	RXD
Inutilisé	4	RXD
GND	5	GND
Inutilisé	6	Inutilisé
CTS	7	CTS
RTS	8	RTS
Inutilisé	9	Inutilisé

Connexion du commutateur à un terminal

1. Reliez le câble simulateur de modem (série) au connecteur ASCII DTE RS-232 du terminal (Console).
2. Reliez le câble d'interface au connecteur série du commutateur (reportez-vous à la Figure 3-4).

Figure 3-4. Connexion série au commutateur



Connexion secteur

1. Connectez un câble électrique de 5 pieds (1,5 m) avec raccordement à la terre à la prise secteur CA située sur le panneau arrière (reportez-vous à la Figure 3-5).
2. Connectez le câble d'alimentation à une prise de courant CA mise à la terre.

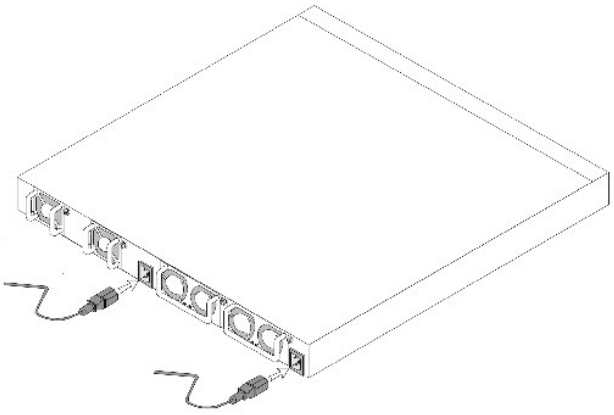
REMARQUE : Nous recommandons de connecter le deuxième bloc d'alimentation à une source d'alimentation électrique distincte.

3. Assurez-vous que l'appareil est connecté et fonctionne correctement en examinant les DEL des panneaux avant et arrière.

   Pour plus d'informations sur les DEL, reportez-vous à la section «Description du matériel».

4. Répétez la procédure pour le deuxième bloc d'alimentation.

Figure 3-5. Connexion secteur au commutateur



Retour à la page du sommaire

Retour à la page du sommaire

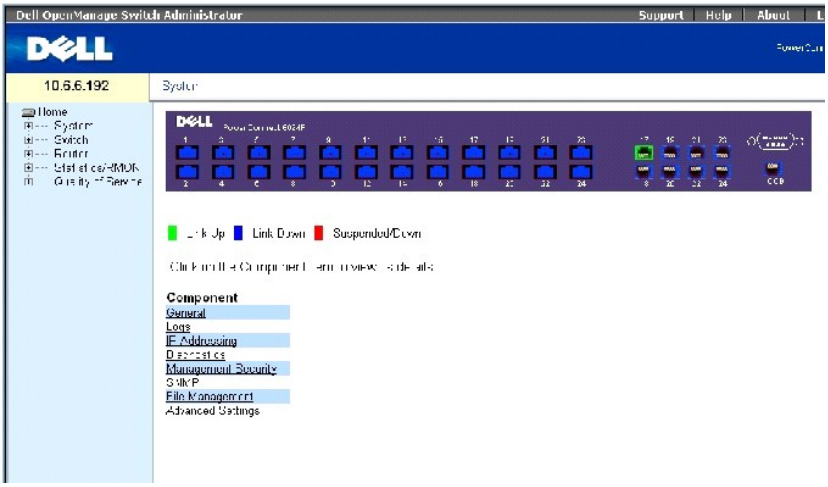
Configuration des informations système

Systèmes Dell PowerConnect 6024/6024F

Ouverture de la page System (Système)

Pour ouvrir la page **System** (Système), cliquez sur **System** (Système) dans l'arborescence (reportez-vous à la Figure 6-1).

Figure 6-1. Système



Définition des informations générales relatives au périphérique

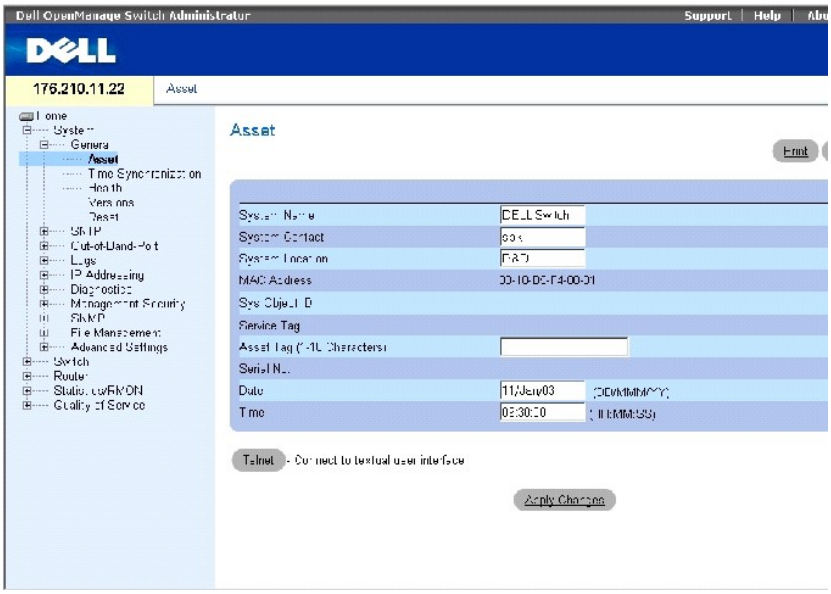
La page **General** (Général) contient des liens vers des pages qui permettent aux gestionnaires de réseau de configurer les paramètres du périphérique.

Configuration des informations relatives au périphérique

La page **Asset** (Inventaire) contient des paramètres permettant de configurer et de visualiser les informations générales relatives au périphérique : nom, emplacement et contact système, adresse MAC du système pour le commutateur et le port de gestion hors bande, ID objet du système, date, heure et durée de fonctionnement du système.

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

Figure 6-2. Inventaire



La page **Asset** (Inventaire) contient les champs suivants :

System Name (Nom système) Nom système affecté au périphérique par l'utilisateur.

System Contact (Contact système) Nom de la personne qui fait office de contact.

System Location (Emplacement système) Emplacement de l'exécution du système.

MAC Address (Adresse MAC) Adresse MAC du commutateur.

Sys Object ID (ID objet système) OID de la base de données MIB.

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

Asset Tag (Numéro d'inventaire) Référence affectée au périphérique par l'utilisateur. Les valeurs possibles pour ce paramètre sont comprises entre 1 et 16.

Serial No. (Numéro de série) Numéro de série du périphérique.

Date (DD/MMM/YY) (Date (JJ/MMM/AA)) Date du jour du système au format jour, mois, année. Exemple : 11/Jan/02 correspond au 11 janvier 2002.

Time (HH/MM/SS) (Heure (HH/MM/SS)) Heure du système au format heures, minutes, secondes. Exemple : 20:12:03 correspond à 20 heures, 12 minutes, 03 secondes.

Définition des informations système

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

Les paramètres du système sont appliqués et le périphérique est mis à jour.

Ouverture d'une session Telnet

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

REMARQUE : Les paramètres Telnet appropriés sont définis avant l'ouverture d'une session Telnet. Pour en savoir plus, reportez-vous à la section «Configuration d'un mot de passe Telnet initial».

2. Cliquez sur **Telnet**.

Configuration des informations relatives au périphérique à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage des champs de la page **Asset** (Inventaire).

Tableau 6-1. Commandes CLI Inventaire

Commande CLI	Description
`hostname name`	Définit ou modifie le nom d'hôte du périphérique.
`snmp-server contact` `text`	Définit un contact pour le système.
`snmp-server location` `text`	Précise l'emplacement du périphérique.
`show clock`	Affiche la date et l'heure de l'horloge système.
`asset-tag` `tag`	Définit le numéro d'inventaire du périphérique.
`show system-id`	Affiche les informations d'identification du système, notamment le numéro de service, le numéro d'inventaire et le numéro de série.
`show system`	Affiche les informations système.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# hostname dell

Console (config)# snmp-server contact Dell_Tech_Supp

Console (config)# snmp-server location New_Yorks

Console (config)# exit
```

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


Console# show clock


15:29:03 Jun 17 2002
```

Définition des paramètres d'heure du système

La page **Time Synchronization** (Synchronisation de l'heure) contient des champs permettant de synchroniser l'heure du système sur l'horloge matérielle locale ou une horloge SNTP externe.

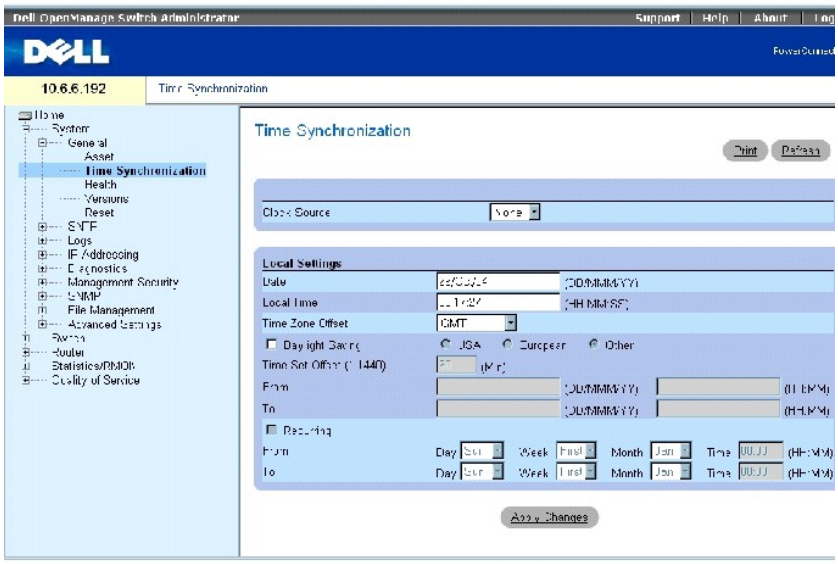
Si l'horloge du système est synchronisée sur une horloge SNTP externe et que cette horloge tombe en panne, la source de l'horloge système bascule automatiquement sur l'horloge matérielle locale.

L'horloge système peut être configurée pour basculer automatiquement sur l'heure d'été.

Pour plus d'informations sur le SNTP, reportez-vous à la section **Configuration des paramètres SNTP**.

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

Figure 6-3. Synchronisation de l'heure



La page **Time Synchronization** (Synchronisation de l'heure) contient les champs suivants :

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

None (Aucune) Indique que l'heure du système est synchronisée sur l'horloge matérielle locale.

SNTP Indique que l'heure du système est synchronisée sur l'horloge d'un serveur SNTP. Pour plus d'informations, reportez-vous à la section «**Configuration des paramètres du SNTP**».

Date Définit la date du système. Le format de ce champ est JJ:MMM:AA.

Local Time (Heure locale) Définit l'heure du système. Le format de ce champ est HH:MM:SS.

Time Zone Offset (Décalage fuseau horaire) Définit, en heures, la différence entre l'heure GMT (Greenwich Mean Time - heure du méridien de Greenwich) et l'heure locale.

L'horloge système peut être programmée pour basculer automatiquement sur l'heure d'été à une date spécifique suivant l'année ou à la même date chaque année. Pour paramétrer une date spécifique suivant l'année, utilisez les paramètres de la zone Daylight Savings (Heure d'été). Pour paramétrer la même date chaque année, utilisez les paramètres de la zone Recurring (Date périodique).

Daylight Savings (Heure d'été) Cochez cette case pour activer l'heure d'été sur le périphérique en fonction de sa localisation géographique. Ce champ peut prendre les valeurs suivantes :

USA (États-Unis) L'horloge du périphérique passe sur l'heure d'été à 2h du matin, le premier dimanche d'avril et revient à l'heure normal à 2h du matin le dernier dimanche d'octobre.

European (Europe) L'horloge du périphérique passe sur l'heure d'été à 1h du matin le dernier dimanche de mars et revient à l'heure normale à 1h du matin le dernier dimanche d'octobre. Cette option concerne les membres de l'Union Européenne et les autres pays européens qui observent la norme de l'UE.

Other (Autre) L'horloge du périphérique passe sur l'heure d'été selon une plage horaire définie par l'utilisateur.

Time Set Offset (1-1440) (Décalage horaire [1-1440]) Pour les pays autres que les États-Unis et l'Europe, la différence entre l'heure normale et l'heure d'été peut être définie en minutes. La valeur par défaut est 60 minutes.

From/To (Du/Au) Définit la date et l'heure auxquelles l'heure d'été commence et se termine pour les pays autres que les États-Unis et l'Europe. Le format de la date est JJ/MMM/AA et le format de l'heure est HH:MM.

Recurring (Date périodique) Cochez cette case pour activer l'heure d'été sur le périphérique en fonction d'un bloc de temps récurrent. Ce champ peut prendre les valeurs suivantes :

From/To (Du/Au) Définit le jour, la semaine, le mois et l'heure à partir desquels l'heure d'été commence et auxquels elle se termine. Le format de l'heure est HH:MM.

Sélection d'une source de l'horloge

1. Ouvrez la page **Time Synchronization** (Synchronisation de l'heure).
2. Renseignez 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. Renseignez les champs de la zone **Local Settings** (Paramètres locaux).

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

Les paramètres de l'horloge locale sont appliqués et le périphérique est mis à jour.

Définition des paramètres d'heure d'été

1. Ouvrez la page **Time Synchronization** (Synchronisation de l'heure).
2. Renseignez les champs de la zone **Daylight Saving** (Heure d'été) ou **Reccuring** (Date périodique).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres d'heure d'été sont appliqués et le périphérique est mis à jour.

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 6-2. Commandes CLI Synchronisation de l'heure

Commande CLI	Description
`clock source {sntp}`	Synchronise l'heure du système sur l'horloge d'un serveur SNTP.
`no clock source`	Synchronise l'heure du système sur l'horloge du périphérique.
`clock timezone hours- offset [minutes minutes- offset] [zone acronym]`	Configure la zone horaire à des fins d'affichage.
`no clock timezone`	Configure l'heure sur l'heure universelle coordonnée (UTC).
`clock summer-time recurring {usa | eu | {week day month hh:mm week day month hh:mm}} [offset offset] [zone acronym]`	Configure le système pour qu'il bascule automatiquement sur l'heure d'été (DST) conformément aux normes américaines ou européennes ou en fonction d'un bloc de temps récurrent défini par l'utilisateur.
`clock summer-time date date month year hh:mm date month year hh:mm [offset offset] [zone acronym]`	Configure le système pour qu'il bascule automatiquement sur l'heure d'été (DST) pendant une période définie par l'utilisateur.
`no clock summer-time`	Configure le système pour qu'il ne passe pas sur l'heure d'été (DST).
`show clock`	Affiche la date et l'heure de l'horloge système.
`show clock [detail]`	Affiche la date et l'heure de l'horloge système, le fuseau horaire et la configuration de l'heure d'été (DST).

Vous trouverez ci-dessous un exemple de commande CLI :

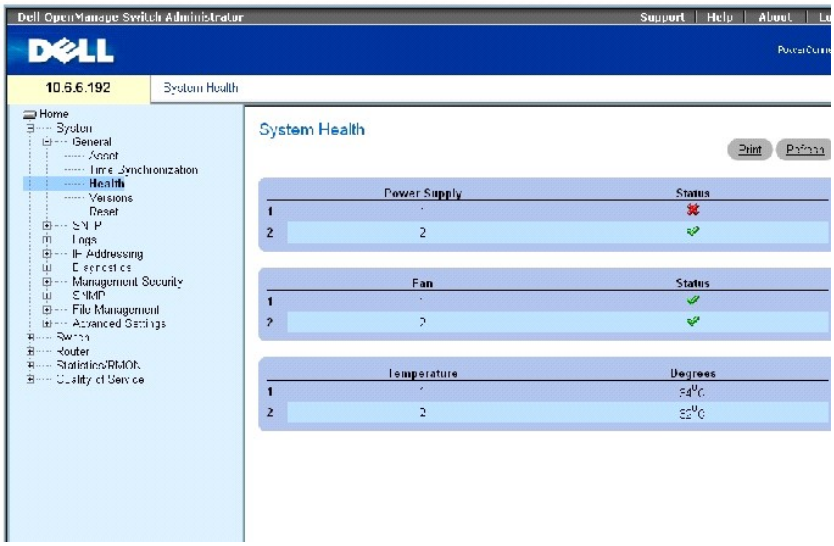
```
Console (config)# clock timezone -6 zone CST
```

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

Configuration des informations sur l'intégrité du système

La page **System Health** (Intégrité du système) affiche des informations sur le périphérique physique, notamment des informations sur les sources d'alimentation et de ventilation du commutateur. Pour afficher la page **System Health** (Intégrité du système), cliquez sur **System** (Système)→ **General** (Général)→ **Health** (Intégrité) dans l'*arborescence*.

Figure 6-4. Intégrité du système



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

Power Supply (Bloc d'alimentation) État du bloc d'alimentation.

Le bloc d'alimentation fonctionne correctement.

Le bloc d'alimentation ne fonctionne pas correctement.

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

Fan (Ventilateur) Indique l'état du ventilateur. Le PowerConnect 6024/6024F est doté de deux ventilateurs.

Le ventilateur fonctionne correctement.

Le ventilateur ne fonctionne pas correctement.

Not Present (Absent) Un ventilateur est absent.

Temperature (Température) Température de fonctionnement actuelle du périphérique.

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).

Tableau 6-3. Commandes CLI Intégrité du système

Commande CLI	Description
show system	Affiche les informations système.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# show system
```

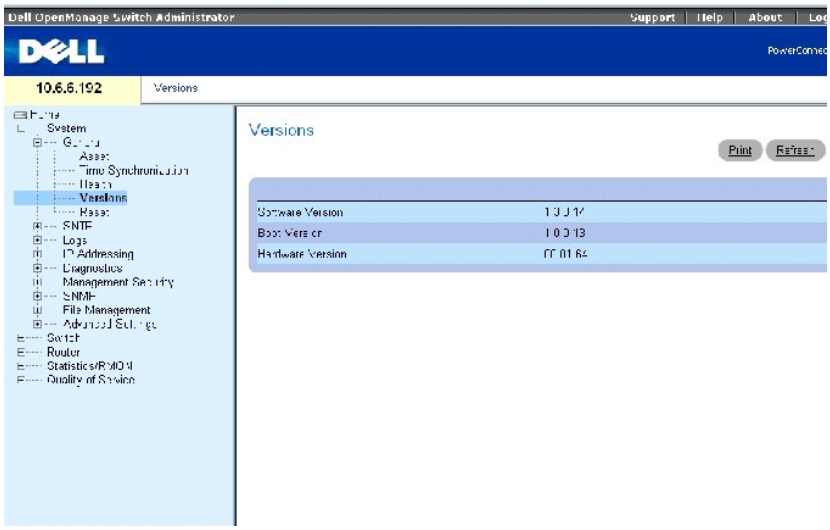
System Description: (Description du système :)	Ethernet Routing Switch (Commutateur de routage Ethernet)
System Up Time (days,hour:min:sec): (Durée de fonctionnement du système (jours,heures:mn:s) :)	0,00:32:04
System Contact: (Contact système :)	
System Name: (Nom système :)	
System Location: (Emplacement système :)	
System MAC Address: (Adresse MAC système :)	00:0d:56:2f:45:30
OOB MAC Address: (Adresse MAC OOB :)	00:00:00:00:00:18
System Object ID: (ID objet système :)	1.3.6.1.4.1.674.10895.3000
Type :	PowerConnect 6024
Main Power Supply Status: (État bloc d'alimentation principal :)	OK
Redundant Power Supply Status: (État bloc	OK

d'alimentation redondant :)	
Fan 1 Status: (État ventilateur 1 :)	OK
Fan 2 Status: (État ventilateur 2 :)	OK
Temperature (Celsius): (Température (Celsius) :)	45
Temperature Sensor Status: (État du capteur de température :)	OK

Informations de version

La page **Versions** contient des informations sur les versions logicielle et matérielle actuellement exécutées. Pour afficher la page **Versions**, cliquez sur **System** (Système)→ **General** (Général)→ **Versions** dans l'arborescence (reportez-vous à la Figure 6-5).

Figure 6-5. Versions



La page **Versions** contient les champs suivants :

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 exécuté sur le 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 6-4. Commande CLI Versions

Commande CLI	Description
show version	Affiche les informations de version du système.

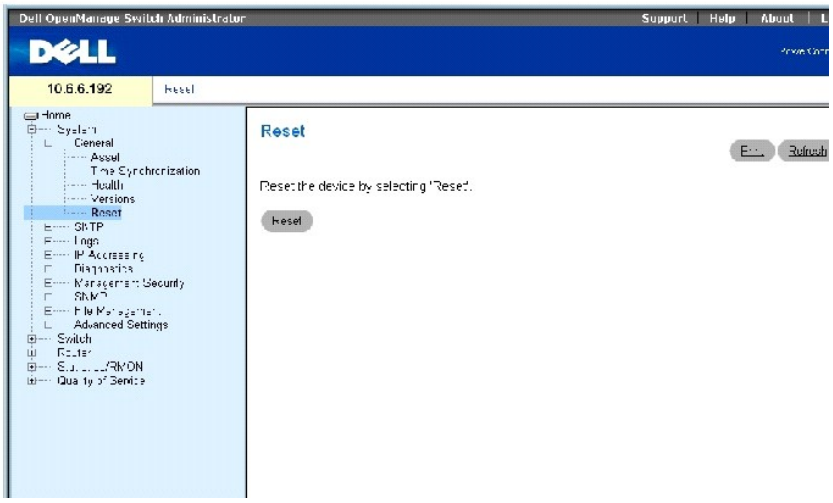
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# show version

SW version 1.0.0.67 ( date 26-Jun-2003 time 18:15:42 )

Boot version 1.0.0.11 ( date 12-Jun-2003 time 15:55:01 )

HW version 00.01.64
```

Réinitialisation du périphérique

La page **Reset** (Réinitialisation) permet de réinitialiser le périphérique. Pour ouvrir la page **Reset** (Réinitialisation), cliquez sur **System** (Système)→ **General** (Général)→ **Reset** (Réinitialisation) dans l'arborescence (reportez-vous à la Figure 6-6).

Figure 6-6. Réinitialisation



REMARQUE : Avant de réinitialiser le périphérique, enregistrez toutes les modifications dans le fichier de configuration en cours d'exécution pour éviter de perdre la configuration matérielle actuelle. Pour obtenir des 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** (Réinitialiser).
3. Lorsque le message de confirmation s'affiche, cliquez sur **OK**.

Le périphérique est réinitialisé. Une fois la réinitialisation effectuée, entrez un nom d'utilisateur et un mot de passe.

Réinitialisation du périphérique à l'aide de l'interface de ligne de commande

1. Si vous n'êtes pas déjà en mode EXEC utilisateur privilégié, tapez `enable`.
2. Si vous souhaitez enregistrer les modifications apportées à la configuration en cours d'exécution du périphérique, tapez `copy running-config startup-config`.
3. Tapez `reload`.
4. Appuyez sur `y`, lorsque vous y êtes invité, si vous souhaitez continuer.

Configuration des paramètres 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.

Les sources de temps sont établies par des Stratums. Les Stratums définissent la précision de l'horloge de référence. Plus le Stratum est haut (zéro représente le plus élevé), plus l'horloge est précise. Le périphérique reçoit l'heure du Stratum 1 ou supérieur.

Vous trouverez ci-dessous des exemples de stratums :

- **Stratum 0** Une horloge temps réel, comme un système GPS, est utilisée comme source d'heure.
- **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.
- **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 :

- **T1** Heure à laquelle la demande originale a été envoyée par le client.
- **T2** Heure à laquelle la demande originale a été reçue par le serveur.
- **T3** Heure à laquelle le serveur a envoyé une réponse.
- **T4** Heure à laquelle le client a reçu la réponse du serveur.

Le périphérique peut interroger les serveurs suivants concernant l'heure : monodiffusion, multidiffusion et diffusion.

Ce type de demande est utilisé pour interroger un serveur dont on ne connaît pas l'adresse IP. Les serveurs SNTP ayant été configurés sur le périphérique sont les seuls à pouvoir être interrogés en cas de demande d'informations de synchronisation. Les valeurs T1 à T4 sont utilisées pour déterminer l'heure du serveur. Cette méthode est préférée pour synchroniser l'heure du périphérique car c'est la plus sûre. Si cette méthode est sélectionnée, seules les informations SNTP en provenance des serveurs SNTP définis sur le périphérique via la page **SNTP Servers** (Serveurs SNTP) sont acceptées.

Ce type de demande est utilisé lorsqu'on ne connaît pas l'adresse IP du serveur. Si cette méthode est sélectionnée, tous les serveurs SNTP sur le réseau peuvent envoyer des informations de synchronisation. Le périphérique est synchronisé lorsqu'il demande de sa propre initiative des informations de synchronisation. La meilleure réponse (stratum le plus bas) obtenue des 3 premiers serveurs SNTP invités à répondre à une demande d'informations de synchronisation sert à 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 l'interrogation par multidiffusion lors d'une demande d'informations d'heure en vue d'une synchronisation de l'heure du périphérique plutôt que l'interrogation par diffusion. Toutefois, cette méthode est moins sûre que l'interrogation par monodiffusion car des paquets SNTP provenant de serveurs SNTP qui ne sont pas configurés sur le périphérique sont acceptés.

Ce type d'information est utilisé lorsqu'on ne connaît pas l'adresse IP du serveur. Lorsqu'un message de diffusion est envoyé à partir d'un serveur SNTP, le client SNTP écoute le message. Si l'interrogation par diffusion est activée, toutes les informations de synchronisation sont acceptées même si elles n'ont pas été demandées par le périphérique. Cette méthode est la moins sûre.

Le périphérique récupère les informations de synchronisation en les demandant activement ou à chaque intervalle d'interrogation. Si l'interrogation par monodiffusion, l'interrogation par multidiffusion et l'interrogation par diffusion sont activées, les informations sont récupérées dans l'ordre indiqué ci-dessous :

- Les informations provenant des serveurs définis sur le périphérique sont privilégiées. Si l'interrogation par monodiffusion n'est pas activée ou si aucun serveur n'est défini sur le périphérique, celui-ci accepte des informations d'heure de tous les serveurs SNTP qui répondent.
- Si plusieurs périphériques de monodiffusion répondent, les informations de synchronisation provenant du périphérique ayant le stratum le plus bas sont privilégiées.
- Si les serveurs ont le même stratum, les informations acceptées sont celles provenant du premier serveur SNTP à avoir répondu.

L'authentification MD5 (condensé de message 5) sauvegarde les chemins de synchronisation du périphérique vers 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.

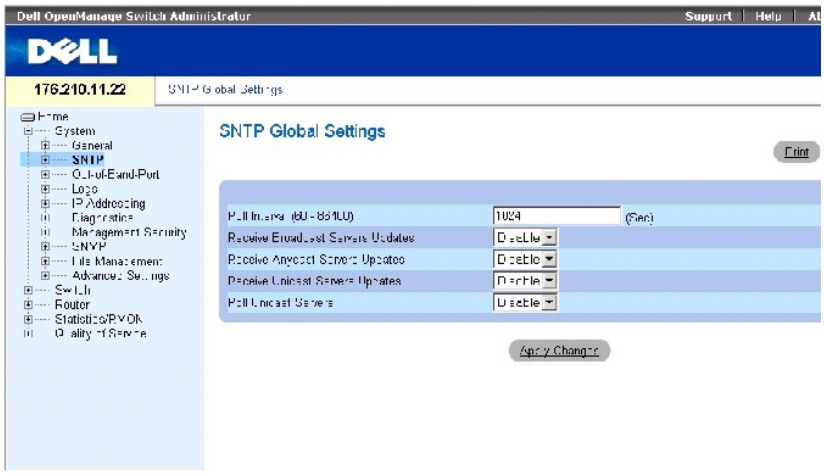
La page SNTP contient des liens vers des pages qui permettent aux gestionnaires de réseau de configurer les paramètres SNTP. Pour ouvrir la page **SNTP**, cliquez sur **System** (Système)→ **SNTP** dans l'*arborescence*.

Définition des paramètres globaux SNTP

La page **SNTP Global Settings** (Paramètres globaux SNTP) fournit des informations permettant de définir les paramètres SNTP.

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

Figure 6-7. Paramètres globaux SNTP



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

Poll Interval (60-86400) (Intervalle d'interrogation [60-86400]) Définit l'intervalle (en secondes) pendant lequel le serveur SNTP est interrogé pour des informations de monodiffusion.

Receive Broadcast Servers Updates (Recevoir des mises à jour de serveurs de diffusion) Lorsqu'elle est activée, cette option permet de demander aux serveurs SNTP des informations d'heure du serveur de diffusion sur les interfaces sélectionnées. Le périphérique est synchronisé à chaque fois qu'un paquet SNTP est reçu, même si la synchronisation n'a pas été demandée.

Receive Anycast Servers Updates (Recevoir des mises à jour de serveurs de multidiffusion) Lorsqu'elle est activée, cette option permet de demander aux

serveurs SNTP des informations sur l'heure du serveur de multidiffusion. Le périphérique est synchronisé uniquement lorsqu'une demande de synchronisation est envoyée à partir du périphérique.

Receive Unicast Servers Updates (Recevoir des mises à jour de serveurs de monodiffusion) Lorsqu'elle est activée, cette option permet de demander aux serveurs SNTP définis sur le périphérique des informations sur l'heure du serveur de monodiffusion. Si les champs **Receive Broadcast Servers Updates** (Recevoir des mises à jour de serveurs de diffusion), **Receive Anycast Servers Updates** (Recevoir des mises à jour de serveur de multidiffusion) et **Receive Unicast Servers Updates** (Recevoir des mises à jour de serveurs de monodiffusion), l'heure du système est configurée suivant les informations d'heure du serveur de monodiffusion.

Poll Unicast Servers (Interroger serveurs monodiffusion) Lorsqu'elle est activée, cette option permet d'envoyer des demandes d'informations d'heure du serveur de 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 de la page **SNTP Global Settings** (Paramètres globaux SNTP).

Tableau 6-5. Commandes CLI Paramètres globaux SNTP

Commande CLI	Description
`sntp client poll timer seconds`	Définit la période d'interrogation du client SNTP
`sntp broadcast client enable`	Active les clients de diffusion SNTP
`sntp unicast client enable`	Active les clients de monodiffusion SNTP prédéfinis
`sntp unicast client poll`	Active l'interrogation des serveurs de monodiffusion SNTP prédéfinis
`show sntp configuration`	Affiche la configuration du SNTP.
`show sntp status`	Affiche l'état du SNTP.

Vous trouverez ci-dessous un exemple de commande CLI :

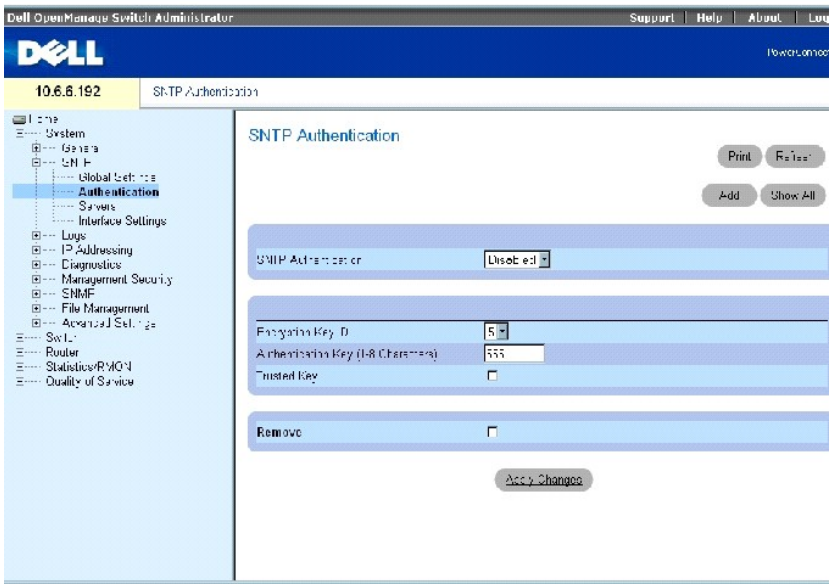
```
Console (config)# sntp anycast client enable
```

Définition des méthodes d'authentification du SNTP

La page **SNTP Authentication** (Authentification du SNTP) active l'authentification du SNTP entre le périphérique et un serveur SNTP. Le serveur SNTP est également sélectionné dans la page **SNTP Authentication** (Authentification du SNTP).

Cliquez sur **System** (Système)→ **SNTP**→ **Authentication** (Authentification) dans l'arborescence pour ouvrir la page **SNTP Authentication** (Authentification du SNTP).

Figure 6-8. Authentification du SNTP



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

SNTP Authentication (Authentification du SNTP) Lorsqu'elle est activée, cette option permet d'activer l'authentification d'une session SNTP entre le périphérique et un serveur SNTP.

Encryption Key ID (ID de clé de cryptage) Dresse la liste des ID de clé définis par l'utilisateur utilisés pour authentifier le serveur SNTP et le périphérique. Les valeurs possibles pour ce champ sont comprises entre 1 et 4294967295.

Authentication Key (Clé d'authentification) (**1 à 8** caractères) Clé utilisée pour l'authentification.

Trusted Key (Clé de confiance) Cochez cette case pour spécifier la clé de cryptage utilisée (monodiffusion/multidiffusion) ou choisie (diffusion) pour authentifier le serveur SNTP.

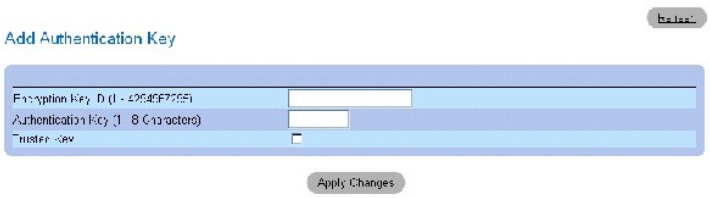
Remove (Supprimer) Cochez cette case pour supprimer la clé d'authentification sélectionnée.

Ajout d'une clé d'authentification du SNTP

1. Ouvrez la page **SNTP Authentication** (Authentification du SNTP).
2. Cliquez sur Add (Ajouter).

La page **Add Authentication Key** (Ajout d'une clé d'authentification) s'ouvre :

Figure 6-9. Ajout d'une clé d'authentification



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

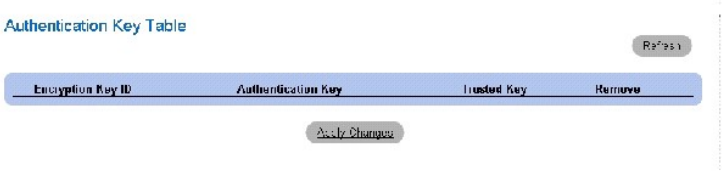
La clé d'authentification du SNTP est ajoutée et le périphérique est mis à jour.

Affichage de la table des clés d'authentification

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

La page **Authentication Key Table** (Table des clés d'authentification) s'ouvre :

Figure 6-10. Table des clés d'authentification



Suppression d'une clé d'authentification

1. Ouvrez la page **SNTP Authentication** (Authentification du SNTP).
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 **Authentication Key Table** (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 SNTP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page **SNTP Authentication** (Authentification du SNTP).

Tableau 6-6. Commandes CLI Authentification du SNTP

Commande CLI	Description
sntp authenticate	Exige l'authentification du trafic NTP (protocole de temps réseau) provenant des serveurs.
sntp authentication- key *number* **md5** *value*	Définit une clé d'authentification pour le SNTP.
sntp trusted-key key-number	Définit la clé d'authentification utilisée pour authentifier le serveur SNTP.
show sntp configuration	Affiche la configuration du SNTP.

Vous trouverez ci-dessous un exemple de commande CLI :

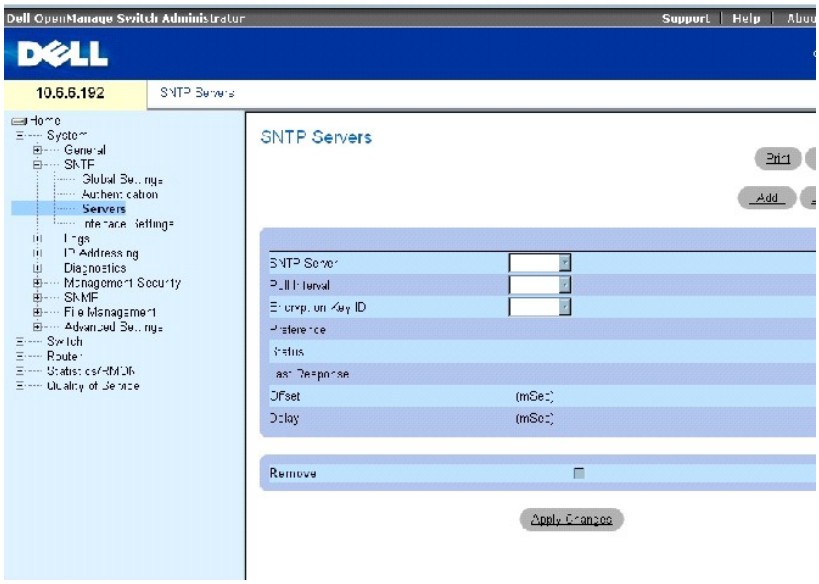
```
Console (config)# sntp authentication-key 8 md5 ClkKey

Console (config)# sntp trusted-key 8

Console (config)# sntp authenticate
```

Définition des serveurs SNTP

La page **SNTP Servers** (Serveurs SNTP) contient des informations permettant d'activer des serveurs SNTP et d'ajouter de nouveaux serveurs SNTP.

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

Figure 6-11. Serveurs SNTP



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

SNTP Server (Serveur SNTP) Dresse la liste des adresses IP de serveur SNTP définies par l'utilisateur. Vous pouvez définir jusqu'à huit serveurs SNTP.

Poll Interval (Intervalle d'interrogation) Active l'interrogation du serveur SNTP pour récupérer des informations sur l'heure du système.

Encryption Key ID (ID de clé de cryptage) Dresse la liste des ID de clé définis par l'utilisateur utilisés pour toute communication entre le serveur SNTP et le périphérique. L'ID de la clé de cryptage est défini dans la page **SNTP Authentication** (Authentification du SNTP).

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 (État) L'état du serveur SNTP en fonctionnement. Ce champ peut prendre les valeurs suivantes :

Up (Opérationnel) Le serveur SNTP fonctionne normalement.

Down (non opérationnel) Indique qu'aucun serveur SNTP n'est actuellement disponible. Par exemple, le serveur SNTP n'est pas connecté ou il est arrêté.

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

Unknown (Inconnu) L'état des informations SNTP actuellement envoyées n'est pas connu. Par exemple, le périphérique est actuellement en train de chercher une interface.

Last Response (Dernière réponse) Heure de la dernière réponse reçue du serveur SNTP.

Offset (Décalage) Différence d'horodatage entre l'horloge locale du périphérique et l'heure reçue du serveur SNTP.

Delay (Retard) Temps nécessaire pour atteindre le serveur SNTP.

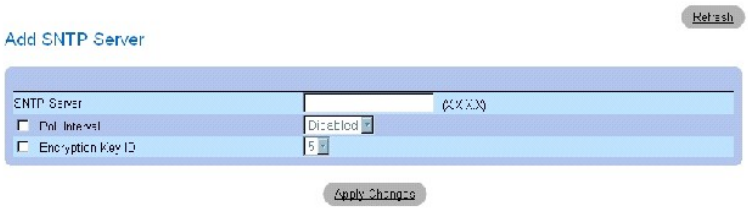
Remove (Supprimer) Sélectionnez cette case pour supprimer un serveur SNTP de la liste **SNTP Servers** (Serveurs SNTP).

Ajout d'un serveur SNTP

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

La page **Add SNTP Server** (Ajout d'un serveur SNTP) s'ouvre :

Figure 6-12. Ajout d'un serveur SNTP



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

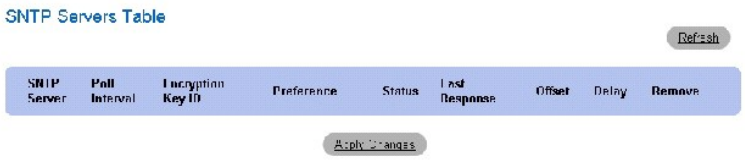
Le serveur SNTP est ajouté et le périphérique est mis à jour.

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 6-13. 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 dans la liste **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 6-7. Commandes CLI Authentification du SNTP

Commande CLI	Description
	Définit un serveur SNTP pouvant être utilisé pour la synchronisation des informations d'heure.

sntp server {*ip- address* | *hostname*} [**poll**] [**key** *keyid*]	
no sntp server *ip- address*	Supprime un serveur de la liste des serveurs SNTP.

Vous trouverez ci-dessous un exemple de commande CLI :

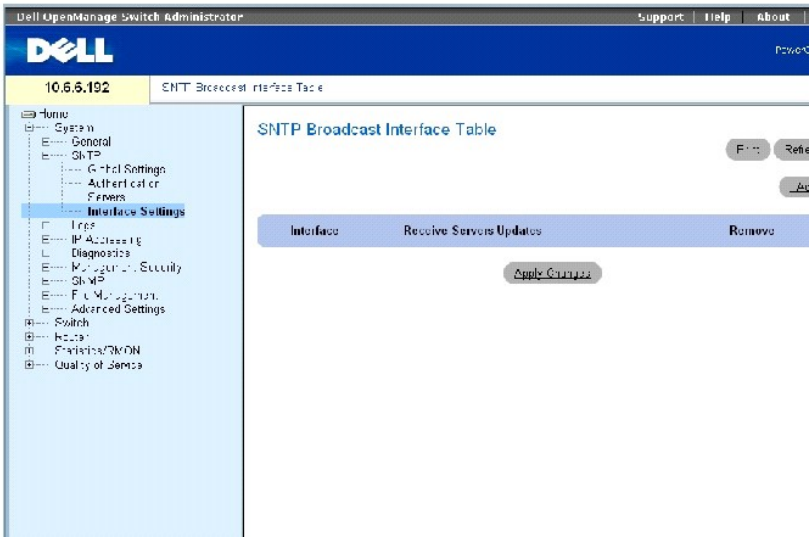
```
Console (config)# sntp server 100.1.1.1 poll key 10
```

Définition des interfaces SNTP

La page **SNTP Broadcast Interface Table** (Table des interfaces de diffusion SNTP) contient des champs permettant de configurer le SNTP sur différentes interfaces.

Pour ouvrir la page **SNTP Broadcast Interface Table** (Table des interfaces de diffusion SNTP), cliquez sur **System** (Système)→ **SNTP**→ **Interfaces Settings** (Paramètres des interfaces).

Figure 6-14. Table des interfaces de diffusion SNTP



La page **SNTP Broadcast Interface Table** (Table des interfaces de diffusion SNTP) contient les champs suivants :

Interface Affiche une liste d'interfaces sur lesquelles le SNTP peut être activé.

Receive Servers Updates (Recevoir des mises à jour de serveur) Active ou désactive la réception de mises à jour SNTP sur une interface.

Remove (Supprimer) Sélectionnez cette case à cocher pour désactiver le SNTP sur une interface.

Activation du SNTP sur une interface

1. Ouvrez la page **SNTP Broadcast Interface Table** (Table des interfaces de diffusion SNTP).
2. Cliquez sur **Add** (Ajouter).

La page **Add SNTP Interface** (Ajout d'une interface SNTP) s'ouvre.

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

SNTP est activé sur l'interface 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 de la page **SNTP Broadcast Interface Table** (Table des interfaces de diffusion SNTP).

REMARQUE : Lors de la définition d'interfaces de diffusion ou de multidiffusion, au moins une adresse IP doit être définie.

Tableau 6-8. Commandes CLI Paramètres d'interface SNTP

Commande CLI	Description
client sntp enable	Active le client de diffusion et de multidiffusion SNTP (protocole de temps de réseau simple) sur une interface.
show sntp configuration	Affiche la configuration du SNTP.

L'exemple qui suit montre les commandes CLI permettant de configurer des interfaces SNTP :

```
Console (config)# interface ethernet g1

Console (config-if)# sntp client enable

Console (config-if)# end

Console# show sntp configuration

Polling interval: 7200 seconds.

MD5 Authentication keys: 8, 9

Authentication is required for synchronization.

Trusted Keys: 8,9

Unicast Clients Polling: Enabled.

Server          Polling          Encryption Key
```

----------	--------	----------	
176.1.1.8	Enabled	9	
176.1.8.179	Disabled	Disabled	
Broadcast Clients: Enabled			
Broadcast Clients Poll: Enabled			
Broadcast Interfaces: g1			

Configuration des ports de gestion hors bande (OOB)

Cette section décrit la gestion des fonctions suivantes du périphérique via le port de gestion hors bande. Elle comprend des informations sur le serveur de journalisation à distance hors bande, la passerelle hors bande par défaut, les paramètres de l'interface IP hors bande, le serveur TACACS+ hors bande et le serveur RADIUS hors bande.

Lorsque ces fonctions sont gérées via le port de gestion hors bande, la gestion intrabande de ces fonctions est désactivée. Utilisez l'interface SNMP pour configurer ces fonctions via le port hors bande.

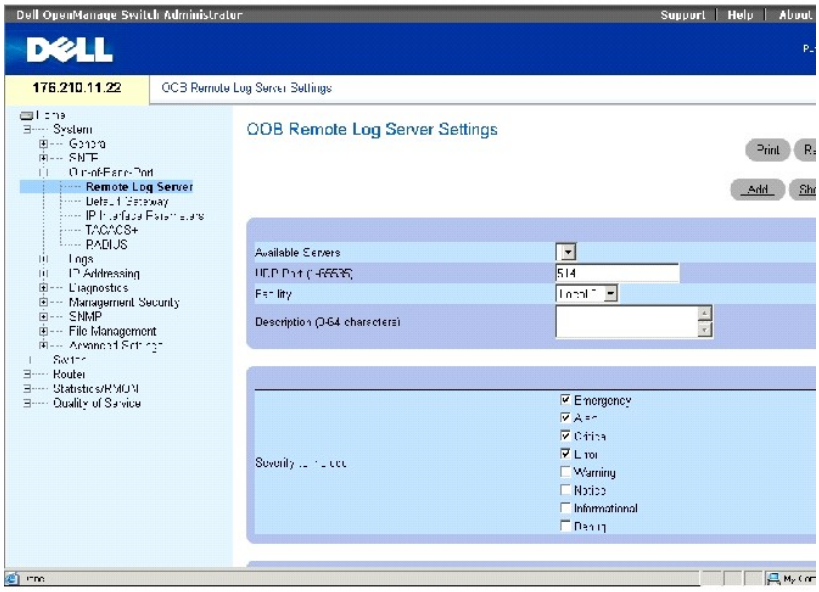
Pour ouvrir la page **OOB Configuration** (Configuration OOB), cliquez sur **System** (Système)→ **Out of Band** (Hors bande) dans l'*arborescence*.

Configuration des serveurs de journalisation à distance hors bande

La page **OOB Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance OOB) contient les champs permettant d'afficher les serveurs de journalisation hors bande disponibles. Par ailleurs, de nouveaux serveurs de journalisation hors bande peuvent être définis ainsi que le niveau de gravité des journaux envoyés au serveur.

Pour ouvrir la page **OOB Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance hors bande), cliquez sur **System** (Système)→ **Out-of-Band Port** (Port hors bande)→ **Remote Log Server** (Serveur de journalisation à distance) dans l'*arborescence*.

Figure 6-15. Paramètres des serveurs de journalisation à distance OOB



La page **OOB Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance OOB) contient les champs suivants :

Available Servers (Serveurs disponibles) Serveurs auxquels les journaux peuvent être envoyés.

UDP Port (1-65535) (Port UDP (1-65535)) Port UDP à partir duquel les journaux sont envoyés. La valeur par défaut est 514.

Facility (Voie de transmission) Application définie par l'utilisateur à partir de laquelle les journaux système sont envoyés au serveur distant. Une seule voie de transmission peut être affectée à 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 1, local 2, local 3, local 4, local 5, local 6 et local 7.

Description (0-64 characters) (Description (0-64 caractères)) Affiche la description du serveur définie par l'utilisateur.

Severity to Include (Niveau de gravité à inclure) Niveau de gravité du journal. Lorsqu'un niveau de gravité est sélectionné, tous les niveaux de gravité supérieurs à ce niveau sont automatiquement sélectionnés.

Delete Server (Supprimer serveur) Permet de supprimer un serveur de la liste **Available Servers** (Serveurs disponibles).

La page **OOB Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance OOB) contient également une liste de niveaux de gravité. Ces niveaux de gravité sont les mêmes que ceux de la page **RAM Log Table** (Table des journaux en RAM).

Envoi de journaux à un serveur de journalisation hors bande

1. Ouvrez la page **OOB Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance OOB).
2. Renseignez les champs **UDP Port** (Port UDP), **Facility** (Voie de transmission) et **Description**.
3. Sélectionnez le type de journal et le niveau de gravité.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

REMARQUE : Avant d'ajouter un nouveau serveur, déterminez l'adresse IP du serveur de journalisation à distance hors bande.

Définition d'un nouveau serveur de journalisation hors bande

1. Ouvrez la page **OOB Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance OOB).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add an OOB Log Server** (Ajout d'un serveur de journalisation OOB).
3. Renseignez les champs de la boîte de dialogue.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le serveur est défini et ajouté à la liste **Available Servers** (Serveurs disponibles).

Suppression d'un serveur de journalisation hors bande

1. Ouvrez la page **OOB Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance OOB).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la page **OOB Remote Log Servers Table** (Table des serveurs de journalisation à distance OOB).
3. Sélectionnez un serveur et cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Configuration des serveurs de journalisation à distance hors bande à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI applicables aux champs de la page **OOB Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance OOB).

Tableau 6-9. Commande CLI Paramètres des serveurs de journalisation à distance hors bande

Commande CLI	Description
logging *oob/ip- address* [**port** *port*] [**severity** *level*] [**facility** *facility*] [**description** *text]*	Définit un nouveau serveur de journalisation à distance.

Vous trouverez ci-dessous un exemple de commande CLI :

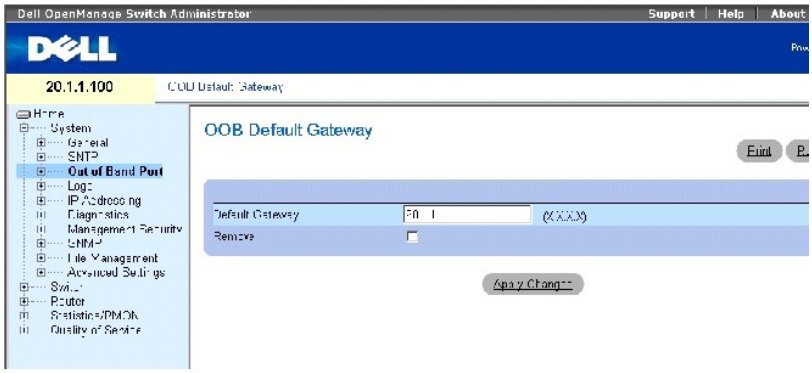
```
Console (config)#logging oob/10.2.2.2 severity critical facility local0 description syslog_server_1
```

Définition de passerelles hors bande par défaut

La page **OOB Default Gateway** (Passerelle OOB par défaut) permet de définir des périphériques passerelles. 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. La suppression de l'interface IP à laquelle une passerelle par défaut est connectée entraîne la suppression de la passerelle par défaut.

Pour ouvrir la page **OOB Default Gateway** (Passerelle OOB par défaut), cliquez sur **System** (Système)→ **Out-of-Band Port** (Port hors bande)→ **Default Gateway** (Passerelle par défaut) dans l'*arborescence*.

Figure 6-16. Passerelle OOB par défaut



La page **OOB Default Gateway** (Passerelle OOB par défaut) contient le paramètre suivant :

Default Gateway (Passerelle par défaut) Indique l'adresse IP du périphérique faisant office de passerelle.

Sélection d'un périphérique passerelle hors bande

1. Ouvrez la page **OOB Default Gateway** (Passerelle OOB par défaut).
2. Indiquez une adresse IP dans le champ **Default Gateway** (Passerelle par défaut).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le périphérique passerelle hors bande est défini et le périphérique est mis à jour.

Tableau 6-10. Commandes CLI Passerelle hors bande par défaut

Commande CLI	Description
`ip default gateway` *ip- address*	Définit la passerelle IP hors bande.

Vous trouverez ci-dessous un exemple de commande CLI :

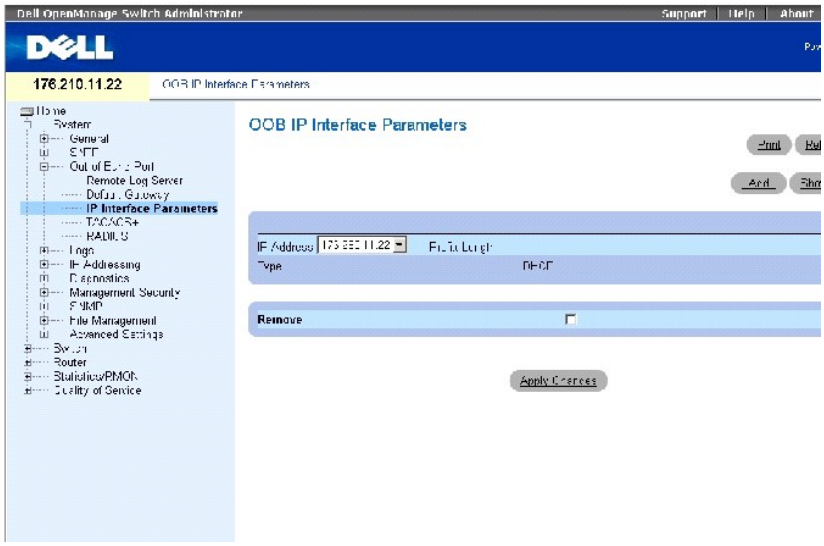
```
Console (config)# interface out-of-band-eth

Console (config-oob)# ip address 10.0.0.1 /8

Console (config-oob)# ip default-gateway 10.1.1.1
```

Définition des paramètres d'interface IP hors bande

La page **OOB IP Interface Parameters** (Paramètres d'interface IP hors bande) contient des paramètres permettant d'affecter des adresses IP hors bande aux interfaces.

Pour ouvrir la page **OOB IP Interface Parameters** (Paramètres d'interface IP OOB), cliquez sur **System** (Système)→ **Out-of-Band Port** (Port hors bande)→ **IP Interface Parameters** (Paramètres d'interface IP) dans l'*arborescence*.

Figure 6-17. Paramètres d'interface IP OOB



La page **OOB IP Interface Parameters** (Paramètres d'interface IP OOB) contient les paramètres suivants :

IP Address (Adresse IP) Adresse IP de l'interface hors bande.

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.

Type Moyens par lesquels l'interface IP hors bande a été créée ; DHCP ou statique.

Remove (Supprimer) Lorsqu'elle est cochée, cette option permet de supprimer l'interface de la liste déroulante **IP Address** (Adresse IP).

REMARQUE : Vous pouvez configurer des adresses IP DHCP pour la gestion hors bande dans la page **DHCP IP Interface** (Interface IP DHCP) (**System** (Système)→ **IP Address** (Adresse IP)→ **DHCP IP Interface** (Interface IP DHCP).

Ajout d'une interface IP

1. Ouvrez la page **OOB IP Interface Parameters** (Paramètres d'interface IP OOB).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add a Static OOB IP Interface** (Ajout d'une interface IP OOB statique).
3. Le champ **Network Mask** (Masque de réseau) définit le masque de sous-réseau de l'adresse IP source.
4. Renseignez les champs de la page.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle interface est ajoutée et le périphérique est mis à jour.

Suppression d'adresses IP

1. Ouvrez la page **OOB IP Interface Parameters** (Paramètres d'interface IP OOB).
2. Cliquez sur **Show All** (Afficher tout).
3. La page **Interface Parameters Table** (Table des paramètres d'interface) s'ouvre.
4. Sélectionnez une adresse IP dans la liste déroulante **IP Address** (Adresse IP).
5. Sélectionnez une entrée de la table **Interface Parameters Table** (Table des paramètres d'interface).
6. Cochez la case **Remove** (Supprimer).

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

L'adresse IP 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 applicables aux champs de la page **OOB IP Interface Parameters** (Paramètres d'interface IP OOB).

Tableau 6-11. Commandes CLI Paramètres d'interface IP hors bande

Commande CLI	Description
`interface out-of- band-eth`	Configure le port Ethernet hors bande et définit le mode de configuration de l'interface.
`ip address ip- address {mask | prefix-length}`	Définit une adresse IP.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address 192.168.0.1 /8
```

Configuration des serveurs TACACS+ hors bande

Le périphérique offre 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 :

- **Authentication** (Authentification) Permet une authentification pendant la connexion par le biais des noms d'utilisateur et des mots de passe définis par les utilisateurs.
- **Authorization** (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.

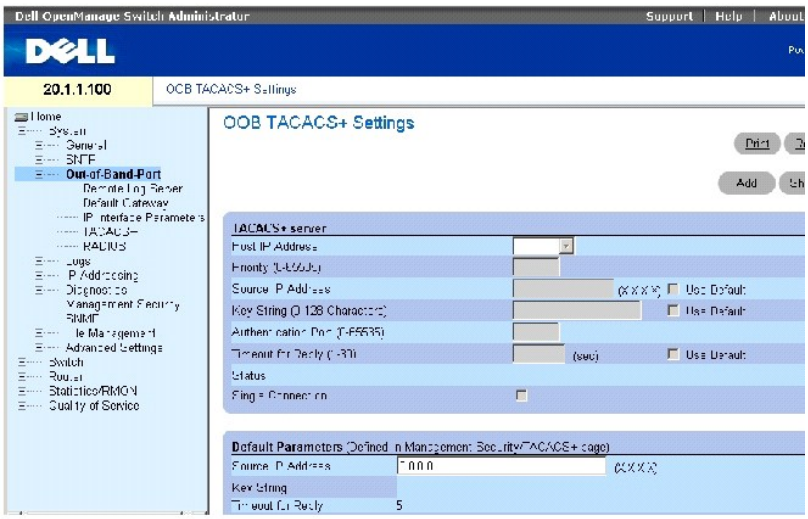
Des serveurs TACACS+ peuvent être définis sur des ports intrabande via la page **TACACS+ Settings** (Paramètres TACACS+) ou sur le port hors bande.

Le protocole TACACS+ assure l'intégrité du réseau grâce à des échanges en protocole crypté entre le périphérique et le serveur TACACS+.

La page **OOB TACACS+ Settings** (Paramètres TACACS+ OOB) contient les paramètres TACACS+ définis par l'utilisateur et par défaut du port de gestion hors bande.

Pour ouvrir la page **OOB TACACS+ Settings** (Paramètres TACACS+ OOB), cliquez sur **System** (Système)→ **Out-of-Band-Port** (Port hors bande)→ **TACACS+** dans l'*arborescence*.

Figure 6-18. Paramètres TACACS+ OOB



La page **OOB TACACS+ Settings** (Paramètres TACACS+ OOB) contient les champs suivants

Host IP Address (Adresse IP hôte) Adresse IP du serveur TACACS+.

Priority (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 (Clé de codage) (0-128 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 (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) (Délai de réponse (1-30)) Délai qui s'écoule avant l'expiration de la connexion entre le périphérique et le serveur TACACS+. La plage des valeurs possibles pour ce champ 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 paramètres 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 (Clé de codage) (0-128 caractères) Clé d'authentification et de cryptage par défaut des communications TACACS+ entre le périphérique et le serveur TACACS+.

Timeout for Reply (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+.

REMARQUE : Vous pouvez définir les valeurs par défaut mentionnées ci-dessus dans la page **TACACS+ Settings** (Paramètres TACACS+) (**System** (Système)→ **Management Security** (Sécurité de gestion)→ **TACACS+**).

Définition des paramètres TACACS+

1. Ouvrez la page **OOB TACACS+ Settings** (Paramètres TACACS+ OOB).
2. Renseignez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres TACACS+ sont mis à jour sur le périphérique.

Ajout d'un serveur TACACS+

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

La page **Add OOB TACACS+ Host** (Ajout d'un hôte TACACS+ OOB) s'ouvre.

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

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

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

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

La page **TACACS+ Table** (Table TACACS+) s'ouvre.

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

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

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

Le tableau suivant récapitule les commandes CLI applicables aux champs de la page **OOB TACACS+ Settings** (Paramètres TACACS+ OOB).

Tableau 6-12. Commandes CLI Paramètres TACACS+ hors bande

Commande CLI	Description
tacacs-server host {*oob/ip-address* | hostname} [single-connection] [port port-number] [timeout timeout] [key key-string] [source source] [priority priority]	Définit un serveur TACACS+ hôte.

no tacacs-server host {ip-address | hostname}	Supprime un serveur TACACS+ hôte donné.
tacacs-server key [key-string]	Désigne la clé d'authentification et de cryptage utilisée pour toutes les communications TACAS entre le périphérique et le serveur TACACS+. Cette clé doit correspondre à la clé de cryptage utilisée sur le serveur TACACS démon. (Plage des valeurs : 0 à 128 caractères)
no tacacs-server key	Revient à la valeur par défaut.
tacacs-server timeout *timeout*	Spécifie la valeur du délai en secondes. (Plage : 1-30)
no tacacs-server timeout	Revient à la valeur par défaut.
tacacs-server source-ip *oob/ip-address*	Spécifie l'adresse IP source. (Plage : adresse IP valide)
no tacacs-server source-ip *oob/ip-address*	Revient à la valeur par défaut.
show tacacs [*oob/ip-address*]	Affiche la configuration et les statistiques d'un serveur TACACS+.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# tacacs-server host oob/172.16.8.1 key abc

Console (config)# end

Console# show tacacs

                                                                    

Device Configuration

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

IP address  Status     Port  Single      TimeOut  Source  Priority
                           Connection          IP
----------  ---------  ----  ----------  -------  ------  --------
No TACACS server is configured.

                                                                    

OOB host Configuration

IP address  Status     Port  Single      TimeOut  Source  Priority
                           Connection          IP
----------  ---------  ----  ----------  -------  ------  --------
172.16.8.1  Not        49    No          Global   Global  0
            Connected
                                                                    

Global Values

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

                                                                    
```

TimeOut: 5						
Device Configuration						

Source IP: 0.0.0.0						
OOB host Configuration						

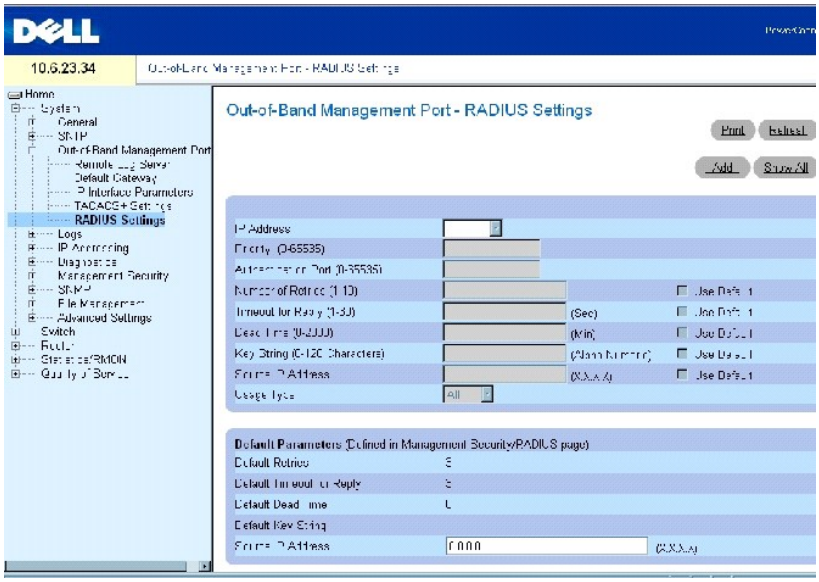
Source IP : 0.0.0.0						

Configuration de serveurs RADIUS hors bande

La page **OOB RADIUS Settings** (Paramètres RADIUS OOB) contient les paramètres RADIUS définis par l'utilisateur et par défaut du port de gestion hors bande. Pour plus d'informations sur les serveurs RADIUS, reportez-vous à la section «**Configuration des paramètres TACACS+**».

Pour ouvrir la page **OOB RADIUS Settings** (Paramètres RADIUS OOB), cliquez sur **System** (Système)→ **Out-of-Band Port** (Port hors bande)→ **RADIUS** dans l'arborescence (reportez-vous à la Figure 6-19, Paramètres RADIUS OOB).

Figure 6-19. Paramètres RADIUS OOB



La page **OOB RADIUS Settings** (Paramètres RADIUS OOB) contient les champs suivants :

IP Address (Adresse IP) Adresse IP du port hors bande d'authentification.

Priority (0-65535) (Priorité [0-65535]) Priorité du port hors bande. Les valeurs possibles sont comprises entre 0 et 65535.

Authentication Port (Port d'authentification) Port utilisé pour vérifier l'authentification du serveur RADIUS.

Number of Retries (1-10) (Nombre de tentatives [1-10]) Nombre de demandes de transmission envoyées au serveur RADIUS avant la survenue d'un échec. Les valeurs possibles pour ce champ sont comprises entre 1 et 10. La valeur par défaut est 3. En l'absence de valeur spécifique à l'hôte, la valeur globale s'applique à chaque hôte.

Timeout for Reply (1-30) (Délai de réponse [1-30]) Délai en secondes pendant lequel le périphérique attend une réponse du serveur RADIUS avant expiration. Les valeurs possibles pour ce champ sont comprises entre 1 et 30. La valeur par défaut est 3. En l'absence de valeur spécifique à l'hôte, la valeur globale s'applique à chaque hôte.

Dead Time (0-2000) (Délai d'inactivité [0-2000]) Délai (en minutes) pendant lequel un serveur RADIUS est écarté pour répondre à des demandes de service. La plage est comprise entre 0 et 2000. En l'absence de valeur spécifique à l'hôte, la valeur globale s'applique à chaque hôte.

Key String (0-128 Characters) (Clé de codage [0-128 caractères]) Clé de codage utilisée pour authentifier et crypter toutes les communications RADIUS entre le périphérique et le serveur RADIUS. Cette clé doit correspondre au cryptage RADIUS. En l'absence de valeur spécifique à l'hôte, la valeur globale s'applique à chaque hôte.

Source IP Address (Adresse IP source) Adresse IP du périphérique ayant accès au serveur RADIUS.

Les paramètres RADIUS par défaut sont définis par l'utilisateur. Les paramètres par défaut sont appliqués aux nouveaux serveurs RADIUS définis. Si aucune valeur par défaut n'est définie, les valeurs par défaut du système sont appliquées aux nouveaux serveurs RADIUS. Les paramètres par défaut des serveurs RADIUS sont les suivants :

Default Timeout for Reply (Délai de réponse par défaut) Durée par défaut pendant laquelle le périphérique attend une réponse du serveur RADIUS avant expiration.

Default Retries (sec) (Nombre de tentatives par défaut [s]) Nombre par défaut de demandes de transmission envoyées au serveur RADIUS avant la survenue d'un échec.

Default Dead Time (sec) (Délai d'inactivité par défaut [s]) Délai (en minutes) par défaut 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 (Clé de codage par défaut) Clé de codage par défaut utilisée pour authentifier et crypter toutes les communications RADIUS entre le périphérique et le serveur RADIUS. Cette clé doit correspondre au cryptage RADIUS.

REMARQUE : Vous pouvez définir les valeurs par défaut mentionnées ci-dessus dans la page **RADIUS Settings** (Paramètres RADIUS) (**System** (Système)→ **Management Security** (Sécurité de gestion)→ **RADIUS**).

Source IP Address (Adresse IP source) Adresse IP par défaut d'un périphérique ayant accès au serveur RADIUS.

Définition des paramètres RADIUS hors bande

1. Ouvrez la page **OOB RADIUS Settings** (Paramètres RADIUS OOB).
2. Renseignez les champs suivants : **Default Timeout for Reply** (Délai de réponse par défaut), **Default Retries** (Nombre de tentatives par défaut), **Default Dead Time** (Délai d'inactivité par défaut) et **Default Key** (Clé de codage par défaut).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres RADIUS sont mis à jour sur le périphérique.

Ajout d'un serveur RADIUS hors bande

1. Ouvrez la page **OOB RADIUS Settings** (Paramètres RADIUS OOB).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add OOB RADIUS Server** (Ajout d'un serveur RADIUS OOB).

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

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

Suppression d'un serveur RADIUS hors bande de la liste des serveurs RADIUS

1. Ouvrez la page **OOB RADIUS Settings** (Paramètres RADIUS OOB).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la liste **OOB RADIUS Servers** (Serveurs RADIUS OOB).
3. Sélectionnez un serveur RADIUS et cochez la case **Remove** (Supprimer).
4. 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 applicables aux champs de la page **OOB RADIUS Settings** (Paramètres RADIUS OOB).

Tableau 6-13. Commandes CLI Paramètres RADIUS hors bande

Commande CLI	Description
`radius-server host ip- address [auth-port auth- port-number] [timeout timeout] [retransmit retries] [deadtime deadtime] [key key- string] [source source] [priority priority]`	Définit un serveur RADIUS hôte.
`no radius-server host ip- address`	Supprime un serveur RADIUS hôte donné.
`radius-server source-ip source`	Définit l'adresse IP source utilisée pour communiquer avec les serveurs RADIUS.
`no radius-server-ip`	Revient à la valeur par défaut.
`radius-server timeout timeout`	Définit la durée pendant laquelle un routeur attend une réponse d'un serveur hôte.
`no radius-server deadtime`	Définit le délai d'inactivité sur 0.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)#interface out-of-band eth 1
```

```
Console radius-server host oob/10.2.2.2 key 123
```

Gestion des journaux

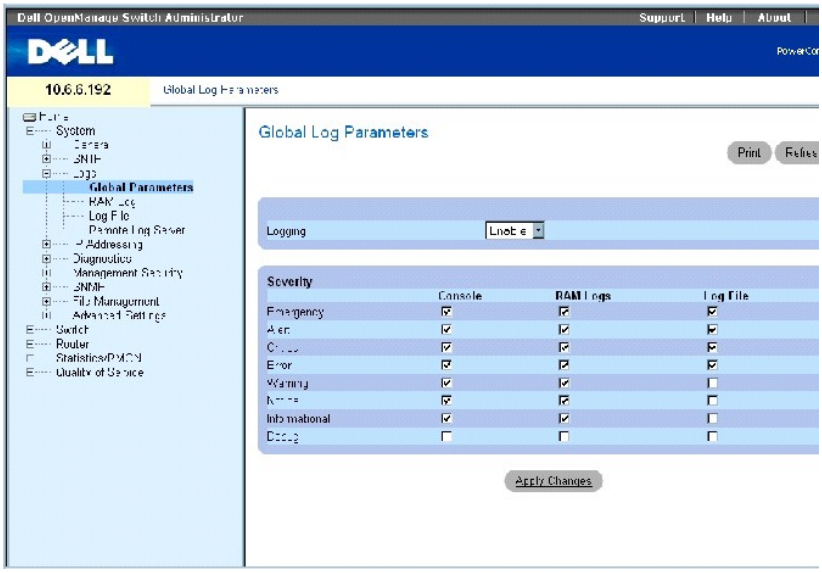
La page **Logs** (Journaux) contient des liens vers différentes pages de journalisation. Pour afficher la page **Logs** (Journaux), cliquez sur **System** (Système)→ **Logs** (Journaux) dans l'*arborescence*.

Paramètres globaux de journalisation

La page **Global Log Parameters** (Paramètres globaux de journalisation) contient des champs permettant d'activer globalement la journalisation et des champs permettant de définir les paramètres de journalisation. Les messages de journalisation **Severity** (Gravité) sont classés par ordre décroissant de gravité.

Pour ouvrir la page **Global Log Parameters** (Paramètres globaux de journalisation), cliquez sur **System** (Système)→ **Logs** (Journaux)→ **Global Parameters** (Paramètres globaux) dans l'*arborescence*.

Figure 6-20. Paramètres globaux de journalisation



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

Logging (Journalisation) Active la journalisation générale pour les journaux en mémoire cache, dans un fichier et sur serveur. Tous les messages imprimés sur la Console sont enregistrés dans les fichiers journaux. Ce champ peut prendre les valeurs suivantes :

Enable (Activer) Active l'enregistrement des journaux dans la mémoire cache (RAM), dans un fichier (FLASH) et sur un serveur externe.

Disable (Désactiver) Désactive l'enregistrement des journaux. Il n'est pas possible de désactiver la journalisation des journaux imprimés sur la Console.

Emergency (Urgence) Niveau d'avertissement le plus élevé. Si le périphérique est inactif ou ne fonctionne pas correctement, un journal d'urgence est enregistré sur le périphérique.

Alert (Alerte) Deuxième plus haut niveau d'avertissement. Un journal d'alerte est enregistré en cas de dysfonctionnement grave du périphérique ; lorsque les fonctions du périphérique 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) Une erreur s'est produite sur le périphérique ; un port est déconnecté, par exemple.

Warning (Avertissement) Niveau d'avertissement le plus faible.

Notice (Mise en garde) Fournit des informations sur le périphérique aux administrateurs réseau.

Informational (Informations) Fournit des informations sur le périphérique.

Debug (Débogage) Fournit des informations détaillées sur le journal. Seul le personnel du support technique est autorisé à accéder à ce paramètre.

Les cases à cocher apparaissent sous les trois colonnes suivantes :

Console Journaux envoyés à la Console.

RAM Logs (Journaux RAM) Journaux envoyés à la RAM (mémoire cache).

Log File (Fichier journal) Journaux envoyés au fichier (FLASH).

Activation des journaux

1. Ouvrez la page **Global Log Parameters** (Paramètres globaux de journalisation).
2. Sélectionnez **Enable** (Activer) dans le menu déroulant **Logging** (Journalisation).
3. Sélectionnez le type de journal et le niveau de gravité à l'aide des cases à cocher.

REMARQUE : Lorsque vous sélectionnez un niveau de gravité, tous les niveaux de gravité supérieurs à ce niveau sont automatiquement sélectionnés.

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

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

Activation de la journalisation globale à l'aide de l'interface de ligne de commande

Le tableau suivant récapitule les commandes CLI applicables aux champs de la page **Global Log Parameters** (Paramètres globaux de journalisation).

Tableau 6-14. Commandes CLI Paramètres globaux de journalisation

Commande CLI	Description
`logging on`	Active la journalisation des messages d'erreur.
`logging ip-address [port port] [severity level] [facility facility] [description text]`	Consigne les messages sur un serveur syslog.
`logging Console level`	Limite les messages consignés sur la Console en fonction de leur gravité.
`logging buffered level`	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.

Vous trouverez ci-dessous un exemple de commande CLI :

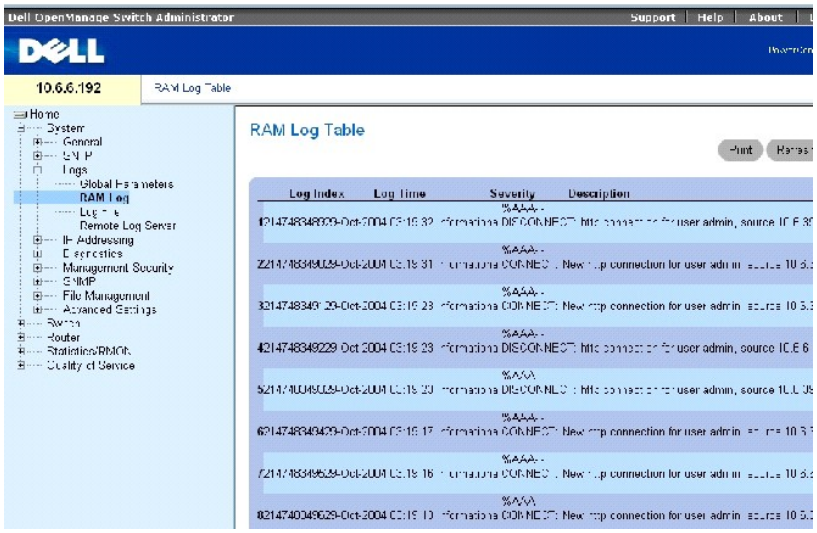
```
Console (config)# logging on

Console (config)# logging 10.1.1.1 severity critical

Console (config)# logging Console errors

Console (config)# logging buffered debugging

Console (config)# logging file alerts



Console # clear logging

Clear Logging Buffer [y/n]? y
```

Table des journaux en RAM

La page **RAM Log Table** (Table des journaux RAM) contient des informations relatives aux entrées de journaux stockées en RAM (mémoire cache), notamment l'heure de création du journal, sa gravité ou encore sa description.

Pour afficher la page **RAM Log Table** (Table des journaux RAM), cliquez sur **System** (Système)→ **Logs** (Journaux)→ **RAM Log** (Journal en RAM) dans l'arborescence (reportez-vous à la Figure 6-21).

Figure 6-21. Table des journaux en RAM



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

Log Index (Index du journal) Indique le numéro du journal dans la table des journaux en RAM.

Log Time (Heure du journal) Heure de création du journal dans la table des journaux en RAM.

Severity (Gravité) Niveau de gravité du journal.

Description Description du journal.

Suppression d'informations de journalisation

1. Ouvrez la page **RAM Log Table** (Table des journaux en RAM).
2. Cliquez sur **Clear Logs** (Effacer journaux).

Les informations de journalisation sont supprimées de la table des fichiers journaux et le périphérique est mis à jour.

Affichage de la page RAM Log Table (Table des journaux en RAM) 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 **RAM Log Table** (Table des journaux en RAM).

Tableau 6-15. Commandes CLI 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 messages du tampon de journalisation.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console # show logging

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

Buffer Logging: Level info. Buffer Messages: 30 Logged, 30 Displayed, 200 max.

File Logging: Level error. File Messages: 1 Logged, 30 Dropped.

1 messages were not logged

10-jan-2003 16:53:44 : %MSCM-I-NEWTERM : New TELNET connection from 143.166.155.18


10-Jan-2003 16:53:14 :%MSCM-I-TERMTERMINATED: TELNET connection from 143.166.155.18 terminated
```

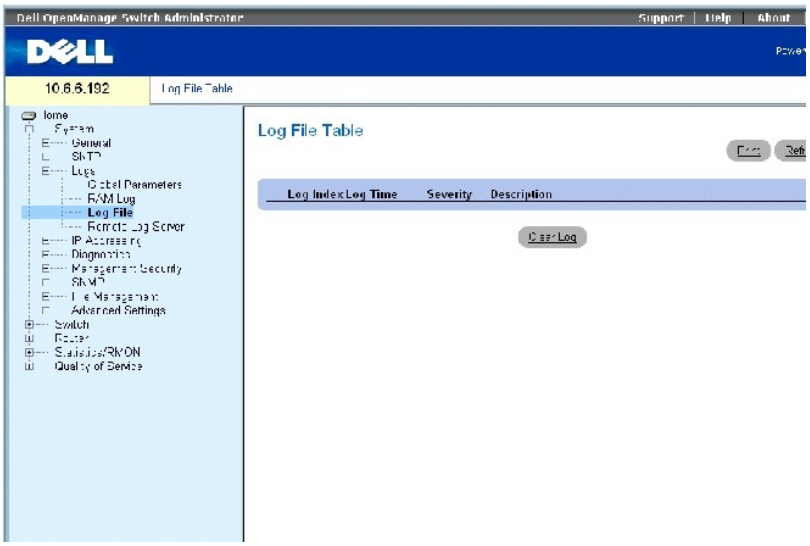
```
10-Jan-2003 16:41:26 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18


10-Jan-2003 09:24:59 :%INIT-I-Startup: Cold Startup
```

Table des fichiers journaux

La page **Log File Table** (Table des fichiers journaux) contient des informations sur des entrées de journaux spécifiques, notamment l'heure de création du journal, son niveau de gravité et sa description.

Pour afficher la page **Log File Table** (Table des fichiers journaux), cliquez sur **System** (Système)→ **Logs** (Journaux)→ **Log File** (Fichier journal) dans l'arborescence (reportez-vous au Tableau 6-22).

Figure 6-22. Table des fichiers journaux



La page **Log File Table** (Table des fichiers journaux) contient les champs suivants :

- **Log Index** (Index du journal) Numéro du journal dans la table **Log File Table** (Table des fichiers journaux).
- **Log Time** (Heure du journal) Heure de création du journal dans la table **Log File Table** (Table des fichiers journaux).
- **Severity** (Gravité) Niveau de gravité du journal.
- **Description** Description du journal.

Affichage de la table des fichiers journaux 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 **Log File Table** (Table des fichiers journaux).

Tableau 6-16. Commandes CLI Table des fichiers journaux

Commande CLI	Description
`show logging file`	Affiche l'état de la journalisation et les messages syslog stockés dans le fichier de journalisation.
	Efface les messages du tampon de journalisation.

clear logging	

Vous trouverez ci-dessous un exemple de commande CLI :

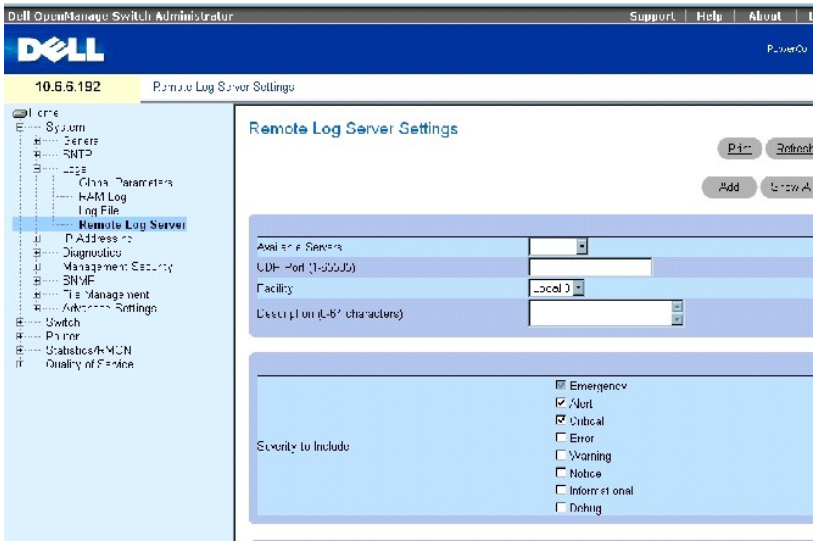
```
Console # show logging file

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

Buffer Logging: Level info. Buffer Messages: 30 Logged, 30 Displayed, 200 max.

File Logging: Level error. File Messages: 1 Logged, 30 Dropped.

1 messages were not logged

10-jan-2003 16:53:44 : %MSCM-I-NEWTERM : New TELNET connection from 143.166.155.18

10-Jan-2003 16:53:14 :%MSCM-I-TERMTERMINATED: TELNET connection from 143.166.155.18 terminated

10-Jan-2003 16:41:26 :%MSCM-I-NEWTERM: New TELNET connection from 143.166.155.18

10-Jan-2003 09:24:59 :%INIT-I-Startup: Cold Startup

10-Jan-2003 09:22:51 :%LINK-I-Up: Oob-eth 1

10-Jan-2003 09:22:51 :%LINK-W-Down: g24

10-Jan-2003 09:22:51 :%LINK-W-Down: g23

10-Jan-2003 09:22:51 :%LINK-W-Down: g22

10-Jan-2003 09:22:51 :%LINK-W-Down: g21
```

page

La page **Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance) contient des champs permettant d'afficher les serveurs de journalisation disponibles. Par ailleurs, de nouveaux serveurs de journalisation peuvent être définis ainsi que le niveau de gravité des journaux envoyés au serveur.

Pour ouvrir la page **Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance), cliquez sur **System** (Système)→ **Logs** (Journaux)→ **Remote Log Server** (Serveur de journalisation à distance).

Figure 6-23. Paramètres des serveurs de journalisation à distance



La page **Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance) contient les champs suivants :

Available Servers (Serveurs disponibles) Serveurs auxquels les journaux peuvent être envoyés.

UDP Port (1-65535) (Port UDP [1-65535]) Port UDP à partir duquel les journaux sont envoyés. La valeur par défaut est 514.

Facility (Voie de transmission) Application définie par l'utilisateur à partir de laquelle les journaux système sont envoyés au serveur distant. Une seule voie de transmission peut être affectée à 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. Les valeurs possibles pour ce champ sont **Local 0** - **Local 7**.

Description Description du serveur. La longueur maximale est de 64 caractères.

Severity (Gravité) Niveau de gravité du journal. Lorsqu'un niveau de gravité est sélectionné, tous les niveaux de gravité supérieurs à ce niveau sont automatiquement sélectionnés.

Delete Server (Supprimer serveur) Permet de supprimer un serveur de la liste **Available Server** (Serveurs disponibles). Si vous cochez cette case, le serveur est supprimé de la liste. Si vous ne cochez pas cette case, le serveur n'est pas supprimé de la liste.

La page **Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance) contient également une liste de niveaux de gravité. Ces niveaux de gravité sont les mêmes que ceux de la page **RAM Log Table** (Table des journaux en RAM).

Envoi de journaux à un serveur

1. Ouvrez la page **Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance).
2. Renseignez les champs **UDP Port** (Port UDP), **Facility** (Voie de transmission) et **Description**.

3. Sélectionnez le type de journal et le niveau de gravité à l'aide des cases à cocher **Log Parameters** (Paramètres de journalisation).

REMARQUE : Lorsque vous sélectionnez un niveau de gravité, tous les niveaux de gravité supérieurs à ce niveau sont automatiquement sélectionnés.

4. 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) pour afficher la page **Add a Log Server** (Ajout d'un serveur de journalisation).

REMARQUE : Avant d'ajouter un nouveau serveur, déterminez l'adresse IP du serveur de journalisation à distance.

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

La page **Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance) n'affiche le serveur dans la liste **Available Server** (Serveurs disponibles) qu'après l'actualisation manuelle de la page.

Suppression d'un serveur de journalisation

1. Ouvrez la page **Remote Log Server Settings** (Paramètres des serveurs de journalisation à distance).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la **page Log Server Table** (Table des serveurs de journalisation).
3. Sélectionnez un serveur et cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

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

Le tableau suivant répertorie les commandes CLI permettant d'utiliser les journaux de serveurs distants.

Tableau 6-17. Commandes CLI Serveur de journalisation à distance

Commande CLI	Description
`logging` *`ip-address`* `[port port] [severity` *`level`*`] [facility` *`facility`*`] [`*`description text`*`]`	Consigne les messages sur un serveur distant.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config) # logging 10.1.1.1 severity critical
```

Définition de l'adressage IP

La page **IP Addressing** (Adressage IP) permet d'affecter des adresses IP aux interfaces et aux passerelles par défaut et de définir des paramètres ARP et DHCP pour les interfaces.

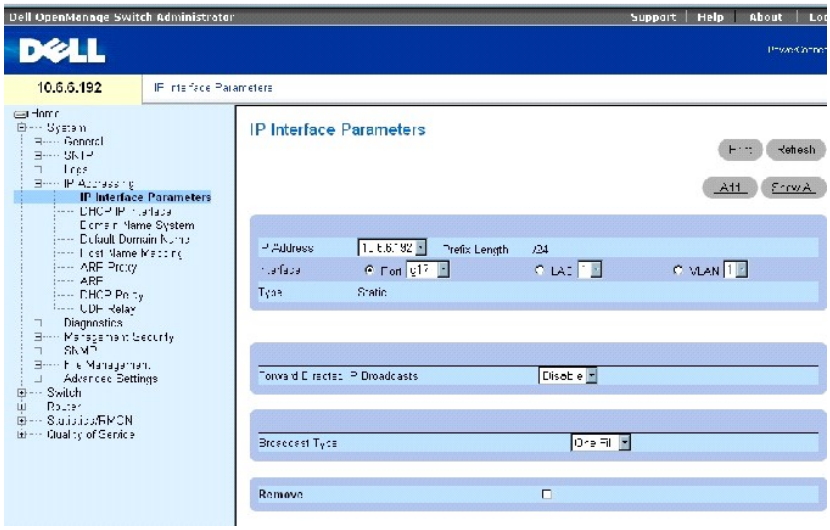
Pour ouvrir la page **IP Addressing** (Adressage IP), cliquez sur **System** (Système)→ **IP Addressing** (Adressage IP) dans l'*arborescence*.

Définition d'interfaces IP

La page **IP Interface Parameters** (Paramètres d'interface IP) contient les paramètres permettant d'affecter des adresses IP aux interfaces.

Pour ouvrir la page **IP Interface Parameters** (Paramètres d'interface IP), cliquez sur **System** (Système)→ **IP Addressing** (Adressage IP)→ **Interface Parameters** (Paramètres d'interface) dans l'*arborescence*.

Figure 6-24. Paramètres d'interface IP



La page **IP Interface Parameters** (Paramètres d'interface IP) contient les champs suivants :

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. Les valeurs possible pour ce champ sont : **Port**, **LAG** ou **VLAN**.

Pour obtenir des informations sur la configuration des groupes de liaisons agrégées (LAG), reportez-vous à la section «Agrégation des ports». Pour obtenir des informations sur la configuration des VLAN, 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 indique que l'adresse de diffusion de l'interface est du type One Fill (255.255.255.255).

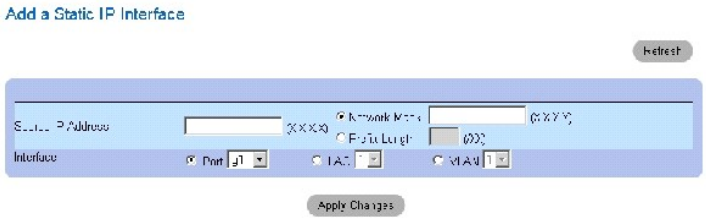
Zero Fill indique que l'adresse de diffusion de l'interface est du type Zero Fill (0.0.0.0).

Remove (Supprimer) Lorsqu'elle est cochée, cette option permet de supprimer l'interface du menu déroulant **IP Address** (Adresse IP).

Ajout d'une interface IP

1. Ouvrez la page **IP Interface Parameters** (Paramètres d'interface IP).
2. Cliquez sur **Add** (Ajouter) pour ouvrir la page **Add a Static IP Interface** (Ajout d'une interface IP statique).

Figure 6-25. Ajout d'une interface IP statique



3. Renseignez les champs de la page.

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

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

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

La nouvelle interface est ajoutée et le périphérique est mis à jour.

Modification 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) pour afficher la page **Interface Parameters Table** (Table des paramètres d'interface).
3. Sélectionnez une adresse IP et cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse IP est supprimée et le périphérique est mis à jour.

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

Le tableau suivant récapitule les commandes CLI équivalentes applicables aux champs de la page **IP Interface Parameters** (Paramètres d'interface IP).

Tableau 6-18. Commandes CLI Paramètres d'interface IP

Commande CLI	Description
`ip address ip-address {mask | prefix-length}`	Définit une adresse IP.
`no ip address [ip- address]`	Supprime une adresse IP.
`show ip interface [ethernet s | vlan vlan- id | port-channel number]`	Affiche l'état d'utilisabilité des interfaces IP.
`directed-broadcast`	Active la traduction d'une diffusion dirigée en diffusions physiques.

Vous trouverez ci-dessous un exemple de commande CLI :

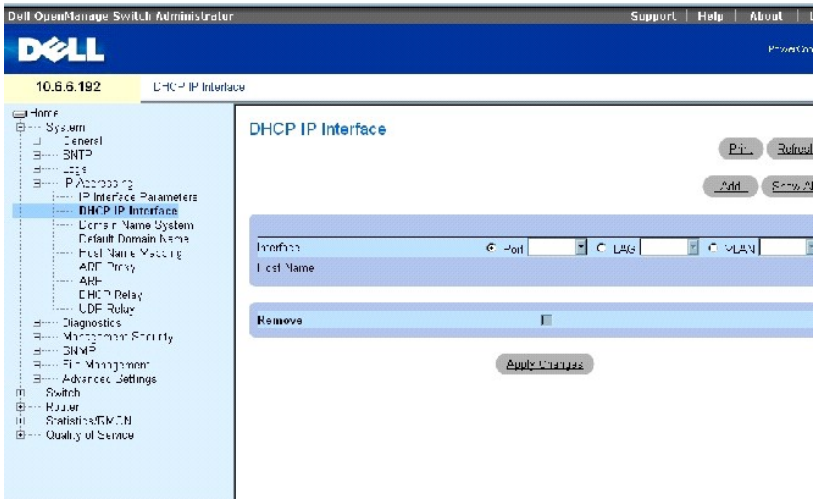
```
Console (config)# interface vlan 1

Console (config-if)# ip address 192.168.1.1 255.255.255.0

Console (config-if)# no ip address 192.168.1.1
```

Définition de paramètres d'interface IP DHCP

La page **DHCP IP Interface** (Interface IP DHCP) définit les clients DHCP connectés au périphérique.

Pour ouvrir la page **DHCP IP Interface** (Interface IP DHCP), cliquez sur **System** (Système)→ **IP Addressing** (Adressage IP)→ **DHCP IP Interface** (Interface IP DHCP) dans l'*arborescence*.

Figure 6-26. Interface IP DHCP



La page **DHCP IP Interface** (Interface IP DHCP) contient les champs suivants :

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.

Remove (Supprimer) Lorsqu'elle est cochée, cette option permet de supprimer des clients DHCP.

Ajout de clients DHCP

1. Ouvrez la page **DHCP IP Interface** (Interface IP DHCP).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add DHCP IP Interface** (Ajout d'une interface IP DHCP).
3. Renseignez les informations de cette page et 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

1. Ouvrez la page **DHCP IP Interface** (Interface IP DHCP).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **DHCP IP Interface Table** (Table des interfaces IP DHCP).
3. Sélectionnez une entrée de client DHCP.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Définition d'interfaces IP DHCP à l'aide de commandes CLI

Le tableau suivant récapitule la commande CLI permettant de définir des clients DHCP.

Tableau 6-19. Commandes d'interface IP DHCP

Commande CLI	Description
`ip address dhcp [hostname` *`hostname`*`]`	Permet d'acquérir une adresse IP sur une interface Ethernet à partir du protocole DHCP (Dynamic Host Configuration Protocol - protocole de configuration dynamique de l'hôte)

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config-if)# ip address dhcp hostname LA01
```

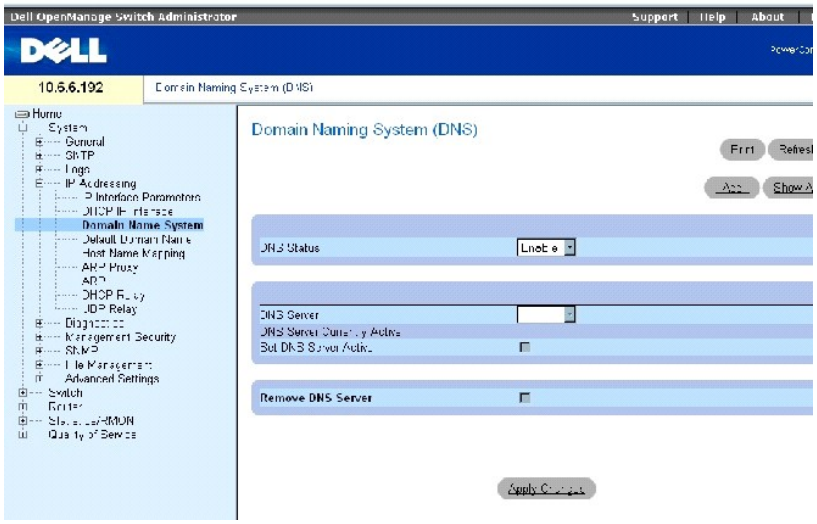
Configuration de systèmes de noms de domaine

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 noms de domaine) dans l'*arborescence*.

Figure 6-27. Système de noms de domaine (DNS)



La page **Domain Naming System (DNS)** (Système de noms de domaine (DNS)) contient les champs suivants :

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 dans la page **Add DNS Server** (Ajout d'un serveur DNS).

DNS Server Currently Active (Serveur DNS actuellement actif) Serveur DNS actuellement actif.

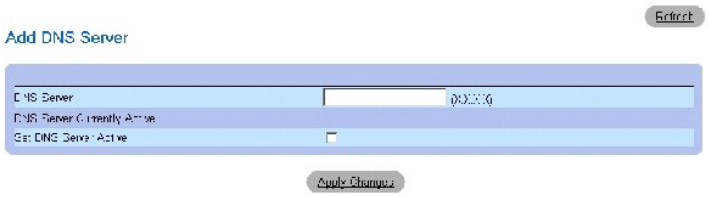
Remove DNS Server (Supprimer serveur DNS) Lorsqu'elle est cochée, cette option permet de supprimer le serveur DNS sélectionné.

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** (Ajout d'un serveur DNS) s'ouvre :

Figure 6-28. Ajout d'un serveur DNS



La page **Add DNS Server** (Ajout d'un serveur DNS) contient les champs suivants :

DNS Server (Serveur DNS) Définit l'adresse IP du serveur DNS.

DNS Server Currently Active (Serveur DNS actuellement actif) Indique le serveur DNS actuellement actif.

Set DNS Server Active (Définir le serveur DNS comme actif) Cochez cette case pour définir le serveur DNS comme étant le serveur DNS actif.

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

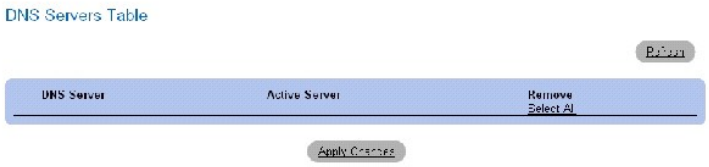
Le nouveau serveur DNS est défini et le périphérique est mis à jour.

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 page **DNS Server Table** (Table des serveurs DNS) s'ouvre :

Figure 6-29. Table des serveurs DNS



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 page **DNS Server Table** (Table des serveurs DNS) s'ouvre.
4. Sélectionnez une entrée de la table **DNS Server Table** (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 de commandes CLI

Le tableau suivant récapitule les commandes CLI permettant de configurer des serveurs DNS.

Tableau 6-20. Commandes CLI Serveur DNS

Commande CLI	Description
ip name-server *server-address*	Définit les serveurs de noms disponibles. Vous pouvez définir jusqu'à huit serveurs de noms.
no ip name-server *server-address*	Supprime un serveur de noms.
ip domain-name *name*	Définit un nom de domaine par défaut que le logiciel utilise pour compléter les noms d'hôte non qualifiés.(Plage : 1 à 158 caractères)
no ip domain-name	Supprime le nom de domaine par défaut (DNS)
clear host {name | *}	Supprime les entrées de la mémoire cache nom d'hôte-à-adresse.
show hosts [*name*]	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'hôte et des adresses.
ip domain-lookup	Active le système DNS de traduction des noms d'hôte en adresses IP.
no ip domain-lookup	Désactive le système DNS de traduction des noms d'hôte en adresses IP.

Vous trouverez ci-dessous un exemple de commande CLI :

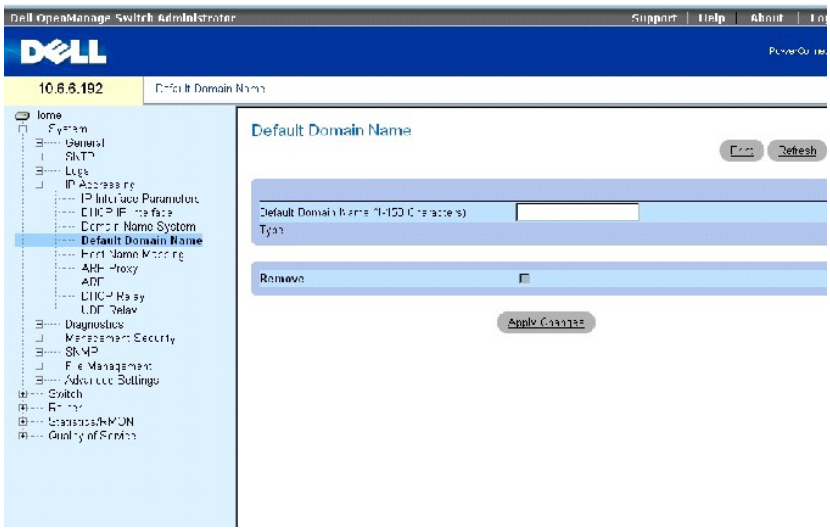
```
Console (config)# ip name-server 176.16.1.18
```

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

Figure 6-30. Nom de domaine par défaut



La page **Default Domain Name** (Nom de domaine par défaut) contient les champs suivants :

Default Domain Name (1-158 characters) (Nom de domaine par défaut [1 à 158 caractères]) Contient un serveur de noms de domaine DNS défini par l'utilisateur. Une fois configuré, le nom de domaine par défaut s'applique à tous les noms d'hôte non qualifiés.

Type Indique que le nom de domaine par défaut a été créé de façon dynamique ou statique.

Remove (Supprimer) Lorsqu'elle est sélectionnée, cette option permet de supprimer le nom de domaine par défaut.

Définition de noms de domaine DNS à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI permettant de configurer des noms de domaine DNS.

Tableau 6-21. Commandes CLI Nom de domaine DNS

Commande CLI	Description
ip domain-name name	Définit un nom de domaine par défaut que le logiciel utilise pour compléter les noms d'hôte non qualifiés.
no ip domain-name	Supprime le nom de domaine par défaut (DNS).
show hosts [*name*]	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'hôte et des adresses.

Vous trouverez ci-dessous un exemple de commande CLI :

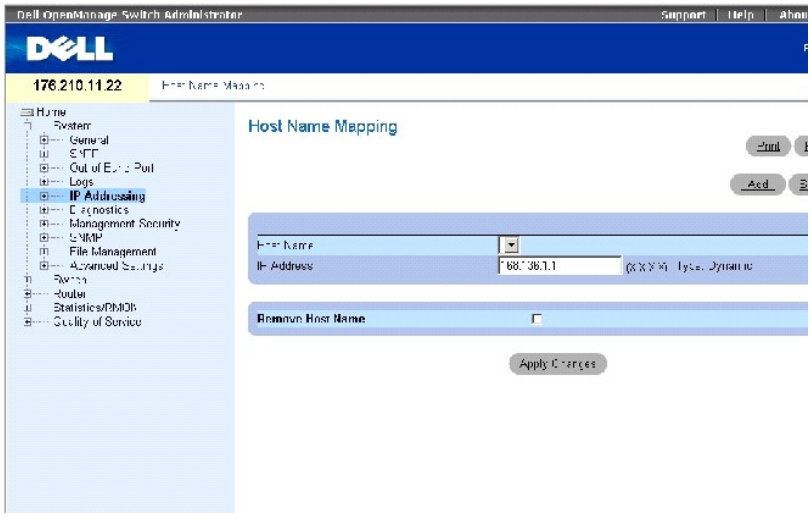
Console (config)# **ip domain-name** dell.com

Adressage d'hôtes de domaine

La page **Host Name Mapping** (Adressage de noms d'hôte) fournit des paramètres permettant d'affecter une adresse IP à un nom d'hôte statique. La page **Host Name Mapping** (Adressage de noms d'hôte) fournit une seule adresse IP par hôte.

Pour ouvrir la page **Host Name Mapping** (Adressage de noms d'hôte), cliquez sur **System** (Système)→ **IP Addressing** (Adressage IP)→ **Host Name Mapping** (Adressage de noms d'hôte).

Figure 6-31. Adressage de noms d'hôte



La page **Host Name Mapping** (Adressage de noms d'hôte) contient les champs suivants :

Host Name (Nom d'hôte) Dresse la liste des noms d'hôte. Les noms d'hôte sont définis dans la page **Add Host Name Mapping** (Ajout d'un adresse de nom d'hôte). Chaque hôte fournit une adresse IP.

IP Address (X.X.X.X) (Adresse IP [X.X.X.X]) Fournit une adresse IP assignée 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.

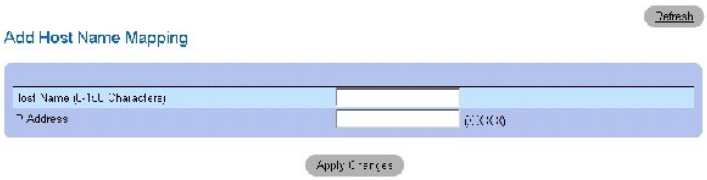
Remove Host Name (Supprimer nom d'hôte) Lorsqu'elle est cochée, cette option permet de supprimer l'adressage d'hôte DNS.

Ajout de noms de domaine d'hôte

1. Ouvrez la page **Host Name Mapping** (Adressage de noms d'hôte).
2. Cliquez sur **Add** (Ajouter).

La page **Add Host Name Mapping** (Ajout d'un adressage de nom d'hôte) s'ouvre :

Figure 6-32. Ajout d'un adressage de nom d'hôte



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

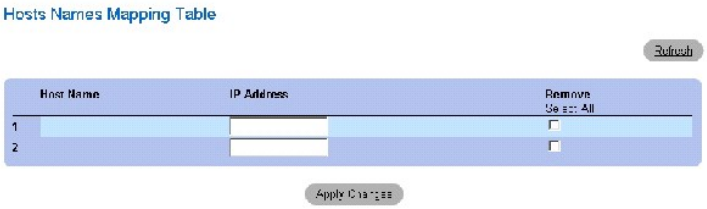
L'adresse IP est adressée au nom d'hôte et le périphérique est mis à jour.

Affiche de la table d'adressage des noms d'hôte

1. Ouvrez la page **Host Name Mapping** (Adressage de noms d'hôte).
2. Cliquez sur **Show All** (Afficher tout).

La page **Host Name Mapping Table** (Table d'adressage des noms d'hôte) s'ouvre :

Figure 6-33. Table d'adressage des noms d'hôte



Suppression d'un nom d'hôte de l'adressage des adresses IP

1. Ouvrez la page **Host Name Mapping** (Adressage de noms d'hôte).
2. Cliquez sur **Show All** (Afficher tout).

La page **Host Name Mapping Table** (Table d'adressage des noms d'hôte) s'ouvre.

3. Sélectionnez une entrée dans la table **Host Name Mapping Table** (Table de mise en correspondance des hôtes).
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée sélectionnée dans la **table d'adressage des noms d'hôte** est supprimée et le périphérique est mis à jour.

Adressage d'une adresse IP à des noms d'hôte de domaine à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'adressage de noms d'hôte de domaine à des adresses IP.

Tableau 6-22. Commandes CLI Nom d'hôte de domaine

Commande CLI	Description
`ip host name address`	Définit l'adressage statique nom d'hôte-à-adresse dans la mémoire cache de l'hôte.

no ip host namename	Supprime l'adressage nom-à-adresse.
clear host {name | *}	Supprime les entrées de la mémoire cache nom d'hôte-à-adresse.
clear host dhcp {nom | *}	Supprime les entrées reçues du protocole DHCP (Dynamic Host Configuration Protocol) de la mémoire cache nom d'hôte-à-adresse.
show hosts [*name*]	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'hôte et des adresses.

Vous trouverez ci-dessous un exemple de commande CLI :

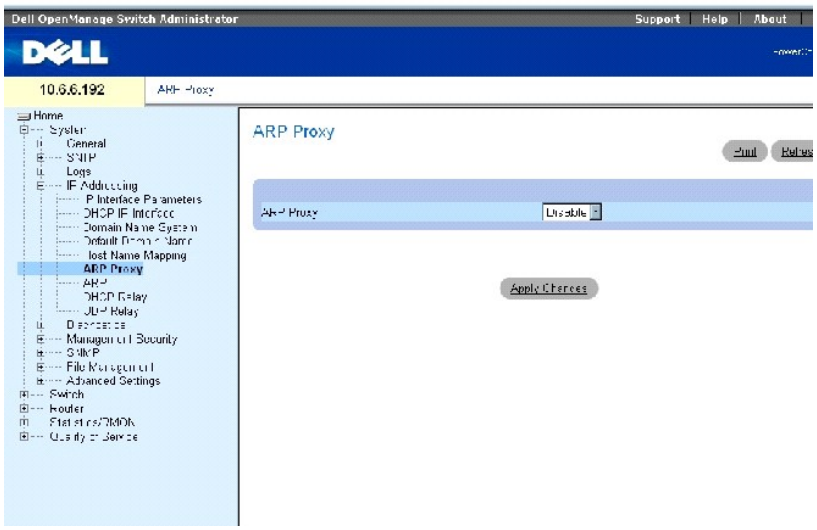
Console (config)# **ip host** accounting.abc.com 176.10.23.1

Activation du proxy ARP

Le protocole de résolution d'adresse (ARP) est un protocole TCP/IP qui convertit les adresses IP en adresses physiques. La page **ARP Proxy** (Proxy ARP) permet aux gestionnaires de réseau d'activer le proxy ARP sur le commutateur.

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

Figure 6-34. Proxy ARP



Le champ **ARP Proxy** (Proxy ARP) permet au périphérique de répondre aux demandes ARP pour les noeuds localisés. Si ce champ est désactivé, le périphérique répond avec sa propre adresse MAC.

Activation d'ARP

1. Ouvrez la page **ARP Proxy** (Proxy ARP).
2. Sélectionnez **Enabled** (Activé) dans le champ **ARP Proxy** (Proxy ARP).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le proxy ARP est activé sur le périphérique.

Activation du protocole ARP à l'aide de commandes CLI

Le tableau suivant contient les commandes CLI permettant d'activer le proxy ARP.

Tableau 6-23. Commandes CLI Proxy ARP

Commande CLI	Description
`ip proxy-arp`	Active le proxy ARP
`no ip proxy-arp`	Désactive le proxy ARP

Vous trouverez ci-dessous un exemple de commande CLI :

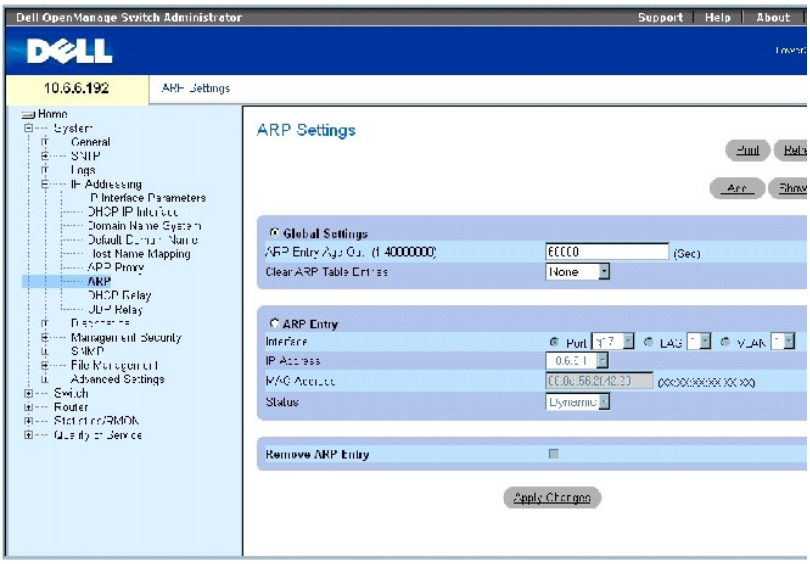
```
Console (config)# ip proxy-arp
```

Définition des paramètres ARP

La page **ARP Settings** (Paramètres ARP) permet de définir des paramètres ARP pour une interface IP. La table ARP sert à maintenir une corrélation entre chaque adresse MAC et son adresse IP correspondante. Elle peut être renseignée statiquement par l'utilisateur. Lorsqu'une entrée ARP statique est définie, une entrée permanente, qui sera utilisée par le système pour traduire les adresses IP en adresse MAC, est placée dans la table.

Pour ouvrir la page **ARP Settings** (Paramètres ARP), cliquez sur **System** (Système)→ **IP Addressing** (Adressage IP)→ **ARP** dans l'*arborescence*.

Figure 6-35. Paramètres ARP



La page **ARP Settings** (Paramètres ARP) contient les champs suivants :

Global Settings (Paramètres globaux) Sélectionnez cette option pour activer les champs des paramètres globaux ARP.

ARP Entry Age Out (0- 40000000) (Délai d'expiration de l'entrée ARP (0-40000000)) Pour tous les périphériques, durée (en secondes) qui s'écoule entre les demandes ARP portant sur une entrée de la table ARP. Ce délai écoulé, l'entrée est supprimée de la table. La plage est comprise entre 0 et 4000000, zéro indiquant que les entrées ne sont jamais effacées de la mémoire cache.

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 :

Other (Autre) L'entrée ARP n'a pas été apprise dynamiquement et n'est pas une entrée statique.

Invalid (Incorrecte) L'entrée ARP est incorrecte.

Dynamic (Dynamique) L'entrée ARP a été apprise dynamiquement.

Static (Statique) L'entrée ARP est une entrée statique.

Remove ARP Entry (Supprimer entrée ARP) Lorsqu'elle est cochée, cette option permet de supprimer une entrée ARP.

Ajout d'une entrée dans la table ARP

1. Ouvrez la page **ARP Settings** (Paramètres ARP).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add ARP Entry** (Ajout d'une entrée ARP).

Figure 6-36. Ajout d'une entrée ARP

3. Sélectionnez une interface et renseignez les champs de la page.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée statique de table ARP est ajoutée et le périphérique est mis à jour.

Modification d'une entrée de table ARP

1. Ouvrez la page **ARP Settings** (Paramètres ARP).
2. Sélectionnez une entrée de la table.
3. Modifiez les champs souhaités pour une interface donnée.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée statique de la table **ARP Table** (Table ARP) est modifiée et le périphérique est mis à jour.

Suppression d'une entrée de table ARP

1. Ouvrez la page **ARP Settings** (Paramètres ARP).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la page **ARP Table** (Table ARP).
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 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 permettant de configurer l'ARP.

Tableau 6-24. Commandes CLI Paramètres ARP

Commande CLI	Description
`arp ip_addr hw_addr {ethernet interface- number | vlan vlan-id | port-channel number | out-of-band-eth oob- interface}`	Ajoute une entrée permanente dans la mémoire cache du protocole de résolution d'adresses (ARP).
`arp timeout`	Configure la durée pendant laquelle une entrée est conservée dans la mémoire cache ARP.
`show arp`	Affiche les entrées de la table ARP.

Vous trouverez ci-dessous un exemple de commande CLI :

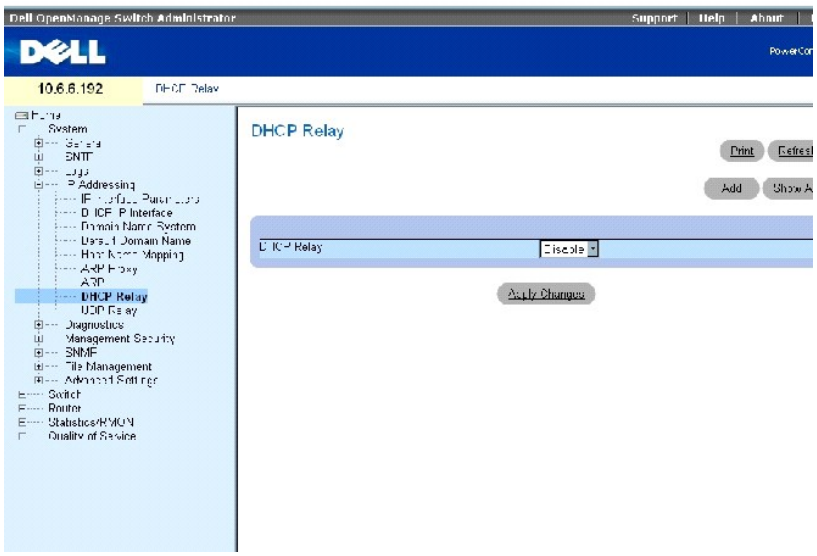
```
Console (config)# arp timeout 5


f Console (config)# arp 10.1.1.1 0060.704C.73FF ethernet g5


Console# show arp


Interface  IP Address  HW Address      Status


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


g20        10.1.1.1    0060.704c.73ff  dynamic
```

Définition des paramètres du relais DHCP

La page **DHCP Relay** (Relais DHCP) permet de fournir des informations pour l'établissement d'une configuration DHCP sur plusieurs serveurs DHCP afin d'assurer une redondance. Les adresses IP sont contrôlées et distribuées une par une pour éviter toute surcharge du périphérique.

Pour ouvrir la page **DHCP Relay** (Relais DHCP), cliquez sur **System** (Système)→ **IP Addressing** (Adressage IP)→ **DHCP Relay** (Relais DHCP) dans l'*arborescence*.

Figure 6-37. Relais DHCP



Activation du relais DHCP

1. Ouvrez la page **DHCP Relay** (Relais DHCP).
2. Sélectionnez **Enable** (Activer) dans le menu déroulant **DHCP Relay** (Relais DHCP).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée **DHCP Relay** (Relais DHCP) est ajoutée à la table des relais DHCP.

Ajout d'une entrée de relais DHCP

1. Ouvrez la page **DHCP Relay** (Relais DHCP).
2. Cliquez sur **Add** (Ajouter) pour ouvrir la page **Add DHCP Server** (Ajout d'un serveur DHCP).
3. Entrez une **valeur** dans **New DHCP Server** (Nouveau serveur DHCP).

   Les serveurs DHCP agissent comme un relais DHCP si ce paramètre n'est pas égal à 0.0.0.0. Les demandes DHCP ne sont relayées que si le contenu de leur champ SEC (secondes) est supérieur ou égal à la valeur de seuil. Les serveurs DHCP locaux peuvent ainsi répondre en premier.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

   Le serveur DHCP est ajouté à la table des relais DHCP.

Suppression d'une entrée de la table des relais DHCP

1. Ouvrez la page **DHCP Relay** (Relais DHCP).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **DHCP Servers Table** (Table des serveurs DHCP).
3. Sélectionnez un **serveur DHCP** et cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Définition des serveurs de relais DHCP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI permettant de définir des serveurs de relais DHCP.

Tableau 6-25. Commandes CLI Serveur de relais DHCP

Commande CLI	Description
`ip dhcp relay enable`	Active les fonctions de relais du protocole de configuration dynamique de l'hôte (DHCP) sur le routeur.
`ip dhcp relay address ip_address`	Définit les serveurs DHCP disponibles pour le relais DHCP.

Vous trouverez ci-dessous un exemple de commande CLI permettant d'activer le service de relais DHCP :

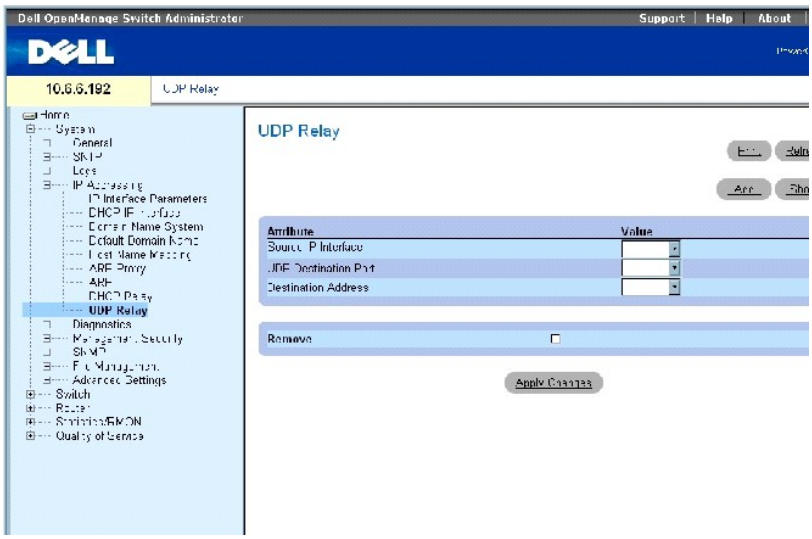
```
Console (config)# ip dhcp relay enable
```

Configuration d'un relais UDP

Le relais UDP permet aux paquets UDP d'atteindre d'autres réseaux. Cette fonction permet la navigation lorsque les stations de travail et les serveurs sont sur des réseaux différents.

Pour ouvrir la page **UDP Relay** (Relais UDP), cliquez sur **System** (Système)→ **IP Addressing** (Adressage IP)→ **UDP Relay** (Relais UDP) dans l'*arborescence*.

Figure 6-38. Relais UDP



La page **UDP Relay** (Relais UDP) contient les champs suivants :

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

0.0.0.0 à 0.255.255.255.

127.0.0.0 à 127.255.255.255.

UDP Destination Port (1-65535) (Port de destination UDP [1-65535]) Numéro d'identification du port UDP de destination des paquets UDP à relayer. Le tableau suivant répertorie les allocations de port UDP.

Tableau 6-26. Allocations de port UDP

Numéro de port UDP	Acronyme	Application
7	Echo	Echo
11	SysStat	Utilisateur actif
15	NetStat	NetStat
17	Quote	Citation du jour
19	CHARGEN	Générateur de caractères
20	FTP-data	Données FTP
21	FTP	FTP
37	Time	Temps
42	NAMESERVER	Serveur de nom d'hôte
43	NICNAME	Qui est-ce
53	DOMAIN	Serveur de nom de domaine
69	TFTP	Transfert de fichiers simple
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Temps réseau
137	NetBiosNameService	Serveur NT vers connexions de station
138	NetBiosDatagramService	Serveur NT vers connexions de station
139	NetBIOS	Serveur SessionService NT vers connexions de station
161	SNMP	Gestion de réseau simple
162	SNMP-trap	Interruptions de gestion de réseau simple
513	who	Démon Unix Rwho
514	Syslog	Journal système

525	timed	Démon temps

Destination Address (Adresse de destination) Interface IP qui reçoit les relais de paquets UDP. Si le contenu de ce champ est 0.0.0.0, les paquets UDP sont ignorés. Si le contenu de ce champ est 255.255.255.255, les paquets UDP sont acheminés par inondation vers toutes les interfaces IP.

Ajout d'une entrée de relais UDP

1. Ouvrez la page **UDP Relay** (Relais UDP).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add UDP Relay** (Ajout d'un relais UDP).
3. Entrez l'adresse IP du serveur UDP dans le champ **UDP Destination Port** (Port de destination UDP).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le serveur DHCP est ajouté à la table des relais DHCP.

Modification d'une entrée de la table des relais UDP

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

1. Ouvrez la page **UDP Relay** (Relais UDP).
2. Renseignez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée UDP est ajoutée à la table des **relais UDP** et le périphérique est mis à jour.

Suppression d'une entrée de la table des relais UDP

1. Ouvrez la page **UDP Relay** (Relais UDP).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la page **UDP Relay Table** (Table des relais UDP).
3. Sélectionnez un serveur de relais UDP et cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Configuration de la table des relais UDP à l'aide de commandes CLI

Le tableau suivant récapitule la commande CLI permettant de configurer le relais UDP.

Tableau 6-27. Commande CLI Relais UDP

Commande CLI	Description
`helper-address` *`address`* `[`*`udp-port-list`*`]`	Permet de transmettre des diffusions UDP (User Datagram Protocol - protocole de datagramme utilisateur) reçues sur une interface. Cette commande ne permet pas la transmission de paquets via BOOTP/DHCP. Pour transmettre des paquets via BOOTP/DHCP, utilisez les commandes de relais **ip dhcp relay enable**, **ip dhcp relay address** et **show ip dhcp**. Pour obtenir des informations sur ces commandes, reportez-vous à la section **Définition des paramètres de relais DHCP**.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config-ip)# helper-address 172.16.9.9 49 53
```

Exécution de diagnostics sur les câbles

La page **Diagnostics** permet d'effectuer des tests de câbles virtuels pour câbles en cuivre et en fibres optiques.

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

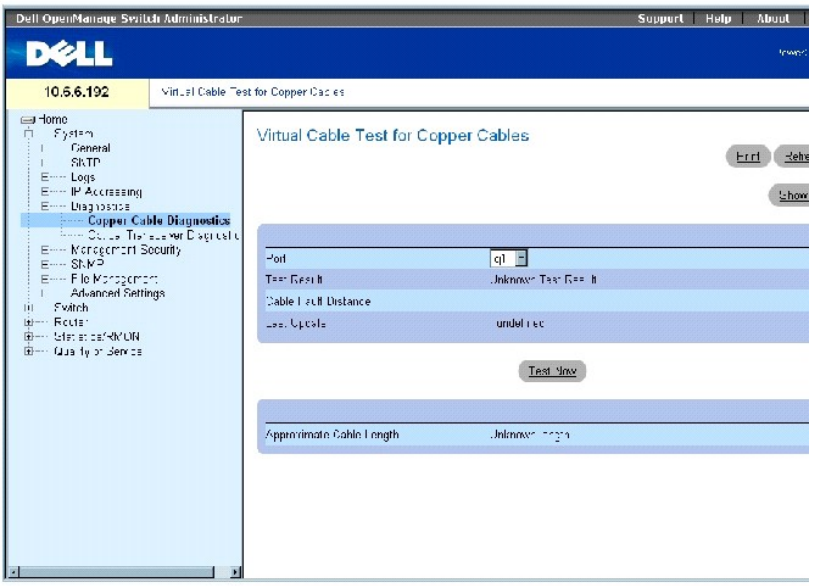
La page **Diagnostics** contient des liens vers des pages de diagnostics pour câble en cuivre et émetteurs-récepteurs optiques.

Affichage des diagnostics sur les câbles en cuivre

La page **Virtual Cable Test for Copper Cables** (Test de câbles virtuels pour câbles en cuivre) permet de tester 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 mesurant jusqu'à 120 mètres. 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 **Virtual Cable Test for Copper Cables** (Test de câbles virtuels pour câbles en cuivre), cliquez sur **System** (Système)→ **Diagnostics**→ **Copper Cable Diagnostics** (Diagnostics de câbles en cuivre) dans l'*arborescence*.

Figure 6-39. Test de câbles virtuels pour câbles en cuivre



La page **Virtual Cable Test for Copper Cables** (Test de câbles virtuels pour câbles en cuivre) contient les champs suivants :

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 est ouvert.

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 du 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 gb/s.

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 **Virtual Cable Test for Copper Cables** (Test de câbles virtuels pour câbles en cuivre).
3. Cliquez sur **Test Now** (Tester maintenant).

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

Affichage de la table des résultats des tests de câbles virtuels

1. Ouvrez la page **Virtual Cable Test for Copper Cables** (Test de câbles virtuels pour câbles en cuivre).
2. Cliquez sur **Show All** (Afficher tout) pour exécuter les tests et afficher la page **Virtual Cable Test Results Table** (Table des résultats des tests de câbles virtuels).

Réalisation de tests de câbles en cuivre à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI permettant de réaliser des tests de câbles en cuivre.

Tableau 6-28. Commandes CLI Test de câbles en cuivre

Commande CLI	Description
`test copper-port tdr`*`interface`*	Effectue les tests VCT.
`show copper-port tdr` *`interface`*	Affiche les résultats des derniers tests VCT effectués sur les ports.
`show copper-port cable-length` *`interface`*	Affiche une estimation de la longueur du câble en cuivre raccordé à un port.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# show copper-ports cable-length

Port  Length [meters]

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

g1    < 50

g2    Copper not active

g3    110-140

g4    Fiber
```

REMARQUE : La longueur de câble renvoyée par les tests VCT 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. L'écart peut être de 20 mètres maximum et la mesure de la longueur de câble ne fonctionnera pas pour les liaisons 10 Mb/s.

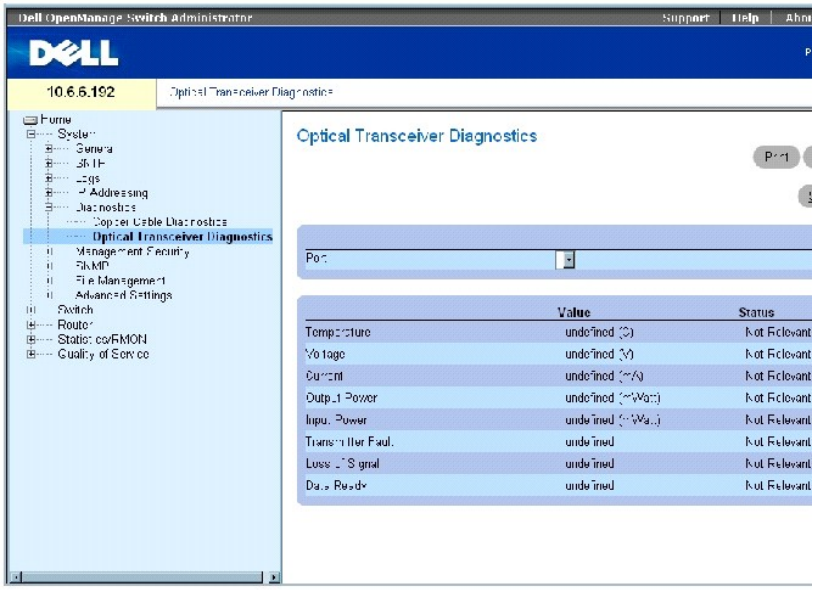
Affichage des diagnostics d'émetteurs-récepteurs optiques

La page **Optical Transceiver Diagnostics** (Diagnostics d'émetteurs-récepteurs optiques) permet de tester les 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'émetteurs-récepteurs optiques) dans l'*arborescence*.

REMARQUE : Les diagnostics d'émetteurs-récepteurs optiques ne peuvent être réalisés que si la liaison est présente.

Figure 6-40. Diagnostics d'émetteurs-récepteurs optiques



La page **Optical Transceiver Diagnostics** (Diagnostics d'émetteurs-récepteurs optiques) contient les champs suivants :

Port Adresse IP du port sur lequel le câble est testé.

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) Indique que l'émetteur-récepteur est sous tension et que 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) pour exécuter le test et ouvrir la page **Virtual Cable Test Results Table** (Table des résultats des tests de câbles virtuels).

Réalisation de tests de câbles en fibres optiques à l'aide de commandes CLI

Le tableau suivant récapitule la commande CLI permettant de réaliser des tests de câbles en fibres optiques.

Tableau 6-29. Commande CLI Test de câbles en fibres optiques

Commande CLI	Description
`show fiber-ports optical- transceiver [interface] [detailed]`	Affiche les diagnostics d'émetteurs-récepteurs optiques.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# show fiber-ports optical-transceiver
```

Les colonnes suivantes apparaissent à l'écran :

- **Temp** Température de l'émetteur-récepteur mesurée en interne
- **Voltage** (Tension) Tension d'alimentation mesurée en interne
- **Current** (Courant) Courant de polarisation de l'émetteur-transmetteur mesuré
- **Output Power** (Puissance de sortie) Puissance de sortie de l'émetteur-transmetteur en milliwatts
- **Input Power** (Puissance d'entrée) Puissance reçue de l'émetteur-récepteur mesurée en milliwatts
- **TX Fault** (Défaillance d'émetteur-transmetteur) Défaillance de l'émetteur-transmetteur

REMARQUE : Les émetteurs-récepteurs Finisar ne prennent pas en charge le diagnostic de défaillance de l'émetteur-transmetteur.

- **LOS** Perte de signal
- **Data Ready** (Données prêtes) Indique que l'émetteur-récepteur est sous tension et que les données sont prêtes
- **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) permet de définir des paramètres de gestion pour garantir la sécurité des ports, des utilisateurs et des serveurs.

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

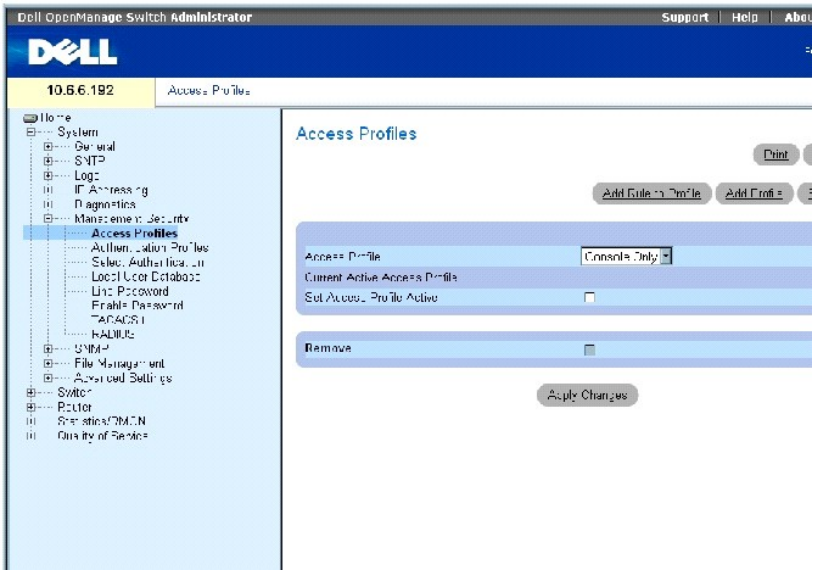
Les méthodes d'accès de gestion varient d'un groupe d'utilisateurs à un autre. Par exemple, le groupe d'utilisateurs 1 ne peut accéder au périphérique que via une session HTTP alors que le groupe d'utilisateur 2 peut y accéder par le biais de sessions HTTP et Telnet.

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) permet de configurer des listes de gestion et d'appliquer ces listes à des interfaces spécifiques.

Pour ouvrir la page **Access Profiles** (Profils d'accès), cliquez sur **System** (Système)→ **Management Security** (Sécurité de gestion)→ **Access Profiles** (Profils d'accès) dans l'*arborescence*.

Figure 6-41. Profils d'accès



Access Profile (Profil d'accès) Dresse la liste de tous les profils d'accès. La valeur par défaut est **Console Only** (Console uniquement), 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 actuellement actif) Profil d'accès actuellement actif.

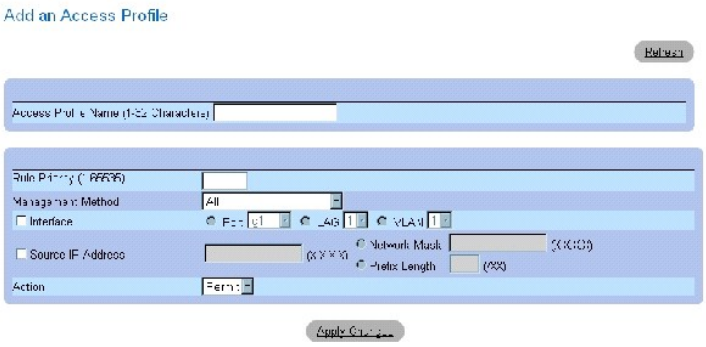
Set Access Profile Active (Définir le profil d'accès comme actif) Active un profil d'accès.

Remove (Supprimer) Lorsqu'elle est cochée, cette option permet de supprimer un profil d'accès de la liste **Access Profile Name** (Nom des profils d'accès).

Ajout d'un profil d'accès

1. Ouvrez la page **Access Profiles** (Profils d'accès).
2. Cliquez sur **Add Profile** (Ajouter un profil) pour ouvrir la page **Add an Access Profile** (Ajout d'un profil d'accès).

Figure 6-42. Ajout d'un profil d'accès



La page **Add an Access Profile** (Ajout d'un profil d'accès) contient les champs suivants :

Access Profile Name (Nom du profil d'accès) Nom du profil d'accès défini par l'utilisateur.

Rule Priority (Priorité de la règle) Indique la 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 **Profile Rules** (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. Tapez le nom du profil dans la zone de texte **Access Profile Name** (Nom du profil d'accès).
4. Renseignez les champs et cliquez sur **Apply Changes** (Appliquer les modifications).

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

Activation d'un profil d'accès

1. Ouvrez la page **Access Profiles** (Profils d'accès).
2. Sélectionnez un profil d'accès dans la liste.
3. Cochez la case **Set Access Profile Active** (Définir le profil d'accès comme actif).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

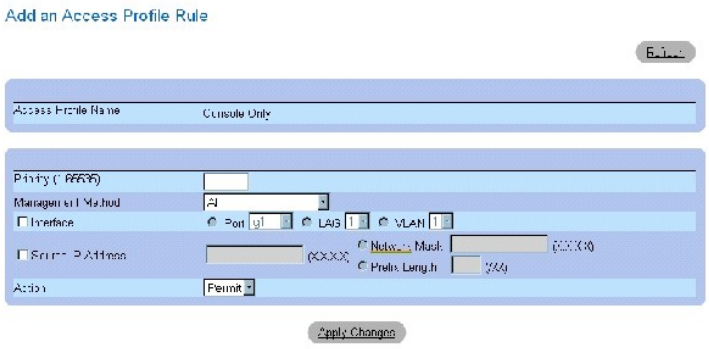
Le profil d'accès est activé pour l'utilisateur.

Ajout de règles à un profil d'accès

1. Ouvrez la page **Access Profiles** (Profils d'accès).
2. Sélectionnez un **profil d'accès** dans le menu déroulant.

   Il s'agit du profil auquel les règles sont ajoutées lorsque la page **Add An Access Profile Rule** (Ajout d'une règle à un profil d'accès) est ouverte.
3. Cliquez sur **Add Rule to Profile** (Ajouter une règle au profil) pour ouvrir la page **Add An Access Profile Rule** (Ajout d'une règle à un profil d'accès).

Figure 6-43. Ajout d'une règle à un profil d'accès



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

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

Suppression d'une règle

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

   La règle 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 de profils d'accès.

Tableau 6-30. Commandes CLI Profil d'accès

Commande CLI	Description
`management access-list` *name* **REMARQUE :** Mettre le *n o m* entre guillemets s'il contient des espaces. Exemple : «groupe de travail 1»	Définit une liste d'accès de gestion et crée le contexte de la liste d'accès pour la configuration.
`permit [ethernet` *interface- number* `| vlan` *vlan-id* `| port- channel` *number*`]` `[service` *service*`]`	Définit des conditions d'autorisation de port pour la liste d'accès de gestion.

permit ip-source ip-address [mask mask | *prefix-length*] [ethernet *interface-number* | vlan *vlan-id* | port-channel *number*] [service *service*]	Définit des conditions d'autorisation de port pour la liste d'accès de gestion et la méthode de gestion sélectionnée.
deny [ethernet *interface- number* | vlan *vlan-id* | port- channel *number*] [service *service*]	Définit des conditions de refus de port pour la liste d'accès de gestion et la méthode de gestion sélectionnée.
deny ip-source ip-address [mask mask | *prefix-length*] [ethernet *interface-number* | vlan *vlan-id* | port-channel *number*] [service *service*]	Définit des conditions de refus de port pour la liste d'accès de gestion et la méthode de gestion sélectionnée.
management access-class {Console-only | *name*}	Définit la liste d'accès utilisée pour les connexions de gestion actives.
show management access-list [*name*]	Affiche les listes d'accès de gestion actives.
show management access-class	Affiche des informations sur la classe d'accès de gestion.

Vous trouverez ci-dessous un exemple de commande CLI :

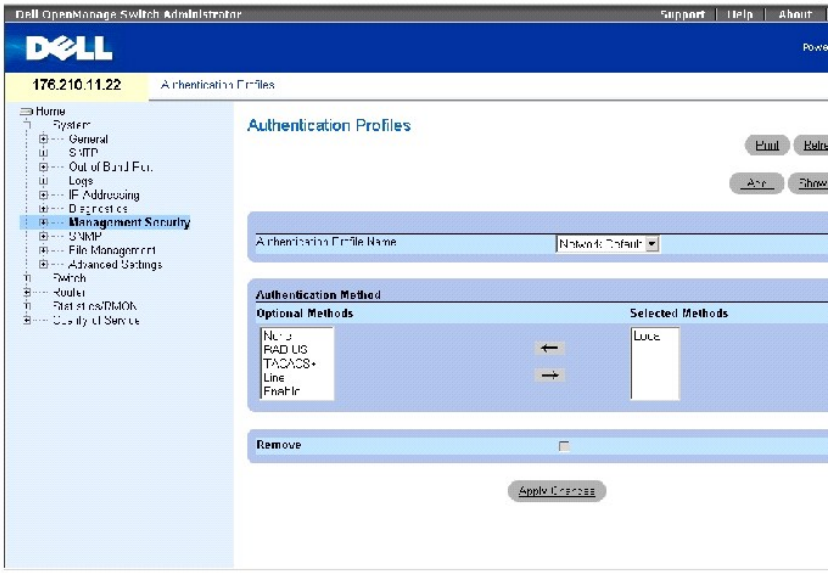
```
Console (config)# management access-list mlist

Console (config-macl)# permit ethernet g1

Console (config-macl)# permit ethernet g9

Console (config-macl)# exit

Console# show management access-class

Management access-class is enabled, using access list mlist
```

Définition de profils d'authentification

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

Pour 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 6-44. Profils d'authentification



La page **Authentication Profiles** (Profils d'authentification) contient les champs suivants :

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) Authentification des utilisateurs 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 sur les serveurs RADIUS, reportez-vous à la section «**Configuration des paramètres RADIUS**».

TACACS+ L'authentification des utilisateurs est effectuée sur le serveur TACACS+. Pour plus d'informations sur les serveurs TACACS+, reportez-vous à la section «**Configuration des paramètres TACACS+**».

Line (Ligne) Le mot de passe de ligne est utilisé pour l'authentification.

Enable (Activer) Le mot de passe d'activation est utilisé pour l'authentification.

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

Selected Methods (Méthodes sélectionnées) Méthodes d'authentification sélectionnées.

Ajout d'un profil d'authentification

1. Ouvrez la page **Authentication Profiles** (Profils d'authentification).

2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add Authentication Profile** (Ajout d'un profil d'authentification).
3. Entrez le nom du profil (1 à 12 caractères) dans le champ **Profile Name** (Nom du profil).

REMARQUE : Le nom du profil ne doit pas comprendre d'espaces.

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

Des sessions sont affectées à un profil d'authentification.

Sélection d'une méthode d'authentification

1. Ouvrez la page **Authentication Profiles** (Profils d'authentification).
2. Sélectionnez un élément dans la liste du champ **Authentication Profile Name** (Nom du profil d'authentification).
3. Sélectionnez une **méthode facultative** à l'aide des flèches.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Suppression d'une entrée de profils d'authentification

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

La table **Authentication Profiles** (Profils d'authentification) s'ouvre.

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

L'entrée est supprimée.

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

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition de profils d'authentification.

Tableau 6-31. Commandes CLI Profil d'authentification

Commande CLI	Description
`aaa authentication login {default | list-name} method1 [method2...]`	Configure l'authentification des connexions.
`no aaa authentication login {default | list-name}`	Supprime un profil d'authentification des connexions.
`show authentication methods`	Affiche des informations sur les méthodes d'authentification.

Vous trouverez ci-dessous un exemple de commande CLI :

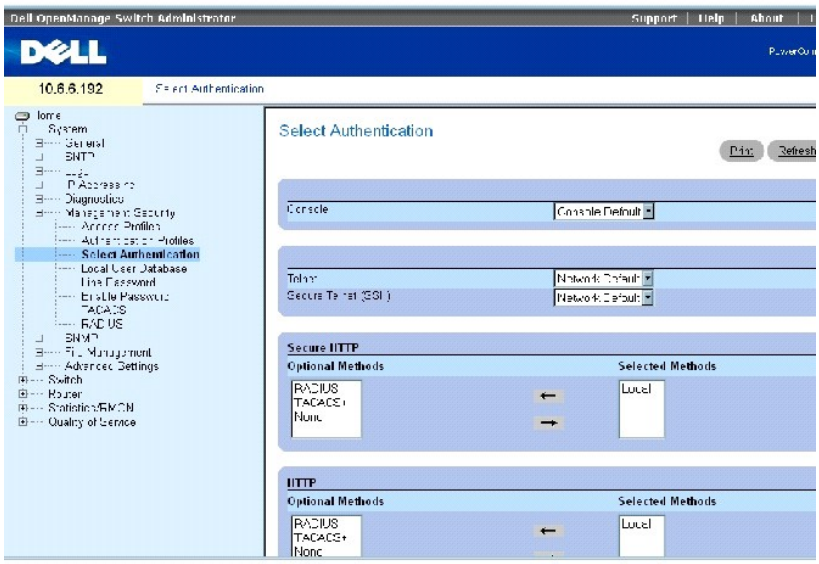
```
Console (config)# aaa authentication login default radius local enable none

Console (config)# no aaa authentication login default
```

Sélection de profils d'authentification

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

Pour ouvrir la page **Select Authentication** (Sélection d'une authentification), cliquez sur **System** (Système)→ **Management Security** (Sécurité de gestion)→ **Select Authentication** (Sélectionner une authentification) dans l'*arborescence*.

Figure 6-45. Sélection d'une authentification



La page **Select Authentication** (Sélection d'une authentification) contient les champs suivants :

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 distante 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+.

Local, None (Locale, aucune) Authentification effectuée localement dans un premier temps. Si l'authentification ne peut pas être vérifiée, aucune méthode d'authentification n'est utilisée.

RADIUS, None (RADIUS, aucune) Authentification effectuée au niveau du serveur RADIUS dans un premier temps. Si l'authentification ne peut pas être vérifiée, aucune méthode d'authentification n'est utilisée.

TACACS+, None (TACACS+, aucune) Authentification effectuée au niveau du serveur TACACS+ dans un premier temps. Si l'authentification ne peut pas être vérifiée, aucune méthode d'authentification n'est utilisée.

Local, RADIUS (Locale, RADIUS) Authentification effectuée localement dans un premier temps. Si l'authentification ne peut pas être vérifiée localement, le serveur RADIUS authentifie la méthode de gestion. Si le serveur RADIUS ne peut pas authentifier la méthode de gestion, la session est bloquée.

Local, TACACS+ (Locale, TACACS+) Authentification effectuée localement dans un premier temps. Si l'authentification ne peut pas être vérifiée localement, le serveur TACACS+ authentifie la méthode de gestion. Si le serveur TACACS+ ne peut pas authentifier la méthode de gestion, la session est bloquée.

RADIUS, Local (RADIUS, locale) Authentification effectuée au niveau du serveur RADIUS dans un premier temps. Si l'authentification ne peut pas être vérifiée au niveau du serveur RADIUS, la session est authentifiée localement. Si la session ne peut pas être authentifiée localement, la session est bloquée.

TACACS+, Local (TACACS+, locale) Authentification effectuée au niveau du serveur TACACS+ dans un premier temps. Si l'authentification ne peut pas être vérifiée au niveau du serveur TACACS+, la session est authentifiée localement. Si la session ne peut pas être authentifiée localement, la session est bloquée.

Local, RADIUS, None (Locale, RADIUS, aucune) Authentification effectuée localement dans un premier temps. Si l'authentification ne peut pas être vérifiée localement, le serveur RADIUS authentifie la méthode de gestion. Si le serveur RADIUS ne peut pas authentifier la méthode de gestion, la session est autorisée.

RADIUS, Local, None (RADIUS, locale, aucune) Authentification effectuée au niveau du serveur RADIUS dans un premier temps. Si l'authentification ne peut pas être vérifiée au niveau du serveur RADIUS, la session est authentifiée localement. Si la session ne peut pas être authentifiée localement, la session est autorisée.

Local, TACACS+, None (Locale, TACACS+, aucune) Authentification effectuée localement dans un premier temps. Si l'authentification ne peut pas être vérifiée localement, le serveur TACACS+ authentifie la méthode de gestion. Si le serveur TACACS+ ne peut pas authentifier la méthode de gestion, la session est autorisée.

TACACS+, Local, None (TACACS+, locale, aucune) Authentification effectuée au niveau du serveur TACACS+ dans un premier temps. Si l'authentification ne peut pas être vérifiée au niveau du serveur TACACS+, la session est authentifiée localement. Si la session ne peut pas être authentifiée localement, la session est autorisée.

Application d'une liste de méthodes 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 de méthodes 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).

Un profil d'authentification est affecté à des sessions de Console.

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

Un profil d'authentification est affecté à des 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. Sous HTTP, sélectionnez une méthode d'authentification dans le champ **Optional Methods** (Méthodes optionnelles) et cliquez sur le bouton flèche droite.

La méthode d'authentification sélectionnée passe dans le champ Selected Methods (Méthodes sélectionnées).

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

La 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. Sous **Secure HTTP** (HTTP sécurisé), sélectionnez une méthode d'authentification dans le champ **Optional Methods** (Méthodes optionnelles) et cliquez sur le bouton flèche droite.

La méthode d'authentification sélectionnée passe dans le champ Selected Methods (Méthodes sélectionnées).

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

La séquence d'authentification est affectée à des sessions HTTP sécurisées.

Affectation de profils ou de séquences d'authentification de méthodes d'accès

Le tableau suivant récapitule les commandes CLI pour l'affectation de méthodes d'accès, de listes de méthodes d'authentification ou de séquences.

Tableau 6-32. Commandes CLI Méthodes d'accès

Commande CLI	Description
`enable authentication {default | list-name}`	Définit la liste de méthodes d'authentification à utiliser lorsque l'utilisateur accède à des niveaux de privilèges supérieurs sur une Console ou une session Telnet à distance.
`login authentication {default | list-name}`	Définit la liste de méthode d'authentification pour une Console ou une session Telnet à distance.
	Définit les méthodes d'authentification pour les utilisateurs de serveurs http.

ip http authentication method1 [*method2...*]	
ip https authentication method1 [*method2...*]	Définit les méthodes d'authentification pour les utilisateurs de serveurs https.
show authentication methods	Affiche des informations sur les méthodes d'authentification.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# show authentication methods

Login Authentication Method Lists

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

VDefault : Local



Enable Authentication Method Lists

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

Console_Default : Enable None

Network_Default : Enable



Line      Login Method List    Enable Method List

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

Console   Default              Default

Telnet    Default              Default

SSH       Default              Default



http : Local

https : Local
```

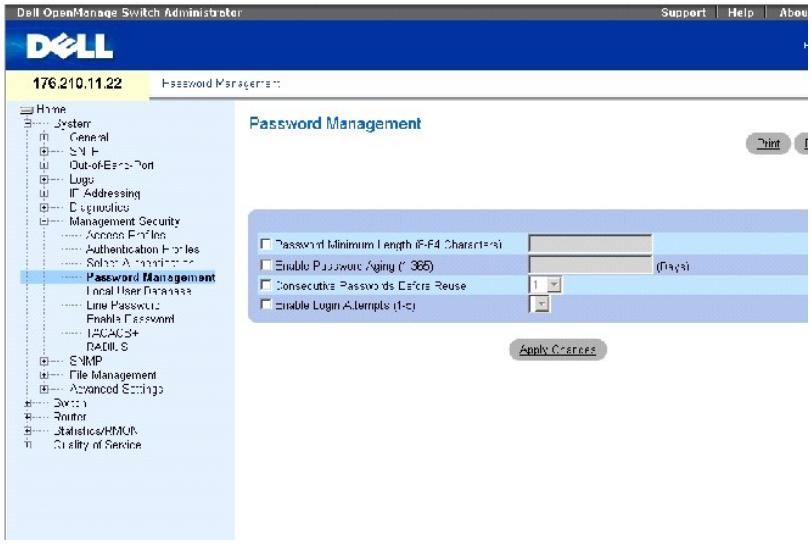
Gestion des mots de passe

La gestion du mot de passe offre une sécurité réseau accrue et un contrôle amélioré du mot de passe. Les mots de passe d'accès SSH, Telnet, HTTP, HTTPS et SNMP sont des fonctions de sécurité affectées, comprenant :

- Définition des longueurs minimales de mot de passe
- Expiration du mot de passe
- Interdiction de réutiliser fréquemment les mêmes mots de passe
- Verrouillage des utilisateurs en cas d'échec des tentatives de connexion

Pour ouvrir la page **Password Management** (Gestion du mot de passe), cliquez sur **System** (Système)→ **Management Security** (Sécurité de gestion)→ **Password Management** (Gestion du mot de passe) dans l'*arborescence*.

Figure 6-46. Gestion du mot de passe



La page **Password Management** (Gestion du mot de passe) contient les champs suivants :

Password Minimum Length (8-64 Characters) (Longueur minimale du mot de passe [8-64 caractères]) Lorsqu'elle est cochée, cette option indique le nombre minimum de caractères que doit comporter le mot de passe. Par exemple, l'administrateur peut définir que tous les mots de passe de ligne doivent comprendre au moins 10 caractères.

Enable Password Aging (1-365) (Activer l'expiration du mot de passe) Lorsqu'elle est cochée, cette option indique le délai qui s'écoule avant l'expiration du mot de passe. Les valeurs possibles sont comprises entre 1 et 365 jours.

Consecutive Passwords Before Reuse (Mots de passe consécutifs avant réutilisation) Indique le nombre de mots de passe différents devant être définis avant qu'un ancien mot de passe puisse être réutilisé. Les valeurs possibles sont comprises entre 1 et 10.

REMARQUE : L'utilisateur est prévenu qu'il doit modifier le mot de passe avant que celui-ci n'expire. Les utilisateurs Web ne visualisent pas cette notification.

Enable Login Attempts (1-5) (Nombre de tentatives de connexion autorisées) Lorsqu'elle est sélectionnée, cette option permet de verrouiller un utilisateur lorsque celui-ci tente de se connecter avec un mot de passe inapproprié un nombre de fois supérieur à celui défini. Par exemple, si le nombre maximum de tentatives de connexion a été défini sur cinq et que l'utilisateur tente de se connecter cinq fois en utilisant un mot de passe non valide, le périphérique verrouille l'utilisateur à la sixième tentative. La plage de valeur pour ce champ est comprise entre 1 et 5.

Définition des contraintes de mot de passe

1. Ouvrez la page **Password Management** (Gestion du mot de passe).
2. Renseignez les champs concernés.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Définition de contraintes de mot de passe à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des mots de passe de la page **Password Management** (Gestion du mot de passe).

Tableau 6-33. Commandes CLI Gestion du mot de passe

Commande CLI	Description
`password min-length length`	Définit la longueur minimale requise pour les mots de passe.
`passwords aging days`	Définit le délai d'expiration des mots de passe de la base de données locale.
`passwords history number`	Définit le nombre de modifications de mot de passe requises pour qu'un mot de passe de la base de données locale puisse être réutilisé
`passwords lock-out number`	Verrouille un compte utilisateur au bout d'un certain nombre de tentatives de connexion infructueuses.
`show password configuration`	Affiche des informations sur la gestion du mot de passe.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# password min-length 8

Console (config)# password aging 120

Console (config)# passwords history 2

Console (config)# passwords lock-out 3

Console (config)# exit

Console# show passwords configuration

Minimal length: 8

Aging: 120 days

History: 2
```

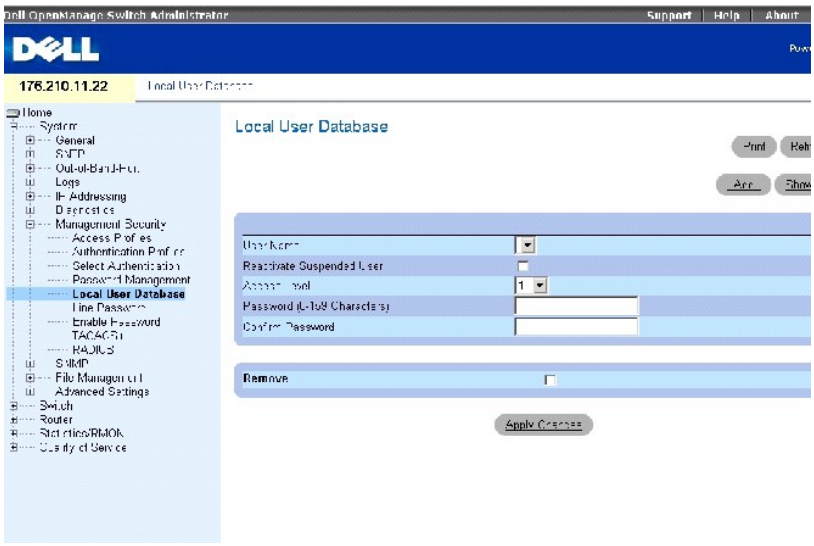
```
Lock-out: Disabled
```

Définition des bases de données d'utilisateurs locales

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

Pour ouvrir la page **Local User Database** (Base de données d'utilisateurs locale), cliquez sur **System** (Système)→ **Management Security** (Sécurité de gestion) → **Local User Database** (Base de données d'utilisateurs locale) dans l'*arborescence*.

Figure 6-47. Base de données d'utilisateurs locale



La page **Local User Database** (Base de données d'utilisateurs locale) contient les champs suivants :

User Name (Nom d'utilisateur) Liste d'utilisateurs.

Reactivated Suspended User (Utilisateur suspendu réactivé) Permet de réactiver les droits d'accès d'un utilisateur donné. Les droits d'accès peuvent avoir été suspendus suite à une tentative de connexion infructueuse.

Access Level (1-15) (Niveau d'accès) Niveau d'accès des utilisateurs, le niveau le plus faible étant **1** et le niveau le plus élevé étant **15**.

Password (Mot de passe) Mot de passe défini par l'utilisateur.

Confirm Password (Confirmer le mot de passe) Confirme le mot de passe défini par l'utilisateur.

Remove (Supprimer) supprime des utilisateurs de la liste **User Name** (Noms d'utilisateur).

Affectation de droits d'accès à un utilisateur

1. Ouvrez la page **Local User Database** (Base de données d'utilisateurs locale).

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 de l'utilisateur sont définis et le périphérique est mis à jour.

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

1. Ouvrez la page **Local User Database** (Base de données d'utilisateurs locale).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add User** (Ajout d'un utilisateur).
3. Renseignez les champs.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

REMARQUE : Vous pouvez définir jusqu'à 30 utilisateurs sur le périphérique.

Réactivation d'un utilisateur suspendu

1. Ouvrez la page **Local User Database** (Base de données d'utilisateurs locale).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la **page Local User Table** (Table des utilisateurs locaux).
3. Sélectionnez une entrée dans le champ **User Name** (Nom d'utilisateur).
4. Cochez la case Reactivate Suspended User (Réactiver l'utilisateur suspendu).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les droits d'accès de l'utilisateur sont réactivés et le périphérique est mis à jour.

Suppression d'utilisateurs de la base de données d'utilisateurs locale

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

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

Affectation d'utilisateurs à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affichage des champs de la page **Local User Database** (Base de données d'utilisateurs locale).

Tableau 6-34. Commandes CLI Base de données d'utilisateurs locale

Commande CLI	Description
`username name [password password] [privilege level] [encrypted]`	Définit un système d'authentification reposant sur le nom des utilisateurs.
`set username name active`	Réactive un compte utilisateur verrouillé.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)#username bob password lee privilege 15
```

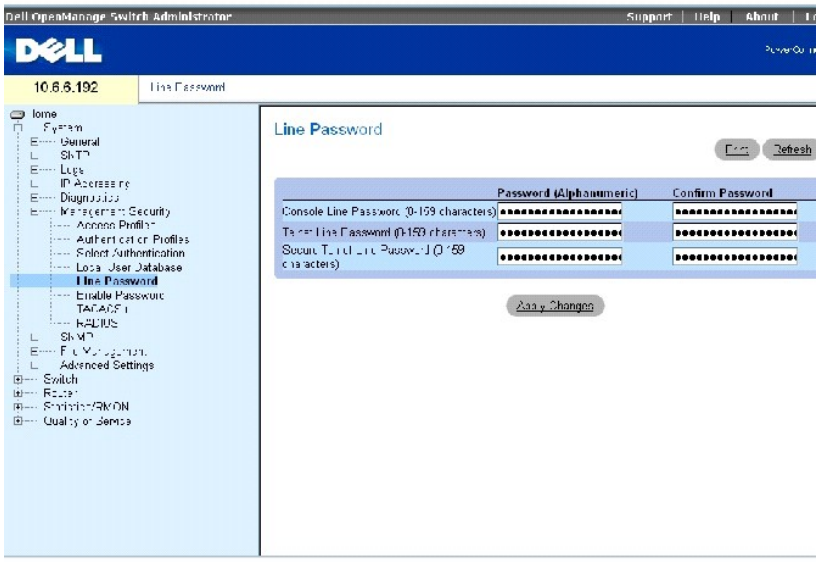
```
Console# set username bob active
```

Définition de mots de passe de ligne

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

Pour ouvrir la page **Line Password** (Mot de passe de ligne), cliquez sur **System**→ **Management Security**→ **Line Password** (Système→ Sécurité de gestion→ Mot de passe de ligne) dans l'*arborescence*.

Figure 6-48. Mot de passe de ligne



La page **Line Password** (Mot de passe de ligne) contient les champs suivants :

Line Password for Console/Telnet/Secure Telnet (Mot de passe de ligne pour la Console/Telnet/Telnet sécurisé) Mot de passe de ligne permettant d'accéder au périphérique via une Console, Telnet ou une session Telnet sécurisée.

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

1. Ouvrez la page **Line Password** (Mot de passe de ligne).
2. Renseignez le champ **Line Password** (Mot de passe de ligne) pour le type de session que vous utilisez pour vous connecter au périphérique.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mot de passe de ligne pour le type de session utilisée 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 définition de mots de passe de ligne.

Tableau 6-35. Commandes CLI Mot de passe de ligne

Commande CLI	Description
`password password [encrypted]`	Définit un mot de passe de ligne.

Vous trouverez ci-dessous un exemple de commande CLI :

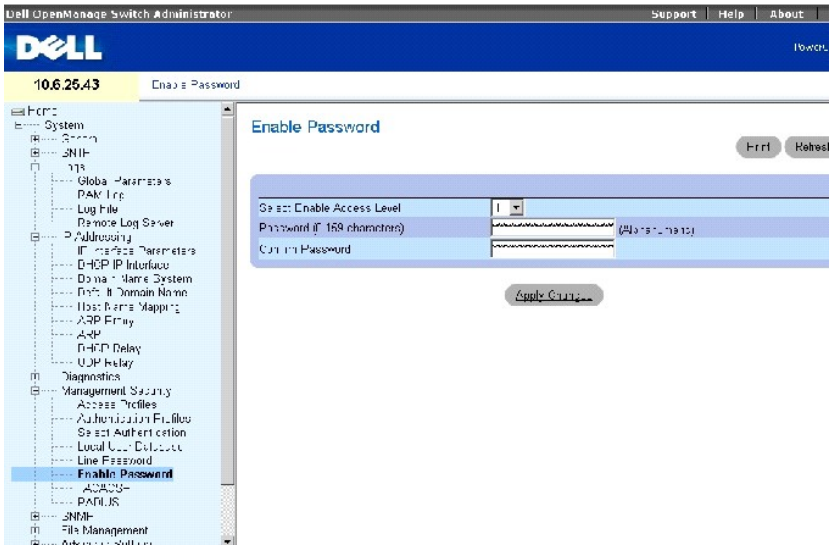
```
Console (config-line)# password ****
```

Définition du mot de passe d'activation

La page **Modify Enable Password** (Modification du mot de passe d'activation) permet de définir un mot de passe local pour contrôler l'accès aux différents niveaux de privilège (1-15).

Pour ouvrir la page **Modify Enable Password** (Modification du mot de passe d'activation), cliquez sur **System** (Système)→ **Management Security** (Sécurité de gestion)→ **Enable Password** (Mot de passe d'activation) dans l'*arborescence*.

Figure 6-49. Modification du mot de passe d'activation



La page **Modify Enable Password** (Modification du mot de passe d'activation) contient les champs suivants :

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 (Mot de passe) Mot de passe d'activation actuel.

Confirm Password (Confirmer le mot de passe) Confirme 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** (Modification du mot de passe d'activation).
2. Renseignez les champs de la boîte de dialogue.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le nouveau mot de passe 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** (Modification du mot de passe d'activation).

Tableau 6-36. Commandes CLI Mot de passe d'activation

Commande CLI	Description
`enable password [level level] password [encrypted]`	Définit un mot de passe local pour contrôler l'accès aux utilisateurs et niveaux de privilèges.
`show users accounts`	Affiche des informations sur la base de données d'utilisateurs locale.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# enable password level 15 dell

Console# show users accounts

Username   Privilege

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

Bob        15

Jim        15

Dell       1515
```

Configuration des paramètres TACACS+

Le périphérique offre 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 :

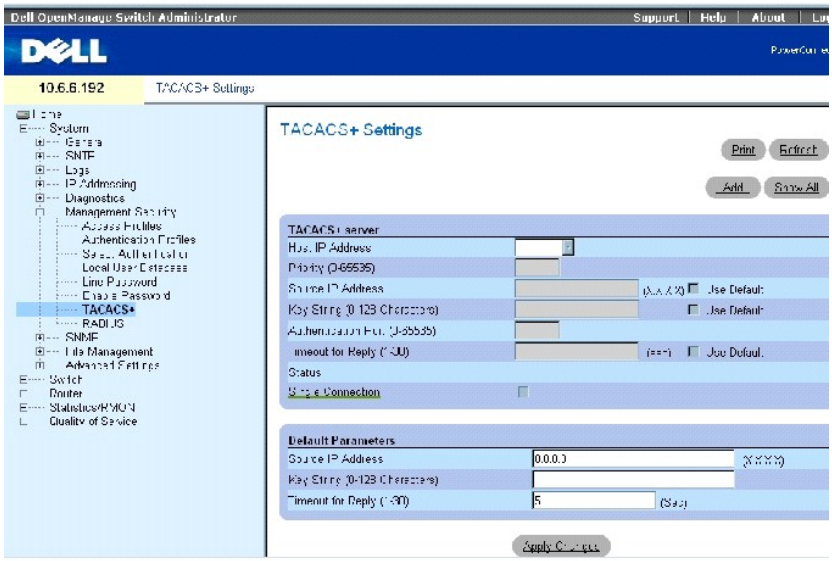
- **Authentication** (Authentification) Permet une authentification pendant la connexion par le biais des noms d'utilisateur et des mots de passe définis par les utilisateurs.
- **Authorization** (Autorisation) Réalisée à la connexion. Une fois l'authentification terminée, une session d'autorisation 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+.

La page **TACACS+ Settings** (Paramètres TACACS+) contient les paramètres TACACS+ définis par l'utilisateur et par défaut du port de gestion intrabande.

Pour ouvrir la page **TACACS+ Settings** (Paramètres TACACS+), cliquez sur **System** (Système)→ **Management Security** (Sécurité de gestion)→ **TACACS+** dans l'*arborescence*.

Figure 6-50. Paramètres TACACS+



La page **TACACS+ Settings** (Paramètres TACACS+) contient les champs suivants :

Host IP Address (Adresse IP hôte) Adresse IP du serveur TACACS+.

Priority (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 (Clé de codage) (0-128 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 (Port d'authentification) (0 à 65535) Numéro du port par où passe la session TACACS+. Le port 49 est le port par défaut.

Timeout FOR Reply (1_30) (Délai de réponse [1-30]) 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 (Clé de codage) (0-128 caractères) Clé d'authentification et de cryptage par défaut des communications TACACS+ entre le périphérique et le serveur TACACS+.

Timeout for Reply (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+.

REMARQUE : Les paramètres par défaut mentionnés ci-dessus s'appliquent également à la page **OOB TACACS+ Settings** (Paramètres TACACS+ OOB) (**System** (Système)→ **Out-of- Band-Port** (Port hors bande)→ **TACACS+**).

Définition des paramètres TACACS+

1. Ouvrez la page **TACACS+ Settings** (Paramètres TACACS+).
2. Renseignez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres TACACS+ sont mis à jour sur le périphérique.

Ajout d'un serveur TACACS+

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

La page **Add TACACS+ Host** (Ajout d'un hôte TACACS+) s'ouvre.

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

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

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

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

La page **TACACS+ Table** (Table TACACS+) s'ouvre.

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

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

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

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des champs de la page **TACACS+ Settings** (Paramètres TACACS+).

Tableau 6-37. Commandes CLI Paramètres TACACS+

Commande CLI	Description
`tacacs-server host {adresse- ip | nom-hôte} [connexion-unique] [port numéro-port] [timeout délai] [key clé-codage] [source source] [priority priorité]`	Définit un serveur TACACS+ hôte.
`no tacacs-server host {ip-address | hostname}`	Supprime un serveur TACACS+ hôte donné.
`tacacs-server key [key- string]`	Désigne la clé d'authentification et de cryptage utilisée pour toutes les communications TACACS entre le routeur et le serveur TACACS+. Cette clé doit correspondre à la clé de cryptage utilisée sur le serveur TACACS démon. (Plage : 0 à 128 caractères)
`no tacacs-server key`	Revient à la valeur par défaut.
`tacacs-server timeout` *`timeout`*	Spécifie la valeur du délai en secondes. (Plage : 1-30)
`no tacacs-server timeout`	Revient à la valeur par défaut.
`tacacs-server source-ip ip-address`	Spécifie l'adresse IP source. (Plage : adresse IP valide)
`no tacacs-server source- ip ip-address`	Revient à la valeur par défaut.
`show tacacs+` [*`ip-address`*]	Affiche la configuration et les statistiques d'un serveur TACACS+.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# tacacs-server host 171.16.8.1 port 49 key abc

Console (config)# end

Console# show tacacs

                                                                    

Device Configuration

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

IP address  Status      Port  Single Connection  TimeOut  Source IP  Priority
```

---------- -	---------	----	----------	-------	------	--------
171.16.8.1	Not Connected	49	No	Global	Global	0
OOB Host Configuration						
IP address	Status	Port	Single Connection	TimeOut	Source IP	Priority
---------- -	---------	----	----------	-------	------	--------
No TACACS server is configured.						
Device Configuration						

Source IP: 0.0.0.0						
OOB host Configuration						

Source IP : 0.0.0.0						

Configuration des paramètres RADIUS

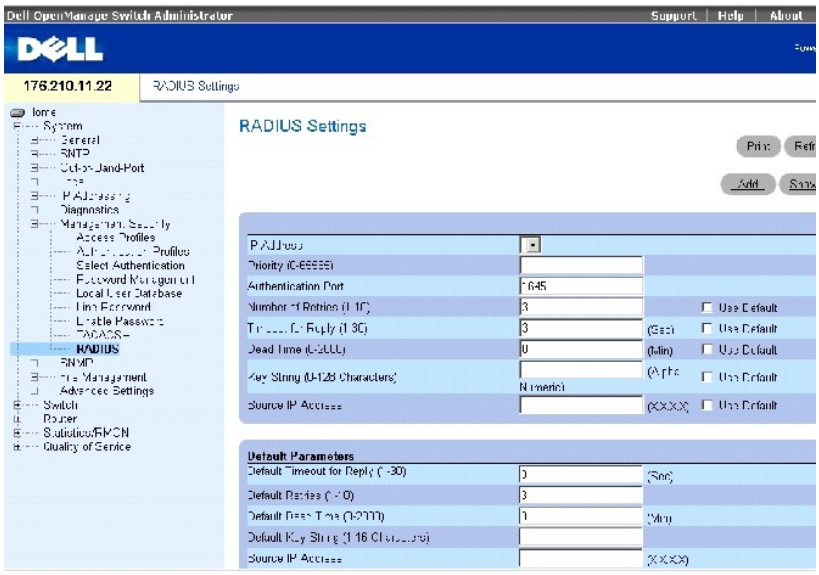
Les serveurs RADIUS (Remote Authorization Dial-In User Service) permettent d'augmenter la sécurité des réseaux. Un serveur RADIUS gère une base de données d'utilisateurs qui contient les informations d'authentification pour chaque utilisateur. Les serveurs RADIUS assurent une méthode d'authentification centralisée pour :

- L'accès Telnet
- L'accès Web
- L'accès Console à commutateur

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

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

Figure 6-51. Paramètres RADIUS



La page **RADIUS Settings** (Paramètres RADIUS) contient les champs suivants :

IP Address (Adresse IP) Adresse IP du port d'authentification.

Priority (0-65535) (Priorité (0-65535) Indique la priorité du port. Les valeurs possibles sont comprises entre 0 et 65535.

Authentication Port (Port d'authentification) Identifie le port d'authentification utilisé pour vérifier l'authentification du serveur RADIUS.

Number of Retries (1-10) (Nombre de tentatives [1-10]) Nombre de demandes de transmission envoyées au serveur RADIUS avant la survenue d'un échec. Les valeurs possibles sont comprises entre 1 et 10. La valeur par défaut est trois. En l'absence de valeur spécifique à l'hôte, la valeur globale s'applique à chaque hôte. Cliquez sur **Use Default** (Utiliser la valeur par défaut) pour utiliser la valeur par défaut.

Timeout for Reply (1-30) (Délai de réponse [1-30]) Délai en secondes pendant lequel le périphérique attend une réponse du serveur RADIUS avant expiration. Les valeurs possibles sont comprises entre 1 et 30. La valeur par défaut est trois. En l'absence de valeur spécifique à l'hôte, la valeur globale s'applique à chaque hôte. Cliquez sur **Use Default** (Utiliser la valeur par défaut) pour utiliser la valeur par défaut.

Dead Time (0-2000) (Délai d'inactivité [0-2000]) Délai (en minutes) pendant lequel un serveur RADIUS est écarté pour répondre à des demandes de service. La plage est comprise entre 0 et 2000. En l'absence de valeur spécifique à l'hôte, la valeur globale s'applique à chaque hôte. Cliquez sur **Use Default** (Utiliser la valeur par défaut) pour utiliser la valeur par défaut.

Key String (0-128 Characters) (Clé de codage [0-128 caractères]) Clé de codage utilisée pour authentifier et crypter toutes les communications RADIUS entre le périphérique et le serveur RADIUS. Cette clé doit correspondre au cryptage RADIUS. En l'absence de valeur spécifique à l'hôte, la valeur globale s'applique à chaque hôte.

Source IP Address (Adresse IP source) Adresse IP du périphérique ayant accès au serveur RADIUS.

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

Default Retries (1-10) (Nombre de tentatives par défaut [1-10]) Nombre de demandes de transmission par défaut envoyées au serveur RADIUS avant la survenue d'un échec.

Default Timeout for Reply (1-30) (Délai de réponse par défaut [1-30]) Nombre de demandes de transmission envoyées au serveur RADIUS avant la survenue d'un échec. Les valeurs possibles sont comprises entre 1 et 30.

Default Dead Time (0-2000) (Délai d'inactivité par défaut [0-2000]) Définit le délai par défaut (en minutes) 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 (0-128 characters) (Clé de codage par défaut [0-128 caractères]) Clé de codage par défaut utilisée pour authentifier et crypter toutes les communications RADIUS entre le périphérique et le serveur RADIUS. Cette clé doit correspondre au cryptage RADIUS.

Source IP Address (Adresse IP source) Adresse IP par défaut d'un périphérique ayant accès au serveur RADIUS.

Ajout d'un serveur RADIUS

1. Ouvrez la page **RADIUS Settings** (Paramètres RADIUS).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add RADIUS Server** (Ajout d'un serveur RADIUS).
3. Renseignez les champs de la boîte de dialogue.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Définition des paramètres RADIUS

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

Les paramètres RADIUS sont mis à jour sur le périphérique.

Modification des paramètres des serveurs RADIUS

1. Ouvrez la page **RADIUS Settings** (Paramètres RADIUS).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la liste **RADIUS Servers List** (Liste des serveurs RADIUS).
3. Modifiez les champs de la boîte de dialogue.
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) pour afficher la liste **RADIUS Servers List** (Liste des serveurs RADIUS).
3. Sélectionnez un serveur RADIUS et cochez la case **Remove** (Supprimer).

Le serveur RADIUS est supprimé de la liste.

Définition des serveurs RADIUS à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des champs de la page **RADIUS Settings** (Paramètres RADIUS).

Tableau 6-38. Commandes CLI Serveur RADIUS

Commande CLI	Description
`radius-server timeout timeout`	Définit la durée pendant laquelle un routeur attend une réponse d'un serveur hôte.
`radius-server retransmit retries`	Définit le nombre de tentatives de recherche de la liste des serveurs RADIUS hôtes.
`radius-server deadtime deadtime`	Configure les serveurs non disponibles pour qu'ils soient ignorés.
`radius-server key key- string`	Définit la clé d'authentification et de cryptage utilisée pour toutes les communications RADIUS entre le routeur et l'environnement RADIUS.
`radius-server host ip- address [auth-port auth-port-number] [timeout timeout] [retransmit retries] [deadtime deadtime] [key key-string] [source source] [priority priority]`	Définit un serveur RADIUS hôte.
`show radius-servers`	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 127 timeout 20

Console# show radius-servers

IP address  Auth   Acct   TimeOut  Retransmit  Deadtime   Source IP  Priority

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


172.16.1.1  164    51646  3        3           0                     01
172.16.1.2  164    51646  3        3           0                     02
```

Définition des paramètres SNMP

Le protocole **SNMP** (Simple Network Management Protocol - protocole de gestion de réseau simple) fournit une méthode de gestion des périphériques réseau. Le périphérique prend en charge SNMP version 1, SNMP version 2 et SNMP version 3.

REMARQUE : Par défaut, SNMPv2 est automatiquement activé sur le périphérique. Pour activer SNMPv3, un identifiant moteur local doit être défini pour le périphérique. Cet identifiant doit être une chaîne de caractères définie par l'utilisateur ou une chaîne de caractères par défaut générée en fonction de l'adresse MAC du périphérique. Pour obtenir des informations sur la configuration de l'identifiant moteur local, reportez-vous à la section **Définition des paramètres globaux SNMP**.

SNMP v1 et v2

L'agent SNMP gère 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 à l'agent SNMP sont contrôlés par des chaînes d'accès.

SNMP v3

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

- **Authentication** Assure l'intégrité des données et l'authentification de l'origine des données.
- **Privacy** (Confidentialité) Protection du contenu du message contre toute divulgation. Le mode CBC (Cipher-Bock-Chaining - chiffrement par chaînage de bloc) est utilisé pour le cryptage. Il est possible d'activer uniquement l'authentification sur un message SNMP ou d'activer à la fois l'authentification et la confidentialité sur un message SNMP. Toutefois, la confidentialité ne peut pas être activée sans authentification.
- **Timeliness** (Ponctualité) Protection contre les délais de temporisation des messages ou la redondance des messages. L'agent SNMP compare le message entrant aux informations d'heure du message.
- **Key Management** (Gestion de la clé) Définit la génération, les mises à jour et l'utilisation de la clé.

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

- Sécurité
- Contrôle d'accès aux fonctions
- Interruptions

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

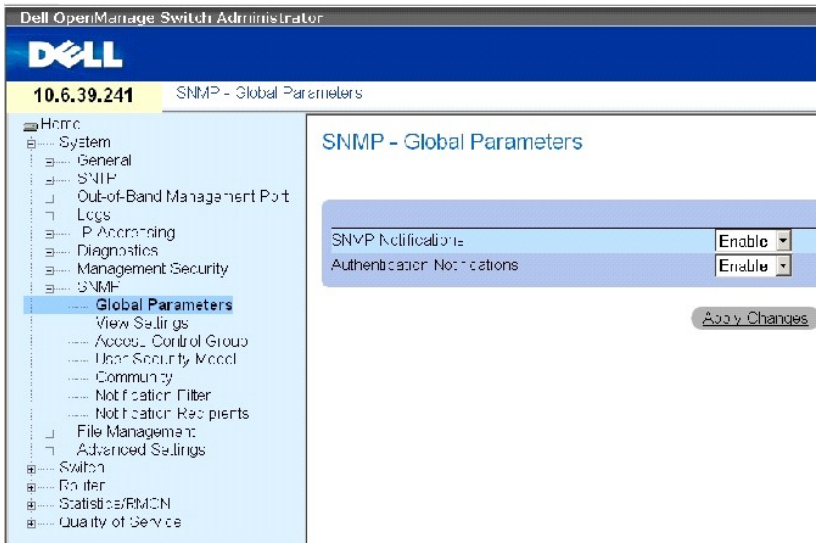
La page SNMP permet de définir les paramètres SNMP. Pour ouvrir la page SNMP, cliquez sur **System** (Système)→ **SNMP** dans l'*arborescence*.

Définition des paramètres globaux SNMP

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

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

Figure 6-52. Paramètres globaux



La page **Global Parameters** (Paramètres globaux) contient les paramètres suivants :

SNMP Notifications (Notifications SNMP) Active ou désactive l'envoi de notifications SNMP par le périphérique.

Authentication Notifications (Notifications d'authentification) Active ou désactive l'envoi d'interruptions SNMP par le périphérique en cas d'échec de l'authentification.

Activation des notifications SNMP

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

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

Activation des notifications d'authentification

1. Ouvrez la page **Global Parameters** (Paramètres globaux).
2. Sélectionnez **Enable** (Activer) dans le champ **Authentication Notifications** (Notifications d'authentification).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Activation des notifications SNMP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des champs de la page **Global Parameters** (Paramètres globaux).

Tableau 6-39. Commandes CLI Notification SNMP

Commande CLI	Description

snmp-server engineID local {*engineid-string* | default}	Définit l'ID moteur SNMP sur le périphérique local.
show snmp	Affiche la configuration actuelle du périphérique SNMP.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# snmp-server enable traps

Console (config)# snmp-server trap authentication

Console (config)# end

Console# show snmp
```

Community-String	Community-Access	IP address
------------	-----------------	-----------------
public	read only	All
private	read write	172.16.1.1
private	read write	172.17.1.1
OOB management stations		
Community-String	Community-Access	IP address
------------	-----------------	-----------------
private	read write	176.16.8.9
Traps are enabled.		
Authentication trap is enabled.		
Trap-Rec-Address	Trap-Rec-Community	Version
192.122.173.42	public	2

OOB trap receivers		
Trap-Rec-Address	Trap-Rec-Community	Version
176.16.8.9	public	2
System Contact: Robert		
System Location: Marketing		

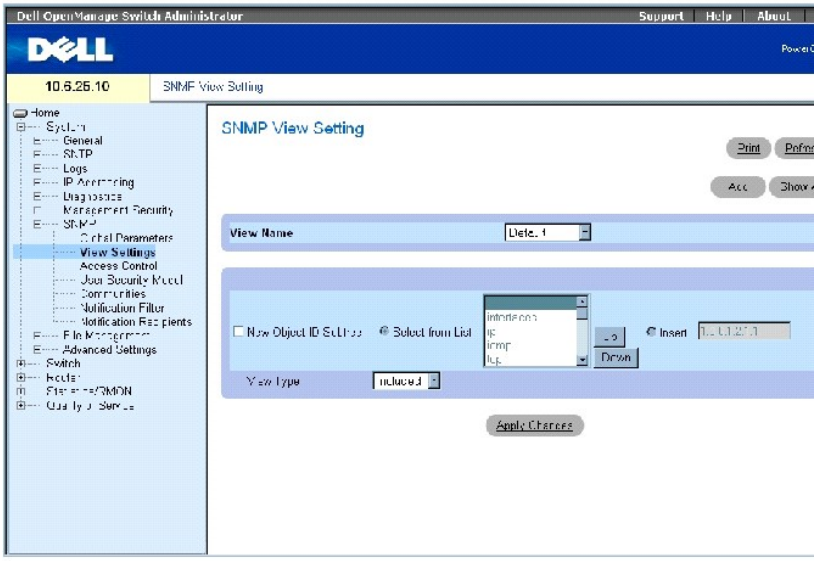
Définition des vues SNMP

Les vues SNMP autorisent ou bloquent l'accès aux fonctions du périphérique ou aux aspects fonctionnels. Par exemple, une vue peut être définie pour permettre au groupe SNMP A d'accéder uniquement en lecture seule au routage et au SNMP B d'y accéder en lecture-écriture. L'accès aux fonctions est possible via le nom ou l'ID objet de la MIB.

La page **SNMP View Setting** (Paramétrage des vues SNMP) permet de définir des vues SNMP.

Pour ouvrir la page **SNMP View Setting** (Paramétrage des vues SNMP), cliquez sur **System** (Système)→ **SNMP**→ **View Settings** (Paramètres des vues) dans l'*arborescence*.

Figure 6-53. Paramétrage des vues SNMP



La page **SNMP View Setting** (Paramétrage des vues SNMP) contient les champs suivants :

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

New Object ID Subtree (Nouvelle sous-arborescence d'ID objet) Définit les OID des fonctions du périphérique à inclure ou exclure dans la vue.

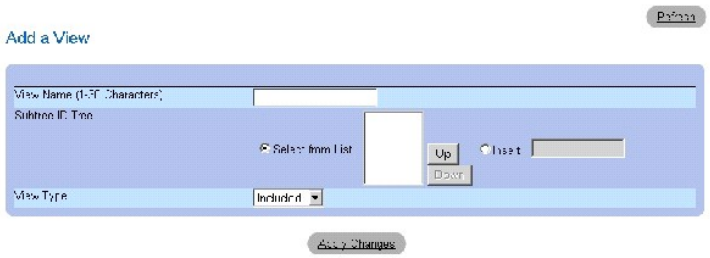
View Type (Type de vue) Lorsqu'elle est cochée, cette option permet d'accéder à une fonction ou un aspect fonctionnel sélectionné dans la vue SNMP.

Ajout d'une vue

1. Ouvrez la page **SNMP View Setting** (Paramétrage des vues SNMP).
2. cliquez sur **Add** (Ajouter).

La page **Add A View** (Ajout d'une vue) s'ouvre :

Figure 6-54. Ajout d'une vue



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

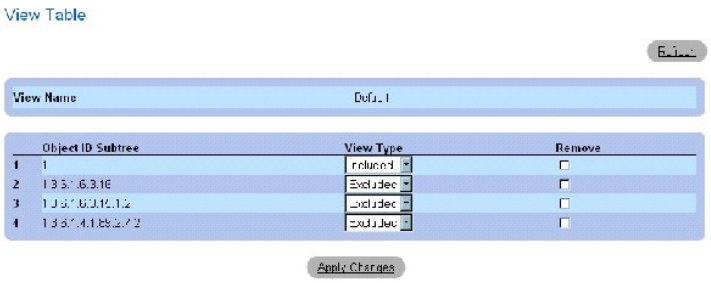
La vue SNMP est ajoutée et le périphérique est mis à jour.

Affichage de la table des vues

1. Ouvrez la page **SNMP View Setting** (Paramétrage des vues SNMP).
2. Cliquez sur **Show All** (Afficher tout).

La page **View Table** (Table des vues) s'ouvre :

Figure 6-55. Table des vues



Suppression de vues SNMP

1. Ouvrez la page **SNMP View Setting** (Paramétrage des vues SNMP).
2. Cliquez sur **Show All** (Afficher tout).

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

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

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

Définition des vues SNMP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des champs de la page **SNMP View Setting** (Paramétrage des vues SNMP).

Tableau 6-40. Commandes CLI Vue SNMP

Commande CLI	Description
show snmp views [*viewname*]	Affiche la configuration des vues.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# snmp-server view user1 1 included

Console (config)# end

Console # show snmp views
```

Name	OID Tree	Type
----------	----------	----------
user1	iso	included
Default	iso	included
Default	snmpVacmMIB	excluded
Default	usmUser	excluded
Default	rndCommunityTable	excluded
DefaultSuper	iso	included

Définition du contrôle d'accès au SNMP

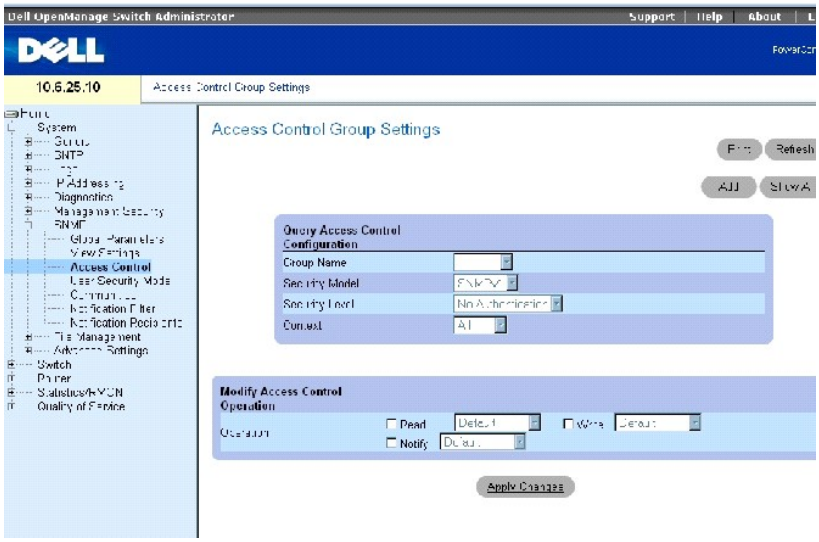
La page **Access Control Group** (Groupe de contrôle d'accès) fournit des informations concernant la création des groupes SNMP et l'affectation des privilèges d'accès au SNMP. Les groupes permettent aux gestionnaires de réseau d'affecter des droits d'accès à certaines fonctions du périphérique ou certains aspects

des fonctionnels.

Le port hors bande est traité comme un périphérique distinct lors de l'utilisation des fonctions SNMP. Des vues peuvent être limitées aux MIB hors bande, aux MIB du périphérique ou à toutes les MIB.

Pour ouvrir la page **Access Control Group** (Groupe de contrôle d'accès), cliquez sur **System** (Système)→ **SNMP**→ **Access Control** (Contrôle de l'accès) dans l'*arborescence*.

Figure 6-56. Groupe de contrôle d'accès



La page **Access Control Group** (Groupe de contrôle d'accès) contient les champs suivants :

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

Security Model (Modèle de sécurité) Définit la version SNMP associée au groupe. Ce champ peut prendre les valeurs suivantes :

SNMPv1 La version SNMPv1 est définie pour le groupe.

SNMPv2 La version SNMPv2 est définie pour le groupe.

SNMPv3 La version SNMPv3 est définie pour le groupe.

Security Level (Niveau de sécurité) Niveau de sécurité associé au groupe. Les niveaux de sécurité ne s'appliquent qu'aux groupes SNMPv3. Ce champ peut prendre les valeurs suivantes :

No Authentication (Pas d'authentification) Aucun niveau de sécurité, qu'il s'agisse de l'authentification ou de la confidentialité, n'est associé au groupe.

Authentication (Authentification) Authentifie les messages SNMP sans les crypter.

Privacy (Confidentialité) Authentifie les messages SNMP et les crypte.

Operation (Opération) Définit les droits d'accès du groupe. Ce champ peut prendre les valeurs suivantes :

Read (Lecture) Sélectionnez une vue qui restreint l'accès de gestion au contenu de l'agent. Si aucune vue n'est sélectionnée, tous les objets, à l'exception de la table-communauté et des tables des accès et des utilisateurs SNMPv3, peuvent être visualisés.

Write (Écriture) Sélectionnez une vue qui autorise l'accès de gestion en lecture-écriture au contenu de l'agent mais pas de la communauté.

Notify (Notifier) Sélectionnez une vue qui autorise l'envoi d'interruptions SNMP ou d'informations.

Context (Contexte) Contexte pour lequel le groupe d'accès est configuré. Ce champ peut prendre les valeurs suivantes :

Router (Routeur) Le groupe d'accès est configuré pour la gestion intrabande.

OOB Le groupe d'accès est configuré pour la gestion hors bande.

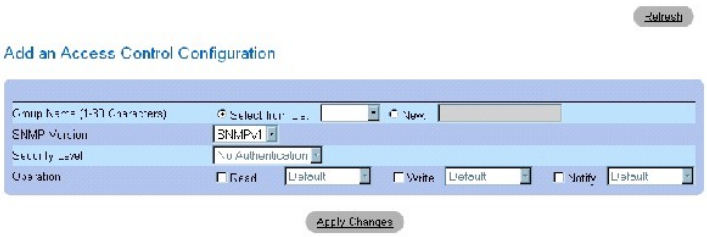
All (Tout) Le groupe d'accès est configuré pour la gestion intrabande et hors bande

Définition de groupes SNMP

1. Ouvrez la page **Access Control Group** (Groupe de contrôle d'accès).
2. Cliquez sur **Add** (Ajouter).

La page **Add an Access Control Group** (Ajout d'un groupe de contrôle d'accès) s'ouvre :

Figure 6-57. Ajout d'un groupe de contrôle d'accès



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

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

Affichage de la table des accès

1. Ouvrez la page **Access Control Group** (Groupe de contrôle d'accès).
2. Cliquez sur **Show All** (Afficher tout).

La page **Access Table** (Table des accès) s'ouvre :

Figure 6-58. Access Table (Table des accès)

Suppression d'un groupe

1. Ouvrez la page **Access Control Group** (Groupe de contrôle d'accès).
2. Cliquez sur **Show All** (Afficher tout).

   La page **Access Table** (Table des accès) s'ouvre.
3. Sélectionnez un groupe.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

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

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des champs de la page **Access Control Group** (Groupe de contrôle d'accès).

Tableau 6-41. Commandes CLI Contrôle d'accès au SNMP

Commande CLI	Description
snmp-server group *groupname* {**v1** | **v2** | **v3** {**noauth** | **auth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]	Configure un nouveau groupe SNMP (Simple Network Management Protocol - protocole de gestion de réseau simple) ou une table qui adresse des utilisateurs SNMP à des vues SNMP.
show snmp groups [*groupname*]	Affiche la configuration des groupes

Vous trouverez ci-dessous un exemple de commande CLI :

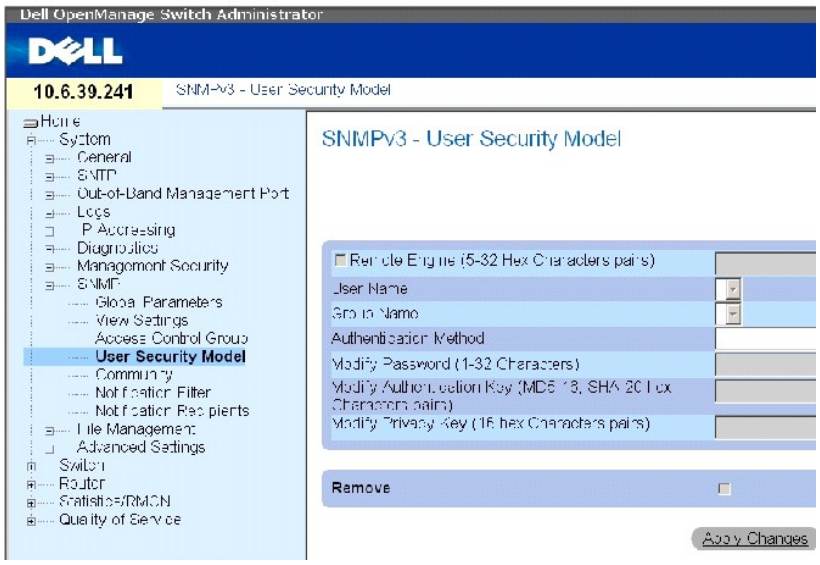
```
Console (config)# snmp-server group user-group v3 priv read user- view
```

Affectation de la sécurité utilisateur SNMP

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

Pour ouvrir la page **SNMPv3 User Security Model (USM)** (Modèle de sécurité utilisateur (USM) SNMPv3), cliquez sur **System** (Système)→ **SNMP**→ **User Security Model** (Modèle de sécurité utilisateur) dans l'*arborescence*.

Figure 6-59. Modèle de sécurité utilisateur (USM) SNMPv3



La page **SNMPv3 User Security Model (USM)** (Modèle de sécurité utilisateur (USM) SNMPv3) contient les champs suivants :

Engine ID (ID moteur) Identifie le périphérique activé par SNMPv3 à distance auquel l'utilisateur sélectionné est connecté.

Remote Engine ID (ID moteur distant) Indique que l'utilisateur est configuré sur un périphérique activé par SNMPv3 à distance. Si l'ID moteur est défini, les périphériques distants reçoivent des messages d'informations.

User Name (Nom d'utilisateur) Dresse la liste des noms d'utilisateur définis par l'utilisateur.

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

Authentication Method (Méthode d'authentification) Définit la méthode d'authentification utilisé pour authentifier les utilisateurs. Ce champ peut prendre les valeurs suivantes :

None (Aucune) Pas d'authentification des utilisateurs.

MD5 Password (Mot de passe MD5) Les utilisateurs sont authentifiés via le niveau d'authentification HMAC-MD5-96. L'utilisateur doit spécifier un mot de passe.

SHA Password (Mot de passe SHA) Les utilisateurs sont authentifiés via le niveau d'authentification HMAC-SHA-96. L'utilisateur doit entrer un mot de passe.

MD5 Key (Clé MD5) Les utilisateurs sont authentifiés via le niveau d'authentification HMAC-MD5-96. L'utilisateur doit entrer des clés d'authentification et de confidentialité.

SHA Key (Clé SHA) Les utilisateurs sont authentifiés via le niveau d'authentification HMAC-SHA-96. L'utilisateur doit entrer des clés d'authentification et de confidentialité.

Password (Mot de passe) (0-32 caractères) Modifie le mot de passe défini par l'utilisateur qui s'applique au groupe. Les mots de passe peuvent comprendre jusqu'à 32 caractères. Un mot de passe n'est défini que si la méthode d'authentification est MD5 Password (Mot de passe MD5) ou SHA Password (Mot de passe SHA).

Authentication Key (Clé d'authentification) (MD5-16 caractères hexa ; SHA-20 caractères hexa) Spécifie la clé d'authentification. Une clé d'authentification n'est définie que si la méthode d'authentification est MD5 Key (Clé MD5) ou SHA Key (Clé SHA).

Privacy Key (Clé de confidentialité) (16 caractères hexa) Spécifie un mot de passe pour l'authentification et la génération d'une clé DES pour la confidentialité. Une clé de confidentialité n'est définie que si la méthode d'authentification est MD5 Key (Clé MD5) ou SHA Key (Clé SHA).

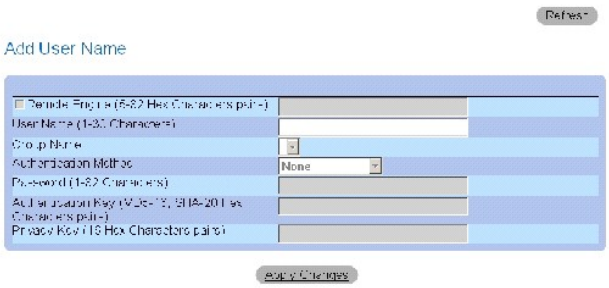
Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime un utilisateur donné d'un groupe donné.

Ajout d'utilisateurs SNMPv3 à un groupe

1. Ouvrez la page **SNMPv3 User Security Model (USM)** (Modèle de sécurité utilisateur (USM) SNMPv3).
2. Cliquez sur **Add** (Ajouter).

La page **Add SNMPv3 User Name** (Ajout d'un nom d'utilisateur SNMPv3) :

Figure 6-60. Ajout d'un nom d'utilisateur SNMPv3



3. Renseignez les champs concernés.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).
5. L'utilisateur est ajouté au groupe et le périphérique est mis à jour.

Affichage de la table des modèles de sécurité utilisateur

1. Ouvrez la page **SNMPv3 User Security Model (USM)** (Modèle de sécurité utilisateur (USM) SNMPv3).
2. Cliquez sur **Show All** (Afficher tout).

La page **SNMPv3 User Security Model Table** (Table des modèles de sécurité utilisateur SNMPv3) s'ouvre :

Figure 6-61. Table des modèles de sécurité utilisateur SNMPv3

Suppression d'une entrée de la table des modèles de sécurité utilisateur

1. Ouvrez la page **SNMPv3 User Security Model (USM)** (Modèle de sécurité utilisateur (USM) SNMPv3).
2. Cliquez sur **Show All** (Afficher tout).

   La page **SNMPv3 User Security Model Table** (Table des modèles de sécurité utilisateur SNMPv3) s'ouvre.
3. Sélectionnez une entrée.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Définition d'utilisateurs SNMP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des champs de la page **SNMPv3 User Security Model (USM)** (Modèle de sécurité utilisateur (USM) SNMPv3).

Tableau 6-42. Commandes CLI Utilisateur SNMP

Commande CLI	Description
show snmp users [*username*]	Affiche la configuration des utilisateurs.

```
Console (config)# snmp-server user John auth-md5 1234

Console (config)# end

Console (config)# show snmp users
```

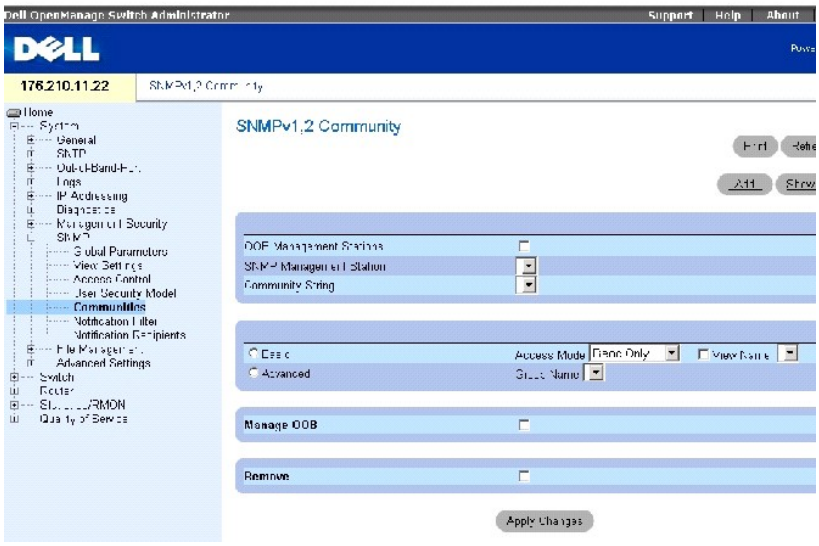
Name	Group Name	Auth Method	Remote
-------	----------	-----------	------
John	user-group	**MD5**	

Définition de communautés

Les droits d'accès sont gérés en définissant des communautés dans la page **SNMPv1, 2 Community** (Communauté SNMPv1,2). Lorsqu'un nom de communauté est modifié, les droits d'accès qui lui sont associés le sont également. Une communauté SNMP n'est définie que pour SNMP v1 et SNMP v2.

Pour ouvrir la page **SNMPv1, 2 Community** (Communauté SNMPv1, 2), cliquez sur **System** (Système)→ **SNMP**→ **Communities** (Communautés) dans l'*arborescence*.

Figure 6-62. Communauté SNMPv1, 2



La page **SNMPv1, 2 Community** (Communauté SNMPv1, 2) contient les champs suivants :

OOB Management Station (Station de gestion OOB) Cochez cette case pour créer une communauté SNMP distincte pour le port hors bande. Si cette case n'est pas cochée, l'accès au périphérique par la station de gestion s'effectue via les ports intrabande.

SNMP Management Station (Station de gestion SNMP) Dresse la liste des adresses IP de la station de gestion pour lesquelles des chaînes communautaires ont été définies.

REMARQUE : Seuls les super-utilisateurs peuvent utiliser la même communauté pour configurer des ports hors bande et intrabande.

Community String (Chaîne communautaire) Dresse la liste des chaînes communautaires définies par l'utilisateur qui fonctionnent comme un mot de passe et permettent au périphérique d'authentifier la station de gestion SNMP. Une chaîne communautaire peut comprendre jusqu'à 20 caractères.

Basic (Basique) Active le mode SNMP de base pour la communauté sélectionnée. Ce champ peut prendre les valeurs suivantes :

Access Mode (Mode d'accès) Définit les droits d'accès de la communauté. Ce champ peut prendre les valeurs suivantes :

Read-Only (Lecture seule) L'accès de gestion s'effectue en lecture seule. Aucune modification ne peut être apportée à la communauté.

Read-Write (Lecture-écriture) L'accès de gestion s'effectue en lecture-écriture. Des modifications peuvent être apportées à la configuration du périphérique mais pas à la communauté.

SNMP-Admin (Admin-SNMP) L'utilisateur a accès à toutes les options de configuration du périphérique et peut également apporter des modifications à la communauté.

View Name (Nom de vue) Dresse la liste des vues SNMP définies par l'utilisateur

Advanced (Avancé) Dresse la liste des groupes définis par l'utilisateur. Lorsque le mode SNMP Advanced (SNMP avancé) est sélectionné, les règles de contrôle de l'accès au SNMP comprenant le groupe sont activées pour la communauté sélectionnée. Le mode Advanced (Avancé) active également des groupes SNMP pour des communautés SNMP spécifiques. Le mode SNMP Advanced (SNMP avancé) n'est défini qu'avec SNMPv3.

Manage OOB (Gérer OOB) Lorsque cette case est cochée, la gestion SNMP est fournie aux stations de gestion hors bande connectées au périphérique via le port hors bande uniquement.

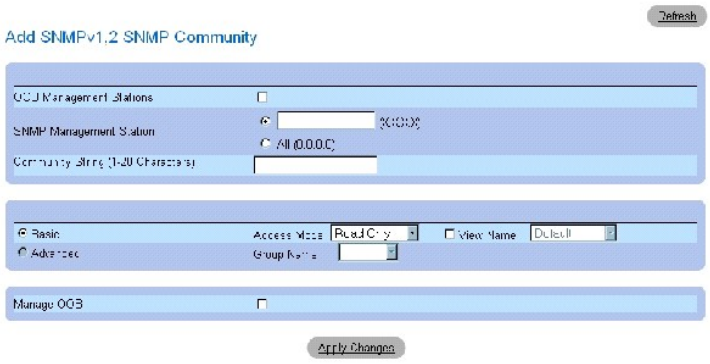
Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime une communauté.

Définition d'une nouvelle communauté

1. Ouvrez la page **SNMPv1, 2 Community** (Communauté SNMPv1, 2).
2. Cliquez sur **Add** (Ajouter).

La page **Add SNMPv1,2 Community** (Ajout d'une communauté SNMPv1, 2) s'ouvre :

Figure 6-63. Ajout d'une communauté SNMPv1, 2



3. Renseignez les champs concernés.

Outre les champs de la page **SNMPv1, 2 Community** (Communauté SNMPv1, 2), la page **Add SNMPv1,2 Community** (Ajout d'une communauté SNMPv1, 2) contient le champ **All (0.0.0.0)** (Tout [0.0.0.0.]) qui indique si une communauté SNMP est définie pour une station de gestion donnée ou pour toutes les stations de gestion.

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

La nouvelle communauté est enregistrée et le périphérique est mis à jour.

Suppression de communautés

1. Ouvrez la page **SNMPv1, 2 Community** (Communauté SNMPv1, 2).
2. Cliquez sur **Show All** (Afficher tout).

La page **SNMPv1,2 Community Tables** (Tables des communautés SNMPv1, 2) s'ouvre.

3. Sélectionnez une communauté et cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée de la communauté 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 la définition des champs de la page **SNMPv1, 2 Community** (Communauté SNMPv1, 2).

Tableau 6-43. Commandes CLI Communauté SNMP

Commande CLI	Description
`snmp-server community community [ro | rw | su] [ip-address] [view view-name][type {router | oob}]`	Configure la chaîne d'accès à la communauté afin d'autoriser l'accès au protocole SNMP.
`snmp-server community-group community group-name [ip-address] [type {router | oob}]`	Configure la chaîne d'accès à la communauté afin d'autoriser un accès restreint au protocole SNMP en fonction des droits d'accès du groupe.
`show snmp`	Affiche la configuration actuelle du périphérique SNMP.

Vous trouverez ci-dessous un exemple de commande CLI :

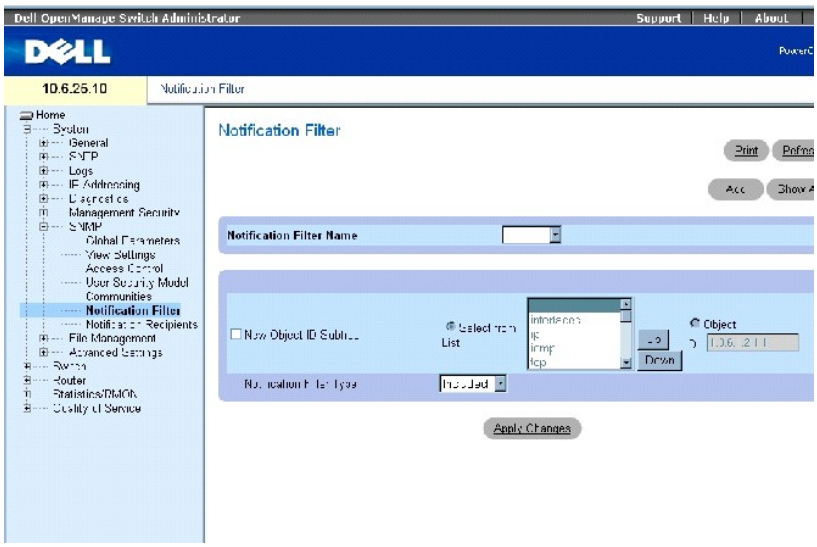
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

Définition de filtres de notification SNMP

La page **Notification Filter** (Filtre de notification) permet de filtrer des interruptions en fonction des OID. Chaque OID est lié à une fonction du périphérique ou un aspect fonctionnel. La page **Notification Filter** (Filtre de notification) permet aux gestionnaires de réseau de filtrer des notifications.

Pour ouvrir la page **Notification Filter** (Filtre de notification), cliquez sur **System** (Système)→ **SNMP**→ **Notification Filters** (Filtres de notification) dans l'*arborescence*.

Figure 6-64. Filtre de notification



La page **Notification Filter** (Filtre de notification) contient les champs suivants :

Notification Filter Name (Nom de filtre de notification) Dresse la liste des filtres de notification définis par l'utilisateur. Un nom de filtre de notification peut contenir jusqu'à 30 caractères.

New Object Identifier Subtree (Nouvelle sous-arborescence d'identifiants objet) OID pour lesquels des notifications sont envoyées ou bloquées. Si un filtre est associé à un OID, des interruptions ou des informations sont générées et envoyées aux destinataires d'interruption. Les ID objet sont sélectionnés dans la zone *Select from List* (Sélectionner dans la liste) ou spécifiés dans le champ *Object ID* (ID objet).

Notification Filter Type (Type du filtre de notification) Indique si des informations ou des interruptions sont envoyées en fonction de l'OID aux destinataires des interruptions.

Excluded (Exclus) Restreint l'envoi des interruptions ou des informations OID.

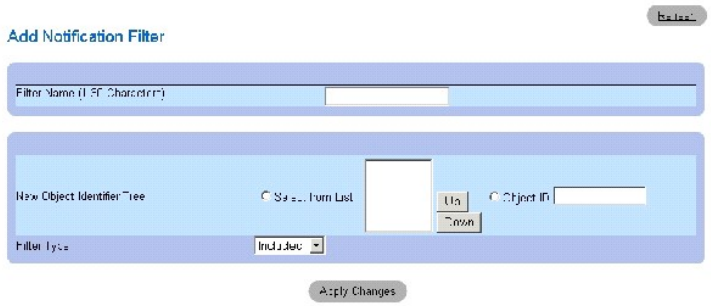
Included (Inclus) Envoie des interruptions ou des informations OID.

Ajout de filtres SNMP

1. Ouvrez la page **Notification Filter** (Filtre de notification).
2. Cliquez sur **Add** (Ajouter).

La page Add Filter (Ajout d'un filtre) s'ouvre :

Figure 6-65. Ajout d'un filtre



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

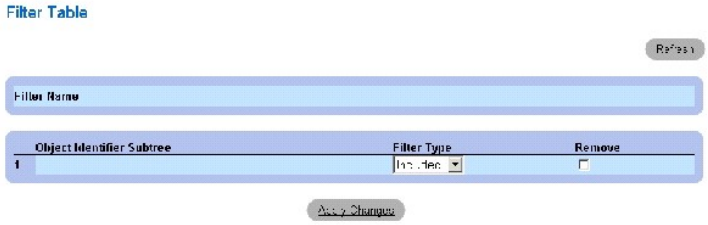
Le nouveau filtre est ajouté et le périphérique est mis à jour.

Affichage de la table des filtres

1. Ouvrez la page **Notification Filter** (Filtre de notification).
2. Cliquez sur **Show All** (Afficher tout).

La page **Filter Table** (Table des filtres) s'ouvre :

Figure 6-66. Table des filtres



Suppression d'un filtre

1. Ouvrez la page **Notification Filter** (Filtre de notification).
2. Cliquez sur **Show All** (Afficher tout).

   La page **Filter Table** (Table des filtres) s'ouvre :
3. Sélectionnez une entrée de la **table des filtres**.
4. Cochez la case **Remove** (Supprimer).

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

Configuration des filtres de notification à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des champs de la page **Notification Filter** (Filtre de notification).

Tableau 6-44. Commandes CLI Filtre de notification SNMP

Commande CLI	Description
`snmp-server filter filter-name oid-tree {included | excluded}`	Crée ou met à jour un filtre de notification SNMP.
`show snmp filters [filtername]`	Affiche la configuration des filtres de notification SNMP

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# snmp-server filter user1 1 included

Console (config)# end

Console # show snmp filters

Name        OID Tree      Type
----------  ------------  --------
user1       iso           Included
```

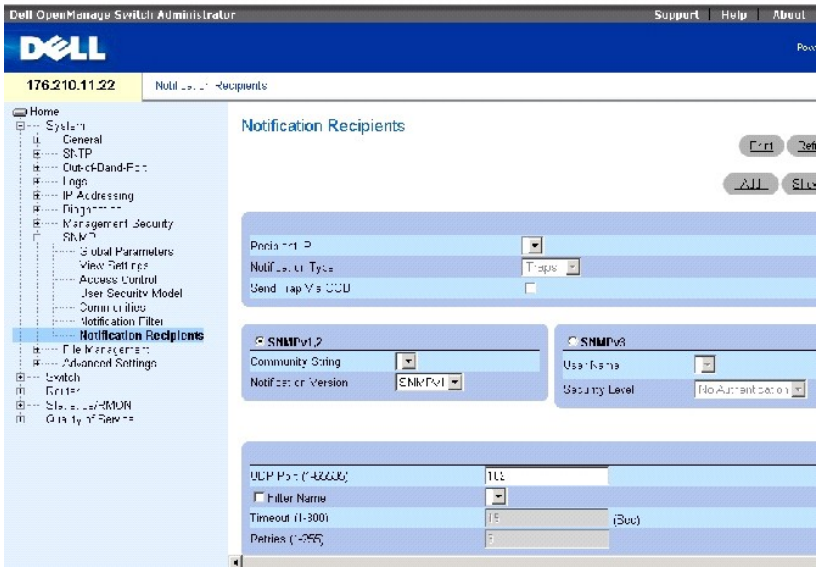
Définition des destinataires de notification

La page **Notification Recipients** (Destinataires de notification) contient des informations concernant la définition des filtres qui déterminent l'envoi d'interruptions à des utilisateurs spécifiques et le type d'interruption envoyé. Les filtres de notification SNMP offrent les services suivants :

- Identification des cibles des interruptions de gestion
- Filtrage des interruptions
- Sélection des paramètres de génération des interruptions
- Mise en place de vérifications du contrôle d'accès

Pour ouvrir la page **Notification Recipients** (Destinataires de notification), cliquez sur **System** (Système)→ **SNMP**→ **Notification Recipient** (Destinataire de notification) dans l'*arborescence*.

Figure 6-67. Destinataires de notification



La page **Notification Recipients** (Destinataires de notification) contient les champs suivants :

Recipient IP (IP destinataire) Contient une liste des adresses IP des destinataires de notification, définie par l'utilisateur.

Notification Type (Type de notification) Type de la notification envoyée. Ce champ peut prendre les valeurs suivantes :

Trap (Interruption) Des interruptions sont envoyées.

Inform (Information) Des informations sont envoyées.

SNMPv1,2 Les versions SNMP 1 ou 2 sont activées pour le destinataire sélectionné. Ce champ peut prendre les valeurs suivantes :

Community String (Chaîne communautaire) Dresse la liste des chaînes communautaires. Sélectionnez une chaîne communautaire à envoyer avec la notification.

Notification Version (Version de notification) Détermine la version de la notification. Ce champ peut prendre les valeurs suivantes :

SNMP V1 Des interruptions de type SNMP version 1 sont envoyées.

SNMP V2 Des interruptions ou des informations de type SNMP version 2 sont envoyées.

SNMPv3 SNMP version 3 est activé pour le destinataire sélectionné. Ce champ peut prendre les valeurs suivantes :

User Name (Nom d'utilisateur) Dresse la liste des utilisateurs. Sélectionnez un nom d'utilisateur pour générer des notifications.

Security Level (Niveau de sécurité) Niveau de sécurité associé aux notifications. Ce champ peut prendre les valeurs suivantes :

No Authentication (Pas d'authentification) Le paquet n'est ni authentifié, ni crypté.

Authentication (Authentification) Le paquet est authentifié.

Privacy (Confidentialité) Le paquet est à la fois authentifié et crypté.

UDP Port (1-65535) (Port UDP [1-65535]) Port UDP utilisé pour envoyer les notifications. La valeur par défaut est 162.

Filter Name (Nom de filtre) Cochez cette case pour appliquer un filtre SNMP défini par l'utilisateur aux notifications et sélectionner un filtre SNMP de la liste.

Timeout (1-300) (Délai [1-300]) Délai d'attente (en secondes) avant que le périphérique ne renvoie des informations. La valeur par défaut est 15 secondes.

Retries (1-255) (Nombre de tentatives [1-255]) Nombre maximum de fois où le périphérique renvoie une demande d'informations. La valeur par défaut est 3.

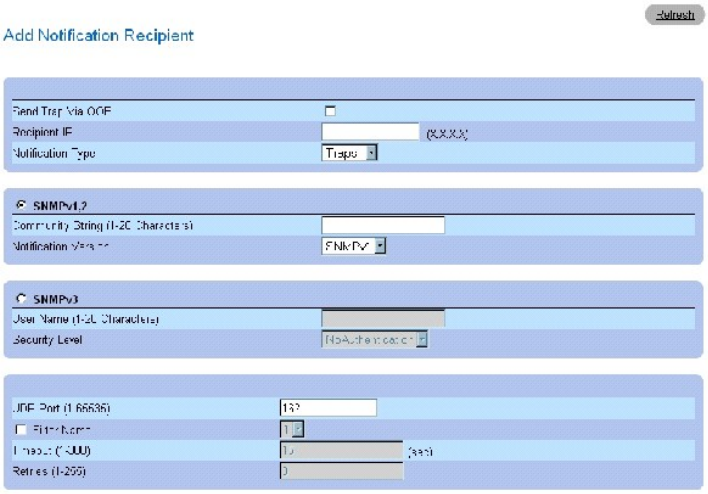
Remove Notification Recipient (Supprimer destinataire de notification) Lorsqu'elle est cochée, cette option supprimer le destinataire de notification sélectionné.

Ajout d'un nouveau destinataire de notification

1. Ouvrez la page **Notification Recipients** (Destinataires de notification).
2. Cliquez sur **Add** (Ajouter).

La page **Add Notification Recipient** (Ajout d'un destinataire de notification) s'ouvre :

Figure 6-68. Ajout d'un destinataire de notification



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

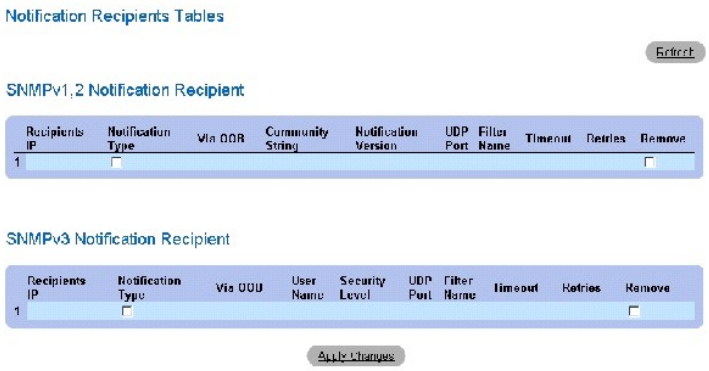
Le destinataire de notification est ajouté et le périphérique est mis à jour.

Affichage de la page Notification Recipients Tables (Table des destinataires de notification)

1. Ouvrez la page **Notification Recipients** (Destinataires de notification).
2. Cliquez sur **Show All** (Afficher tout).

La page **Notification Recipients Table** (Table des destinataires de notification) s'ouvre :

Figure 6-69. Table des destinataires de notification



Suppression de destinataires de notification

1. Ouvrez la page **Notification Recipients** (Destinataires de notification).
2. Cliquez sur **Show All** (Afficher tout).

La page Notification Recipients Tables (Table des destinataires de notification) s'ouvre.

3. Sélectionnez un ou plusieurs destinataires de notification dans les tables **SNMPV1,2 Notification Recipient Table** (Table des destinataires de notification SNMPV1, 2) et/ou **SNMPv3 Notification Recipient Table** (Table des destinataires de notification SNMPv3).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les destinataires sont supprimés et le périphérique est mis à jour.

Définition de destinataires de notification SNMP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des champs de la page **Notification Recipients** (Destinataires de notification).

Tableau 6-45. Commandes CLI Destinataires de notification SNMP

Commande CLI	Description
`snmp-server host {ip- address | hostname} community-string [traps | informs] [1 | 2] [udp-port port] [filter filtername] [timeout seconds] [retries retries]`	Crée ou met à jour un destinataire de notification recevant des notifications de type SNMP version 1 ou 2.
	Crée ou met à jour un destinataire de notification recevant des notification de type SNMP version 3.

snmp-server v3-host {ip-address | hostname} username [traps | informs] {noauth | auth | priv} [udp-port port] [filter filtername] [timeout seconds] [retries retries]	

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# snmp-server host 12.1.1.1 Dell-community

Console (config)# end

Console# show snmp

Community-String    Community-Access    View name    IP address    Type
------------------  ------------------  -----------  ------------  ----

Community-String    Group name          IP address                 Type
------------------  ------------------  -------------------------  ----

OOB management stations

Community-String    Community-Access    View name    IP address    Type
------------------  ------------------  -----------  ------------  ----

Community-String    Group name          IP address                 Type
------------------  ------------------  -------------------------  ----

Traps are enabled.

Authentication-failure trap is enabled.
```

```
Version 1,2 notifications

Target Address  Type  Community  Version  Udp Port  Filter name  To Sec  Retries
--------------  ----  ---------  -------  --------  -----------  ------  -------
```

12.1.1.1	Trap	Dell_comm unity	2	162		1500	3
OOB Notification Receivers							
Target Address	Type	Community	Version	Udp Port	Filter name	To Sec	Retries
--------	----	---------	----	----	-------	---	-------
Version 3 notifications							
Target Address	Type	Username	Security Level	Udp Port	Filter name	To Sec	Retries
--------	----	--------	-------	----	-------	---	-------
OOB Notification Receivers							
Target Address	Type	Username	Security Level	Udp Port	Filter name	To Sec	Retries
--------	----	--------	-------	----	-------	---	-------

Gestion des fichiers

La page **File Management** (Gestion des fichiers) permet de gérer les logiciels du périphérique, le fichier image et les fichiers de configuration. Des fichiers peuvent être téléchargés ou chargés via un serveur TFTP.

Présentation des fichiers de gestion

La structure des fichiers de gestion s'établit comme suit :

- **Startup configuration file** (Fichier de configuration de démarrage) Conserve la configuration exacte du périphérique lors de sa mise sous tension ou de son redémarrage. Le fichier de démarrage gère les commandes de configuration, et les commandes de configuration du fichier de configuration d'exécution peuvent être enregistrées dans le fichier de démarrage.
- **Running configuration file** (Fichier de configuration 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
- **Backup Configuration File** (Fichier de configuration de sauvegarde) Contient une copie de sauvegarde de la configuration du périphérique Le fichier de sauvegarde est mis à jour 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.
- **Image Files** (Fichiers image) Des images du système sont enregistrées dans deux secteurs Flash appelés images (Image 1 et Image 2). L'image active stocke la copie active tandis 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 de l'amorçage.

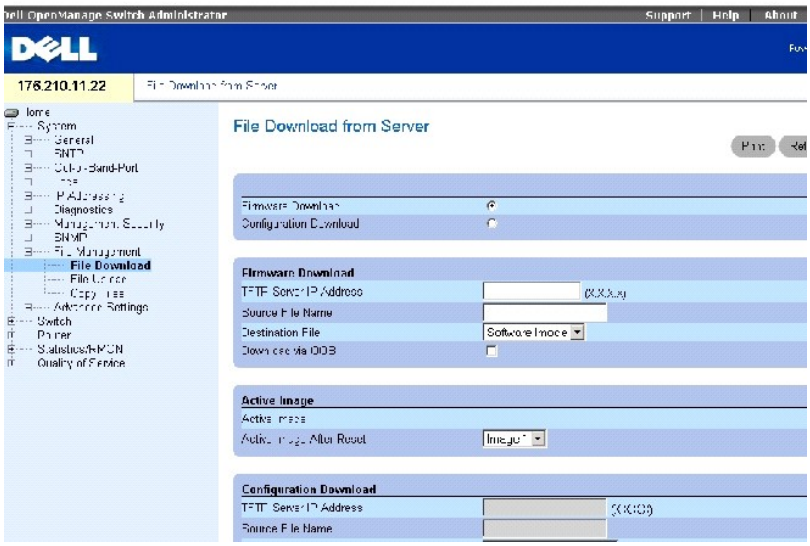
Pour ouvrir la page **File Management** (Gestion des fichiers), cliquez sur **System** (Système)→ **File Management** (Gestion des fichiers) dans l'*arborescence*.

Téléchargement de fichiers

La page **File Download From Server** (Téléchargement de fichiers à partir du serveur) contient des champs permettant de télécharger les logiciels sur le périphérique à partir du serveur TFTP. Le fichier image peut également être téléchargé à partir de la page **File Download from Server** (Téléchargement de fichiers à partir du serveur).

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 6-70. Téléchargement de fichiers à partir du serveur



La page **File Download From Server** (Téléchargement de fichier à partir du serveur) contient les champs suivants :

Firmware Download (Téléchargement du micrologiciel) Lorsqu'elle est sélectionnée, cette option indique que le fichier micrologiciel est téléchargé. Si cette option est sélectionnée, les champs **Configuration Download** (Téléchargement de la configuration) sont grisés.

Configuration Download (Téléchargement de la configuration) Lorsqu'elle est sélectionnée, cette option indique que le fichier de configuration est téléchargé. Si l'option **Configuration Download** (Téléchargement de la configuration) est sélectionnée, les champs **Firmware Download** (Téléchargement du micrologiciel) sont grisés.

Firmware TFTP Server IP Address (Adresse IP du serveur TFTP pour micrologiciel) Adresse IP du serveur TFTP à partir duquel les fichiers sont téléchargés.

Firmware Source File Name (Nom du fichier micrologiciel source) Fichier micrologiciel à télécharger.

Firmware Destination File (Fichier micrologiciel de destination) Indique si le fichier est téléchargé vers le fichier image ou le fichier de démarrage.

Firmware Download via OOB (Téléchargement du micrologiciel via OOB) Télécharge le fichier micrologiciel via le port de gestion hors bande.

Active Image (Image active) Fichier image actuellement actif.

Active Image After Reset (Image active après réinitialisation) Fichier image actif après la réinitialisation du périphérique. Les valeurs possibles sont les suivantes :

Image 1 Le fichier image 1 est actif après la réinitialisation du périphérique.

Image 2 Le fichier image 2 est actif après la réinitialisation du périphérique.

Configuration File TFTP Server IP Address (Adresse IP du serveur TFTP pour fichier de configuration) Adresse IP du serveur TFTP à partir duquel les fichiers de configuration sont téléchargés.

Configuration File Source File Name (Nom du fichier de configuration source) Fichier de configuration à télécharger.

Configuration File Destination (Destination du fichier de configuration) Fichier de destination vers lequel les fichiers de configuration sont téléchargés. Ce champ peut prendre les valeurs suivantes :

Running Configuration (Configuration d'exécution) Télécharge les fichiers de configuration d'exécution.

Startup Configuration (Configuration de démarrage) Télécharge les fichiers de configuration de démarrage.

Backup Configuration (Configuration de sauvegarde) Télécharge les fichiers de configuration de sauvegarde.

Configuration Download via OOB (Téléchargement de la configuration via OOB) Télécharge le fichier de configuration via le port de gestion hors bande.

Téléchargement de fichiers

1. Ouvrez la page **File Download From Server** (Téléchargement de fichiers à partir du serveur).
2. Vérifiez l'adresse IP du serveur TFTP et assurez-vous que l'image logicielle ou le fichier de démarrage à télécharger est disponible sur le serveur TFTP.
3. Renseignez les champs **TFTP Server IP Address** (Adresse IP du serveur TFTP), **Source File Name** (Nom du fichier source) (chemin d'accès complet sans l'adresse IP du serveur TFTP) et **Destination File** (Fichier de destination) (image logicielle ou fichier de démarrage).

REMARQUE : Le fichier image remplace l'image non active. Il est recommandé d'indiquer que l'image non active deviendra l'image active après la réinitialisation et de réinitialiser le périphérique après le téléchargement.

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

Le logiciel est téléchargé sur le périphérique.

Activation des fichiers image

1. Ouvrez la page **File Download From Server** (Téléchargement de fichiers à partir du serveur).
2. Sélectionnez l'image à activer dans le menu déroulant **Active Image After Reset** (Image active après réinitialisation).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le fichier image est sélectionné.

REMARQUE : Pour activer le fichier image sélectionné, réinitialisez le périphérique. Pour obtenir des 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 définition des champs de la page **File Download From Server** (Téléchargement de fichiers à partir du serveur).

Tableau 6-46. Commandes CLI Téléchargement

Commande CLI	Description
`copy` *`source-url destination-url`*	Copie un fichier d'une source vers une destination.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console # copy tftp://172.16.101.101/file1 image

Accessing file 'file1' on 172.16.101.101...

Loading file1 from 172.16.101.101:

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

[OK]

Copy took 0:01:11 [hh:mm:ss]
```

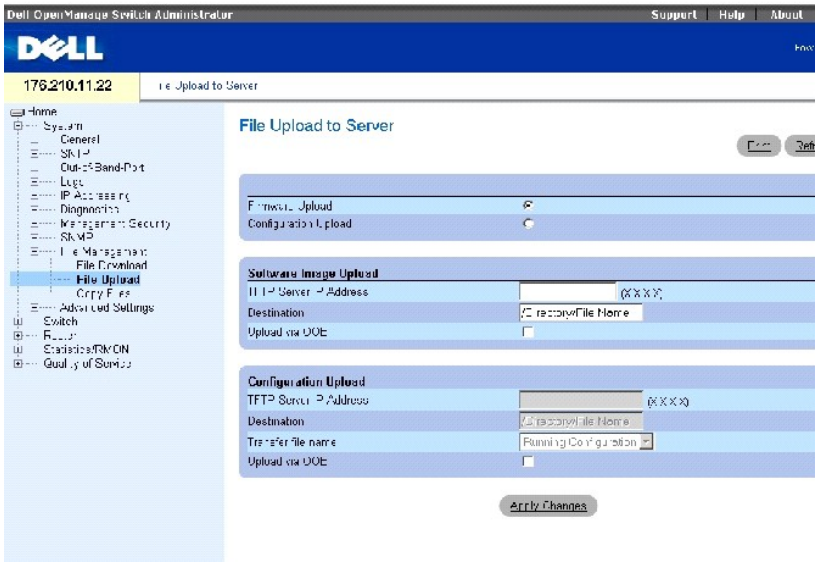
REMARQUE : Les points d'exclamation («!») indiquent que le téléchargement du fichier s'effectue normalement.

Chargement de fichiers

La page **File Upload to Server** (Chargement de fichiers sur le serveur) contient des champs permettant de charger les fichiers sur le périphérique à partir du serveur TFTP. 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 des fichiers)→ **File Upload** (Téléchargement de fichiers) dans l'*arborescence*.

Figure 6-71. Chargement de fichiers sur le serveur



La page **File Upload to Server** (Chargement des fichiers sur le serveur) contient les champs suivants :

Firmware Upload (Chargement du micrologiciel) Indique que le fichier micrologiciel est chargé. Si l'option **Firmware Upload** (Chargement du micrologiciel) est sélectionnée, les champs **Configuration Upload** (Chargement de la configuration) sont grisés.

Configuration Upload (Chargement de la configuration) Indique que le fichier de configuration est chargé. Si l'option **Configuration Upload** (Chargement de la configuration) est sélectionnée, les champs **Firmware Upload** (Chargement du micrologiciel) sont grisés.

Software Image Upload TFTP Server IP Address (Adresse IP du serveur TFTP de chargement de l'image logicielle) Adresse IP du serveur TFTP sur lequel l'image logicielle est chargée.

Software Image Upload Destination (Destination du chargement d'image du logiciel) Chemin d'accès au fichier image du logiciel vers lequel le fichier est chargé.

Software Image Upload via OOB (Chargement de l'image logicielle via OOB) Indique que l'image logicielle est chargée via le port de gestion hors bande.

Configuration Upload TFTP Server IP Address (Adresse IP du serveur TFTP de chargement de la configuration) Adresse IP du serveur TFTP sur lequel le fichier de configuration est chargé.

Configuration Upload Destination (Destination du chargement de la configuration) 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 la configuration) Fichier logiciel qui est chargé. Ce champ peut prendre les valeurs suivantes :

Running Configuration (Configuration d'exécution) Charge le fichier de configuration d'exécution.

Startup Configuration (Configuration de démarrage) Charge les fichiers de configuration de démarrage.

Backup Configuration (Configuration de sauvegarde) Charge les fichiers de configuration de sauvegarde.

Configuration Upload via OOB (Chargement de la configuration via OOB) Indique que le fichier de configuration est chargé via le port de gestion hors bande.

Chargement de fichiers

1. Ouvrez la page **File Upload to Server** (Chargement de fichiers sur le serveur).
2. Renseignez les champs applicables de la page.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le logiciel est chargé vers le serveur.

Chargement de fichiers à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des champs de la page **File Upload to Server** (Chargement de fichiers sur le serveur).

Tableau 6-47. Commandes CLI Chargement

Commande CLI	Description
`copy source-url destination-url`	Copie un fichier d'une source vers une destination.

Vous trouverez ci-dessous un exemple de commande CLI :

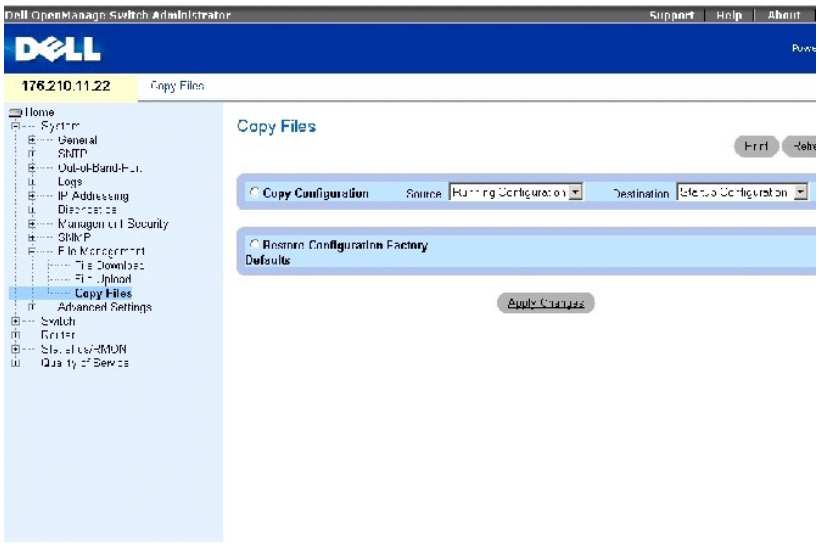
```
-----------------------------------------------------

Console#copy image tftp:16.1.1.200/file1
```

Copie de fichiers

La page **Copy Files** (Copie de fichiers) permet de copier et de restaurer les fichiers de configuration par défaut.

Pour ouvrir la page **Copy Files** (Copie de fichiers), cliquez sur **System** (Système)→ **File Management** (Gestion des fichiers)→ **Copy** (Copier) dans l'*arborescence*.

Figure 6-72. Copie de fichiers



La page **Copy Files** (Copie de fichiers) contient les champs suivants :

Copy Configuration (Copier la configuration) Indique qu'un fichier de configuration doit être copié.

Source Fichier de configuration source (exécution, démarrage, sauvegarde) à partir duquel le fichier est copié.

Destination Fichier de configuration de destination (exécution, démarrage, sauvegarde) vers lequel le fichier est copié.

Restore Configuration Factory Defaults (Restaurer les paramètres de configuration usine) Lorsqu'elle est cochée, cette option indique que les fichiers de configuration d'origine doivent être réinitialisés. Si elle n'est pas cochée, les paramètres de configuration actuels sont conservés.

REMARQUE : La copie de fichiers dans le fichier de configuration d'exécution ajoute uniquement des données de configuration ; le fichier n'est en aucun cas remplacé.

Copie de fichiers

1. Ouvrez la page **Copy Files** (Copie de fichiers).
2. Sélectionnez **Copy** (Copier) ou **Restore** (Restaurer) et renseignez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le fichier est copié.

Copie de fichiers à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des champs de la page **Copy Files** (Copie de fichiers).

Tableau 6-48. Commandes CLI Copie de fichiers

Commande CLI	Description
copy *source-url destination-url*	Copie un fichier d'une source vers une destination.
	Supprime le fichier de configuration de démarrage.

`delete startup-config`	

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# delete startup-config
```

Définition de paramètres avancés

Les paramètres avancés permettent de définir divers attributs globaux du périphérique. Les modifications apportées à ces attributs n'entrent en vigueur qu'après la réinitialisation du périphérique. Cliquez sur **System** (Système)→**Advanced Settings** (Paramètres avancés) dans l'arborescence pour ouvrir la page **Advanced Settings** (Paramètres avancés).

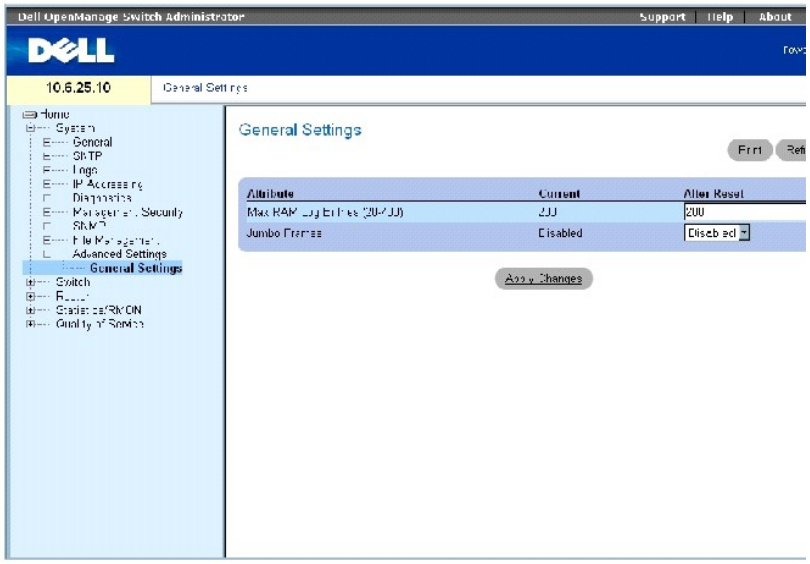
La page **Advanced Settings** (Paramètres avancés) contient un lien permettant de configurer des paramètres généraux.

Configuration des paramètres généraux

La page **General Settings** (Paramètres généraux) permet de définir les paramètres généraux du périphérique.

Pour ouvrir la page **General Settings**, cliquez sur **System** (Système)→ **Advanced Settings** (Paramètres avancés)→ **General** (Général) dans l'*arborescence*.

Figure 6-73. Paramètres généraux



La page **General Settings** (Paramètres généraux) contient les champs suivants :

Current (Actuel) Nombre maximum d'entrées.

After Reset (Après réinitialisation) Nombre maximum d'entrées après la réinitialisation du périphérique. Lorsqu'une valeur est saisie dans cette colonne, la mémoire est allouée à la table de champs.

Max RAM Log Entries (20-400) (Nombre maxi d'entrées de journal en RAM) Nombre maximum d'entrées dans les tables des journaux en RAM. La valeur par défaut est 200 entrées.

Jumbo Frames (Trames Jumbo) Permettent de transporter des 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. Les trames internes peuvent être activées en activant les trames Jumbo.

Activation des paquets jumbo

1. Ouvrez la page **General Settings** (Paramètres généraux).
2. Sélectionnez **Enabled** (Activé) dans le champ **Jumbo packets** (Paquets jumbo).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paquets jumbo sont activés sur le périphérique.

Affichage des paramètres généraux à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des champs de la page **General Settings** (Paramètres généraux).

Tableau 6-49. Commandes CLI Paramètres généraux

Commande CLI	Description
`logging buffered size` *`number`*	Définit le nombre de messages syslog stockés dans la mémoire tampon interne (RAM).
`port jumbo-frame`	Active les paquets jumbo pour le périphérique.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# logging buffered size 300
```

```
Console (config)# port jumbo-frame
```

Retour à la page du sommaire

Configuration des informations du commutateur

Systèmes Dell PowerConnect 6024/6024F

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

La page **Network Security** (Sécurité du réseau) permet de définir la sécurité du réseau à travers des listes de contrôle d'accès et des ports verrouillés. Pour ouvrir la page **Network Security** (Sécurité du réseau), cliquez sur **Switch** (Commutateur)→ **Network Security** (Sécurité du réseau).

La page **Network Security** (Sécurité du réseau) contient des liens qui vous permettent de procéder aux configurations suivantes : authentification basée sur le port, sécurité du port, ACL basées sur IP, ACL basées sur MAC et liaisons des ACL.

Authentification basée sur le port (802.1x)

L'authentification basée sur le port permet d'authentifier les utilisateurs d'un système en fonction du port, via un serveur externe. Seuls les utilisateurs authentifiés et approuvés du système peuvent transmettre et recevoir des données. Les ports sont authentifiés via le serveur RADIUS, à l'aide du protocole EAP (protocole d'authentification extensible).

Le réseau 802.1x se compose de trois éléments :

- **Authenticators** (Authentifiants) Désigne le port authentifié avant d'autoriser l'accès au système.
- **Supplicants** (Demandeur) Désigne l'hôte connecté au port authentifié qui demande à accéder aux services du système.
- **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 :

- **Controlled Access** (Accès contrôlé) Permet la communication entre l'utilisateur et le système, si l'utilisateur est autorisé.
- **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 les VLAN. Il reste toujours des VLAN spécifiques disponibles sur le commutateur, même si des ports spécifiques rattachés aux 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 :

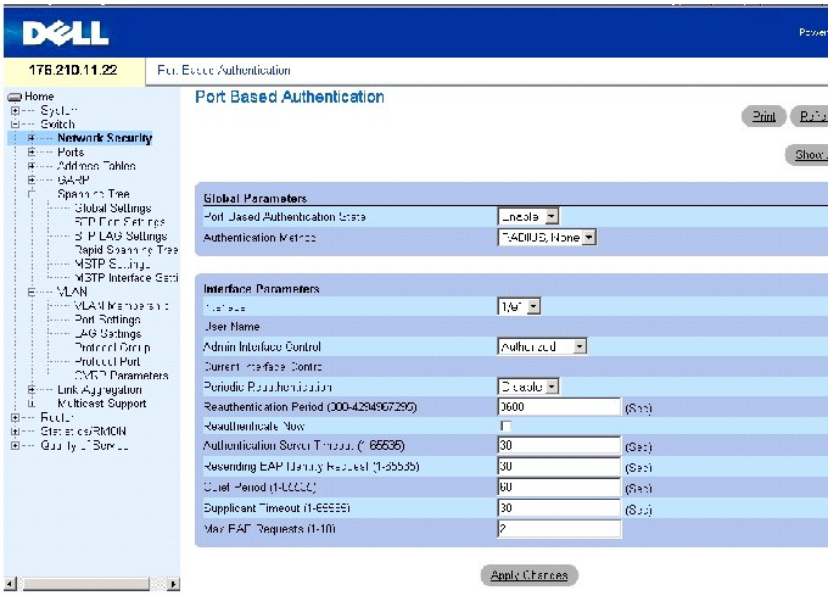
- **Single Host Mode** (Mode Hôte unique) Permet uniquement à l'hôte autorisé d'accéder au port.
- **Multiple Host Mode** (Mode Hôtes multiples) Permet à plusieurs hôtes d'être rattachés à un seul port. Il suffit d'avoir un seul hôte autorisé pour que tous les hôtes puissent accéder au réseau. Si l'authentification 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 7-1. Authentification basée sur le port



La page **Port Based Authentication** (Authentification basée sur le port) contient les champs suivants :

Port Based Authentication State (État de l'authentification basée sur le port) 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 :

RADIUS, None (Aucune) Indique que l'authentification du port est réalisée d'abord à l'aide du serveur RADIUS. Si le serveur RADIUS est introuvable, aucune méthode d'authentification n'est utilisée. Cependant, en cas d'échec, le port reste non autorisé et il n'est pas accessible.

RADIUS Indique que l'authentification s'exécute au niveau du serveur RADIUS.

None (Aucune) Indique qu'aucune méthode d'authentification n'est utilisée.

Interface Contient une liste d'interfaces à authentifier.

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 :

Auto L'authentification basée sur le port est activée au niveau du port. L'interface passe de l'état «autorisé» à l'état «non autorisé» et vice-versa au gré des échanges d'authentification entre le périphérique et le client.

Authorized (Autorisé) Met l'interface dans l'état «autorisé» sans authentification. L'interface envoie et reçoit un trafic normal sans authentification basée sur le port du client.

Unauthorized (Non autorisé) Refuse l'accès au système d'interface sélectionné en passant cette interface sur l'état «non autorisé». Le périphérique ne peut pas fournir de services d'authentification au client par cette interface.

Current Interface Control (Contrôle de l'interface en cours) État d'autorisation du port en cours. Un astérisque s'affiche si le port est actuellement arrêté.

Periodic Reauthentication (Réauthentification périodique) Réauthentifie régulièrement le port sélectionné.

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 (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]) Durée qui s'écoule avant que des demandes EAP soient renvoyées. La valeur de ce champ est exprimée en secondes. La valeur par défaut est 30 secondes.

Quiet Period (1-65535) (Période de repos [1-65535]) Définit la durée pendant laquelle le périphérique reste à l'état de repos après un échec d'authentification. Ce champ peut prendre les valeurs 0 à 65535. Ces valeurs sont exprimées en secondes. La valeur par défaut est 60 secondes.

Supplicant Timeout (1-65535) (Délai demandeur [1-65535]) Définit la durée 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.

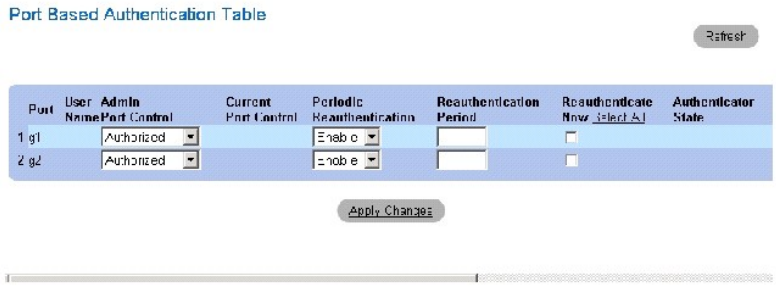
Max EAP Requests (1-10) (Nombre maxi de demandes EAP) Nombre maximum de fois que le périphérique peut envoyer une demande EAP avant de redémarrer le processus d'authentification s'il ne reçoit pas de réponse. Ce champ peut prendre des valeurs comprises entre 1 et 10. Il est paramétré par défaut sur 2 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 page **Port Based Authentication Table** (Table des authentifications basées sur le port) s'ouvre :

Figure 7-2. Table des authentifications basées sur le port



La page **Port Based Authentication Table** (Table des authentifications basées sur le port) contient les champs suivants :

Copy Parameters From Port No. (Copier les paramètres à partir du n° de port) Port à partir duquel les paramètres sont copiés.

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

Copy To (Copier vers) Copie les paramètres d'un port vers les ports sélectionnés.

Select All (Sélectionner tout) Sélectionne tous les ports de la table **Port Based Authentication Table** (Table des authentifications basées sur le port).

Copie des paramètres dans la table Port Based Authentication Table (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 page **Port Based Authentication Table** (Table des authentifications basées sur le port) s'ouvre.

3. Sélectionnez l'interface dans le champ **Copy Parameters from** (Copier les paramètres à partir de).
4. Cochez la case **Copy to** (Copier vers) pour définir les interfaces vers lesquelles les paramètres de l'authentification basée sur le port seront copiés.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont copiés dans le port sélectionné dans la table **Port Based Authentication Table** (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 de commandes CLI

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

Tableau 7-1. Commandes CLI Authentification basée sur le port

Commande CLI	Description
aaa authentication dot1x default *method1* [*method2*.]	Spécifie une ou plusieurs méthodes AAA (authentification, autorisation et comptabilisation) à utiliser sur les interfaces qui exécutent IEEE 802.1X.
dot1x system-auth- control	Active 802.1X globalement.
dot1x port-control {auto | force-authorized | force- unauthorized}	Contrôle manuellement l'état d'autorisation du port.
dot1x max-req *count*	Définit le nombre maximum de fois où le périphérique envoie un EAP au client avant de relancer le processus d'authentification.
dot1x re- authenticate [**ethernet** *interface*]	Entame manuellement une réauthentification de tous les ports activés 802.1X ou du port activé 802.1X spécifié.
dot1x re- authentication	Active la réauthentification périodique du client.
dot1x timeout quiet- period seconds	Définit le nombre de secondes pendant lesquelles le périphérique reste au repos après un échec d'authentification.
dot1x timeout re- authperiod *seconds*	Définit le nombre de secondes qui s'écoulent entre deux tentatives de réauthentification.
dot1x timeout server-timeout *seconds*	Définit la durée de la retransmission de paquets vers le serveur d'authentification.
dot1x timeout supp- timeout *seconds*	Définit la durée de la retransmission d'une trame de demande EAP au client.
dot1x timeout tx-period *seconds*	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.
show dot1x [**ethernet** *interface*]	Affiche l'état 802.1X pour le périphérique ou l'interface spécifiée.
show dot1x users [username username]	Affiche les utilisateurs 802.1X pour le périphérique.
show dot1x statistics ethernet interface	Affiche les statistiques 802.1X pour l'interface spécifiée.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# show dot1x
```

Port	Admin Mode (Mode Admin)	Oper Mode (Mode fonct)	Reaut Control (Contrôle Réauthent)	Reauth Period (Période Réauthent)	Username (Nom d'utilisateur)
----	----------	----------	-------	------	--------
g11	Auto	Authorized (Autorisé)	Ena (Activ)	3600	Bob
g12	Auto	Authorized (Autorisé)	Ena (Activ)	3600	John
g13	Auto	Unauthorized (Non autorisé)	Ena (Activ)	3600	Clark
g14	Force-aut (Auth	Authorized (Autorisé)	Dis (Désact)	3600	-

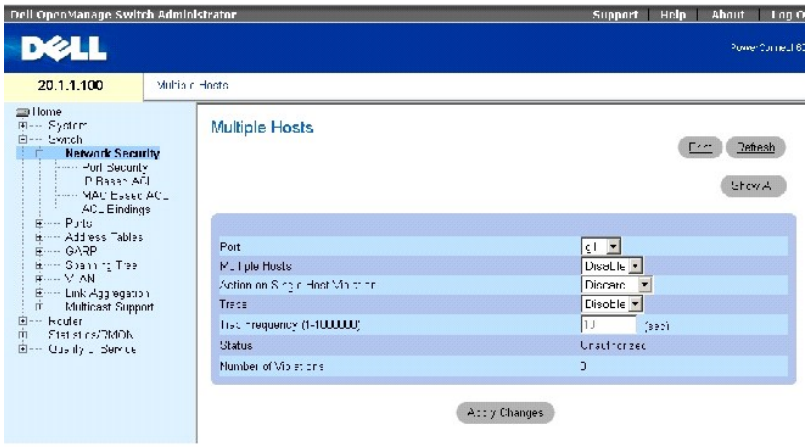
	forcée)				

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 7-3. Hôtes multiples



La page **Multiple Hosts** (Hôtes multiples) contient les champs suivants :

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

Multiple Hosts (Hôtes multiples) Permet ou non à un hôte unique d'autoriser plusieurs hôtes à accéder au système. Ce paramètre doit être activé pour désactiver le filtrage 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 prendre les valeurs suivantes :

Forward (Transmettre) Transmet les paquets provenant d'une source inconnue ; toutefois, l'adresse MAC n'est pas apprise.

Discard (Mettre au rebut) Se débarasse des paquets provenant d'une source non apprise. Il s'agit de la valeur par défaut.

Discard Shutdown (Mettre au rebut et fermer) Se débarasse des paquets provenant d'une source non apprise et ferme le port. Les ports restent fermés jusqu'à ce que le périphérique soit réinitialisé.

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

Trap Frequency (1-1000000) (Fréquence des interruptions (1-1000000)) Définit la fréquence d'envoi des interruptions à l'hôte. La valeur par défaut est

10 secondes.

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

Unauthorized (Non autorisé) Indique que le contrôle du port est **Force Unauthorized** (Non autorisation forcée), la liaison du port est coupée ou le contrôle du port est Auto, mais un client n'a pas été authentifié via ce port.

Not in auto mode (Pas en mode Auto) Indique que le contrôle du port est **Forced Authorized** (Autorisation forcée) et que les clients ont totalement accès au port.

Single-host Lock (Verrouillage unique d'un hôte) Indique que le contrôle du port est *Auto* et qu'un seul client a été authentifié via ce port.

No Single Host (Pas d'hôte unique) Indique que le mode Multiple Host (Hôtes multiples) est activé.

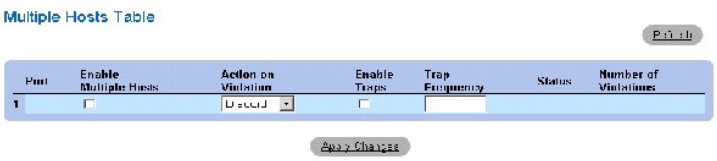
Number of Violations (Nombre de violations) Nombre de paquets arrivés sur l'interface en mode Single-host (Hôte unique), depuis un hôte dont l'adresse MAC n'est pas celle du client (demandeur).

Affichage de la page Multiple Hosts Table (Table des hôtes multiples)

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

La page **Multiple Hosts Table** (Table des hôtes multiples) s'ouvre.

Figure 7-4. Table des hôtes multiples



Activation des hôtes multiples à l'aide de commandes CLI

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

Tableau 7-2. Commandes CLI Hôtes multiples

Commande CLI	Description
dot1x multiple-hosts	Autorise plusieurs hôtes (clients) sur un port autorisé 802.1X dont la commande de configuration d'interface dot1x port-control est paramétrée sur auto.
dot1x single-host- violation {forward |discard |discard- shutdown}[trap seconds]	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.

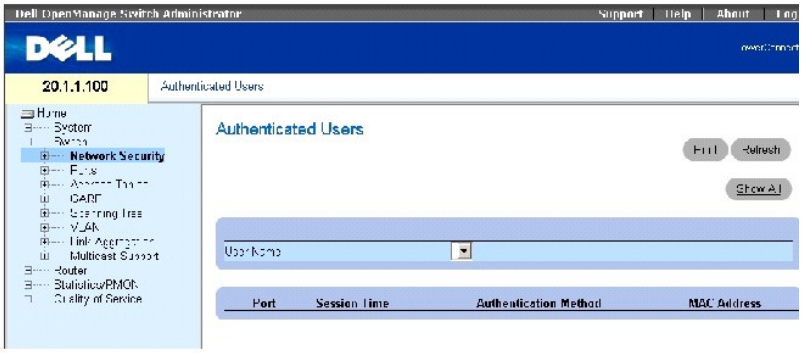
```
Console (config)# interface ethernet g11

Console (config-if)# dot1x multiple-hosts
```

Authentification d'utilisateurs

La page **Authenticated Users** (Utilisateurs authentifiés) affiche des listes d'utilisateurs avec accès au port.

Pour ouvrir la page **Authenticated Users** (Utilisateurs authentifiés), cliquez sur **Switch** (Commutateur)→ **Network Security** (Sécurité du réseau)→ **Authenticated Users** (Utilisateurs authentifiés).

Figure 7-5. Utilisateurs authentifiés



La page **Authenticated Users** (Utilisateurs authentifiés) contient les champs suivants :

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

Port Répertorie les numéros de port utilisés pour l'authentification. Les ports sont répertoriés par nom d'utilisateur.

Session Time (Durée de session) Durée de connexion de l'utilisateur au périphérique. Le format de ce champ est **Jours:Heures:Minutes:Secondes**. Exemple : 3 jours: 2 heures: 4 minutes: 39 secondes.

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

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

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

MAC Address Adresse MAC du client (demandeur).

Affichage de la table des utilisateurs authentifiés

1. Ouvrez la page **Authenticated Users** (Utilisateurs authentifiés).

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

La page **Authenticated Users Table** (Table des utilisateurs authentifiés) s'ouvre :

Figure 7-6. Table des utilisateurs authentifiés

Affichage de l'authentification d'utilisateurs à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'authentification des utilisateurs comme indiqué dans la page **Authenticated Users** (Utilisateurs authentifiés).

Tableau 7-3. Commandes CLI Ajout d'un nom d'utilisateur

Commande CLI	Description
`show dot1x users [username username]`	Affiche les utilisateurs 802.1X pour le périphérique.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# show dot1x users

Port  Username (Nom d'utilisateur)  Session Time (Durée session)  Auth Method (Méthode auth)  MAC Address (Adresse MAC)
----  --------                     ------------                  -----------                 -----------------
g12   Bob                          00:09:27                      À distance                  00:80:c8:b9:dc:1d
```

Configuration de la sécurité de port

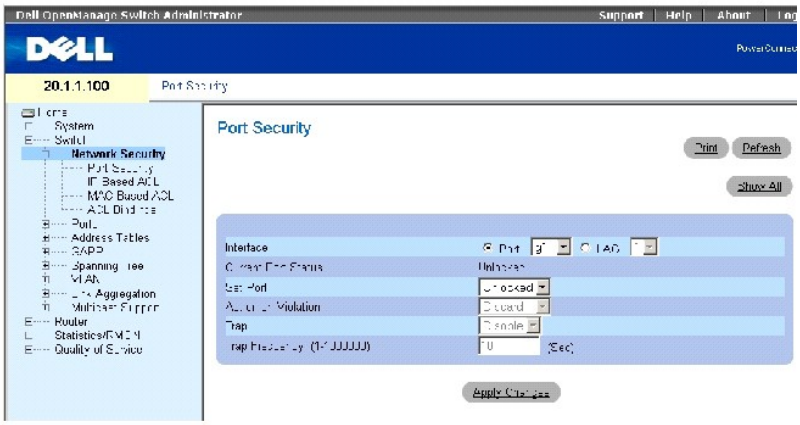
La sécurité du réseau peut être augmentée en limitant l'accès à un port spécifique aux utilisateurs possédant des adresses MAC spécifiques. Les adresses MAC peuvent être apprises de façon dynamique jusqu'à ce point ou bien configurées de façon statique. La sécurité des ports verrouillés contrôle les 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 sur un port verrouillé sont transmis, ignorés sans interruption, ignorés avec interruption ou le port d'entrée est désactivé.

La sécurité de 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 ne peuvent être activés qu'à partir de la page **Port Configuration** (Configuration 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 7-7. Sécurité des ports



Interface Indique si l'option port verrouillé est activée sur un port ou un LAG.

Current Port Status (État actuel du port) Indique si le port est actuellement verrouillé et désactivé ou s'il est déverrouillé.

Set Port (Définir le port) Permet de verrouiller le port. Lorsqu'un port est verrouillé, toutes les adresses en cours qui ont été apprises de façon dynamique par le commutateur sur ce port sont transformées en adresse MAC statiques. Lorsque le port est déverrouillé, ces adresses sont supprimées de la liste statique.

Action on Violation (Action si violation) Action à appliquer aux paquets qui arrivent sur le port. Le champ est grisé si le port est déverrouillé. Ce champ peut prendre les valeurs suivantes :

Discard (Mettre au rebut) Se débarasse des paquets provenant d'une source non apprise. Il s'agit de la valeur par défaut.

Forward (Transmettre) Transmet les paquets provenant d'une source inconnue. L'adresse MAC n'est pas apprise.

Shutdown (Arrêter) Ignore le paquet provenant d'une source non apprise et envoie une interruption. Le port d'entrée est désactivé.

Trap (Interruption) Active ou désactive l'envoi d'une interruption lorsqu'un paquet est reçu sur un port verrouillé.

Trap Frequency (Fréquence d'interruption) Délai (en secondes) entre deux interruptions.

Définition d'un port verrouillé

1. Ouvrez la page **Port Security** (Sécurité des ports).
2. Sélectionnez un type et un numéro d'interface.
3. Sélectionnez **Locked** (Verrouillé) dans le menu déroulant **Set Port** (Définir le port).
4. Renseignez les autres champs.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port verrouillé est ajouté à la table **Port Security table** (Table de sécurité de port) et le périphérique est mis à jour.

Copie des paramètres dans la table Locked Ports Table (Table des ports verrouillés)

1. Ouvrez la page **Port Security** (Sécurité des ports).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la page **Port Security Table** (Table de sécurité de port).

   Les champs de cette page sont les mêmes que ceux de la page **Port Security** (Sécurité de port).
3. Dans le champ **Copy Parameters from** (Copier les paramètres à partir de), sélectionnez une interface dans le menu déroulant **Port** ou **LAG**.

   Les définitions de sécurité de port de cette interface sont copiées vers les interfaces sélectionnées (reportez-vous à l'étape 5).
4. Cochez la case **Copy to** (Copier vers) pour sélectionner les interfaces dans lesquelles les définitions de sécurité de port seront copiées.

   Ou

   Cliquez sur **Select All** (Sélectionner tout) pour copier les définitions vers tous les ports ou tous les LAG.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

   Les paramètres sont copiés vers les ports ou les LAG sélectionnés dans la table **Port Security Table** (Table de sécurité de port) et le périphérique est mis à jour.

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 l'option de sécurité Locked Port (Port verrouillé) comme indiqué dans la page **Port Security** (Sécurité de port).

Tableau 7-4. Commandes CLI Option de sécurité Port verrouillé

Commande CLI	Description
`port security [forward | discard | discard-shutdown] [trap seconds]`	Verrouille l'apprentissage de nouvelles adresses sur une interface.
`show ports security [ethernet interface | port-channel port- channel-number]`	Affiche l'état de verrouillage du port.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface ethernet g1

Console (config-if)# port security forward trap 100

Console (config-if)# exit

Console (config)# exit
```

Console # **show ports security**

Port	status (état)	Action	Trap (Interruption)	Frequency (Fréquence)	Counter (Compteur)
----	------	------	----	---------	-------
g1	Locked (Verrouillé)	Forward (Transmettre)	Enabled (Activée)	100	0
g2	Unlocked (Déverrouillé)	-	-	-	-
...					
g24	Unlocked (Déverrouillé)	-	-	-	-
ch1 (canal1)	Unlocked (Déverrouillé)	-	-	-	-
...					
ch7 (canal7)	Unlocked (Déverrouillé)	-	-	-	-

Définition des ACL basées sur IP

Les listes de contrôle d'accès (ACL) permettent aux gestionnaires de réseau de définir des actions et des règles de classification pour des ports d'entrée spécifiques. Votre commutateur peut prendre en charge jusqu'à 1 024 ACL. Les paquets arrivant à un port d'entrée avec une ACL activée sont soit admis soit refusés à l'entrée du port, qui est désactivé. S'ils sont refusés, l'utilisateur peut désactiver le port.

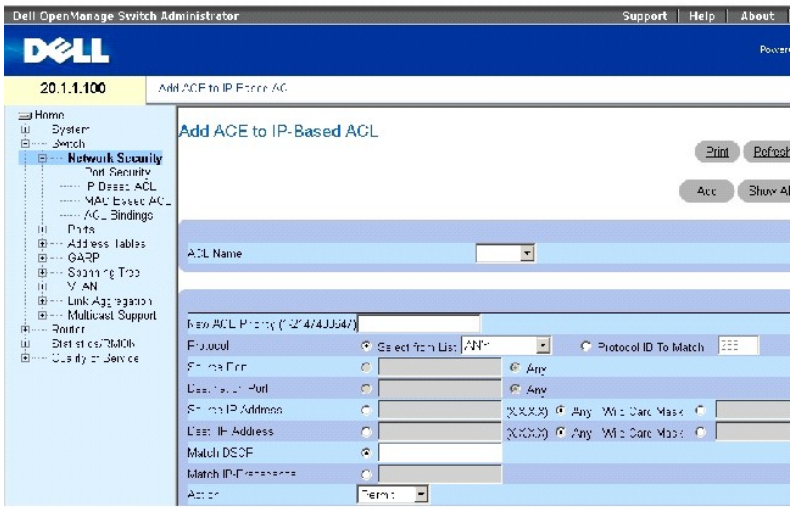
Par exemple, un administrateur réseau peut définir une règle ACL qui établit que le port numéro 20 peut recevoir des paquets TCP ; toutefois, si un paquet UDP est reçu, il est rejeté.

Les ACL sont constituées d'éléments de contrôle d'accès (ACEs) qui sont les filtres qui déterminent les classifications du trafic. Le nombre total d'ACE pouvant être définis dans toutes les ACL est 1 024.

Utilisez la page **Add ACE to IP Based ACL** (Ajout d'un ACE à une ACL basée sur IP) pour définir les ACE basés sur IP.

Pour ouvrir la page **Add ACE to IP Based ACL** (Ajout d'un ACE à une ACL basée IP), cliquez sur **Switch** (Commutateur)→ **Network Security** (Sécurité du réseau)→ **IP Based ACL** (ACL basée sur IP).

Figure 7-8. Ajout d'un ACE à une ACL basée sur l'adresse IP



La page **Add ACE to IP Based ACL** (Ajout d'un ACE à une ACL basée sur IP) contient les champs suivants :

ACL Name (Nom de l'ACL) ACL définies par l'utilisateur.

New ACE Priority (Nouvelle priorité des ACE) Priorité des ACE qui détermine quel ACE correspond à quel paquet, d'après une première mise en correspondance.

Protocol (Protocole) Permet la création d'un ACE basé sur un protocole spécifique.

Select from List (Choisir dans une liste) Sélectionnez cette option pour choisir dans une liste les protocoles sur lesquels l'ACE sera basé.

Protocol ID To Match (ID protocole de mise en correspondance) Cliquez dans cette zone pour ajouter un protocole défini par l'utilisateur suivant lequel les paquets seront mis en correspondance avec l'ACE.

REMARQUE : Tapez «any» (tous) pour sélectionner tous les protocoles IP.

Source Port (Port source) Port source TCP/UDP. Activé uniquement lorsque **800/6-TCP ou 800/17-UDP** sont sélectionnés dans le menu déroulant **Select from List** (Choisir dans une liste).

Destination Port (Port de destination) Port de destination TCP/UDP. Activé uniquement lorsque **800/6-TCP** ou **800/17-UDP** sont sélectionnés dans le menu déroulant **Select from List** (Choisir dans une liste).

Source IP Address (Adresse IP source) Met en correspondance l'adresse IP du port source à partir de laquelle les paquets sont envoyés à l'ACE.

Wild Card Mask (Masque à caractères génériques) Masque à caractères génériques de l'adresse IP source. Les masques à caractères génériques indiquent quels bits sont utilisés et lesquels sont ignorés. 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.

Dest. IP Address (Adresse IP de destination) Met en correspondance l'adresse IP du port de destination à partir de laquelle les paquets sont envoyés à l'ACE.

Wild Card Mask (Masque à caractères génériques) Masque à caractères génériques de l'adresse IP de destination. Sélectionnez **Match DSCP** (DSCP de correspondance) ou **Match IP Precedence** (Précédence IP de correspondance) :

Match DSCP (DSCP de correspondance) Met en correspondance la valeur DSCP des paquets et l'ACE. Soit la valeur DSCP, soit la valeur IP Precedence est utilisée pour mettre en correspondance les paquets et les ACL.

Match IP Precedence (Précédence IP de correspondance) Met en correspondance la valeur IP Precedence des paquets et l'ACE. Soit la valeur DSCP, soit la valeur IP Precedence est utilisée pour mettre en correspondance les paquets et les ACL.

Action Action de transmission de l'ACL. Ce champ peut prendre les valeurs suivantes :

Permit (Autoriser) Transmet les paquets qui répondent aux critères des ACL.

Deny (Refuser) Rejette les paquets qui répondent aux critères des ACL.

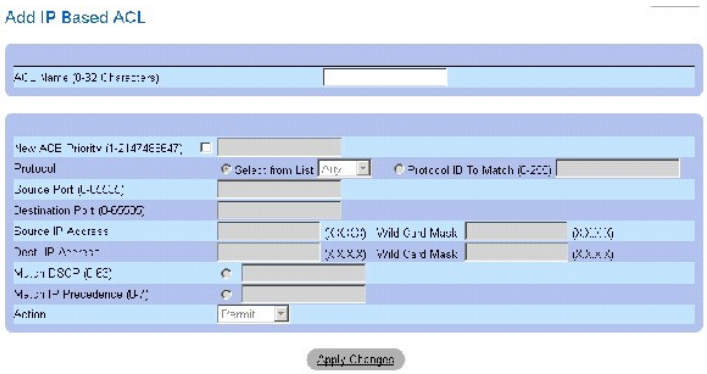
Shutdown (Arrêter) Ignore le paquet qui répond aux critères des ACL et désactive le port auquel le paquet était adressé. Les ports sont réactivés à partir de la page **Ports Configuration** (Configuration des ports). Reportez-vous à la section «Définition de la configuration des ports».

Pour connaître tous les ACE rattachés à l'ACL, cliquez sur **Show All** (Afficher tout).

Ajout d'une ACL basée sur IP

1. Ouvrez la page **Add ACE to IP Based ACL** (Ajout d'un ACE à une ACL basée sur IP).
2. Cliquez sur Add (Ajouter) pour ouvrir la page **Add IP Based ACL** (Ajout d'une ACL basée sur IP).

Figure 7-9. Ajout d'une ACL basée sur IP



3. Renseignez le champ **ACL Name** (Nom de l'ACL).
4. Cochez la case **New ACE Priority** (Nouvelle priorité des ACE) et renseignez tous les champs de la page.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'ACL basée sur IP est définie et le périphérique est mis à jour.

Modification d'un ACE basé sur IP

REMARQUE : Les ACE peuvent être modifiés uniquement lorsque l'ACL à laquelle ils appartiennent n'est pas liée à une interface.

1. Ouvrez la page **Add ACE to IP Based ACL** (Ajout d'un ACE à une ACL basée sur IP).
2. Cliquez sur **Show All** (Afficher tout) pour afficher tous les ACE de l'ACL.
3. Sélectionnez une ACL dans le champ **ACL Name** (Nom de l'ACL).
4. Modifiez les champs comme vous le désirez.

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

L'ACE basé sur IP est modifié et le périphérique est mis à jour.

Ajout de nouveaux ACE à une ACL basée sur IP

1. Ouvrez la page **Add ACE to IP Based ACL** (Ajout d'un ACE à une ACL basée sur IP).
2. Sélectionnez une ACL dans le champ **ACL Name** (Nom de l'ACL).
3. Renseignez les champs de la boîte de dialogue.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'ACE est affecté à l'ACL basée sur IP.

5. Cliquez sur Apply Changes (Appliquer les modifications) et renseignez les paramètres des nouveaux ACE de l'ACL existante

Réorganisation d'ACE dans une ACL

1. Ouvrez la page **Add ACE to IP Based ACL** (Ajout d'un ACE à une ACL basée sur IP) et sélectionnez l'ACL concernée dans le menu déroulant **ACL Name** (Nom de l'ACL).
2. Cliquez sur **Show All** (Afficher tout).

La page **ACEs Associated with IP-ACL** (ACE associés à l'ACL IP) s'affiche.

3. Entrez un numéro de priorité qui classera l'ACE comme vous le désirez.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'ACE est réorganisé et le périphérique est mis à jour.

Suppression d'ACL

1. Ouvrez la page **Add ACE to IP Based ACL** (Ajout d'un ACE à une ACL basée sur IP) et sélectionnez l'ACL concernée dans le menu déroulant **ACL Name** (Nom de l'ACL).
2. Cliquez sur **Show All** (Afficher tout).

La page **ACEs Associated with IP-ACL** (ACE associés à l'ACL IP) s'affiche.

3. Cochez la case **Remove ACL** (Supprimer ACL)
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'ACL basée sur IP est supprimée et le périphérique est mis à jour.

Affectation d'ACE basés sur IP aux ACL à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affectation d'ACE basés sur IP à des ACL comme indiqué dans la page Add ACE to IP Based ACL (Ajout d'un ACE à une ACL basée sur IP).

Tableau 7-5. Commandes CLI Ajout d'ACE basés sur IP à des ACL

Commande CLI	Description
`ip access-list` *name*	Crée des ACL IP et passe en mode de configuration des listes d'accès IP.
	Autorise le trafic si les conditions définies dans l'instruction d'autorisation sont satisfaites.

permit {any | *protocol*} {any | source *source-wildcard*} {any | destination *destination-wildcard*} [dscp *dscp number* | ip-precedence *ip-precedence*]	
deny [disable-port] {any | *protocol*} {any | source *source-wildcard*} {any | destination *destination- wildcard*} [dscp *dscp number* | ip-precedence *ip-precedence*]	Refuse le trafic si les conditions définies dans l'instruction de refus sont satisfaites.
show access-lists [*name*]	Affiche les listes de contrôle d'accès définies sur le commutateur.

Vous trouverez ci-dessous un exemple de commande CLI :

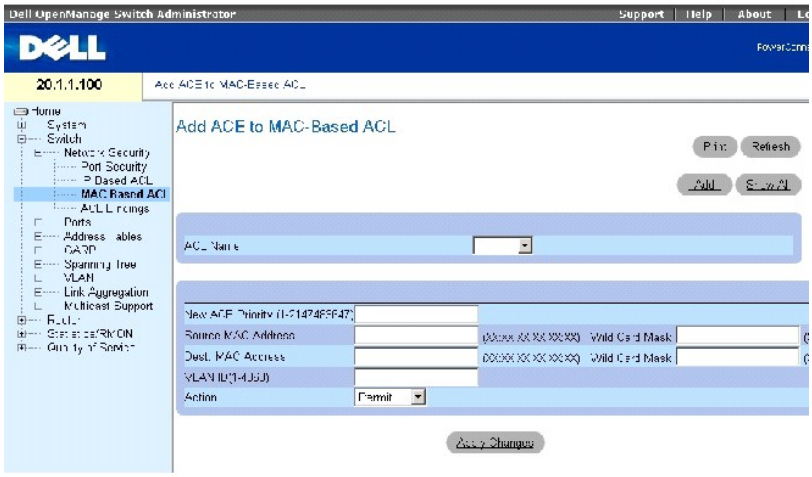
```
Console (config)# ip access-list Dell

Console (config-ip-al)# permit rsvp 12.1.1.1 0.0.0.0 any dscp 56

Console (config-ip-al)# deny any 192.1.1.10 0.0.0.255 any

Console# show access-lists

IP access list one

permit ip host 12.1.1.1 any

permit rsvp host 176.30.40.1 any

Console# show access-lists

IP access list Dell

permit rsvp 12.1.1.1 0.0.0.0 any dscp 56

deny any 192.1.1.10 0.0.0.255 any
```

Définition d'ACL basées sur MAC

La page **Add ACE to MAC Based ACL** (Ajout d'un ACE à une ACL basée sur MAC) permet aux administrateurs réseau de définir une ACL basée sur MAC. Pour obtenir une explication des ACL, reportez-vous à la section «**Définition des ACL basées sur IP**».

Pour ouvrir la page **Add ACE to MAC Based ACL** (Ajout d'un ACE à une ACL basée sur MAC), sélectionnez **Switch** (Commutateur)→ **Network Security** (Sécurité du réseau)→ **MAC based ACL** (ACL basée sur MAC).

Figure 7-10. Ajout d'un ACE à une ACL basée sur MAC



La page **Add ACE to MAC Based ACL** (Ajout d'un ACE à une ACL basée sur MAC) contient les champs suivants :

ACL Name (Nom de l'ACL) ACD définie par l'utilisateur.

New ACE Priority (Nouvelle priorité des ACE) Priorité des ACE qui détermine quel ACE correspond à quel paquet, d'après une première mise en correspondance.

Source MAC Address (Adresse MAC source) Met en correspondance l'adresse MAC source à partir de laquelle les paquets sont envoyés à l'ACE.

Wild Card Mask (Masque à caractères génériques) Masque à caractères génériques de l'adresse MAC source. Des caractères génériques sont utilisés pour masquer entièrement ou partiellement une adresse MAC source. Les masques à caractères génériques indiquent quels bits sont utilisés et lesquels sont ignorés. Un masque à caractères génériques FF:FF:FF:FF:FF:FF indique qu'aucun bit n'est important. Un masque à caractères génériques 00.00.00.00.00.00 indique que tous les bits sont importants.
Par exemple, si l'adresse MAC source est E0:3B:4A:C2:CA:E2 et que le masque à caractères génériques est 00:3B:4A:C2:CA:FF, les deux premiers bits de l'adresse MAC sont utilisés tandis que les deux derniers bits sont ignorés.

Destination MAC Address (Adresse MAC de destination) Met en correspondance l'adresse MAC de destination à partir de laquelle les paquets sont envoyés à l'ACE.

Wild Card Mask (Masque à caractères génériques) Masque à caractères génériques de l'adresse MAC de destination. Des caractères génériques sont utilisés pour masquer entièrement ou partiellement une adresse MAC de destination.

VLAN ID (ID VLAN) Met en correspondance l'ID VLAN du paquet et l'ACE. Les valeurs de ce champ sont comprises entre 1 et 4094.

Action Indique l'action de transmission de l'ACL. Ce champ peut prendre les valeurs suivantes :

Permit (Autoriser) Transmet les paquets qui répondent aux critères des ACL.

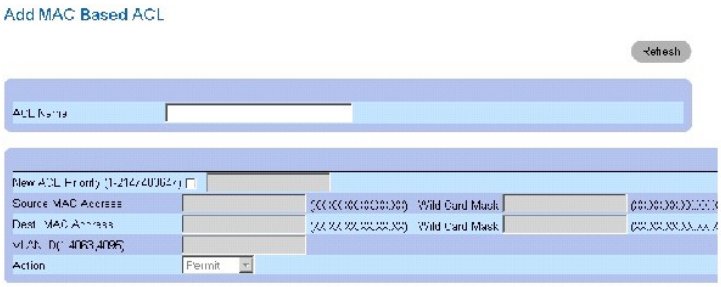
Deny (Refuser) Rejette les paquets qui répondent aux critères des ACL.

Shutdown (Arrêter) Ignore le paquet qui répond aux critères des ACL et désactive le port auquel le paquet était adressé. Les ports sont réactivés à partir de la page **Ports Configuration** (Configuration des ports). Reportez-vous à la section «Définition de la configuration des ports».

Ajout d'une ACL basée sur MAC

1. Ouvrez la page **Add ACE to MAC Based ACL** (Ajout d'un ACE à une ACL basée sur MAC).
2. Cliquez sur **Add** (Ajouter) pour ouvrir la page **Add MAC Based ACL** (Ajout d'une ACL basée sur MAC).

Figure 7-11. Ajout d'une ACL basée sur MAC



3. Renseignez le champ **ACL Name** (Nom de l'ACL).
4. Pour ajouter un nouvel ACE à l'ACL nouvellement créée, cochez la case **New ACE Priority** (Nouvelle priorité des ACE) et renseignez les champs adresse MAC **Source** et de **Destination**, **VLAN ID** (ID VLAN) et **Action**.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'ACL basée sur MAC est définie et le périphérique est mis à jour.

Modification d'un ACE basé sur MAC

1. Ouvrez la page **Add ACE to MAC Based ACL** (Ajout d'un ACE à une ACL basée sur MAC).
2. Sélectionnez une ACL dans le champ **ACL Name** (Nom de l'ACL).
3. Modifiez les champs souhaités.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Ajout d'ACE à une ACL basée sur MAC

REMARQUE : Des ACE peuvent être ajoutés uniquement lorsque l'ACL n'est pas liée à une interface.

1. Ouvrez la page **Add ACE to MAC Based ACL** (Ajout d'un ACE à une ACL basée sur MAC).
2. Sélectionnez une ACL dans le champ **ACL Name** (Nom de l'ACL).
3. Renseignez les champs **New ACE Priority** (Nouvelle priorité des ACE), adresse MAC **Source** et de **Destination**, **VLAN ID** (ID VLAN) et **Action**.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'ACE est affecté à l'ACL basée sur MAC.

REMARQUE : Pour ajouter plusieurs ACE à une ACL existante, cliquez sur **Apply Changes** (Appliquer les modifications) et complétez les paramètres des nouveaux ACE.

Affichage des ACE associés à une ACL

1. Ouvrez la page **Add ACE to MAC Based ACL** (Ajout d'un ACE à une ACL basée sur MAC).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **ACEs Associated with MAC ACL** (ACE associés à l'ACL MAC).

Suppression d'ACL

REMARQUE : Des ACL peuvent être supprimées uniquement lorsqu'elles ne sont pas liées à une interface.

1. Sélectionnez une ACL.
2. Ouvrez la page **Add ACE to MAC Based ACL** (Ajout d'un ACE à une ACL basée sur MAC).
3. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **ACEs Associated with MAC ACL** (ACE associés à l'ACL MAC).
4. Cochez la case **Remove ACL** (Supprimer ACL).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'ACL basée sur MAC est supprimée et le périphérique est mis à jour.

Suppression d'ACE dans une ACL

1. Sélectionnez une ACL.
2. Ouvrez la page **Add ACE to MAC Based ACL** (Ajout d'un ACE à une ACL basée sur MAC).
3. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **ACEs Associated with MAC ACL** (ACE associés à l'ACL MAC).
4. Cochez la case **Remove ACE** (Supprimer ACE) située sur la ligne de l'ACE à supprimer.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'ACL basée sur MAC est supprimée et le périphérique est mis à jour.

Affectation d'ACE basés sur MAC aux ACL à l'aide de commandes CLI

Le tableau ci-dessous récapitule les commandes CLI équivalentes pour l'affectation d'ACE basés sur MAC aux ACL comme indiqué dans la page **Add ACE to MAC Based ACL** (Ajout d'un ACE à une ACL basée sur MAC).

Tableau 7-6. Commandes CLI ACE basée sur MAC

Commande CLI	Description
`mac access-list name`	Crée des ACL MAC de couche 2 et passe en mode de configuration des listes d'accès MAC.
`permit {any | host source source-wildcard} {any | destination destination-wildcard}[vlan vlan-id]`	Autorise le trafic si les conditions définies dans l'instruction d'autorisation sont satisfaites.
`deny [disable-port] {any | source source- wildcard} {any | destination destination- wildcard}[vlan vlan-id]`	Refuse le trafic si les conditions définies dans l'instruction de refus sont satisfaites.
`show access-lists [name]`	Affiche les listes de contrôle d'accès configurées sur le commutateur.

Vous trouverez ci-dessous un exemple de commande CLI :

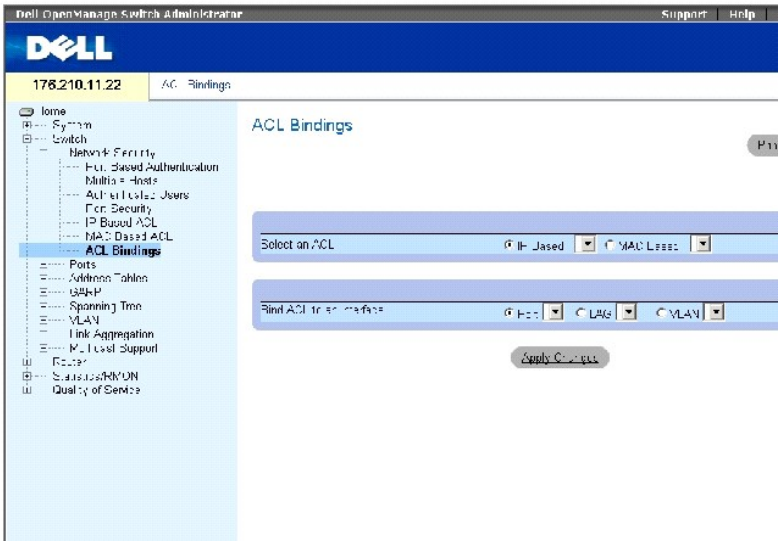
```
Console (config)# mac access-list dell

Console (config-mac-al)# permit 6:6:6:6:6:6 0:0:0:0:0:0 any vlan 4

Console (config-mac-al)# deny 6:6:6:6:6:6 0:0:255:255:255:255
```

Configuration d'une liaison d'une ACL

Lorsqu'une ACL est liée à une interface, toutes les règles d'ACE qui ont été définies sont appliquées à l'interface sélectionnée. La page **ACL Bindings** (Liaisons des ACL) permet d'affecter des listes ACL à des méthodes de classification et à des interfaces.

Pour ouvrir la page **ACL Bindings** (Liaisons des ACL), sélectionnez **Switch** (Commutateur)→ **Network Security** (Sécurité du réseau)→ **ACL Binding** (Liaison des ACL).

Figure 7-12. Liaisons des ACL



La page **ACL Bindings** (Liaisons des ACL) contient les champs suivants :

Select an ACL (Sélectionner une ACL) Indique le type d'ACL avec laquelle les paquets entrants sont mis en correspondance. Les paquets peuvent être mis en correspondance soit avec des ACL basées sur IP, soit avec des ACL basées sur MAC.

Bind ACL to Interface (Lier l'ACL à l'interface) Indique l'interface et le type de l'interface à laquelle l'ACL est rattachée. Vous pouvez rattacher l'ACL à un port, un LAG ou un VLAN.

Affectation d'une ACL à une interface

1. Ouvrez la page **ACL Bindings** (Liaisons des ACL).
2. Sélectionnez le type d'ACL dans le champ **Select ACL** (Sélectionner une ACL).
3. Définissez l'interface à laquelle l'ACL est rattachée dans le champ **Bind ACL to an Interface** (Lier une ACL à une interface).

REMARQUE : Que l'ACL soit affectée à un port, un LAG ou un VLAN, le flux provenant de cette interface d'entrée et ne correspondant pas à l'ACL est soumis à la règle par défaut Drop unmatched packets (Ignorer les paquets sans correspondance).

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

L'ACL est rattachée à l'interface.

Suppression d'un élément dans la table des liaisons des ACL

1. Ouvrez la page **ACL Bindings** (Liaisons des ACL).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **ACL Bindings Table** (Table des liaisons des ACL).
3. Cochez la case **Remove** (Supprimer) de l'élément à supprimer.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'élément sélectionné est supprimé de la table et le périphérique est mis à jour.

Affichage de la table des liaisons des ACL

1. Ouvrez la page **ACL Bindings** (Liaisons des ACL).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **ACL Bindings Table** (Table des liaisons des ACL).

Les champs de la table **ACL Bindings Table** (Table des liaisons des ACL) sont les mêmes que ceux de la page **ACL Bindings** (Liaisons des ACL).

Copie des paramètres dans la table ACL Bindings Table (Table des liaisons des ACL)

1. Ouvrez la page **ACL Bindings** (Liaisons des ACL).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **ACL Bindings Table** (Table des liaisons des ACL).
3. Sélectionnez une interface dans le champ **Copy Parameters from** (Copier les paramètres à partir de).
4. Sélectionnez un port/faisceau dans le menu déroulant **Port/LAG** ou **VLAN**.

Les définitions de cette interface seront copiées vers les ports/faisceaux cibles sélectionnés.

5. Cochez la case **Copy to** (Copier vers) pour modifier l'élément ou bien cliquez sur **Select All** (Tout sélectionner) pour copier les définitions vers tous les ports/faisceaux disponibles.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont copiés vers les ports/faisceaux cibles dans la table **ACL Bindings Table** (Table des liaisons des ACL) et le périphérique est mis à jour.

Affectation de l'appartenance d'une ACL à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour l'affectation de l'appartenance d'une ACL comme indiqué dans la page **ACL Bindings** (Liaisons des ACL).

Tableau 7-7. Commandes CLI Liaisons des ACL

Commande CLI	Description
`class-map class-map-name [match-all | match-any]`	Crée des adressages de classes et passe en mode de configuration des adressages de classes.
`match access-group acl-name`	Définit le critère de correspondance pour classer le trafic.
`show class-map [class-map- name]`	Affiche tous les adressages de classes configurés sur le périphérique.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# class-map class1 match-all

Console (config-cmap)# match access-group dell
```

```
Console (config-cmap)# exit


Console (config)# exit


Console> exit


Console> show class-map class1


Class Map match-all class1 (id4)
```

Configuration des ports

La page **Ports** contient des liens concernant la configuration des fonctionnalités des ports, notamment des fonctions avancées telles que le contrôle des tempêtes informatiques (Storm Control) et la mise en miroir des ports (Port Mirroring), ainsi que la réalisation de tests virtuels des ports.

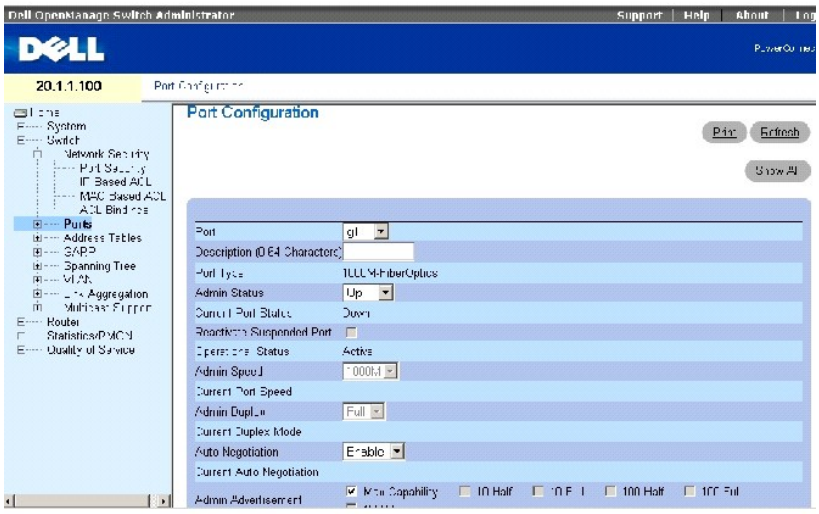
Pour ouvrir la page **Ports**, cliquez sur **Switch** (Commutateur)→ **Ports**.

Définition de la configuration des ports

La page **Port Configuration** (Configuration des ports) permet de définir les paramètres des ports.

Pour ouvrir la page **Port Configuration**, cliquez sur **Switch** (Commutateur)→ **Ports**→ **Port Configuration** (Configuration des ports) dans l'*arborescence*.

Figure 7-13. Configuration des ports



La page **Port Configuration** (Configuration des ports) contient les champs suivants :

Port Numéro du port dont les paramètres sont définis.

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

Port Type Type du port.

Admin Status (État admin) Active ou désactive la transmission du trafic passant par le port.

Current Port Status (État actuel du port) Indique si le port est actuellement actif ou s'il n'est pas opérationnel.

Reactivate Suspended Port (Réactiver un port suspendu) 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) Indique l'état opérationnel du port. Ce champ peut prendre les valeurs suivantes :

Suspended (Suspendu) Le port est actuellement activé mais ne reçoit ni n'envoie de 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. Vous ne pouvez choisir une vitesse admin que si le port est désactivé.

Current Port Speed (Vitesse actuelle du port) Indique la vitesse du port synchronisé (en b/s).

Admin Duplex Indique le mode duplex du port en b/s. **Full** (Intégral) indique que l'interface prend en charge la transmission entre le périphérique et le client 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) Indique le mode duplex du port synchronisé.

Auto Negotiation (Négociation automatique) Active la négociation automatique sur le port.
La négociation automatique est un protocole entre deux partenaires de liaison 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.

Admin Advertisement (Annonce Admin) Définit les capacités annoncées par le port. Ce champ peut prendre les valeurs suivantes :

Max Capability (Capacité maxi) — Indique que toutes les vitesses de port et tous les paramètres du mode Duplex peuvent être acceptés.

10 Half (Semi 10) — Indique que le port annonce une vitesse de 10 mb/s et un mode semi-duplex.

10 Full (Intégral 10) — Indique que le port annonce une vitesse de 10 mb/s et un mode duplex intégral.

100 Half (Semi 100) — Indique que le port annonce une vitesse de 100 mb/s et un mode semi-duplex.

100 Full (Intégral 100) — Indique que le port annonce une vitesse de 100 mb/s et un mode duplex intégral.

1000 Full (Intégral 1000) — Indique que le port annonce une vitesse de 1000 mb/s et un mode duplex intégral.

Current Advertisement (Annonce actuelle) Le port annonce sa vitesse à son port voisin pour démarrer le processus de négociation. Les valeurs possibles pour ce champ sont celles spécifiées dans le champ Admin Advertisement (Annonce Admin).

Neighbor Advertisement (Annonce de voisin) Le port voisin (port auquel l'interface sélectionnée est connectée) annonce ses capacités au port pour démarrer le processus de négociation. Les valeurs possibles sont celles spécifiées dans le champ Admin Advertisement (Annonce Admin).

Back Pressure (Contre-pression) Active le mode Contre-pression sur le port. Le mode Contre-pression est utilisé avec le mode Semi-duplex pour désactiver la capacité des ports à recevoir des messages. La contre-pression n'est pas prise en charge par les ports hors bande.

Current Back Pressure (Contre-pression actuelle) Indique le paramétrage actuel de la contre-pression.

Flow Control (Contrôle de flux) Active ou désactive le contrôle de flux ou active la négociation automatique du contrôle de flux sur le port.

Current Flow Control (Contrôle de flux actuel) Indique le paramétrage actuel du contrôle de flux.

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. Auto MDIX ne fonctionne pas sur les ports FE lorsque la négociation automatique est désactivée. MDIX n'est pas pris en charge par les ports hors bande.

Ce champ peut prendre les valeurs suivantes :

Media Dependent Interface with Crossover (MDIX) (Interface croisée dépendante du support [MDIX]) Utilisée pour les concentrateurs et les commutateurs.

Media Dependent Interface (MDI) (Interface dépendante du support [MDI]) Utilisée pour les stations terminales.

Current MDI/MDIX (MDI/MDIX actuelle) Indique le paramétrage actuel de MDIX sur le périphérique. Ce champ peut prendre les valeurs suivantes :

MDI Le paramétrage MDI actuel est MDI.

MDIX Le paramétrage MDI actuel est MDIX.

Auto Indique que la valeur est définie automatiquement.

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

PVE Active un port comme étant un port PVE (Private VLAN Edge). Lorsqu'un port est défini comme étant un PVE, il contourne la base de données de transmission (FDB) et transmet tout le trafic de monodiffusion, de multidiffusion et de diffusion à une liaison montante (à l'exception des paquets MAC-to-me). Les liaisons montantes peuvent être un port ou un LAG. Le trafic provenant de la liaison montante est réparti sur toutes les interfaces.

Définition des paramètres des ports

1. Ouvrez la page **Port Configuration** (Configuration des ports).
2. Sélectionnez un port dans le champ **Port**.
3. Renseignez les champs de la boîte de dialogue.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres du port sont sauvegardés sur le périphérique.

Affichage de la table des ports

1. Ouvrez la page **Port Configuration** (Configuration des ports).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **Port Configuration Table** (Table de configuration des ports).

Configuration des ports à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des ports comme indiqué dans la page **Port Configuration** (Configuration des ports).

Tableau 7-8. Commandes CLI Configuration des ports

Commande CLI	Description
`interface ethernet interface`	Passe au mode de configuration de l'interface afin de configurer une interface de type Ethernet.
`description string`	Ajoute une description à une configuration d'interface.
`shutdown`	Désactive les interfaces qui font partie du contexte en cours de définition.
`set interface active {ethernet interface | port- channel port-channel- number}`	Réactive une interface qui a été arrêtée pour des raisons de sécurité.
`speed {10 | 100 | 1000}`	Configure la vitesse d'une interface Ethernet donnée lorsque la négociation automatique n'est pas utilisée.
`duplex {half | full}`	Configure le fonctionnement en mode Duplex intégral/Semi-duplex d'une interface Ethernet donnée lorsque la négociation automatique n'est pas utilisée.
`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}`	Configure le contrôle de flux sur une interface donnée.
`mdix {on | auto}`	Active l'inverseur automatique sur une interface ou un canal de port donné.
`show interfaces configuration [ethernet interface | port-channel port-channel-number oob- eth interface]`	Affiche la configuration de toutes les interfaces configurées.
	Affiche l'état de toutes les interfaces configurées.

show interfaces status [ethernet *interface* | port- channel *port-channel- number* oob-eth *interface*]	
show interfaces description [ethernet *interface* | port-channel *port-channel-number* oob- eth *interface*]	Affiche la description de toutes les interfaces configurées.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface ethernet g18

Console (config-if)# description RD_SW#3

Console (config-if)# speed 100

Console (config-if)# shutdown

Console (config-if)# no shutdown

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> set interface active ethernet g9
```

```
Console> show interfaces status
```

					Flow (Contrôle du	Link (État	Back (Contre-	Mdix (Mode
Port	Type	Duplex	Speed (Vitesse)	Neg (Nég)	ctrl flux)	State liaison)	Pressure pression)	Mode Mdix)
---	------	----	---	---	-----	-----	-----	-----
g1	1G- Copper (cuivre)	Full (Intégral)	1000	Enabled (Activée)	Off (Éteint)	Up (Opérationnelle)	Disabled (Désactivée)	Off (Éteint)

g2	1G- Copper (cuivre)	Full (Intégral)	1000	Enabled (Activée)	Off (Éteint)	Up (Opérationnelle)	Disabled (Désactivée)	Off (Éteint)
g3	1G- Copper (cuivre)	Full (Intégral)	1000	Enabled (Activée)	Off (Éteint)	Up (Opérationnelle)	Disabled (Désactivée)	Off (Éteint)

Ch (Canal)	Type	Duplex	Speed (Vitesse)	Neg (Nég)	Flow (Contrôle du control flux)	Link (État State liaison)	Back (Contre-Pressure pression)
---	--------	-----	----	----	------	------	-------
ch1 (canal1)	Unknown (Inconnu)	Unknown (Inconnu)		Unknown (Inconnu)	Off (Éteint)	Not Present (Absente)	Unknown (Inconnu)
ch2 (canal2)	Unknown (Inconnu)	Unknown (Inconnu)		Unknown (Inconnu)	Off (Éteint)	Not Present (Absente)	Unknown (Inconnu)
ch3 (canal3)	Unknown (Inconnu)	Unknown (Inconnu)		Unknown (Inconnu)	Off (Éteint)	Not Present (Absente)	Unknown (Inconnu)
ch4 (canal4)	Unknown (Inconnu)	Unknown (Inconnu)		Unknown (Inconnu)	Off (Éteint)	Not Present (Absente)	Unknown (Inconnu)

```
Console# show interfaces configuration
```

Ch (Canal)	Type	Duplex	Speed (Vitesse)	Neg (Nég)	Flow (Contrôle du control flux)	Admin (État State admin)	Back (Contre-Pressure pression)
---	-------	---	---	----	-------	-----	--------
ch1 (canal1)	Unknown (Inconnu)			Enabled (Activée)	Off (Éteint)	Up (Opérationnelle)	Disabled (Désactivée)
ch2 (canal2)	Unknown (Inconnu)			Enabled (Activée)	Off (Éteint)	Up (Opérationnelle)	Disabled (Désactivée)
ch3 (canal3)	Unknown (Inconnu)			Enabled (Activée)	Off (Éteint)	Up (Opérationnelle)	Disabled (Désactivée)

```
Console# show interfaces description ethernet 1
```

Port	Description
-----	-----------------
g1	connect_to_server (connexion_au_serveur)

Définition de la configuration des LAG

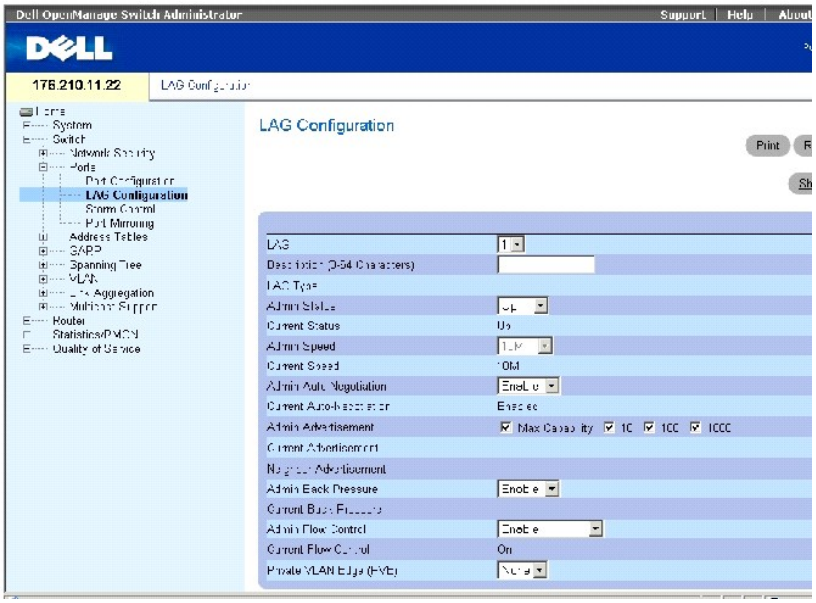
Les commutateurs multicouche prennent en charge le groupage de plusieurs liaisons en une seule liaison logique à capacité ajoutée appelée groupe de liaisons agrégées (LAG). Les LAG sont souvent appelés faisceaux ou liaisons agrégées.

Utilisez la page **LAG Configuration** (Configuration des LAG) pour configurer les paramètres des LAG. Votre commutateur prend en charge jusqu'à sept ports par LAG et sept LAG par système. 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.

Pour plus d'informations sur l'agrégation des ports et l'affectation de ports aux LAG, reportez-vous à la section «Agrégation de ports».

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

Figure 7-14. Configuration des LAG



La page **LAG Configuration** (Configuration des LAG) contient les champs suivants :

LAG Contient la liste des numéros de LAG.

Description (0-64 Characters) (Description (0-64 caractères)) Description du port.

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

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

Current Status (État actuel) Indique si le LAG est actuellement actif.

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

Current Speed (Vitesse actuelle) Indique la vitesse actuelle de fonctionnement 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 Advertisement (Annonce Admin) Définit les capacités annoncées par le LAG. Ce champ peut prendre les valeurs suivantes :

Max Capability (Capacité maxi) - Indique que toutes les vitesses de LAG et tous les paramètres du mode Duplex peuvent être acceptés.

10 - Indique que le port annonce une vitesse de 10 mb/s et un mode duplex intégral.

100 - Indique que le port annonce une vitesse de 100 mb/s et un mode duplex intégral.

1000 - Indique que le port annonce une vitesse de 1000 mb/s et un mode duplex intégral.

Current Advertisement (Annonce actuelle) Le LAG annonce ses capacités à son LAG voisin pour démarrer le processus de négociation. Les valeurs possibles pour ce champ sont celles spécifiées dans le champ Admin Advertisement (Annonce Admin).

Neighbor Advertisement (Annonce de voisin) Le LAG voisin (LAG auquel l'interface sélectionnée est connectée) annonce ses capacités au LAG pour démarrer le processus de négociation. Les valeurs possibles sont celles spécifiées dans le champ Admin Advertisement (Annonce Admin).

Admin Back Pressure (Contre-pression admin) Active ou désactive le mode Contre-pression sur le périphérique. 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) Indique si le mode Contre-pression est activé ou désactivé.

Admin Flow Control (Contrôle de flux admin) Active ou désactive le contrôle de flux ou active la négociation automatique du contrôle de flux sur 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 disponibles.
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) pour afficher la table **LAG Configuration Table** (Table de configuration des LAG).

Configuration des LAG à l'aide de commandes CLI

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

Tableau 7-9. Commandes CLI Configuration des LAG

Commande CLI	Description
`interface port-channel port-channel-number`	Passe au mode de configuration de l'interface d'un canal de port spécifique.
`channel-group port- channel-number mode {on | auto}`	Associe un port à un canal de port.
`show interfaces port- channel [port-channel- number]`	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)# interface ethernet g5

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

Console (config-if)# exit

Console# show interfaces port-channel

Channel     Port

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

Ch 1        Active   g1, g2, g5   Inactive g3

Ch 2        Active   g2

Ch 3        Inactive g8
```

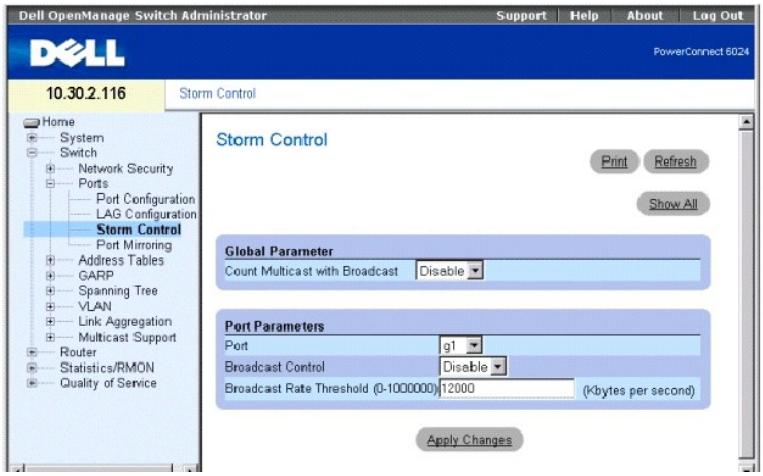
Activation de la fonction de contrôle des tempêtes informatiques

Une tempête de diffusion (Broadcast Storm) 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.

Votre commutateur mesure la fréquence des paquets de diffusion/multidiffusion entrants sur chaque port et ignore les paquets lorsque la fréquence dépasse une limite définie. La fonction de contrôle des tempêtes informatiques est activée par périphérique, à travers la définition du type de paquet et de la vitesse à laquelle les paquets sont transmis. Les ports peuvent également être regroupés de façon à assurer la protection Storm pour l'ensemble du groupe.

La page **Storm Control** (Contrôle des tempêtes informatiques) permet d'activer et de configurer la fonction de contrôle des tempêtes informatiques. Pour ouvrir la page **Storm Control**, cliquez sur **Switch** (Commutateur)→ **Ports**→ **Storm Control** (Contrôle des tempêtes informatiques) dans l'*arborescence*.

Figure 7-15. Page Contrôle des tempêtes informatiques



Count Multicast with Broadcast (Compter multidiffusion et diffusion) **Enable** (Activer) : compte le trafic diffusion et multidiffusion ; **Disable** (Désactiver) : compte uniquement le trafic diffusion.

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

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

Broadcast Rate Threshold (Fréquence seuil diffusion) Définit la fréquence limite (en kilo-octets par seconde) à laquelle les paquets inconnus sont transmis. La plage s'étend de 0 à 148 800. La valeur par défaut est 12 000. Toutes les valeurs sont arrondies au multiple de 64 Ko/s supérieur. Si la valeur du champ est inférieure à 64 Ko/s, elle est arrondie à 64 Ko/s.

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

1. Ouvrez la page **Storm Control** (Contrôle des tempêtes informatiques).
2. Renseignez les champs de cette page.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Copie des paramètres dans la table des paramètres de la fonction de contrôle des tempêtes informatiques

1. Ouvrez la page **Storm Control** (Contrôle des tempêtes informatiques).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **Storm Control Settings Table** (Table des paramètres de la fonction de contrôle des tempêtes informatiques).
3. Choisissez le port à partir duquel vous souhaitez copier les paramètres dans le champ **Copy Parameters from Port** (Copier les paramètres à partir du port).
4. Cochez la case **Copy to** (Copier vers) pour définir les interfaces où les définitions de la fonction de contrôle des tempêtes informatiques seront copiées ou bien cliquez sur **Select All** (Tout sélectionner) pour copier les définitions dans tous les ports.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres sont copiés vers les ports sélectionnés dans la table **Storm Control Settings Table** (Table des paramètres de la fonction de contrôle des tempêtes informatiques) et le périphérique est mis à jour.

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 7-10. Commandes CLI Contrôle des tempêtes informatiques

Commande CLI	Description
`port storm-control include-multicast`	Active la fonction pour compter les paquets multidiffusion et les paquets diffusion.
`port storm-control broadcast enable`	Active la fonction de contrôle des tempêtes informatiques de diffusion.
`port storm-control broadcast rate rate`	Configure la fréquence de diffusion maximale.
`show ports storm-control port`	Affiche la configuration de la fonction de contrôle des tempêtes informatiques.

Vous trouverez ci-dessous un exemple de commande CLI :

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

Console (config)# interface ethernet g1

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

Console (config-if)# port storm-control broadcast rate 100000

Console (config-if)# exit
```

Port	Broadcast and Multicast Storm Control [Kbytes/sec] (Fonction de contrôle des tempêtes informatiques de diffusion et multidiffusion [Ko/s])	
----	----------	
g1		100000
g2		Disabled (Désactivée)
...		
g24		Disabled (Désactivée)

Définition de sessions Port Mirroring (Mise en miroir)

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 peut être utilisée comme outil de diagnostic et/ou de débogage. Elle permet également la surveillance des performances du commutateur.

Les administrateurs réseau configurent la mise en miroir des ports en sélectionnant un port spécifique vers lequel copier tous les paquets et différents ports à partir desquels les paquets sont dupliqués. Avant de configurer la fonction de mise en miroir des ports, notez bien ce qui suit :

- Les ports mis en miroir ne peuvent pas fonctionner plus rapidement que le port de contrôle.
- Le nombre de ports source est limité à huit.
- Une seule session de mise en miroir peut être configurée à la fois.

Les restrictions suivantes s'appliquent aux ports configurés pour être des ports de destination :

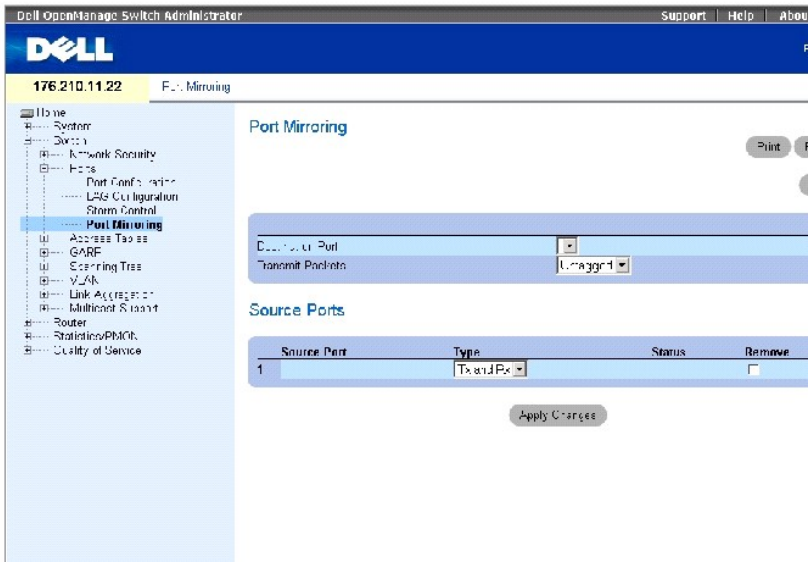
- Les ports ne peuvent pas être configurés comme ports source.
- Les ports ne peuvent pas être membres d'un LAG.
- Des interfaces IP ne sont pas configurées sur le port.
- GVRP n'est pas activé sur le port.
- Le port n'est pas membre d'un VLAN.
- Un seul port de destination peut être défini.

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

- Les ports source ne peuvent pas être membres d'un LAG.
- Les ports ne peuvent pas être configurés comme ports de destination.
- Tous les paquets sont marqués lorsqu'ils sont transmis depuis le port de destination.
- Tous les paquets 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*.

Figure 7-16. Mise en miroir des ports



La page **Port Mirroring** (Mise en miroir des ports) contient les champs suivants :

Destination Port (Port de destination) Contient la liste des numéros de port à partir desquels le trafic des ports peut être copié.

Transmit Packets (Transmission des paquets) Indique si les paquets sont transmis marqués ou non marqués à partir du port de destination.

Source Port (Port source) Numéro du port vers lequel le trafic est mis en miroir.

Type Indique le type du trafic surveillé. Ce champ peut prendre les valeurs suivantes :

TX Surveille uniquement les paquets transmis.

RX Surveille uniquement les paquets reçus.

TX and RX (TX et RX) Surveille les paquets transmis et les paquets reçus.

Status (État) Indique si le port est actuellement surveillé (**Active** [Actif]) ou non (**Not Ready** [Pas prêt]).

Remove (Supprimer) Lorsqu'elle est cochée, cette option permet de supprimer 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 **Add** (Ajouter) pour afficher la page **Add Source Port** (Ajout d'un port source).
3. Sélectionnez un port source dans le menu déroulant **Source Port** (Port source).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle session de mise en miroir des ports est activée pour le port et le périphérique est mis à jour.

Modification d'une session de mise en miroir des ports

1. Ouvrez la page **Port Mirroring** (Mise en miroir des ports).
2. Modifiez les champs.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les champs de la session de mise en miroir des ports sont modifiés et le périphérique est mis à jour.

Suppression 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 supprimée 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 indiqué dans la page **Port Mirroring** (Mise en miroir des ports).

Tableau 7-11. Commandes CLI Mise en miroir des ports

Commande CLI	Description
`port monitor src-interface [rx | tx]`	Démarre une session de surveillance des ports.
`show ports monitor`	Affiche l'état de la surveillance des ports.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config-if)# port monitor g2
```

Configuration des tables d'adresses

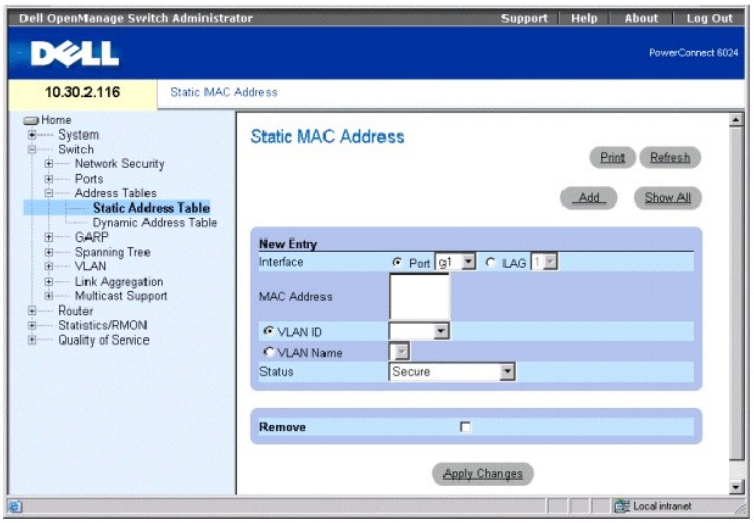
Les adresses MAC sont stockées soit dans la base de données d'adresses statiques, soit dans la base de données d'adresses dynamiques. Les adresses statiques sont définies par l'utilisateurs. Les adresses dynamiques sont apprises par le système et sont effacées après un certain délai. Un paquet adressé à une destination stockée dans l'une des bases de données est transmis immédiatement aux ports. Les tables d'adresses statiques et dynamiques peuvent être triées par interface, par VLAN et par type d'interface. Des adresses peuvent également être ajoutées aux tables d'adresses dynamiques et statiques.

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 Address** (Adresse statique) contient une liste d'adresses MAC statiques. Des adresses statiques peuvent être ajoutées et supprimées de la table des adresses MAC statiques. Pour ouvrir la page **Static Address** (Adresse statique), cliquez sur **Switch** (Commutateur)→ **Address Table** (Table des adresses)→ **Static Address** (Adresse statique) dans l'*arborescence*.

Figure 7-17. Page 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.

REMARQUE : Seules les adresses MAC affectées à l'interface et au VLAN indiqués sont affichées. Pour consulter les adresses MAC affectées à un autre VLAN, choisissez-le dans le sélecteur de VLAN.

VLAN ID 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 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.

Ajout d'une adresse MAC statique

1. Ouvrez la page **Static MAC Address** (Adresse MAC statique).
2. Cliquez sur **Add** (Ajouter) pour ouvrir la page **Add Static MAC Address** (Ajout d'une adresse MAC statique).
3. Renseignez les 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) pour afficher la table **Static MAC Address Table** (Table des adresses MAC statiques).
3. Sélectionnez une entrée de la table.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Configuration des paramètres des adresses statiques à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration des paramètres des adresses statiques comme indiqué dans la page **Static MAC Address** (Adresse MAC statique).

Tableau 7-12. Commandes CLI Adresses statiques

Commande CLI	Description
`bridge address mac-address {ethernet interface | port- channel port-channel- number} [permanent | delete-on-reset | delete- on-timeout | secure]`	Ajoute une adresse source de station de couche MAC statique à la table de pontage.
`show bridge address-table static [vlan vlan] [ethernet interface | port- channel port-channel- number]`	Affiche les entrées créées de façon statique dans la base de données de transmission de pont.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface vlan 1 Console

(config-vlan)# bridge address 3aa2.64b3.a245 ethernet g8 permanent....



Console (config-vlan)# exit

Console (config)# exit

Console> show bridge address-table static



Aging time is 300 sec



Vlan  Mac Address           Port   Type

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

1     3a:a2:64:b3:a2:45     g8     permanent
```

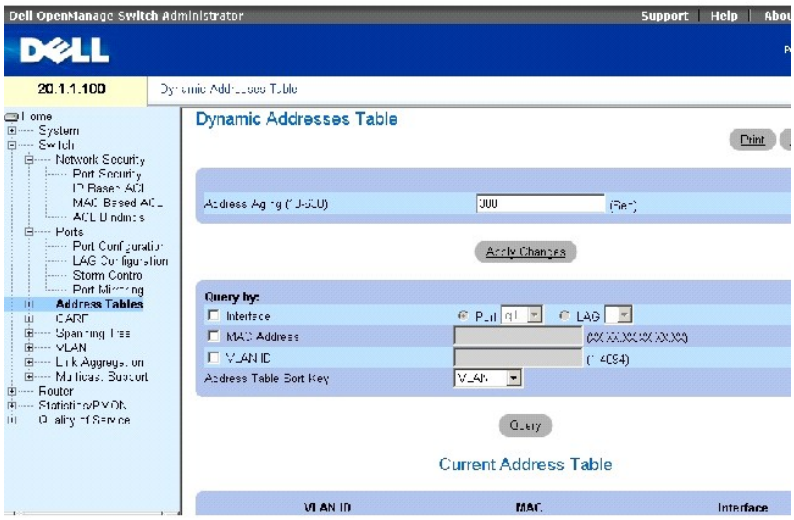
Affichage des adresses dynamiques

La page **Dynamic Addresses 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, VLAN et la clé de tri de la table. Les paquets transmis à une adresse stockée dans la table des adresses sont transmis directement à ces ports.

La page **Dynamic Address Table** (Table des adresses dynamiques) contient également des informations sur le délai d'expiration au bout duquel une adresse MAC dynamique est supprimée de la table.

Pour ouvrir la page **Dynamic Address Table** (Table des adresses dynamiques), cliquez sur **Switch** (Commutateur)→ **Address Tables** (Tables des adresses)→ **Dynamic Addresses Table** (Table des adresses dynamiques) dans l'*arborescence*.

Figure 7-18. Table des adresses dynamiques



La page **Dynamic Address Table** (Table des adresses dynamiques) contient les champs suivants :

Address Aging (10-630) (Expiration adresse (10-630)) Indique le délai d'expiration, en secondes, au bout duquel une adresse MAC dynamique est effacée. La valeur par défaut est 300 secondes.

La table **Dynamic Address Table** (Table des adresses dynamiques) peut être interrogée par :

Port Interface sur laquelle porte l'interrogation d'adresse.

MAC Address (Adresse MAC) Adresse MAC sur laquelle porte l'interrogation d'adresse.

VLAN ID (ID VLAN) Numéro du VLAN (auquel l'adresse MAC est rattachée) sur lequel porte l'interrogation d'adresse.

Address Table Sort Key (Clé de tri de la table des adresses) Indique si la table des adresses dynamiques est triée par adresse, VLAN ou interface.

Définition du délai d'expiration

1. Ouvrez la page **Dynamic Address Table** (Table des adresses dynamiques).
2. Renseignez le champ **Address Aging** (Expiration adresse).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le délai d'expiration est modifié et le périphérique est mis à jour.

Interrogation de la table des adresses dynamiques

1. Ouvrez la page **Dynamic Address Table** (Table des adresses dynamiques).
2. Définissez le paramètre en fonction duquel la table **Dynamic Address Table** (Table des adresses dynamiques) doit être interrogée.

*L*es entrées peuvent être interrogées par **port**, par **adresse MAC** ou par **ID 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.

Table des adresses actuelles

La table des adresses actuelles contient les paramètres d'adresse dynamique en fonction desquels les paquets sont directement transmis aux ports. La table des adresses actuelles contient les champs suivants :

- **VLAN ID** (ID VLAN) Indique la valeur de numéro VLAN.
- **MAC** Indique l'adresse MAC.
- **Port** Indique le numéro du port.

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 indiqué dans la page **Dynamic Address Table** (Table des adresses dynamiques).

Tableau 7-13. Commandes CLI Interrogation et tri

Commande CLI	Description
`bridge aging-time` *`seconds`*	Définit le délai d'expiration de la table d'adresses.
`show bridge address-table [vlan vlan] [ethernet` *`interface`* `| port-channel` *`port-channel-number`*`]`	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 300

Console (config)# exit

Console# show bridge address-table

Aging time is 300 sec

vlan   mac address      port    type
```

```
----    --------------    -----    -----

1       0060.704C.73FF    g8       dynamic

1       0060.708C.73FF    g8       dynamic

200     0010.0D48.37FF    g9       static
```

Configuration du protocole GARP

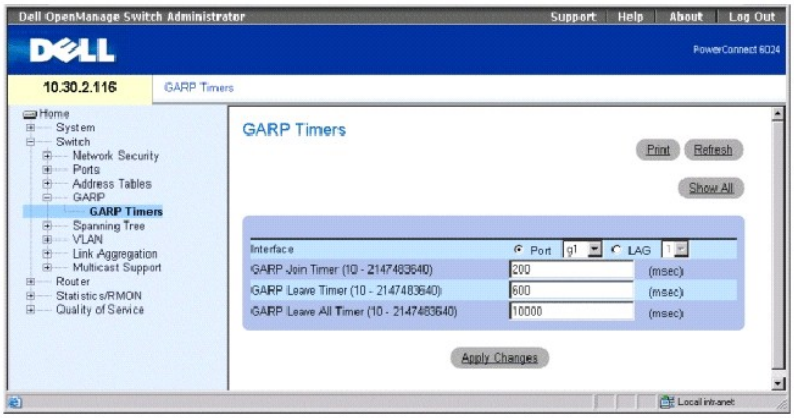
Le protocole GARP (Generic Attribute Registration Protocol) est un protocole universel qui enregistre toutes les informations relatives à la connectivité du réseau ou au style d'appartenance au réseau. Le protocole GARP définit un ensemble de périphériques intéressés par un attribut de réseau donné, tel qu'un VLAN ou une adresse de multidiffusion.

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 paramètres permettant d'activer 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 7-19. Temporisateurs GARP



La page **GARP Timers** (Temporisateur GARP) contient les champs suivants :

Interface Indique si les temporisateurs sont activés sur un port ou sur un LAG.

GARP Join Timer (10 - 2147483640) (Temporisateur Join GARP) 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 (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 d'arrivée (Join). Ce champ peut prendre la valeur 0-2147483640. La valeur par défaut est de 600 ms.

GARP Leave All Timer (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 une valeur comprise entre 0 et 2147483640. La valeur par défaut est 10 000 ms.

Définition des temporisateurs GARP

1. Ouvrez la page **GARP Timers** (Temporisateurs GARP).
2. Renseignez les 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) pour afficher la table **GARP Timers Table** (Table des temporisateurs GARP).
3. Sélectionnez une interface dans le champ **Copy Parameters from** (Copier les paramètres à partir de).
4. Sélectionnez une interface dans le menu déroulant **Port** ou **LAG**.
5. Les définitions de cette interface seront copiées vers 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 7-14 récapitule les commandes CLI équivalentes pour la définition des temporisateurs GARP comme indiqué dans la page **Garp Timers** (Temporisateurs GARP).

Tableau 7-14. Commandes CLI Temporisateurs GARP

Commande CLI	Description
`garp timer {join | leave | leaveall} timer_value`	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 g8

Console (config-if)# garp timer leave 900
```

Configuration du protocole Spanning Tree

Le protocole Spanning Tree (STP) fournit une topologie 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 itinéraires 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.

Le périphérique prend en charge les versions de protocole Spanning Tree suivantes : Classic STP, Rapid STP et Multiple STP.

Classic STP fournit un chemin unique entre les stations terminales, évitant et éliminant ainsi les boucles. Pour des informations sur la configuration de Classic STP, reportez-vous à la section **Defining STP Global Settings** (Définition des paramètres globaux STP).

Rapid STP (RSTP) détecte et utilise des topologies de réseau qui permettent une convergence plus rapide du Spanning Tree sans création de boucles de transmission. Pour des informations sur la configuration de RSTP, reportez-vous à la section **Définition de Rapid Spanning Tree**.

Multiple STP (MSTP) fournit une connectivité complète pour les paquets alloués à un VLAN. MSTP est basé sur RSTP. Par ailleurs, MSTP transmet des paquets affectés à différents VLANS par l'intermédiaire de différentes régions MST. Les régions MST fonctionnent comme un simple pont. MSTP améliore la tolérance de pannes du système et permet un équilibrage de la charge. Pour des informations sur la configuration de MSTP, reportez-vous à la section **Définition de Multiple Spanning Tree**.

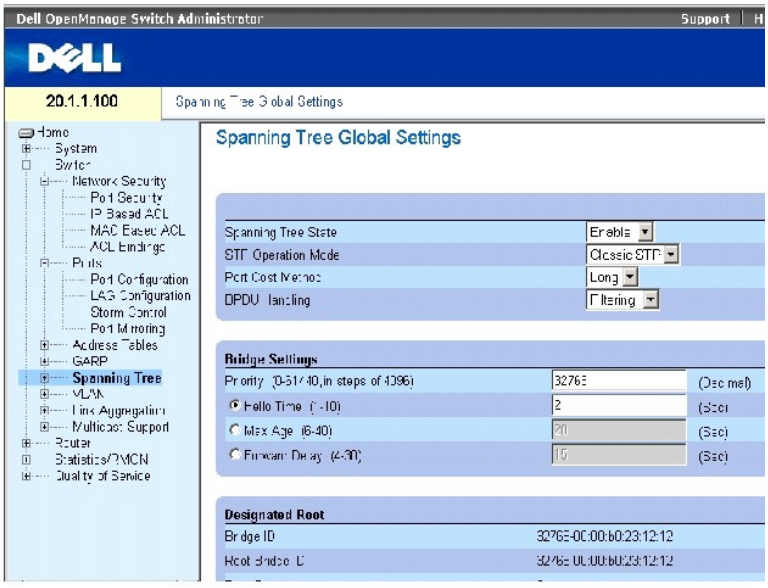
Pour ouvrir la page **Spanning Tree**, cliquez sur **Switch** (Commutateur)→ **Spanning Tree** dans l'*arborescence*.

Définition des paramètres globaux STP

La page **Spanning Tree Global Settings** (Paramètres globaux Spanning Tree) contient des paramètres permettant d'activer le protocole STP sur le périphérique.

Pour ouvrir la page **Spanning Tree Global Settings** (Paramètres globaux Spanning Tree), cliquez sur **Switch** (Commutateur)→ **Spanning Tree**→ **Global Settings** (Paramètres globaux) dans l'*arborescence*.

Figure 7-20. Paramètres globaux Spanning Tree



La page **Spanning Tree Global Settings** (Paramètres globaux Spanning Tree) contient les champs suivants :

Spanning Tree State (État Spanning Tree) Active ou désactive STP, RSTP ou MSTP sur le périphérique.

STP Operation Mode (Mode de fonctionnement STP) Mode STP pour lequel STP est activé sur le périphérique. Ce champ peut prendre les valeurs suivantes : **Classic STP**, **Rapid STP et Multiple STP**.

Path Cost Method (Méthode de coût de résolution) Indique la méthode utilisée pour affecter des coûts de résolution par défaut aux ports STP. Ce champ peut prendre les valeurs suivantes :

Long (Longue) Les valeurs de la méthode de coût de résolution sont comprises entre 1 et 200 000 000.

Short (Courte) Les valeurs de la méthode de coût de résolution sont comprises entre 1 et 65 535. Il s'agit de la méthode par défaut.

Les coûts de résolution affectés à une interface varient selon la méthode sélectionnée :

Interface	Longue	Courte
LAG	20 000	4
1 000 Mbps	20 000	4
100 Mbps	200 000	19
10 Mbps	2 000 000	100

BPDU Handling (Gestion BPDU) Définit la gestion des paquets BPDU lorsque Spanning Tree est désactivé sur une interface. Ce champ peut prendre les valeurs suivantes : Filtering (Filtrage) et Flooding (Inondation). La valeur par défaut est Flooding (Inondation).

Priority (0-65535) (Priorité [0-65535]) Valeur de la priorité du pont. 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.

Hello Time (1-10) Délai Hello Time du commutateur, qui 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]) Délai d'attente maximal du commutateur, qui indique la durée, en secondes, pendant laquelle un pont attend avant de mettre en place une modification de topologie. La valeur par défaut est 20.

Forward Delay (4-30) (Délai avant transmission [4-30]) Délai avant transmission du commutateur, qui indique la durée, en secondes, pendant laquelle un pont reste dans un état d'écoute et d'apprentissage avant de transmettre des paquets. La valeur par défaut est 15.

Bridge ID (ID pont) ID du pont.

Root Bridge ID (ID pont racine) ID 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) Nombre total de modification de l'état STP qui se sont produites.

Last Topology Change (Dernière modification de topologie) Durée qui s'est écoulée depuis la dernière modification topographique. Cette durée s'affiche selon un format jour heure minutes secondes ; par exemple, 5 heures 10 minutes et 4 secondes.

Définition des paramètres globaux STP

1. Ouvrez la page **Spanning Tree Global Settings** (Paramètres globaux Spanning Tree).
2. Sélectionnez le port à activer 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 **Spanning Tree Global Settings** (Paramètres globaux Spanning Tree).
2. Renseignez les champs de la boîte de dialogue.
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 **Spanning Tree Global Settings** (Paramètres globaux Spanning Tree).

Tableau 7-15. Commandes CLI Paramètres globaux STP

Commande CLI	Description
`spanning-tree`	Active la fonctionnalité Spanning Tree.
`spanning-tree mode {stp | rstp}`	Configure le mode du protocole Spanning Tree.
`spanning-tree pathcost method {long | short}`	Configure la méthode de coût de résolution Spanning Tree.
`spanning-tree bpdu {filtering | flooding}`	Configure la gestion des paquets BPDU lorsque Spanning Tree est désactivé sur une interface.
`spanning-tree priority` *priority*	Configure la priorité Spanning Tree.
`spanning-tree hello-time` *seconds*	Configure le délai Hello Time du pont Spanning Tree qui correspond à la fréquence à laquelle le commutateur diffuse des messages Hello aux autres commutateurs.
`spanning-tree max-age` *seconds*	Configure le délai d'attente maximal du pont Spanning Tree.
`spanning-tree forward- time` *seconds*	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.
`show spanning-tree [ethernet` *interface* `| port-channel` *port- channel-number*`]`	Affiche la configuration de Spanning Tree.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# spanning-tree

Console (config)# spanning-tree mode rstp

Console (config)# spanning-tree priority 12288

Console (config)# spanning-tree hello-time 5

Console (config)# spanning-tree max-age 10

Console (config)# spanning-tree forward-time 25

Console (config)# exit

Console# show spanning-tree

Spanning Tree enabled mode RSTP

Root ID Priority 32768

Address 0001.4297.e000

Cost 57

Port g1

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769

Address 0002.4b29.7a00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Number of topology changes 8 last change occurred 00:37:24 ago

Times: hold 1, topology change 35, notification 2

hello 2, max age 20, forward delay 15
```

Interface	Port ID (ID port)			Designated (Désigné)		Port ID (ID port)

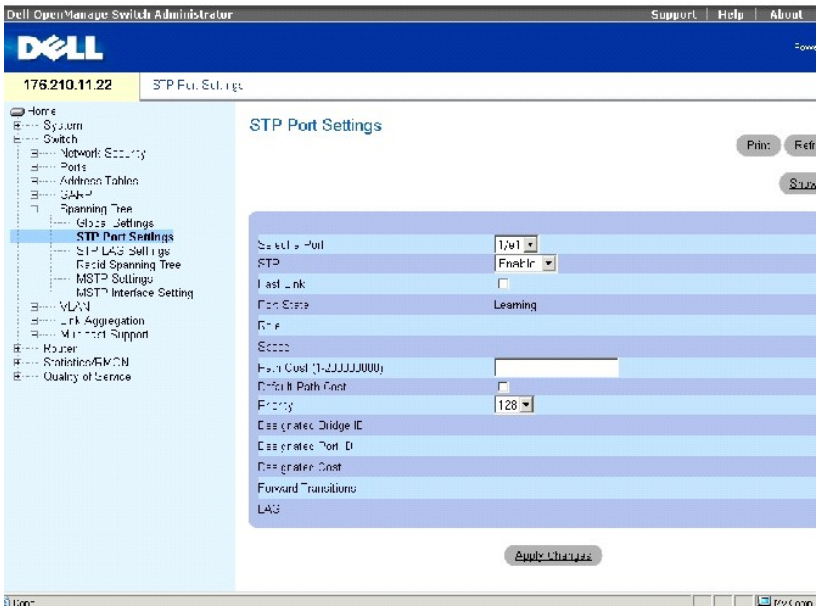
Name (Nom)	Prio	Sts (État)	Enb (Act)	Cost (Coût)	Cost (Coût)	Bridge id (ID pont)		Prio.Nbr (N° prio)	
----	----	----	---	----	----	----	---------	---	---
g1	128	DSBL (DÉSACT)	FAUX	100	0	8 000	00:00:b0:70:09:00	80	001
g2	128	DSBL (DÉSACT)	FALSE (FAUX)	100	0	8 000	00:00:b0:70:09:00	80	002
g3	128	DSBL (DÉSACT)	FALSE (FAUX)	100	0	8 000	00:00:b0:70:09:00	80	003
ch1 (canal1)	128	DSBL (DÉSACT)	TRUE (VRAI)	4	0	8 000	00:00:b0:70:09:00	80	019
ch2 (canal2)	128	DSBL (DÉSACT)	TRUE (VRAI)	4	0	8 000	00:00:b0:70:09:00	80	01a
ch3 (canal3)	128	DSBL (DÉSACT)	TRUE (VRAI)	4	0	8 000	00:00:b0:70:09:00	80	01b

Définition des paramètres des ports STP

La page **STP Port Settings** (Paramètres des ports STP) permet d'affecter des propriétés STP aux ports individuels.

Pour ouvrir la page **STP Port Settings**, cliquez sur **Switch** (Commutateur)→ **Spanning Tree**→ **Port Settings** (Paramètres des ports) dans l'*arborescence*.

Figure 7-21. Paramètres des ports STP



La page **STP Port Settings** (Paramètres des ports STP) contient les champs suivants :

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 Lorsqu'elle est cochée, cette option active le mode Fast Link pour le port. Si le mode Fast Link est activé, 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) Indique l'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) Le protocole STP est actuellement désactivé sur le port. Le port peut transmettre du trafic et apprendre de nouvelles adresses MAC.

Blocking (Blocage) Le port est actuellement bloqué et ne peut pas être utilisé pour transmettre du trafic ou pour apprendre des adresses MAC.

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 (Transmission) Le port est actuellement en mode de transmission. Le port peut transmettre du trafic et apprendre de nouvelles adresses MAC.

Speed (Vitesse) Indique la vitesse de fonctionnement du port.

Path Cost (1-200,000,000) (Coût de résolution (1-200 000 000)) 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) Indique que le coût de résolution par défaut est affecté selon la méthode sélectionnée dans la page **Spanning Tree Global Settings** (Paramètres globaux Spanning Tree).

Priority (0-240) (Priorité (0-240) Valeur de la 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.

Designated Bridge ID (ID du pont désigné) ID du pont désigné.

Designated Port ID (ID du port désigné) ID du port sélectionné.

Designated Cost (Coût désigné) Coût du port participant à la topologie STP. Les ports à moindre coût sont ordinairement moins bloqués si le STP détecte des boucles.

Forward Transitions (Transitions de transmission) Nombre de fois où le port est passé de l'état **Forwarding** (Transmission) à l'état **Disabled** (Désactivé).

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. Renseignez 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), **Path Cost** (Coût de résolution) et **Fast Link** (Liaison rapide).
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 indiqué dans la page **STP Port Settings** (Paramètres des ports STP).

Tableau 7-16. Commandes CLI Paramètres des ports STP

Commande CLI	Description
`spanning-tree disable`	Désactive Spanning Tree sur un port spécifique.
`spanning-tree cost` *`cost`*	Configure le coût de résolution de Spanning Tree pour un port.
`spanning-tree port-priority` *`priority`*	Configure la priorité du port.
`show spanning-tree [ethernet interface | port-channel` *`port-channel-number`*`]`	Affiche la configuration de Spanning Tree.
`spanning-tree portfast`	Active le mode PortFast.

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)# spanning-tree portfast

Console (config-if)# exit

Console (config)# exit

Console# show spanning-tree ethernet g1
```

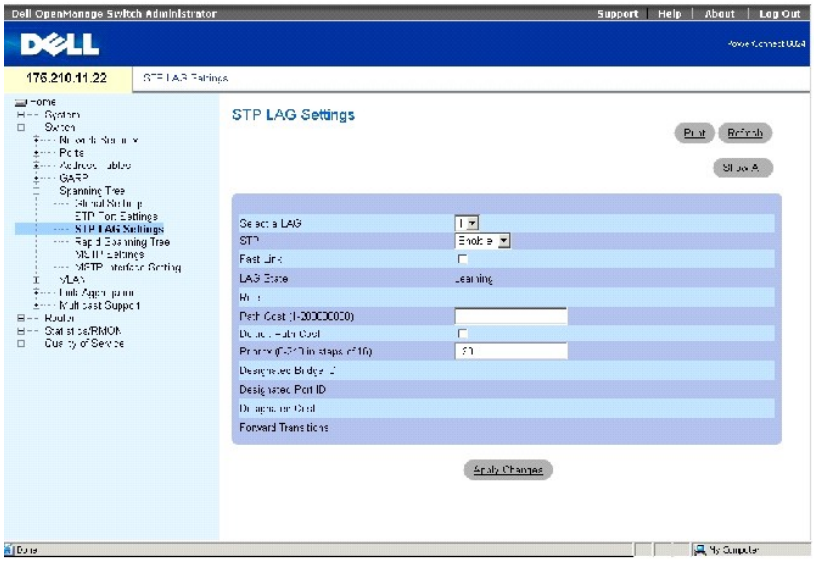
Interface	Port ID (ID port)	Designated (Désigné)			Port ID (ID port)
Name (Nom)	Prio.Nbr (N° prio)	Cost (Coût)	Sts (État)	Cost Bridge ID (ID pont coût)	Prio.Nbr (N° prio)
--------	-------	---	--	-------------------	------
g1	128.1	19	FWD	38 32768 0030.9441.62c1	128.25

```
Spanning tree enabled

Type: point-to- point (configured

: auto)

Port Fast: no (configured: no)
```

Définition des paramètres des LAG STP

La page **STP LAG Settings** (Paramètres des LAG STP) permet d'affecter des paramètres d'agrégation de ports STP. Pour ouvrir la page **STP LAG Settings** (Paramètres des LAG STP), cliquez sur **Switch** (Commutateur)→ **Spanning Tree**→ **LAG Settings** (Paramètres des LAG) dans l'*arborescence*.

Figure 7-22. Paramètres des LAG STP



La page **STP LAG Settings** (Paramètres des LAG STP)contient les champs suivants :

Select a LAG (Sélectionner un LAG) Numéro de LAG dont les paramètres STP vont être modifiés.

STP Active ou désactive le protocole STP sur le LAG.

Fast Link Active le mode Fast Link sur le LAG. Si le mode Fast Link est activé sur 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) Le protocole STP est actuellement désactivé sur le LAG. Le LAG peut transmettre du trafic et apprendre de nouvelles adresses MAC.

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 des 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 (Transmission) Le LAG est actuellement en mode de transmission. 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) 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.

Default Path Cost (Coût de résolution par défaut) Indique que le coût de résolution par défaut est affecté selon la méthode sélectionnée dans la page **Spanning Tree Global Settings** (Paramètres globaux Spanning Tree).

Priority (0-240) (Priorité (0-240)) Valeur de la 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 étapes de 16.

Designated Bridge ID (ID du pont désigné) ID du pont désigné.

Designated Port ID (ID du port désigné) ID du port désigné.

Designated Cost (Coût désigné) Coût du port participant à la topologie STP. Les ports à moindre coût sont ordinairement moins bloqués si le STP détecte des boucles.

Forward Transitions (Transitions de transmission) Nombre de fois où la valeur **LAG State** (État du LAG) est passée de **Forwarding** (Transmission) à **Disabled** (Désactivé).

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 7-17. Commandes CLI Paramètres des LAG STP

Commande CLI	Description
`spanning-tree`	Active la fonctionnalité Spanning Tree.
`spanning-tree cost` *`cost`*	Configure le coût de résolution de Spanning Tree pour un port.
`spanning-tree port-priority` *`priority`*	Configure la priorité du port.
`show spanning-tree [ethernet interface | port-channel` *`port-channel-number`*`]`	Affiche la configuration de Spanning Tree.
`spanning-tree portfast`	Active le mode Port Fast.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface port-channel 1

Console (config-if)# spanning-tree disable
```

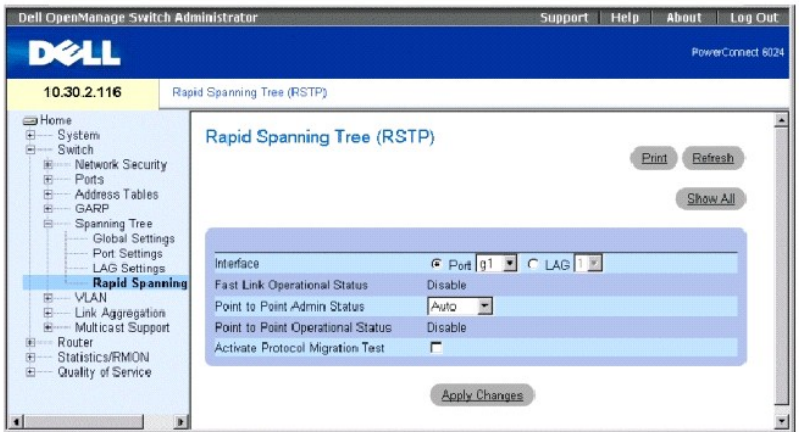
```
Console (config-if)# spanning-tree cost 35000

Console (config-if)# spanning-tree port-priority 96

Console (config-if)# spanning-tree portfast

Console (config-if)# exit

Console (config)# exit

Console# show spanning-tree port-channel 1

Interface Port ID Designated Port ID

Name   Prio  Sts    Enb    Cost   Cost   Bridge Id               Prio.Nbr

------ ----  ------ -----  ------ ------ ----------------------  ----------------
ch1    96    DSBL   FALSE  35000  0      32768 00:00:b0:11:00:00  96



Spanning tree disabled

Port Fast : yes (configured: yes)

Type: point-to-point (configured: auto)

Number of transitions to forwarding state: 0
```

Définition de Rapid Spanning Tree

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. Le délai permet de détecter les boucles possibles et de propager les modifications d'état.

Le protocole RSTP (Rapid Spanning Tree Protocol) détecte et utilise des topologies de réseau qui permettent une convergence plus rapide du Spanning Tree sans création de boucles de transmission. Pour ouvrir la page Rapid Spanning Tree (RSTP) (Protocole RSTP), cliquez sur **Switch** (Commutateur)→ **Spanning Tree**→ **Rapid Spanning Tree** dans l'*arborescence*.

Figure 7-23. Page Rapid Spanning Tree (RSTP)



Interface Port ou LAG sur lequel Rapid STP est activé.

Fast Link Operational Status (État opérationnel Fast Link) Indique si le mode Fast Link (Liaison rapide) est activé ou désactivé sur le port ou le LAG. Si le mode Fast Link est activé sur 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 via la liaison. La liaison restera configurée pour des communications jusqu'à ce que des paquets LCP ou NCP explicites la ferment ou jusqu'à ce qu'un événement extérieur survienne. Il s'agit du type de liaison de port de commutation 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 Migration Test (Activer le test de la migration de protocole) Lorsqu'elle est cochée, cette option permet au protocole PPP d'envoyer des paquets LCP (Link Control Protocol) pour configurer et tester la liaison de données.

Activation du protocole RSTP

1. **Ouvrez la page Rapid Spanning Tree** (Protocole RSTP).
2. Renseignez 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.

Affichage de la table Rapid Spanning Tree (RSTP)

1. **Ouvrez la page Rapid Spanning Tree** (Protocole RSTP).
2. Cliquez sur **Show All** (Afficher tout).

La table **Rapid Spanning Tree (RSTP) Table** (Table RSTP) s'ouvre.

Définition des paramètres Rapid STP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des paramètres RSTP comme indiqué dans la page **RSTP**.

Tableau 7-18. Commandes CLI Paramètres RSTP

Commande CLI	Description
`spanning-tree link-type {point-to-point | shared}`	Remplace le paramètre du type de liaison par défaut.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface ethernet g5

Console (config-if)# spanning-tree link-type shared
```

Définition de Multiple Spanning Tree

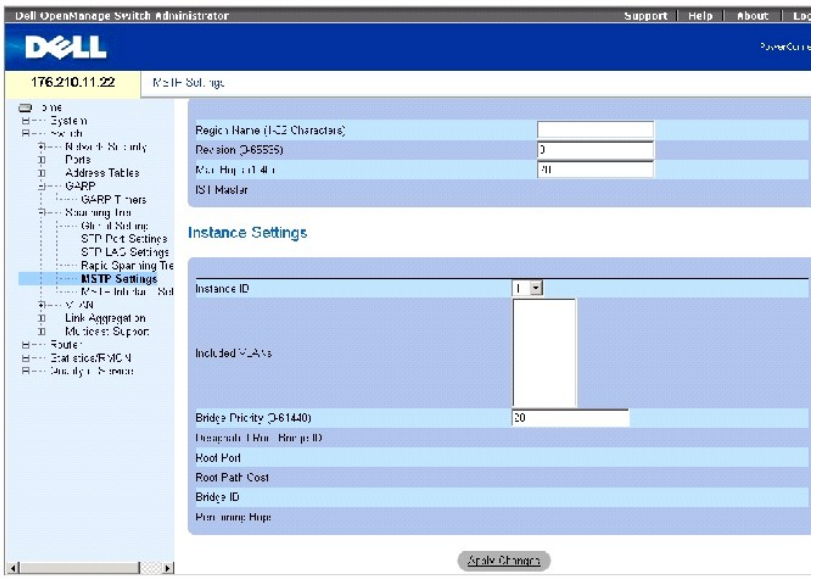
MSTP (Multiple Spanning Tree Protocol) mappe des VLAN en interfaces STP.

MSTP fournit un scénario d'équilibrage de la charge différent. Par exemple, lorsque le port A est bloqué dans une instance STP, ce même port est placé dans l'état Forwarding (Transmission) dans une autre instance STP. La page **MSTP Settings** (Paramètres MSTP) permet de définir jusqu'à seize instances MSTP pour le périphérique.

Par ailleurs, les paquets affectés à différents VLAN sont transmis via différents chemins au sein des régions MST (Multiple Spanning Trees). Les régions sont un ou plusieurs ponts Multiple Spanning Tree interconnectés ayant la même configuration MSTP. Lors de la configuration d'un MST, la région MST à laquelle votre périphérique appartient est définie. Une configuration consiste à indiquer le nom, la révision et la région à laquelle votre périphérique appartient.

Pour ouvrir la page **MSTP Settings** (Paramètres MSTP), cliquez sur **Switch** (Commutateur)→ **Spanning Tree**→ **MSTP Region Configuration** (Configuration des régions MSTP) dans l'*arborescence*.

Figure 7-24. MSTP Settings (Paramètres MSTP)



La page **MSTP Settings** (Paramètres MSTP) contient les champs suivants, divisés en deux sections :

Region Name (1-32) (Nom de la région (1-32)) Indique le nom de la région MST défini par l'utilisateur.

Revision (0-65535) [Révision (0-65535]) Indique le numéro non signé sur 16 bits qui identifie la révision de la configuration MST actuelle. Le numéro de révision est requis pour la configuration MST.

Max Hops (1-40) (Sauts maxi [1-40]) Indique le nombre total de sauts survenant d'une région donnée avant la mise au rebut du BPDU. Une fois le BPDU mis au rebut, les informations sur le port arrivent à expiration. La valeur par défaut de ce champ est 20.

IST Master (IST maître) Indique l'ID Internal Spanning Tree maître. L'IST maître est la racine de l'instance spécifiée ; son instance est 0.

Instance ID (ID instance) Définit l'ID de l'instance Spanning Tree. La plage de valeurs de ce champ est comprise entre 1 et 15.

Included VLANs (VLAN inclus) Mappe les VLAN sélectionnés sur l'instance sélectionnée. Chaque VLAN appartient à une seule instance.

Bridge Priority (0-61440) (Priorité de pont [0-61440]) Définit la priorité du périphérique pour l'instance Spanning Tree sélectionnée.

Designated Root Bridge ID (ID pont racine désigné) Indique l'ID du pont qui présente le coût de résolution le plus faible jusqu'à l'instance racine.

Root Port (Port racine) Indique le port racine de l'instance sélectionnée.

Root Path Cost (Coût de résolution racine) Indique le coût de résolution de l'instance racine jusqu'à la région racine.

Bridge ID (ID pont) Indique l'ID du pont de l'instance sélectionnée.

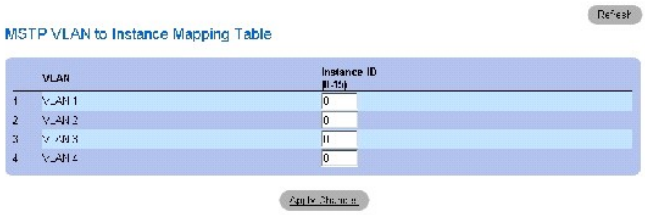
Remaining Hops (Sauts restants) Indique le nombre de sauts restants jusqu'à la prochaine destination.

Affichage de la table d'adressage de VLAN MSTP à des instances

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

La page **MSTP VLAN to Instance Mapping Table** (Table d'adressage de VLAN MSTP à des instances) s'ouvre :

Figure 7-25. Table d'adressage de VLAN MSTP à des instances



Définition d'instances MST à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition de groupes d'instances MST comme indiqué dans la page **MSTP Settings** (Paramètres MSTP).

Tableau 7-19. Commandes CLI Instances MSTP

Commande CLI	Description
`spanning-tree mst configuration`	Active le mode de configuration MST.
`instance instance-id {add | remove} vlan vlan-range`	Adresse des VLAN à l'instance MST.
`name string`	Définit le nom de la configuration.
`revision value`	Définit le numéro de révision de la configuration
`spanning-tree mst instance-id port- priority priority`	Définit la priorité du port.
`spanning-tree mst instance-id priority priority`	Définit la priorité du périphérique pour l'instance Spanning Tree spécifiée.
`spanning-tree mst max- hops hop-count`	Définit le nombre de sauts dans une région MST avant la mise au rebut du BPDU et l'expiration des informations concernant un port.
`spanning-tree mst instance-id cost cost`	Définit le coût de résolution du port en vue de calculs MST
`exit`	Quitte le mode de configuration MST et applique les modifications apportées à la configuration.
`abort`	Quitte le mode de configuration MST sans appliquer les modifications apportées à la configuration.
`show {current | pending}`	Affiche la configuration des régions MST actuelle ou en attente.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# spanning-tree mst configuration

Console (config-mst)# instance 1 add vlan 10-20

Console (config-mst)# name region1

Console (config-mst)# revision 1

Console (config)# spanning-tree mst configuration

Console (config-mst)# instance 2 add vlan 21-30
```

```
Console (config-mst)# name region1


Console (config-mst)# revision 1


Console (config-mst)# show pending
```

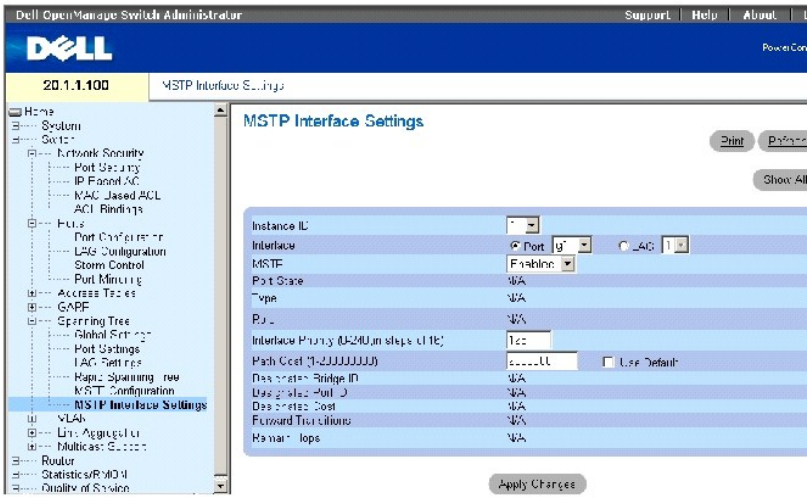
Pending MST configuration (Configuration MST en attente)	
Name: (Nom :) Region1	
Revision: (Révision :) 1	
Instance	Vlans Mapped (VLAN adressés)
--------	------------
0	1-9,31-4094
1	10-20
2	21-30

Définition des paramètres d'interface MSTP

La page **MSTP Interface Setting** (Paramètre d'interface MSTP) permet d'affecter des paramètres MSTP à des interfaces données.

Pour ouvrir la page **MSTP Interface Setting** (Paramètre d'interface MSTP), **cliquez sur Switch** (Commutateur)→ **Spanning Tree**→ **MSTP Interface Setting** (Paramètre d'interface MSTP) dans l'*arborescence*.

Figure 7-26. Paramètre d'interface MSTP



La page **MSTP Interface Setting** (Paramètre d'interface MSTP) contient les paramètres suivants :

Instance ID (ID instance) Répertorie les instances MSTP configurées sur le périphérique. La plage de valeurs possibles pour ce champ est comprise entre 0 et 15.

Interface Affecte soit des ports, soit des LAG à l'instance MSTP sélectionnée.

Port State (État du port) Indique si le port est activé ou désactivé pour l'instance donnée.

Type Indique si MSTP traite le port comme un port point à point ou un port connecté à un concentrateur et si le port est interne à la région MST ou est un port frontière. Si le port est un port frontière, ce paramètre indique également si le périphérique situé de l'autre côté de la liaison fonctionne en mode RSTP ou STP

Role (Rôle) Indique le 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) Indique le port ou le LAG à travail lequel le périphérique désigné est rattaché au LAN.

Alternate (Autre) Fournit un autre chemin vers le périphérique racine à partir de l'interface.

Backup (Sauvegarde) Fournit un chemin de sauvegarde au réseau local (LAN) désigné. Les ports de sauvegarde ne fonctionnent que lorsque deux ports sont connectés à une boucle par une liaison point à point. Les ports de sauvegarde sont également créés lorsqu'un LAN possède au moins deux connexions à un segment partagé.

Disabled (Désactivé) Indique que le port ne participe pas au Spanning Tree.

Interface Priority (Priorité de l'interface) Définit la priorité de l'interface pour l'instance spécifiée. La plage des valeurs possibles est comprise entre 0 et 240, par palier de 16. La valeur par défaut est 128.

Path Cost (Coût de résolution) Indique la contribution du port à l'instance Spanning Tree. La plage des valeurs possibles est comprise entre 1 et 200 000 000.

Default Path Cost (Coût de résolution par défaut) Indique que le coût de résolution par défaut est affecté selon la méthode sélectionnée dans la page **Spanning Tree Global Settings** (Paramètres globaux Spanning Tree).

Designated Bridge ID (ID pont désigné) Numéro d'identification du pont qui permet de connecter la liaison ou le LAN partagé à la racine.

Designated Port ID (ID port désigné) Numéro d'identification du port sur le pont désigné qui permet de connecter la liaison ou le LAN partagé à la racine.

Designated Cost (Coût désigné) Coût de résolution entre la liaison ou la LAN partagé et la racine.

Forward Transitions (Transitions de transmission) Nombre de fois où le port est passé sur l'état **forwarding** (Transmission).

Remaining Hops (Sauts restants) Indique le nombre de sauts restants jusqu'à la prochaine destination.

Affichage de la table des interfaces MSTP

1. Ouvrez la page **MSTP Interface Setting** (Paramètre d'interface MSTP).
2. Cliquez sur **Show All** (Afficher tout).

La page **MSTP Interface Table** (Table d'interface MSTP) s'ouvre :

Figure 7-27. Table des interfaces MSTP

Définition des interfaces MSTP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la définition des interfaces MSTP comme indiqué dans la page **MSTP Interface Setting** (Paramètre d'interface MSTP).

Tableau 7-20. Commandes CLI Interface MSTP

Commande CLI	Description
`spanning-tree mst instance-id cost cost`	Définit le coût de résolution du port en vue de calculs MST
`spanning-tree mst instance-id priority priority`	Définit la priorité du périphérique pour l'instance ST spécifiée.
`show spanning-tree mst- configuration`	Affiche la configuration MST.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config) # interface ethernet g9

Console (config-if) # spanning-tree mst 1 cost 4

Console (config-if)# spanning-tree mst 1 port-priority 142

Console (config-if)# end

Console# show spanning-tree

Spanning Tree enabled mode MSTP
```

```
Default port cost method: long

###### MST 0 Vlans Mapped: 1-9, 21-4094

CST Root ID Priority 32768

Address 00:01:42:97:e0:00

Path Cost 20000

Root Port 1 (ig)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

IST Master ID Priority 32768

Address 00:02:4b:19:7a:00

Path Cost 10000

Rem hops 19

Bridge ID Priority 32768

Address 00:02:4b:29:7a:00

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Max hops 20
```

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, des ajouts et des déplacements du réseau.

Les VLAN possèdent un nombre illimité de ports et peuvent être créés en fonction d'une unité, d'un périphérique, d'une pile spécifique 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 Layer 2. Du fait que les VLAN isolent le trafic à l'intérieur du VLAN, un routeur fonctionnant au niveau Layer 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.

Le marquage des VLAN constitue une méthode de transmission des informations VLAN entre les groupes de VLAN. Il attache une étiquette de 4 octets aux en-têtes de paquets. Le marqueur VLAN indique le VLAN auquel le paquet appartient. Les étiquettes VLAN sont attachées au VLAN soit par la station terminale,

soit par le périphérique réseau. Ils contiennent également les informations de priorité réseau du VLAN.

La combinaison des VLAN et du protocole GVRP permet aux gestionnaires du réseau de définir des noeuds de réseau dans des domaines de diffusion. Le trafic de diffusion et de multidiffusion est confiné dans le groupe de départ.

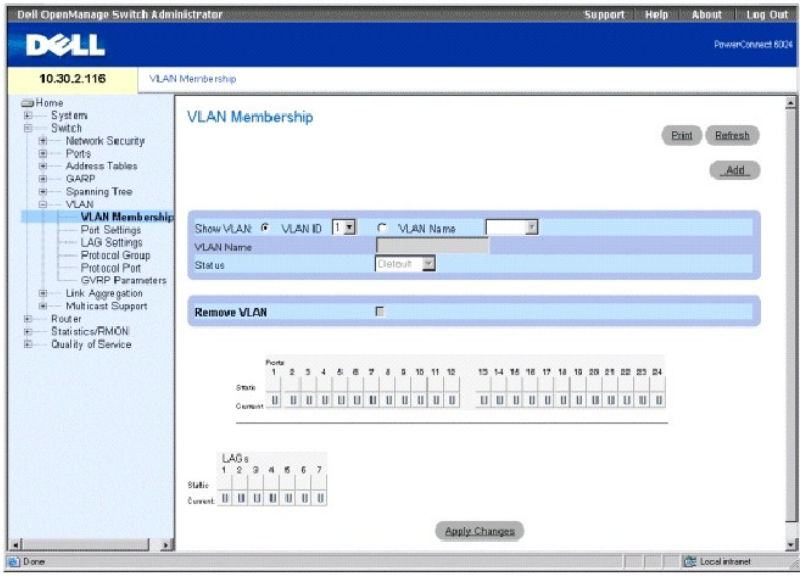
Pour afficher la page **VLAN**, cliquez sur **Switch** (Commutateur)→ **VLAN** dans l'*arborescence*.

Définition de l'appartenance à un VLAN

La page **VLAN Membership** Appartenance à un VLAN) permet de définir des groupes de VLAN.

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 7-28. Page Appartenance à un VLAN



La page **VLAN Membership** (Appartenance à un VLAN) se compose de la table **VLAN Membership Table** (Table d'appartenance à un VLAN) et de la table **VLAN Port Membership Table** (Table d'appartenance à un port VLAN).

Table d'appartenance à un VLAN

La table **VLAN Membership Table** (Table d'appartenance à un VLAN) contient des paramètres permettant d'affecter à des ports l'appartenance à un VLAN. Votre commutateur prend en charge jusqu'à 4095 VLAN. Toutefois, vous ne pouvez réellement créer que 4062 VLAN car :

- Les VLAN 4064 à 4094 sont réservés par le périphérique pour une utilisation en interne,
- Le VLAN 1 est le VLAN dont tous les ports sont membres par défaut,
- Le VLAN 4095 est appelé «le VLAN de mise au rebut».

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) Indique le nom du VLAN défini par l'utilisateur.

Status (État) Indique le type du VLAN. Ce champ peut prendre les valeurs suivantes :

Dynamic (Dynamique) Indique que le VLAN a été créé dynamiquement par le biais du protocole GVRP.

Static (Statique) Indique que le VLAN est défini par l'utilisateur.

Remove VLAN (Supprimer VLAN) Lorsqu'elle est cochée, cette option 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 **Add** (Ajouter) pour ouvrir la page Create New VLAN (Créer un VLAN).
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 VLAN).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le VLAN 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 7-21. Commandes CLI Groupes d'appartenance à un VLAN

Commande CLI	Description
`vlan database`	Passe en mode (VLAN) de configuration de l'interface.
	Crée un VLAN.

`vlan {vlan-range}`	
`name string`	Ajoute un nom à un VLAN.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)#interface vlan 1972

Console (config-if)#name Marketing
```

Table d'appartenance des ports à un VLAN

La table **VLAN Port Membership Table** (Table d'appartenance des ports à un VLAN) contient une **Port Table** (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 7-22. 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.
`U`	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.
`Blank (Blanc)`	L'interface n'est pas membre d'un VLAN. Les paquets associés à l'interface ne sont pas transmis.

La table **VLAN Port Membership Table** (Table d'appartenance des ports à un VLAN) contient les ports et l'état des ports ainsi que les LAG.

Affectation de ports à un groupe de VLAN

1. 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 **Port Membership Table** (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 VLAN** (Supprimer le VLAN).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le VLAN 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 7-23. Commandes CLI Affectations de ports à des groupes de VLAN

Commande CLI	Description
`switchport general acceptable-frame-types tagged-only`	Ignore les trames entrantes non marquées.
`switchport forbidden vlan {add` *`vlan-list`* `| remove` *`vlan-list`*`}`	Interdit l'ajout de VLAN spécifiques au port.

Voici des exemples de commandes CLI :

```
Console (config)# interface ethernet g1
```

```
Console (config-if)#switchport general acceptable-frame-types tagged-only
```

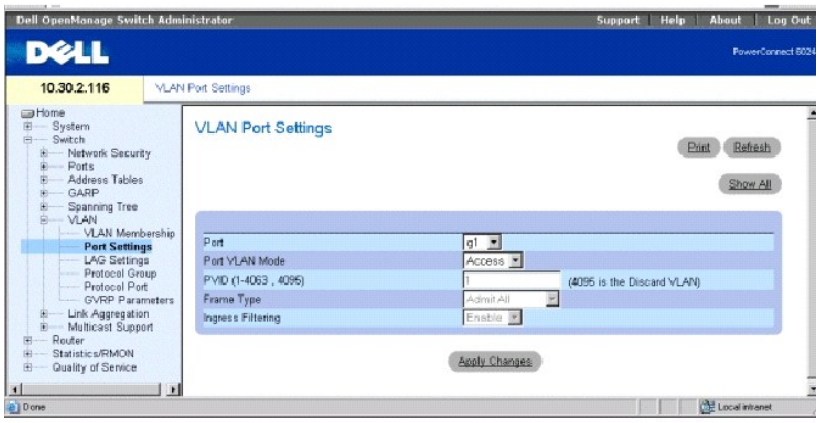
```
Console (config-if)#switchport forbidden vlan add 234-256
```

Définition des paramètres des ports VLAN

La page **VLAN Port Settings** (Paramètres des ports VLAN) contient des paramètres relatifs à la gestion des ports qui font partie d'un VLAN. L'ID VLAN par défaut du port (PVID) est configuré dans 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**, cliquez sur **Switch** (Commutateur)→ **VLAN**→ **Port Settings** (Paramètres des ports) dans l'*arborescence*.

Figure 7-29. Page Paramètres des ports VLAN



Port Numéro de port inclus dans le VLAN.

Port VLAN Mode (Mode VLAN du port) Désigne le 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. L'activation/la désactivation du filtrage en entrée n'est pas non plus possible sur un port d'accès.

Trunk (Segment) Le port appartient aux VLAN dans lesquels tous les ports sont marqués (sauf pour un VLAN natif unique facultatif).

PVID (1-4063, 4095) Affecte un ID VLAN aux paquets non marqués. Les valeurs possibles pour ce champ sont 1 à 4063 et 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 trames accepté sur le port. Ce champ peut prendre les valeurs suivantes :

Admit Tag Only (Admettre uniquement les paquets marqués) Indique que seuls les paquets marqués sont acceptés sur le port.

Admit All (Admettre tout) Indique que les trames marquées et non marquées sont acceptées sur le port.

Ingress Filtering (Filtrage d'entrée) Active ou désactive le filtrage d'entrée sur le port. Le filtrage d'entrée met au rebut les trames lorsque le numéro VLAN correspond à aucun port VLAN.

Affectation des paramètres de port

1. Ouvrez la page **VLAN Port Settings** (Paramètres des ports VLAN).
2. Sélectionnez le port auquel vous souhaitez affecter des paramètres dans le menu déroulant **Port**.
3. Renseignez les autres champs de la page et 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) pour afficher la table **VLAN Port Table** (Table des ports VLAN).

REMARQUE : Lorsqu'un port en mode **Access** (Accès) est choisi, les types de paquets acceptés sur ce port ne peuvent pas être désignés. L'activation ou la désactivation du filtrage en entrée n'est pas non plus possible sur un port d'accès.

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 7-24. Commandes CLI Ports VLAN

Commande CLI	Description
`switchport mode { access | trunk | general}`	Configure le mode d'appartenance VLAN d'un port.
`switchport trunk native vlan vlan-id`	Configure le port en tant que membre du VLAN spécifié et l'ID VLAN en tant que PVID (ID VLAN par défaut du port).
	Configure l'ID VLAN du port (PVID) lorsque l'interface est en mode General (Général).

`switchport general pvid vlan-id`	
`switchport general allowed vlan add vlan- list [ tagged | untagged]`	Ajoute ou supprime des VLAN d'un port général.
`switchport general acceptable-packet- types tagged-only`	Met au rebut les paquets entrants non marqués.
`switchport general ingress-filtering disable`	Désactive le filtrage d'entrée d'un port.
`shutdown`	Désactive les interfaces.
`set interface active {ethernet interface | port-channel port- channel-number}`	Réactive une interface qui a été arrêtée pour des raisons de sécurité.

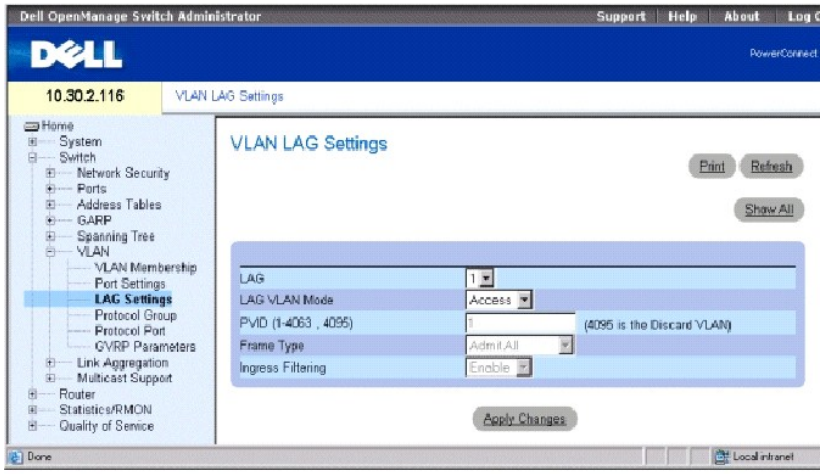
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface ethernet g8

Console (config-if)# switchport mode access

Console (config-if)# switchport trunk native vlan 123

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 acceptable-packet-types tagged-only
```

Définition des paramètres des LAG VLAN

La page **VLAN LAG Settings** (Paramètres des LAG VLAN) contient des paramètres relatifs à la gestion des LAG qui font partie d'un VLAN. Les VLAN sont composés de ports ou de LAG individuels. Les paquets non marqués arrivant sur le commutateur sont marqués avec l'ID LAG spécifié par le PVID. Pour ouvrir la page **VLAN LAG Settings** (Paramètres des LAG VLAN), cliquez sur **Switch** (Commutateur)→ **VLAN**→ **LAG Settings** (Paramètres des LAG) dans l'*arborescence*.

Figure 7-30. Page Paramètres des LAG VLAN



LAG Numéro de LAG inclus dans le VLAN.

LAG VLAN Mode (Mode VLAN du LAG) Indique le mode 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 (Faisceau) Le LAG appartient à des VLAN dans lesquels tous les ports sont marqués (sauf pour un VLAN natif unique facultatif).

PVID (1-4063, 4095) Affecte un ID VLAN aux paquets non marqués. Les valeurs possibles pour ce champ sont 1 à 4063 et 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 met au rebut les paquets lorsque le numéro VLAN correspond à aucun LAG VLAN.

Affectation des paramètres de LAG

1. Ouvrez la page **VLAN LAG Settings** (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 Settings** (Paramètres des LAG VLAN).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **VLAN LAG Table** (Table des LAG VLAN).

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 indiqué dans la page **VLAN LAG Settings** (Paramètres des LAG VLAN).

Tableau 7-25. Commandes CLI Affectation de LAG à des VLAN

Commande CLI	Description
`switchport mode {access | trunk | general}`	Configure le mode d'appartenance VLAN d'un port.
`switchport trunk native vlan vlan-id`	Configure le port en tant que membre du VLAN spécifié et l'ID VLAN en tant que PVID (ID VLAN par défaut du port).
`switchport general pvid vlan-id`	Configure l'ID VLAN du port (PVID) lorsque l'interface est en mode General (Général).
`switchport general allowed vlan add vlan- list [tagged | untagged]`	Ajoute ou supprime des VLAN d'un port général.
`switchport general acceptable-frame-type tagged-only`	Met au rebut les paquets entrants non marqués.
`switchport general ingress-filtering disable`	Désactive le filtrage d'entrée d'un port.

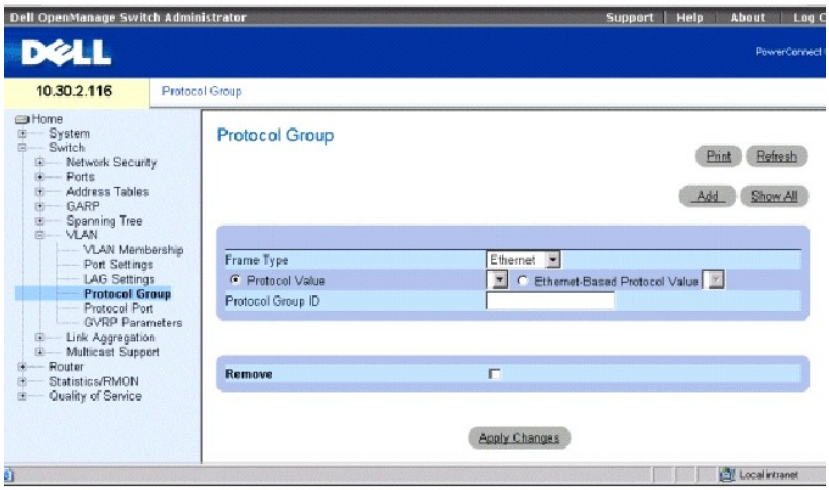
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config-if)# switchport mode access

Console (config-if)# switchport trunk native vlan 123

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 acceptable-frame-type tagged-only
```

Définition des groupes de protocoles VLAN

La page **Protocol Group** (Groupe de protocoles) contient des informations sur les noms des protocoles et le type d'Ethernet du VLAN. Les interfaces peuvent être classées en interfaces basées sur des protocoles spécifiques. Cette classification place l'interface dans un groupe de protocoles. Pour ouvrir la page **Protocol Group** (Groupe de protocoles), cliquez sur **Switch** (Commutateur)→ **VLAN**→ **Protocol Group** (Groupe de protocoles) dans l'*arborescence*.

Figure 7-31. Table des groupes 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.

Protocol Group ID (ID du groupe de protocoles) Numéro ID du groupe VLAN.

Ajout d'un groupe de protocoles

1. Ouvrez la page **Protocol Group** (Groupe de protocoles).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Assign Protocol to Group** (Affectation d'un protocole à un groupe).
3. Renseignez les champs de la page et 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 la page et 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) pour afficher la table **Protocol Group Table** (Table des groupes de protocoles).
3. Cochez la case **Remove** (Supprimer) des 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 contient les commandes CLI pour la configuration des groupes de protocole.

Tableau 7-26. Commandes CLI Groupes de protocoles VLAN

Commande CLI	Description
`map protocol` *`protocol`* `[`*`encapsulation`*`]` `protocols- group` *`group`*	Ajoute un protocole spécifique à un groupe de protocoles désigné, qui peut être utilisé pour l'affectation de VLAN basée sur les protocoles.

Vous trouverez ci-dessous un exemple de mise en correspondance du protocole IP-ARP avec le groupe «213» :

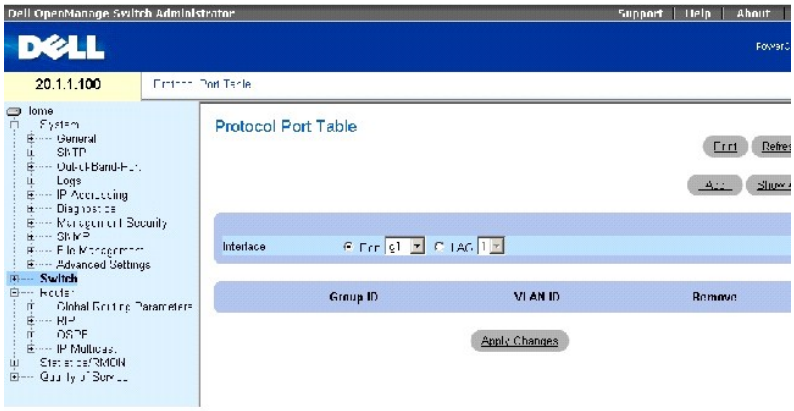
```
Console (config)# vlan database

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 à des groupes de protocole.

Pour ouvrir la page **Protocol Port** (Port de protocole), cliquez sur **Switch** (Commutateur)→ **VLAN**→ **Protocol Port** (Port de protocole) dans l'*arborescence*.

Figure 7-32. Page Port de protocole



Interface Numéro du port ou du LAG ajouté à un groupe de protocoles.

Protocol Group ID (ID du groupe de protocoles) 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 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.

VLAN Name (Nom du VLAN) Lie l'interface à un nom de VLAN défini par l'utilisateur. Le nom du VLAN est défini dans la page **Create a New VLAN** (Créer un VLAN). Ce champ n'est disponible que dans la page **Add Protocol Port** (Ajout d'un port de protocole).

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime l'affectation de port d'un VLAN ou d'un groupe de protocoles.

Ajout d'un port de protocole

1. Ouvrez la page **Protocol Port Table** (Table des ports de protocoles).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add Protocol Port** (Ajout d'un port de protocole).
3. Renseignez les champs de la boîte de dialogue et 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 les commandes CLI pour la définition des ports de protocole.

Tableau 7-27. Commande CLI Ports de protocoles

Commande CLI	Description
`switchport general map protocols-group` *`group`* `vlan` *`vlan- id`*	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 réduire au minimum les besoins en mémoire lors de l'exécution du protocole GVRP, deux variables de réglage propriétaires ont été ajoutées aux variables standard :

- **Maximum number of GVRP VLANs** (Nombre maximal de VLAN GVRP) Nombre de VLAN GVRP autorisés à participer à un fonctionnement GVRP.
- **Maximum number of GVRP VLANs after Reset** (Nombre maximum de VLAN GVRP après réinitialisation) Nombre maximal de VLAN VLAN après une réinitialisation pour le réglage des performances. Cette valeur n'est effective qu'après une réinitialisation.

Le nombre maximal de VLAN GVRP inclut tous les VLAN qui participent au fonctionnement GVRP, qu'ils soient statiques ou dynamiques.

Les observations suivantes doivent être prises en compte lors de la spécification du nombre maximal de VLAN participant au protocole GVRP par le biais de la définition de la valeur «nombre maximal de VLAN GVRP après réinitialisation» :

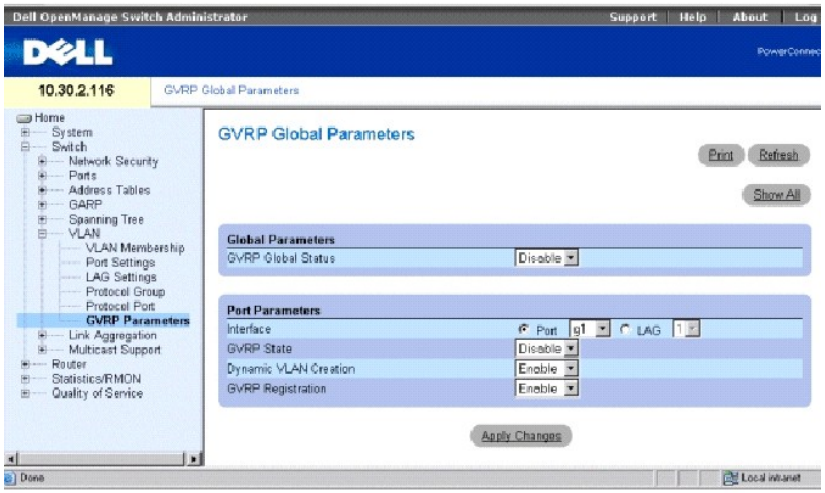
- Le nombre maximal par défaut de VLAN GVRP est égal à 255.
- Le nombre maximal de VLAN (gérés par le biais de la variable Max VLANs MIB) limite le nombre maximal de VLAN GVRP.

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 :

- Le nombre de tous les VLAN statiques à la fois actuellement configurés et en voie d'être configurés.
- 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 255) 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 Global Parameters** (Paramètres globaux GVRP), cliquez sur **Switch** (Commutateur)→ **VLAN**→ **GVRP Parameters** (Paramètres GVRP) dans l'*arborescence*.

Figure 7-33. Page Paramètres globaux 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) Affiche l'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 7-28. Commandes CLI Paramètres globaux GVRP

Commande CLI	Description
`gvrp enable (global)`	Active le protocole GVRP de façon globale.
`gvrp enable (interface)`	Active le protocole GVRP sur une interface.
`gvrp vlan-creation-forbid`	Active ou désactive la création dynamique de VLAN.
`gvrp registration-forbid`	Désenregistre tous les VLAN dynamiques et empêche l'enregistrement dynamique de VLAN sur le port.
`show gvrp configuration [ethernet interface | port- channel port-channel- number]`	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.
`show gvrp error-statistics [ethernet interface | port- channel port-channel- number]`	Affiche les statistiques des erreurs du protocole GVRP.
`show gvrp statistics [ethernet interface | port- channel port-channel- number]`	Affiche les statistiques du protocole GVRP.
`clear gvrp statistics [ethernet interface | port- channel port-channel- number]`	Efface toutes les statistiques du protocole GVRP.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# gvrp enable

Console (config)# interface ethernet g8

Console (config-if)# gvrp enable

Console (config-if)# gvrp vlan-creation-forbid

Console (config-if)# gvrp registration-forbid

Console> show gvrp configuration
```

```
GVRP Feature is currently Enabled on the device.

Maximum VLANs: 4063, Maximum VLANs after reset: 4063.


Port(s)  GVRP-Status Registration Dynamic VLAN Timers(milliseconds)

                                 Creation      Join      Leave      Leave All

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

g1       Disabled    Normal       Enabled       200       600        10000

...

g7       Disabled    Normal       Enabled       200       600        10000

g8       Enabled     Forbidden    Disabled      200       600        10000

g9       Disabled    Normal       Enabled       200       600        10000

...

g24       Disabled    Normal       Enabled       200       600        10000

ch1       Disabled    Normal       Enabled       200       600        10000

...

ch7       Disabled    Normal       Enabled       200       600        10000

...

Console> show gvrp statistics



GVRP statistics:

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

Legend:
```

rJE : Join Empty Received rJIn : Join In Received

rEmp : Empty Received rLIn : Leave In Received

rLE : Leave Empty Received rLA : Leave All Received

sJE : Join Empty Sent sJIn : Join In Sent

sEmp : Empty Sent sLIn : Leave In Sent

sLE : Leave Empty Sent sLA : Leave All Sent

Port	rJE	rJIn	rEmp	rLIn	rLE	rLA	sJE	sJIn	sEmp	sLIn	sLE	sLA
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# clear gvrp statistics ethernet g8

Agrégation des ports

La fonction d'agrégation des liaisons 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.

Votre commutateur prend en charge à la fois les LAG statiques et les LAG LACP (protocole de contrôle d'agrégation de liaison). Les LAG LACP négocient les liaisons de ports d'agrégation 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 configurez des ports d'agrégation :

- Tous les ports d'un LAG doivent être du même type de support.
- Aucun VLAN n'est configuré sur le port.
- Le port n'appartient à aucun autre LAG.
- Il existe une adresse MAC qui peut être affectée à un port.
- Le mode négociation automatique n'est pas configuré sur le port.
- Le port est en mode duplex intégral.
- Tous les ports du LAG possèdent les mêmes modes de filtrage en entrée et de marquage.
- Tous les ports du LAG possèdent les mêmes modes contre-pression et contrôle du flux.
- Tous les ports du LAG ont la même priorité.
- Tous les ports du LAG ont le même type d'émetteur-récepteur.
- PowerConnect 6024/6024F prend en charge jusqu'à sept LAG.
- Les ports peuvent être configurés comme des ports LACP uniquement s'ils ne font pas partie d'un LAG configuré précédemment.

Les ports ajoutés à un LAG perdent leur configuration individuelle. Lorsque des ports sont supprimés d'un LAG, leur configuration d'origine est rétablie.

Votre commutateur utilise une fonction de hachage pour déterminer quels paquets sont transmis 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 commutateur considère une liaison agrégée comme un seul et même port logique.

Pour ouvrir la page **Link Aggregation** (Agrégation de liaisons), cliquez sur **Switch** (Commutateur)→ **Link Aggregation** (Agrégation de liaisons) dans l'*arborescence*.

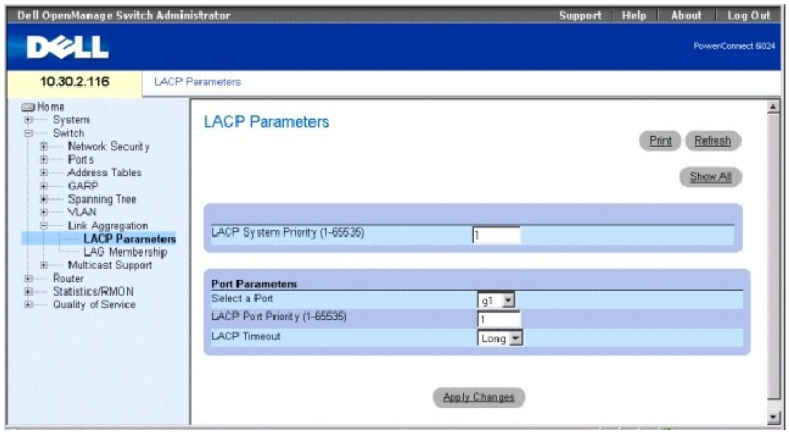
Définition des paramètres LACP

Les ports agrégés peuvent être reliés en groupes de ports à agrégation de liaisons. Chaque groupe est composé de ports ayant la même vitesse, configurés en mode duplex intégral.

Les ports d'un LAG peuvent contenir différents types de supports s'ils fonctionnement à la même vitesse. Les liaisons agrégées peuvent être configurées manuellement ou automatiquement par le biais de l'activation du protocole LACP (Link Aggregation Control Protocol) sur les liaisons appropriées.

Utilisez la page **LACP Parameters** (Paramètres LACP) pour configurer des LAG LACP. 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 7-34. Page Paramètres LACP



La page **LACP Parameters** (Paramètres LACP) contient des sections pour la définition des paramètres globaux et des paramètres de port.

LACP System Priority (1-65535) (Priorité LACP du système) Indique la valeur de priorité LACP pour les paramètres globaux. La valeur par défaut est 1.

Select a Port (Sélectionner un port) Numéro du port auquel les valeurs délai et priorité sont affectées.

LACP Port Priority (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 (Bref) Spécifie un bref délai d'expiration.

Long Spécifie un long délai d'expiration.

Définition des paramètres globaux d'agrégation des liaisons

1. Ouvrez la page **LACP Parameters** (Paramètres LACP).
2. Renseignez les champs **LACP System Priority** (Priorité du système LACP) et **LACP Timeout** (Délai d'expiration LACP).
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. Défilez jusqu'à la table **Port Parameters** (Paramètres des ports).
3. Sélectionnez le port dont vous souhaitez définir les paramètres.
4. Renseignez les champs **LACP System Priority** (Priorité du système LACP) et **LACP Timeout** (Délai d'expiration LACP).
5. 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) pour afficher la page **LACP Parameters Table** (Table des paramètres LACP).

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 indiqué dans la page **Link Aggregation** (Agrégation de liaisons).

Tableau 7-29. Commandes CLI Paramètres LACP

Commande CLI	Description
`lacp system-priority` *value*	Configure la priorité du système.
`lacp port-priority` *value*	Configure la valeur de priorité des ports physiques.

`lacp timeout {long | short}`	Affecte un délai d'expiration LCAP administratif.
`show lacp ethernet *interface* [parameters | statistics | protocol- state]`	Affiche des informations LACP pour les ports Ethernet.

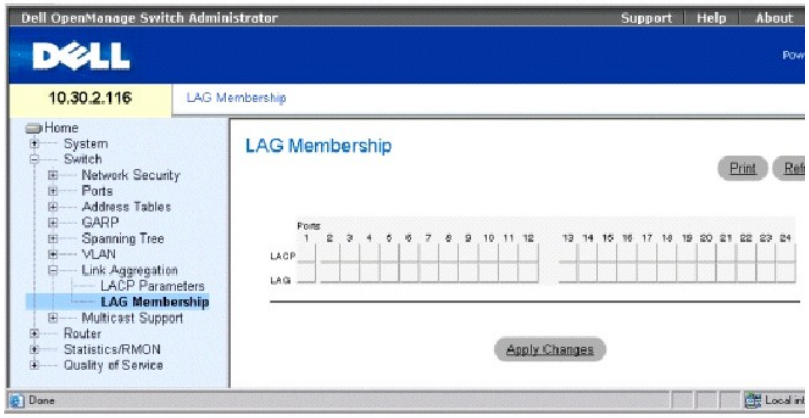
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# lacp system-priority 120

Console (config)# interface ethernet g8

Console (config-if)# lacp port-priority 247

Console (config-if)# lacp timeout long

Console (config-if)# exit

Console# show lacp ethernet g1 statistics

Port 1 LACP Statistics:

LACP PDUs sent:2

LACP PDUs received:2
```

Définition de l'appartenance à un LAG

Votre commutateur prend en charge sept LAG par système et sept ports par LAG. La page **LAG Membership** (Appartenance à un LAG) permet d'affecter des ports à des LAG. Pour ouvrir la page **LAG Membership**, cliquez sur **Switch** (Commutateur)→ **Link Aggregation** (Agrégation de liaisons)→ **LAG Membership** (Appartenance à un LAG) dans l'*arborescence*.

Figure 7-35. Page 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.

Ajout d'un port à un LAG

1. Ouvrez la page **LAG Membership** (Appartenance à un LAG).
2. Faites basculer le bouton situé en dessous du numéro de port pour affecter le paramètre statique et le numéro du LAG.
3. Faites basculer le bouton situé sur la ligne du LACP vers **L** pour ajouter le port à un LAG par le biais du protocole LACP
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port est ajouté au LAG 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 indiqué dans la page **LAG Membership** (Appartenance à un LAG).

Tableau 7-30. Commandes CLI Appartenance à un LAG

Commande CLI	Description
`interface port-channel` *`port-channel-number`*	Passe au mode de configuration de l'interface d'un canal de port spécifique.
`channel-group` *`port- channel-number`* `mode {on | auto}`	Associe 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.
`show interfaces port- channel [`*`port-channel- number`*`]`	Affiche des informations sur le canal de port.

```
Console (config)# interface port-channel 1
```

```
Console (config-if)# channel-group 1 mode on
```

```
Console# show interfaces port-channel

Channel       Port

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

Ch 1          Active    g1, g2    Inactive g3

Ch 2          Active    g2

Ch 3          Inactive  g8
```

Prise en charge de la transmission 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.

Ce périphérique prend en charge les fonctions suivantes :

- **Forwarding L2 Multicast Packets** (Transmission des paquets de multidiffusion L2 Transmet des paquets de multidiffusion de couche 2. Le filtrage de multidiffusion de couche 2 est activé par défaut et ne peut pas être configuré par l'utilisateur.

REMARQUE : Le système prend en charge le filtrage multidiffusion pour 256 groupes de multidiffusion.

- **Filtering L2 Multicast Packets** (Filtrage des paquets de multidiffusion L2) Transmet des paquets de couche 2 à 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 gère le paquet comme une transmission de multidiffusion. Lorsque la transmission du trafic de multidiffusion est effective, elle n'est pas optimale car des ports inappropriés reçoivent également les paquets de multidiffusion. Les paquets en excès entraînent une augmentation du trafic réseau. Les filtres de la transmission de multidiffusion permettent de transmettre des paquets de couche 2 à des sous-ensembles de ports.

Lorsque la surveillance IGMP est activée globalement, tous les paquets IGMP sont transmis à l'unité centrale (UC). L'UC analyse les trames entrantes 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.

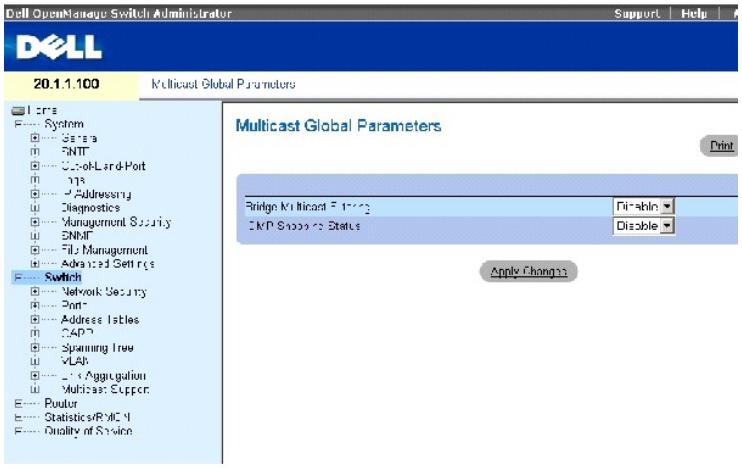
Les ports demandant à rejoindre un groupe de multidiffusion donné émettent un rapport IGMP spécifiant que le groupe de multidiffusion est en train d'accepter des membres. La base de données du filtrage de la multidiffusion est créée.

La page **Multicast Global Parameters** (Paramètres globaux de multidiffusion) permet d'activer la surveillance IGMP sur le périphérique. Pour ouvrir la page **Multicast Global Parameters**, cliquez sur **Switch** (Commutateur)→ **Multicast Support** (Prise en charge de la multidiffusion)→ **Global Parameters** (Paramètres globaux) dans l'*arborescence*.

Figure 7-36. Paramètres globaux de multidiffusion

La page **Multicast Global Parameters** (Paramètres globaux de multidiffusion) contient les champs suivants :

Bridge Multicast Filtering (Filtrage multidiffusion par ponts) Active ou désactive le filtrage multidiffusion par ponts. Cette option est désactivée par défaut.



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 de la transmission multidiffusion et de la surveillance IGMP comme indiqué dans la page **Multicast Support** (Prise en charge de la multidiffusion).

Tableau 7-31. Commandes CLI Transmission de multidiffusion et Surveillance

Commande CLI	Description
`bridge multicast filtering`	Active le filtrage des adresses de multidiffusion.
	Active la surveillance IGMP (Internet Group Management Protocol).

`ip igmp snooping`	

Vous trouverez ci-dessous un exemple de commande CLI :

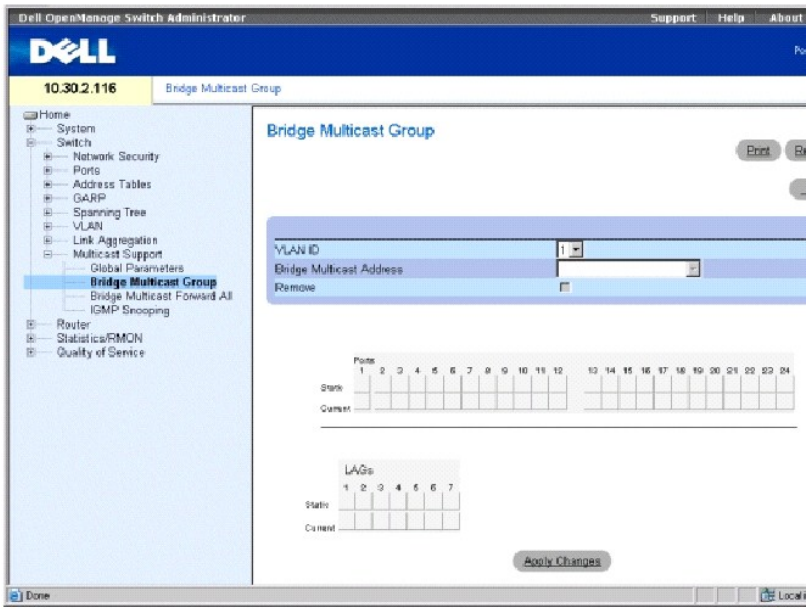
```
Console (config)# bridge multicast filtering

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 pont) permet de créer de nouveaux groupes de services de multidiffusion. 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**, cliquez sur **Switch** (Commutateur)→ **Multicast Support** (Prise en charge de la multidiffusion)→ **Bridge Multicast Address** (Adresse de multidiffusion par ponts) dans l'*arborescence*.

Figure 7-37. Page 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) Lorsqu'elle est cochée, cette case 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 ports IGMP et des membres LAG :

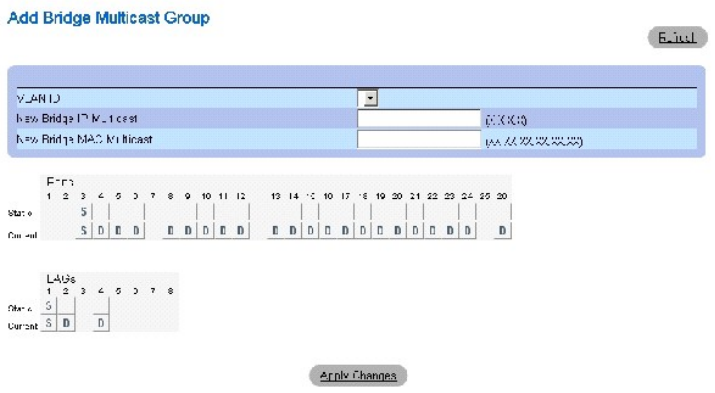
Tableau 7-32. Paramètres de contrôle de la table des membres des ports/LAG IGMP

Contrôle du port	Définition
D	Indique que le port/LAG a rejoint le groupe de multidiffusion de façon dynamique à la ligne *Current* (Actuel).
S	Rattache le port au groupe de multidiffusion en tant que membre statique à la ligne *Static* (Statique). Indique que le port/LAG a rejoint le groupe de multidiffusion de façon statique à la ligne *Current* (Actuel).
F	Indique que le port/LAG est une entrée interdite pour le groupe de multidiffusion.
Blank (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 **Add** (Ajouter) pour afficher la page **Add Bridge Multicast Group** (Ajout d'un groupe de multidiffusion par ponts).

Figure 7-38. Page Ajout d'un groupe de multidiffusion par ponts



3. Renseignez 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 au groupe de multidiffusion sélectionné.
5. Faites basculer un port vers la valeur **F** pour empêcher l'ajout d'adresses de multidiffusion spécifiques à un port spécifique.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adresse de multidiffusion par ponts est affectée au groupe de multidiffusion et 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. Renseignez 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 au groupe de multidiffusion sélectionné.
4. Faites basculer un port vers la valeur **F** pour empêcher l'ajout d'adresses de multidiffusion spécifiques à un port spécifique.
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. Renseignez 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 l'ajout d'adresses de multidiffusion spécifiques à un LAG spécifique.
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 7-33. Commandes CLI Membres du service de multidiffusion

Commande CLI	Description
bridge multicast address {*mac-multicast-address* | *ip-multicast-address*} [add | remove] {ethernet *interface-list* | port- channel *port-channel-number-list* }	Enregistre les adresses de multidiffusion de couche MAC dans la table des ponts et ajoute des ports statiques au groupe.
bridge multicast forbidden address {*mac-multicast- address* | *ip-multicast- address*} [add | remove] {ethernet interface-list | port-channel port-channel- number-list}	Empêche l'ajout d'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 vlan- id] [address mac-multicast- address | *ip-multicast- address*] [format ip | mac]	Affiche des informations sur la table des adresses MAC de multidiffusion.

Vous trouverez ci-dessous un exemple de commande CLI :

```
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
```

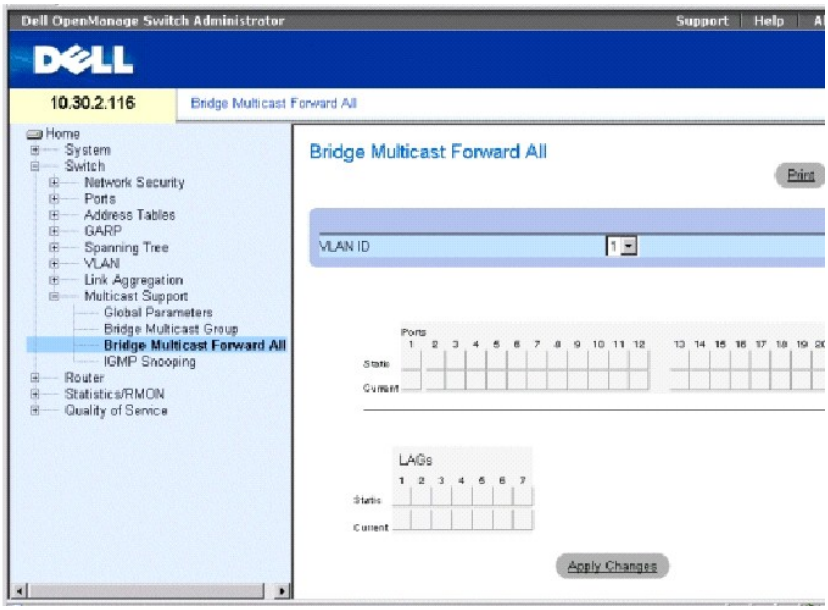
```
Console (config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console (config-if)# exit

Console (config)# exit

Console# show bridge multicast address-table

Vlan   MAC Address      type      Ports

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

1      0100.5e02.0203   static    g1, g2

19     0100.5e02.0208   static    g1-8

19     0100.5e02.0208   dynamic   g9-11

Forbidden ports for multicast addresses:

Vlan   MAC Address      Ports

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

1      0100.5e02.0203   g8

19     0100.5e02.0208   g8

Console# configuration

Console (config)# interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203

Console (config-if)# bridge multicast forbidden address 0100.5e02.0203 add ethernet g9
```

Affectation de paramètres de transmission multidiffusion totale

La page **Bridge Multicast Forward All** (Transmission multidiffusion totale par ponts) permet de rattacher des ports ou des LAG à un commutateur lui-même rattaché à un routeur/commutateur multidiffusion voisin. Une fois la surveillance IGMP activée, les paquets de multidiffusion sont transmis au port ou au VLAN approprié.

Pour ouvrir la page **Bridge Multicast Forward All** (Transmission multidiffusion totale par ponts), cliquez sur **Switch** (Commutateur)→ **Multicast Support** (Prise en charge de la multidiffusion)→ **Bridge Multicast** (Multidiffusion par ponts)→ **Bridge Multicast Forward All** (Transmission multidiffusion totale par ponts) dans l'*arborescence*.

Figure 7-39. Page Transmission multidiffusion totale par ponts



VLAN ID (ID VLAN) Identifie un VLAN et contient des informations sur l'adresse du groupe de multidiffusion.

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 permettant de gérer les paramètres des routeurs et des ports.

Tableau 7-34. Contrôle des ports/routeurs de transmission multidiffusion totale par pont

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	Interdite
Blank (Blanc)	Indique que le port n'est pas rattaché à un routeur ou commutateur multidiffusion.

Rattachement d'un port à un routeur ou commutateur multidiffusion

1. Ouvrez la page **Bridge Multicast Forward All** (Transmission multidiffusion totale par ponts).
2. Renseignez 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 au commutateur multidiffusion.

Rattachement d'un LAG à un routeur ou commutateur multidiffusion

1. Ouvrez la page **Bridge Multicast Forward All** (Transmission multidiffusion totale par ponts).
2. Renseignez 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 au 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** (Transmission multidiffusion totale par ponts).

Tableau 7-35. Commandes CLI Gestion des LAG et des ports rattachés aux routeurs multidiffusion

Commande CLI	Description
`show bridge multicast filtering vlan-id`	Affiche la configuration du filtrage de multidiffusion.
`bridge multicast forward-all {add | remove} {ethernet interface-list | port- channel port-channel- number-list}`	Active la transmission de tous les paquets de 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 :

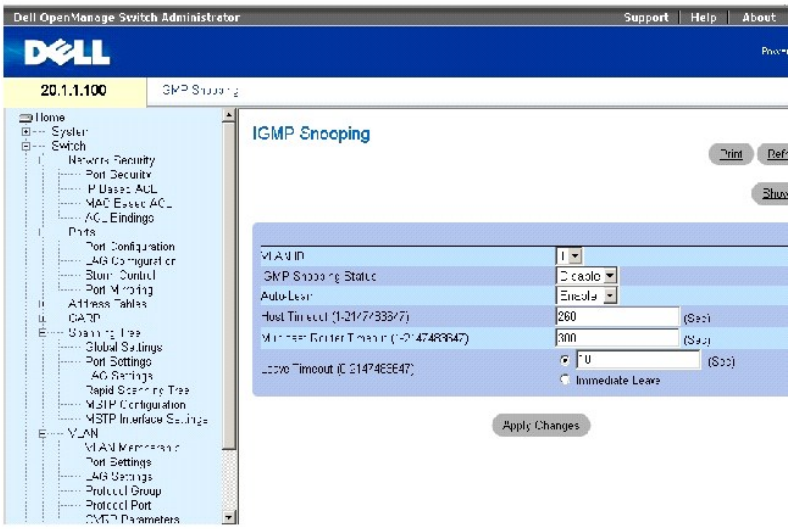
```
Console# show bridge multicast filtering 1

Filtering: Disabled

VLAN: 1

Forward-All

Port      Static      Status

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

g1        -           Filter

g2        -           Filter

...

Console# config
```

```
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)#interface vlan 8

Console (config-if)# bridge multicast address 0100.5e02.0203

add ethernet g1-9

Console (config-if)# exit

Console (config)# exit

Console# configuration

Console (config)# interface vlan 1

Console (config-if)# bridge multicast forward-all add ethernet g8
```

Surveillance IGMP

La page **IGMP Snooping** (Surveillance IGMP) permet d'ajouter des membres IGMP. Pour ouvrir la page **IGMP Snooping**, cliquez sur **Switch** (Commutateur)→ **Multicast Support** (Prise en charge de la multidiffusion)→ **IGMP Snooping** (Surveillance IGMP) dans l'*arborescence*.

Figure 7-40. Surveillance IGMP



VLAN ID 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 (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]) Délai 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) 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) vous permet de définir la période du délai et **Immediate Leave** (Sortie immédiate) indique une période de sortie 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 vous souhaitez activer la surveillance IGMP.
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) pour afficher la table **IGMP Snooping Table** (Table de surveillance IGMP).

Configuration de la surveillance IGMP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI équivalentes pour la configuration de l'option de sécurité Locked Port (Port verrouillé) comme indiqué dans la page **IGMP Snooping** (Surveillance IGMP).

Tableau 7-36. Commandes CLI 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` *`time-out`*	Configure le délai d'expiration de l'hôte.
`ip igmp snooping mrouter- time-out` *`time-out`*	Configure le délai d'expiration du routeur multidiffusion.
`ip igmp snooping leave-time- out {`*`time-out`* `| immediate- leave}`	Configure le délai d'expiration de sortie.
`show ip igmp snooping interface` *`vlan-id`*	Affiche la configuration de la surveillance IGMP.
`show ip igmp snooping mrouter [interface` *`vlan-id`*`]`	Affiche des informations sur les interfaces du routeur multidiffusion apprises de façon dynamique.

Vous trouverez ci-dessous un exemple de commande CLI :

```
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 interface 1000
```

```
IGMP Snooping is globally enabled

IGMP Snooping is enabled on VLAN 1000

IGMP host timeout is 300 sec

IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec

IGMP mrouter timeout is 200 sec

Automatic learning of multicast router ports is enabled

Console> show igmp-snooping mrouter

VLAN      Ports

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

2         g9
```

Retour à la page du sommaire

Retour à la page du sommaire

Configuration du routage

Systèmes Dell PowerConnect 6024/6024F

Présentation du routage

Les périphériques de différents sous-réseaux communiquent entre eux par l'intermédiaire d'un routeur de couche 3 situé entre les VLAN. Le routage est activé par défaut sur votre commutateur. Toutefois, au moins une interface IP doit être configurée pour que le commutateur commence à acheminer le trafic réseau. Les chemins sont configurés statiquement ou à l'aide des protocoles RIP ou OSPF.

Pour plus d'informations sur le protocole RIP, reportez-vous à la section «Configuration du protocole RIP».

Pour plus d'informations sur le protocole OSPF, reportez-vous à la section «Configuration des paramètres et des filtres OSPF».

Configuration des paramètres globaux du routage IP

La page **Global Routing Parameters** (Paramètres globaux de routage) contient des liens qui permettent de configurer le routage. Le mode routage est toujours en marche mais n'est activé que si le système dispose d'une ou plusieurs adresses IP. Pour ouvrir la page **Global Routing Parameters** (Paramètres globaux de routage), cliquez sur **Router** (Routeur)→ **Global Routing Parameters** (Paramètres globaux de routage) dans l'*arborescence*.

La page **Global Routing Parameters** (Paramètres globaux de routage) contient des liens qui permettent d'effectuer les procédures suivantes :

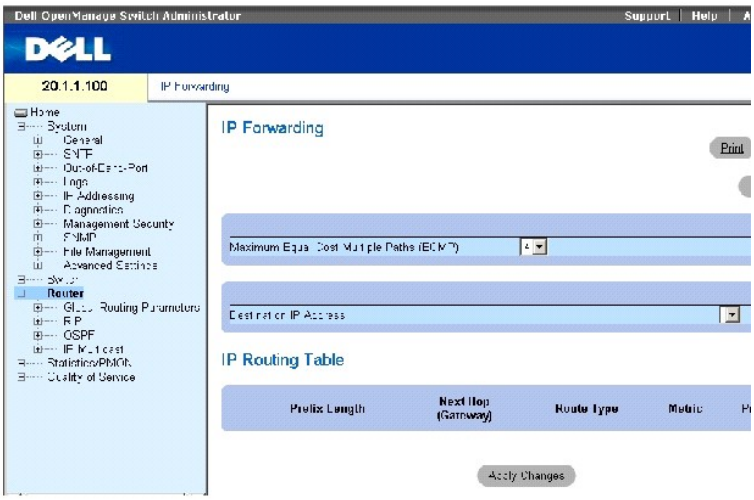
- Configuration de la table des transmissions IP
- Configuration de routes IP statiques
- Configuration du protocole VRRP
- Configuration de l'authentification MD5 du routage
- Configuration des paramètres des chaînes de clés MD5

Configuration de la table des transmissions IP

La page **IP Forwarding** (Transmission IP) permet de visualiser les paramètres de routage déterminant la transmission du trafic IP. Cette page fournit la liste des chemins IP pour les adresses IP de destination sélectionnées, y compris les chemins IP définis statiquement ou dynamiquement. Les chemins IP sont basés sur l'utilisation de masques de réseau, de prochains sauts, de métriques et de protocoles de transmission. Ces paramètres définissent des paquets spécifiques sont transmis ou rejetés. Lorsqu'une adresse IP est configurée sur une interface, elle est intégrée à la table des transmissions IP.

Pour ouvrir la page **IP Forwarding** (Transmission IP), cliquez sur **Router** (Routeur)→ **Global Routing Parameters** (Paramètres globaux de routage)→ **IP Forwarding** (Transmission IP) dans l'*arborescence*.

Figure 8-1. Page Transmission IP



Maximum Equal Cost Multipaths (ECMP) (Nombre maximum de chemins multiples de coûts égaux (ECMP)) Valeur ECMP qui doit être définie lors de la transmission de paquets IP. La valeur ECMP indique le nombre de chemins disponibles depuis le routeur jusqu'à un réseau. La plage de valeurs est comprise entre 1 et 4. Par exemple, la valeur 1 signifie qu'il n'existe qu'un seul chemin jusqu'au réseau. Plus la valeur ECMP est élevée, plus la quantité de ressources mémoire nécessaire est importante. Les modifications apportées à ce champ n'entrent en vigueur qu'après la réinitialisation du périphérique.

Destination IP Address (Adresse IP de destination) Réseau IP de destination.

Prefix Length (Longueur de préfixe) Nombre de bits qui comprennent le préfixe de l'adresse IP de destination. La longueur est comprise entre 1 et 32.

Next Hop (Gateway) (Prochain saut [passerelle]) Adresse du prochain routeur sur la route vers le réseau de destination.

Route Type (Type de route) Définit le traitement du routage distant. Ce champ peut prendre les valeurs suivantes :

Remote (Distant) Le paquet est transmis.

Reject (Refus) Le paquet est rejeté.

Local Le paquet est envoyé à un réseau local.

Metric (Métrique) Nombre de sauts vers le réseau de destination.

Protocol (Protocole) Protocole de routage par lequel cette route a été ajoutée.

Affichage de la table IP Forwarding Table (Table des transmissions IP)

La table **IP Forwarding Table** (Table des transmissions IP) fournit la liste de toutes les routes IP du système.

1. Ouvrez la page **IP Forwarding** (Transmission IP).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **IP Forwarding Table** (Table des transmissions IP).

Affichage des transmissions IP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage des transmissions IP.

Tableau 8-1. Commandes CLI Transmission IP

Commande CLI	Description
`show ip route [address] <ip- address>`	Affiche l'état actuel de la table de routage.
`ip maximum-paths number-paths`	Contrôle le nombre maximum de routes parallèles installées dans une table de routage.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface ip 10.10.10.2

Console (config-ip)# ip maximum-paths 2

Console (config-ip)# exit

Console (config)# exit

Console# exit

Console> show ip route

Codes: C - connected, S - static, R - RIP, O - OSPF, E - OSPF external

R 10.0.0.0/8 is rejected

C 10.0.1.1/32 is directly connected, Loopback0

C 10.0.1.0/24 is directly connected, Ethernet g1

C 10.0.2.0/24 is directly connected, Ethernet g2

R 10.8.2.0/24 [230/50] via 10.0.2.2, 00:17:19, Ethernet g2

S 10.9.1.0/24 [5/2] via 10.0.1.2, 17:19:18, Ethernet g1

S 10.9.1.0/24 [5/3] via 10.0.2.2, Backup Not Active

O 10.8.1.0/24 [30/2000] via 10.0.1.2, 00:39:08, Ethernet g1
```

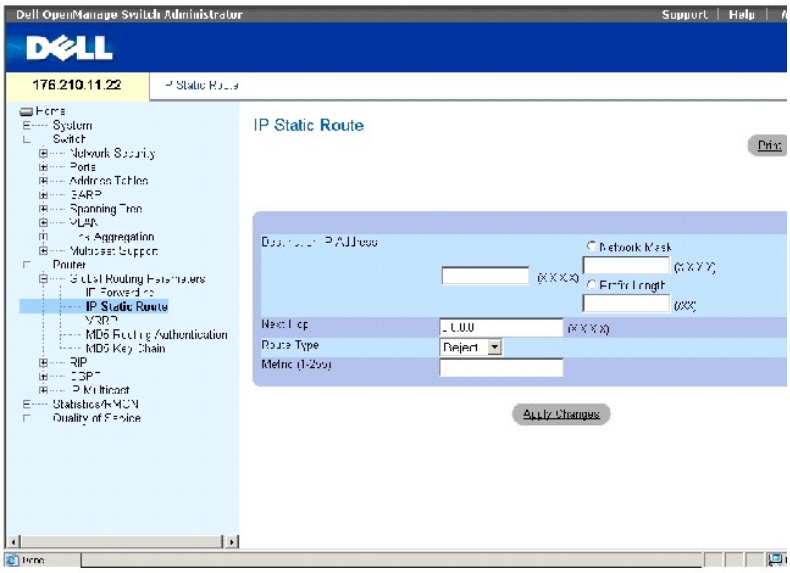
```
S 172.1.0.0/16 [5/3] via 10.0.1.1, 18:21:58, Ethernet g1

S 172.1.1.0/24 [5/3] via 10.0.2.1, 17:12:19, Ethernet g1

S 172.1.1.1/32 [5/3] via 10.0.3.1, 19:51:18, Ethernet g1

Maximum Parallel Paths: 2
```

Configuration de routes IP statiques

La page **IP Static Route** (Route IP statique) permet de définir des routes statiques.

Pour ouvrir la page **IP Static Route** (Route IP statique), cliquez sur **Router** (Routeur)→ **Global Routing Parameters** (Paramètres globaux de routage)→ **IP Static Route** (Route IP statique) dans l'*arborescence*.

Figure 8-2. Page Route IP statique



Destination IP Address (Adresse IP de destination) Réseau IP de destination de la route statique.

Network Mask (Masque de réseau) Masque de réseau de destination de cette route.

Prefix Length (Longueur de préfixe) Nombre de bits qui comprennent le préfixe de l'adresse IP de destination. La longueur est comprise entre 1 et 32.

Next Hop (Prochain saut) Indique l'adresse système suivante sur la route.

Route Type (Type de route) Définit le traitement du routage distant. Ce champ peut prendre les valeurs suivantes :

Remote (Distant) Le paquet est transmis.

Reject (Refus) Le paquet est rejeté.

Local Le paquet est envoyé à un réseau local.

Metric (1-255) (Métrique [1-255]) Nombre de sauts vers le réseau de destination.

Ajout de routes IP statiques

REMARQUE : Seul un routeur directement connecté peut être défini comme passerelle.

1. Ouvrez la page **IP Static Route** (Route IP statique).
2. Renseignez les champs de cette page.

REMARQUE : La sélection de l'option **Reject** (Refus) pour le champ **Route Type** (Type de route) rend inaccessibles les routes vers le réseau désigné.

Pour définir une route statique vers un hôte situé sur un réseau distant, sélectionnez **Remote** (Distant) pour le champ **Route Type** (Type de route).

Pour définir une route statique vers un hôte situé sur un réseau local, sélectionnez **Local** pour le champ **Route Type** (Type de route).

Destination IP Address (Adresse IP de destination) et **Network Mask** (Masque de réseau) désignent l'adresse du réseau distant. **Next Hop** (Prochain saut) est l'adresse d'un routeur directement connecté à votre commutateur.

La valeur de **Destination IP Address** (Adresse IP de destination) est l'adresse de l'hôte. La valeur de **Next Hop** (Prochain saut) doit être renseignée de la façon suivante : 0.0.0.0.

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

La nouvelle route statique est ajoutée et le périphérique est mis à jour.

Suppression d'une route IP statique

1. Ouvrez la page **IP Static Route** (Route IP statique).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **IP Static Route Table** (Table des routes IP statiques).
3. Cochez **Remove** (Supprimer) pour l'adresse IP de destination de la route statique à supprimer.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La route statique est supprimée et le périphérique est mis à jour.

Configuration de la table des routes IP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour la configuration de la table des routes IP statiques.

Tableau 8-2. Commandes CLI Table des routes IP statiques

Commande CLI	Description
`ip route prefix {`*`mask`* `|` *`prefix-length`*`} `*`gateway`* `[metric `*`distance`*`] [reject- route]`	Définit des routes IP statiques.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# ip route 172.16.0.0 255.255.0.0 131.16.1.1
```

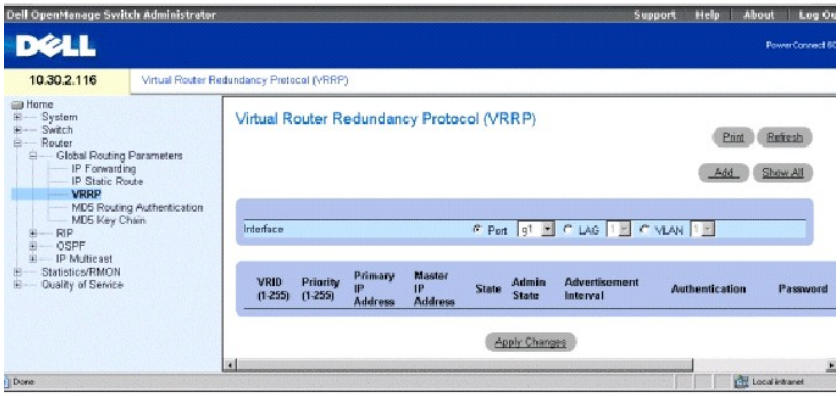
Configuration du protocole VRRP

Le protocole VRRP (Virtual Router Redundancy Protocol - protocole de redondance des routeurs virtuels) définit un protocole d'élection qui affecte dynamiquement la responsabilité du routage à l'un des routeurs VRRP du réseau local (routeur maître). Le processus d'élection permet un basculement dynamique de la responsabilité de routage en cas d'indisponibilité du routeur maître.

L'avantage du VRRP est qu'il élimine le phénomène de points de panne uniques inhérent à l'environnement de routage en fournissant un chemin par défaut à disponibilité supérieure, tout en éliminant le besoin de configurer les protocoles de détection de routeurs ou de routage dynamique sur chaque hôte final.

La page **Virtual Router Redundancy Protocol (VRRP)** (Protocole de redondance des routeurs virtuels [VRRP]) permet de définir les paramètres de routage VRRP du commutateur. Pour ouvrir la page **Virtual Router Redundancy Protocol (VRRP)** (Protocole de redondance des routeurs virtuels [VRRP]), cliquez sur **Router** (Routeur)→ **Global Routing Parameters** (Paramètres globaux de routage)→ **VRRP** dans l'*arborescence*.

Figure 8-3. Page Protocole de redondance des routeurs virtuels (VRRP)



Interface Type et numéro de l'interface connectée au routeur VRRP.

VRID (1-255) (VRID [1-255]) Identifiant du routeur virtuel.

Priority (1-255) (Priorité [1-255]) Priorité de routeur utilisée pour le processus d'élection du routeur virtuel. Cette valeur peut déterminer si un routeur VRRP de priorité supérieure remplace un routeur VRRP de priorité inférieure.

Primary IP Address (Adresse IP primaire) Adresse IP virtuelle associée au routeur virtuel. L'adresse IP primaire est sélectionnée parmi les adresses d'interface actuelles configurées sur un routeur VRRP.

Master IP Address (Adresse IP maîtresse) Routeur VRRP actuellement maître pour ce routeur virtuel.

State (État) État du routeur actuel. Ce champ peut prendre les valeurs suivantes :

Master (Maître) Le routeur fonctionne comme routeur de transmission pour les adresses IP associées au routeur virtuel. Le routeur maître répond aux demandes ARP avec les adresses IP associées dans la cible ARP, transmet les paquets avec l'adresse MAC virtuelle (VMAC) comme adresse MAC de destination et accepte les paquets associés aux adresses IP virtuelles (uniquement si le routeur possède l'adresse IP associée).

Initialize (Initialisation) Le routeur attend un événement de démarrage. À la réception de cet événement, le routeur change d'état.

Backup (Sauvegarde) Sauvegarde du routeur sur le routeur maître. Le routeur contrôle en permanence que le routeur maître est disponible par le biais des annonces périodiques envoyées par le routeur maître ou par les annonces spécifiques envoyées depuis le routeur maître et indiquant qu'il est inactif.

Admin State (État admin) Indique si le routeur est actif ou inactif.

Advertisement Interval (Intervalle d'annonce) Indique la fréquence à laquelle les annonces sont envoyées lorsque le routeur est le routeur maître.

Authentication (Authentification) Indique si un processus d'authentification a été mis en place ou non ou si des mots de passe sont utilisés pour authentifier les échanges du protocole VRRP.

Password (Mot de passe) Mot de passe utilisé pour authentifier les échanges du protocole VRRP.

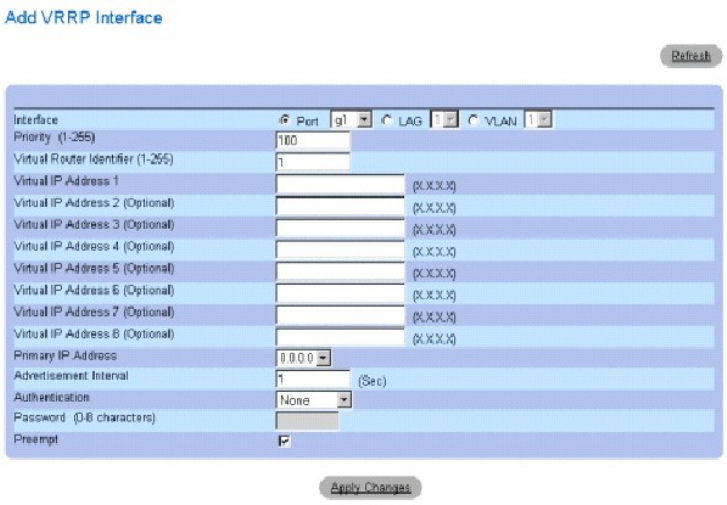
Preempt (Préempt) Lorsqu'elle est cochée, cette option permet aux routeurs VRRP de priorité supérieure de remplacer les routeurs de priorité inférieure.

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime des entrées VRRP de la table VRRP.

Ajout de routeurs à un groupe VRRP

1. Ouvrez la page **Virtual Router Redundancy Protocol (VRRP)** (Protocole de redondance des routeurs virtuels [VRRP]).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add VRRP Interface** (Ajout d'une interface VRRP).

Figure 8-4. Ajout d'une interface VRRP



3. Renseignez les champs.

Pour obtenir des informations sur les champs, reportez-vous à la section «Configuration du protocole VRRP».

REMARQUE : Les interfaces VRRP doivent être définies pour pouvoir passer l'état admin sur **Enabled** (Activé).

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

La nouvelle interface VRRP est ajoutée et le périphérique est mis à jour.

REMARQUE : Si une adresse IP virtuelle non valide est saisie, un message d'avertissement s'affiche mais le routeur virtuel sera tout de même ajouté. Il est recommandé de supprimer cette entrée de la table des routeurs virtuels.

Modification de routeurs VRRP

1. Ouvrez la page **Virtual Router Redundancy Protocol (VRRP)** (Protocole de redondance des routeurs virtuels [VRRP]).
2. Sélectionnez une interface dans le champ **Interface**.
3. Renseignez les champs comme vous le désirez.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Suppression d'une entrée VRRP

1. Ouvrez la page **Virtual Router Redundancy Protocol (VRRP)** (Protocole de redondance des routeurs virtuels [VRRP]).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **VRRP Table** (Table VRRP).
3. Sélectionnez une entrée de la table.
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

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

Configuration du VRRP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour la configuration du VRRP.

Tableau 8-3. Commandes CLI VRRP

Commande CLI	Description
vrrp *virtual-router* ip *ip-address* [*ip- address2...ip-address8*]	Définit le protocole de redondance des routeurs virtuels (VRRP) pour une interface.
vrrp *virtual-router* up	Active le protocole de redondance des routeurs virtuels (VRRP) sur une interface.
vrrp *virtual-router* timer *seconds*	Définit l'intervalle entre l'envoi des messages d'annonces.
vrrp *virtual-router* priority *priority*	Définit la priorité du protocole de redondance des routeurs virtuels (VRRP) sur une interface.
vrrp *virtual-router* source-ip *ip-address*	Définit l'adresse IP source (adresse IP primaire) utilisée pour les messages du protocole de redondance des routeurs virtuels sur une interface.
vrrp *virtual-router* authentication *text*	Active l'authentification du protocole de redondance des routeurs virtuels (VRRP) sur une interface.
vrrp *virtual-router* preempt	Active la préemption du protocole de redondance des routeurs virtuels (VRRP) sur une interface.
show vrrp configuration [ethernet *interface-* number | *vlan vlan-id* | *port-channel number*]	Affiche la configuration du protocole de redondance des routeurs virtuels (VRRP).
	Affiche l'état du protocole de redondance des routeurs virtuels (VRRP).

show vrrp status [ethernet *interface- number* | *vlan vlan-id* | *port-channel number*]	

Configuration du VRRP à l'aide de commandes CLI

Vous trouverez ci-dessous un exemple de commande CLI :

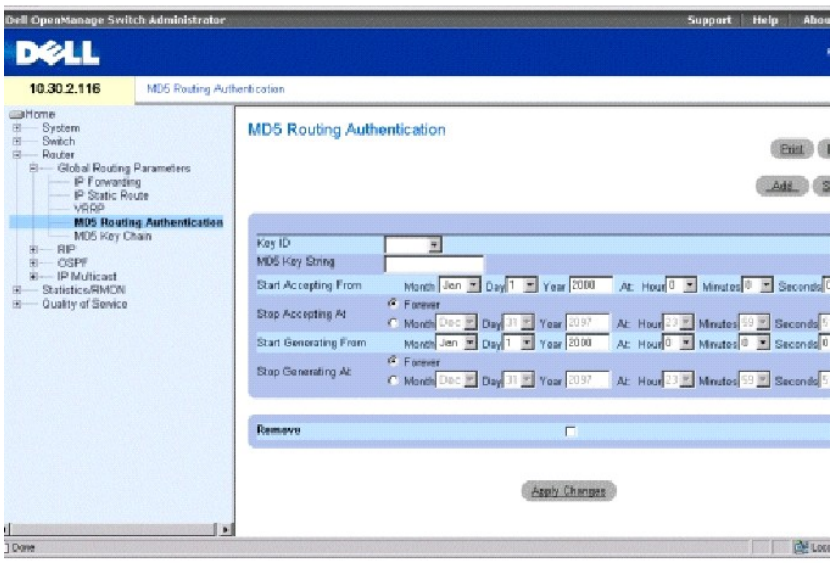
```
Console (config)# interface ethernet g8

Console (config-if)# vrrp 45 ip 172.16.1.1 172.16.2.1

Console (config-if)# vrrp 45 up

Console (config-if)# vrrp 45 timer 100

Console (config-if)# vrrp 45 priority 150

Console (config-if)# vrrp 45 source-ip 168.192.1.1

Console (config-if)# vrrp 45 authentication Dell

Console (config-if)# vrrp 45 preempt

Console (config-if)# exit

Console (config)# exit
```

Configuration de l'authentification MD5 du routage

Les clés MD5 sont utilisées par l'algorithme d'authentification MD5 (condensé de message). Des dates/heures de début et de fin, pour l'envoi et la réception, peuvent être définies pour chaque clé. Des clés actives qui expirent aux dates/heures de la réinitialisation peuvent être configurées. Les interfaces qui communiquent entre elles doivent avoir le même ID de clé. Si les dates/heures de clé se chevauchent côté envoi, le périphérique utilise la clé ayant la dernière heure/date de début. Lors de la réception des paquets, l'interface utilise la clé indiquée sur le paquet par la valeur **Key ID** (ID de clé).

La page **MD5 Routing Authentication** (Authentification MD5 du routage) permet de définir et de gérer des clés. Pour ouvrir la page **MD5 Routing Authentication** (Authentification MD5 du routage), cliquez sur **Router** (Routeur)→ **Global Routing Parameters** (Paramètres globaux de routage)→ **MD5 Routing Authentication** (Authentification MD5 du routage) dans l'*arborescence*.

Figure 8-5. Authentification MD5 du routage



Key ID (ID de clé) Définit l'ID de la clé.

MD5 Key String (Clé de codage) Indique le mot de passe utilisé pour l'authentification du routage.

Start Accepting From (Commencer l'acceptation à partir du) Date et heure auxquelles la clé MD5 commence à accepter le trafic avec la clé MD5 spécifiée. Le format du champ **Start Accept** (Commencer l'acceptation à partir du) est le suivant : **Month Day Year At: Hour Minute Second** (Mois Jour Année À Heures Minutes Secondes).

Stop Accepting At (Arrêter l'acceptation le) Date et heure auxquelles la clé MD5 commence à ne plus accepter le trafic avec la clé MD5 spécifiée. Le format du champ **Stop Accept** (Arrêter l'acceptation le) est le suivant : **Month Day Year At: Hour Minute Second** (Mois Jour Année À Heures Minutes Secondes). Si l'option **Forever** (Toujours) est sélectionnée, aucune limite n'est définie pour l'acceptation du trafic avec les clés MD5.

Start Generating From (Commencer la génération à partir du) Date et heure auxquelles les paquets de protocole sont transmis avec les clés MD5. Le format du champ **Start Generate** (Commencer la génération à partir du) est le suivant : **Month Day Year At: Hour Minute Second** (Mois Jour Année À Heures Minutes Secondes).

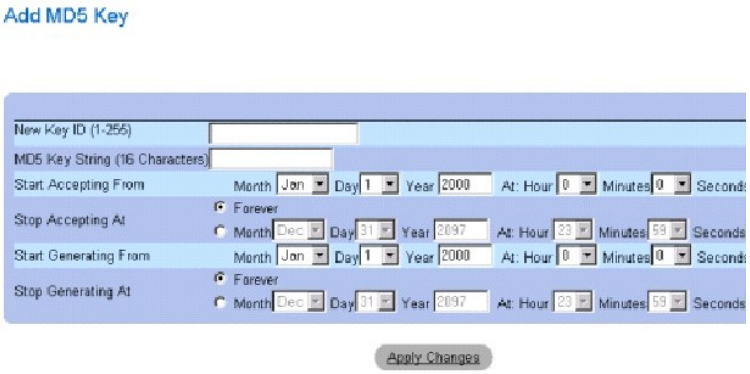
Stop Generating At (Arrêter la génération le) Date et heure auxquelles les paquets de protocole ne sont plus transmis avec les clés MD5. Le format du champ **Stop Generate** (Arrêter la génération le) est le suivant : **Month Day Year At: Hour Minute Second** (Mois Jour Année À Heures Minutes Secondes). Si l'option **Forever** (Toujours) est sélectionnée, aucune limite n'est définie pour l'acceptation du trafic avec les clés MD5.

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime une clé MD5.

Ajout d'une clé MD5

1. Ouvrez la page **MD5 Routing Authentication** (Authentification MD5 du routage).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add MD5 Key** (Ajout d'une clé MD5).

Figure 8-6. Ajout d'une clé MD5



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

La nouvelle clé MD5 est ajoutée à la table **MD5 Key Table** (table des clés MD5) et le périphérique est mis à jour.

Modification d'une clé MD5

1. Ouvrez la page **MD5 Routing Authentication** (Authentification MD5 du routage).
2. Dans le menu déroulant **Entry No.** (Numéro d'entrée), sélectionnez la clé MD5 à modifier.
3. Renseignez les champs de la boîte de dialogue.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle clé MD5 est modifiée et le périphérique est mis à jour.

Suppression d'une clé MD5

1. Ouvrez la page **MD5 Routing Authentication** (Authentification MD5 du routage).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **MD5 Key Table** (Table des clés MD5).
3. Sélectionnez une entrée dans le champ **Key ID** (ID de clé).
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La clé MD5 est supprimée et le périphérique est mis à jour.

Configuration de l'authentification MD5 à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour la configuration de l'authentification MD5.

Tableau 8-4. Commandes CLI Authentification MD5

Commande CLI	Description
key *key-id*	Crée une clé d'authentification.
	Définit la période pendant laquelle une clé d'authentification d'une chaîne de clés

`accept-lifetime { duration time-to-start day-of-the-month` *`day- of-the-month`* `year-to- start key-lifetime- duration-in-seconds } | { infinite time-to- start day-of-the-month` *`day-of-the-month`* `year-to-start } | { time- to-start day-of-the- month` *`day-of-the-month`* `year-to-start time-to- stop day-of-the-month` *`day-of-the-month`* `year- to-stop }`	peut être reçue.
`send-lifetime { duration time-to-start day-of-the-month` *`day- of-the-month`* `year-to- start key-lifetime-duration-in-seconds } | { infinite time-to- start day-of-the-month` *`day-of-the-month`* `year- to-start } | { time- to-start day-of-the- month` *`day-of-the-month`* `year-to-start time-to- stop day-of-the-month` *`day-of-the-month`* `year- to-stop }`	Définit la période pendant laquelle une clé d'authentification d'une chaîne de clés peut être envoyée.

Vous trouverez ci-dessous un exemple de commande CLI :

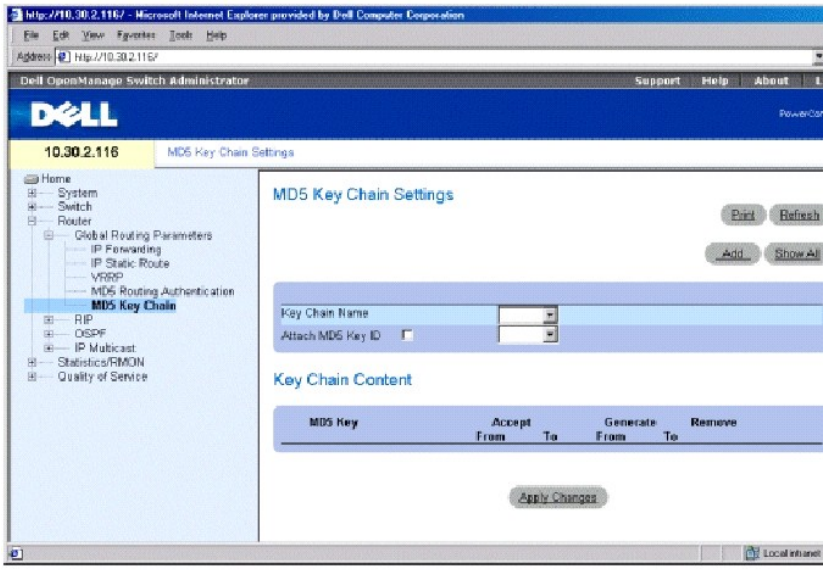
```
Console (config)# key 3

Console (config-key)# accept-lifetime duration 13:30:00 Jan 25 2002 7200

Console (config-key)# send-lifetime duration 14:00:00 Jan 25 2002 3600
```

Configuration des paramètres des chaînes de clés MD5

Une fois définies, les clés sont regroupées dans une «chaîne de clés». Plusieurs clés peuvent être simultanément affectées à chaque interface de routeur. Le regroupement des clés en chaînes de clés facilite l'affectation aux interfaces. Chaque clé peut être comprise dans plusieurs chaînes de clés. Les chaînes de clés sont affectées aux interfaces dans les paramètres d'interface RIP ou OSPF. Les clés MD5 sont ajoutées à une chaîne de clés MD5 pour générer la chaîne de clés.

La page **MD5 Key Chain Settings** (Paramètres des chaînes de clés MD5) permet de définir des chaînes de clés et de leur affecter des clés. Pour ouvrir la page **MD5 Key Chain Settings** (Paramètres des chaînes de clés MD5), cliquez sur **Router** (Routeur)→ **Global Routing Parameters** (Paramètres globaux de routage) → **MD5 Key Chain** (Chaîne de clés MD5) dans l'*arborescence*.

Figure 8-7. Paramètres des chaînes de clés MD5



Key Chain Name (Nom de la chaîne de clés) Noms des chaînes de clés définis par l'utilisateur.

Attach MD5 Key ID (Associer un ID de clé MD5) Indique l'ID de chaîne de clés associé à la chaîne de clés.

MD5 Key (Clé MD5) Clé membre de la chaîne de clés.

Accept From (Accepter à partir du) Date et heure auxquelles la clé MD5 sélectionnée commence à accepter le trafic avec la clé MD5 spécifiée. Le format du champ **Accept From** (Accepter à partir du) est le suivant : **Month Day Year At: Hour Minute Second** (Mois Jour Année À Heures Minutes Secondes). Le champ **Accept From** (Accepter à partir du) est la clé définie dans la page **MD5 Routing Authentication** (Authentification MD5 du routage).

Accept To (Accepter jusqu'au) Date et heure auxquelles la clé MD5 sélectionnée n'accepte plus le trafic avec la clé MD5 spécifiée. Le format de ce champ est le suivant : **Month Day Year At: Hour Minute Second** (Mois Jour Année À Heures Minutes Secondes). Le champ **Accept To** (Accepter jusqu'au) est la clé définie dans la page **MD5 Routing Authentication** (Authentification MD5 du routage).

Generate From (Générer à partir du) Date et heure auxquelles la clé MD5 sélectionnée commence à transmettre le trafic. Le format du champ **Generate From** (Générer à partir du) est le suivant : **Month Day Year At: Hour Minute Second** (Mois Jour Année À Heures Minutes Secondes). Le champ **Generate From** (Générer à partir du) est la clé définie dans la page **MD5 Routing Authentication** (Authentification MD5 du routage).

Generate To (Générer jusqu'au) Date et heure auxquelles la clé MD5 sélectionnée arrête de transmettre le trafic. Le format du champ **Generate To** (Générer jusqu'au) est le suivant : **Month Day Year At: Hour Minute Second** (Mois Jour Année À Heures Minutes Secondes). Le champ **Generate To** (Générer jusqu'au) est la clé définie dans la page **MD5 Routing Authentication** (Authentification MD5 du routage).

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime une clé MD5 de la table des chaînes de clés MD5.

Ajout d'une chaîne de clés MD5

1. Ouvrez la page **MD5 Key Chain Settings** (Paramètres des chaînes de clés MD5).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add Key Chain** (Ajout d'une chaîne de clé).
3. Renseignez les champs **New Key Chain Name** (Nom de la nouvelle chaîne de clés) et **Attach MD5 Key No.** (Associer un numéro de clé MD5).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle chaîne de clés MD5 est ajoutée à la table des chaînes de clés MD5 et le périphérique est mis à jour.

Modification d'une chaîne de clés MD5

1. Ouvrez la page **MD5 Key Chain Settings** (Paramètres des chaînes de clés MD5).
2. Modifiez les champs **Name** (Nom) et/ou **Key Chain ID** (ID de chaîne de clés).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle chaîne de clés MD5 est modifiée et le périphérique est mis à jour.

Suppression d'une chaîne de clés MD5

1. Ouvrez la page **MD5 Key Chain Settings** (Paramètres des chaînes de clés MD5).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **MD5 Key Chain Table** (Table des chaînes de clés MD5).
3. Sélectionnez une entrée dans le champ **Key Chain Name** (Nom de la chaîne de clés).
4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La chaîne de clés MD5 est supprimée et le périphérique est mis à jour.

Configuration des chaînes de clés à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour la configuration des chaînes de clés.

Tableau 8-5. Commandes CLI Chaîne de clés

Commande CLI	Description
key-chain *name- of-chain*	Identifie un groupe de clés d'authentification.
key *key-id*	Identifie une clé d'authentification sur une chaîne de clés.
key-string *text*	Définit une chaîne d'authentification pour une clé.
accept-lifetime *start-time end- time* | {infinite | *start-time* | duration *start- time seconds*} no accept-lifetime	Définit la période pendant laquelle la clé d'authentification est valide pour l'authentification des paquets entrants.
send-lifetime *start-time end- time* | {infinite | *start-time* | duration *start- time seconds*}no send-lifetime	Définit la période pendant laquelle une clé d'authentification est valide pour la génération d'un condensé MD5 pour les paquets sortants.
show key-chains [*name-of-chain*]	Affiche des informations sur la chaîne de clés.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# key chain M

Console (config-key-chain)# key 1

Console (config-key)# key-string mountain

Console (config-key)# accept-lifetime duration 13:30:00 Jan 25 2002 7200

Console (config-key)# send-lifetime duration 14:00:00 Jan 25 2002 3600

Console (config-key)# exit

Console (config)# exit

Console# show key-chains

key chain internal

key 1

accept: 13:30:00 Jan 25 2002 duration 7200

send : 14:00:00 Jan 25 2002 duration 3600
```

```
key 2

accept: 14:30:00 Jan 25 2002 duration 7200

send: 15:00:00 Jan 25 2002 duration 3600

key chain external

key 1

accept: 13:30:00 Jan 25 2002 until 15:30:00 Jan 25 2002

send: 14:00:00 Jan 25 2002 until 15:00:00 Jan 25 2002

key 2

accept: 14:30:00 Jan 25 2002 until 16:30:00 Jan 25 2002

send: 15:00:00 Jan 25 2002 until 16:00:00 Jan 25 2002

25 2002
```

Configuration du protocole RIP

Le protocole d'information de routage (RIP) est la norme Internet la plus couramment utilisée pour les protocoles de passerelle intérieure. Le protocole diffuse des informations de routage pour déterminer la route la plus rapide vers la prochaine destination. Le protocole RIP est un protocole de routage à vecteur de distance le mieux adapté aux petits réseaux. Les routes sont déterminées en fonction du plus petit nombre de sauts. Les mises à jour de routage contiennent des paires de valeurs comprenant une adresse IP et la distance jusqu'au noeud.

Le protocole RIP version 2 :

- prend en charge les masques de sous-réseaux ;
- fournit des méthodes d'authentification ;
- prend en charge les protocoles de routage ;
- fournit une plus grande distribution et une plus petite bande passante, dépassant ainsi les exigences.

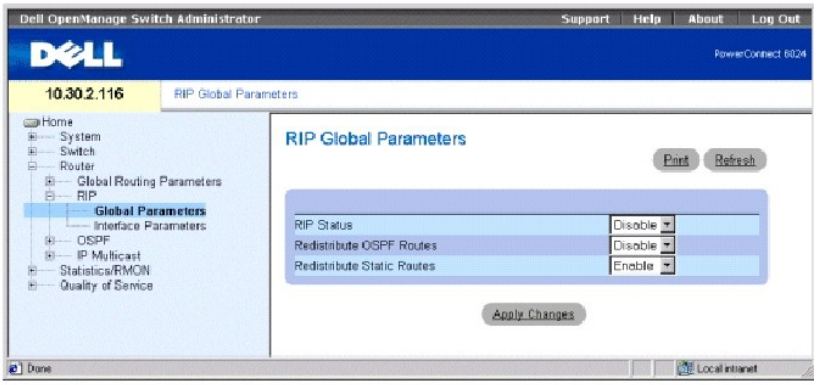
La page **RIP** permet de configurer le protocole RIP. Pour ouvrir la page **RIP**, cliquez sur **Router** (Routeur)→ **RIP** dans l'*arborescence*.

Définition des paramètres globaux du protocole RIP

La page **RIP Global Parameters** (Paramètres globaux RIP) contient des champs pour l'activation du protocole RIP sur le périphérique, la définition de la redistribution d'OSPF et la définition de la redistribution des routes statiques.

Cliquez sur **Router** (Routeur)→ **RIP**→ **Global Parameters** (Paramètres globaux) dans l'arborescence pour afficher la page **RIP Global Parameters** (Paramètres globaux RIP).

Figure 8-8. Page Paramètres globaux RIP



RIP Status (État RIP) Active ou désactive le protocole RIP sur le périphérique.

Redistribute OSPF Routes (Redistribuer les routes OSPF) Lorsqu'elle est activée, cette option redistribue les routes du protocole OSPF au protocole RIP. La redistribution des routes implique l'importation d'interfaces de routage étrangères dans le protocole RIP.

Redistribute Static Routes (Redistribuer les routes statiques) Lorsqu'elle est activée, cette option redistribue les routes des routes statiques au protocole RIP.

Activation du protocole RIP, redistribution des routes OSPF, redistribution des routes statiques

1. Ouvrez la page **RIP Global Parameters** (Paramètres globaux RIP).
2. Sélectionnez **Enabled** (Activé) dans le champ des paramètres globaux RIP à activer.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le protocole RIP est activé sur le périphérique.

Configuration des paramètres globaux RIP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour la configuration des paramètres globaux RIP.

Tableau 8-6. Commandes CLI Paramètres globaux RIP

Commande CLI	Description
`router rip enable`	Active le protocole d'information de routage (RIP) sur le périphérique.
`no router rip enable`	Désactive le protocole d'information de routage (RIP) sur le périphérique.
`router rip redistribute ospf`	Annonce les routes apprises par le protocole OSPF dans le processus RIP.
	Arrête d'annoncer les routes apprises par le protocole OSPF dans le processus RIP.

`no router rip redistribute ospf`	
`router rip redistribute static`	Annonce les routes configurées statiquement dans le processus RIP.
`no router rip redistribute static`	Arrête d'annoncer les routes configurées statiquement dans le processus RIP.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# router rip enable

Console (config)# router rip redistribute ospf

Console (config)# router rip redistribute static

Console (config)# no router rip enable

Console (config)# no router rip redistribute ospf

Console (config)# no router rip redistribute static
```

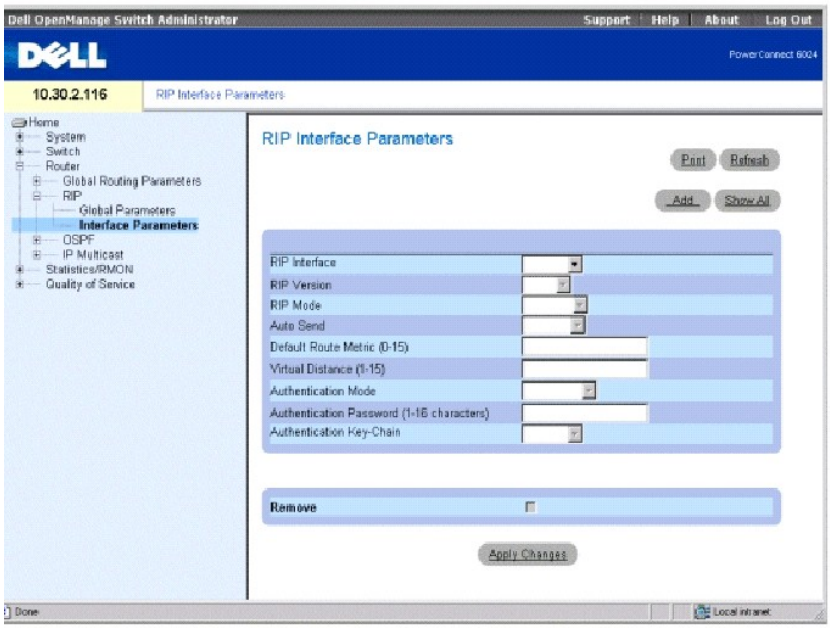
Définition des paramètres d'interface RIP

La page **RIP Interface Parameters** (Paramètres d'interface RIP) permet de définir les adresses IP sur lesquelles le protocole RIP est activé, de définir les métriques de routage, d'activer l'option **Auto Send** (Envoi automatique), de définir la distance virtuelle et de définir l'état IP.

REMARQUE : Pour pouvoir définir une interface RIP, le protocole RIP doit avoir été activé au préalable. Pour plus d'informations, reportez-vous à la section «Activation du protocole RIP, redistribution des routes OSPF, redistribution des routes statiques».

Pour ouvrir la page **RIP Interface Parameters** (Paramètres d'interface RIP), cliquez sur **Router** (Routeur)→ **RIP**→ **RIP Interface Parameters** (Paramètres d'interface RIP) dans l'*arborescence*.

Figure 8-9. Page Paramètres d'interface RIP



RIP Interface (Interface RIP) Adresse IP actuelle de l'interface.

RIP Version (Version RIP) Type de RIP en cours de diffusion. Ce champ peut prendre les valeurs suivantes :

Ver. 1 (Version 1) Diffuse des mises à jour RIP conformes à RFC 1058.

Ver. 2 (Version 2) Indique que le périphérique diffuse des mises à jour RIP 2.

RIP Mode (Mode RIP) Type d'opération RIP. Ce champ peut prendre les valeurs suivantes :

RX Les diffusions de réception RIP sont reçues sur le périphérique.

RX & TX Les diffusions de réception et de transmission RIP sont reçues sur le périphérique.

Auto Send (Envoi auto) Permet au périphérique de publier les messages RIP uniquement dans la métrique par défaut, permettant ainsi aux stations d'apprendre l'adresse du routeur par défaut. Le routeur n'envoie ainsi plus de mises à jour RIP intempestives sur des liaisons ne disposant d'aucun routeur pour les recevoir. Lorsque l'option **Auto Send** (Envoi auto) est active, une brève mise à jour RIP est envoyée, ce qui permet aux stations écoutant le protocole RIP d'effectuer la détection de routeur, etc., et d'envoyer une mise à jour RIP aux routeurs qui pourraient être ajoutés au réseau ultérieurement.

Si une mise à jour RIP est reçue sur une interface, l'option **Auto Send** (Envoi auto) est désactivée sur cette interface et des mises à jour RIP complètes sont envoyées. Si le périphérique détecte un autre message RIP, l'option **Auto Send** (Envoi auto) est désactivée.

Default Route Metric (1-16) (Métrique des routes par défaut (1-16)) Métrique d'entrée des routes par défaut dans les mises à jour RIP originaires de cette interface. Zéro indique qu'aucune route par défaut n'est originaire de cette interface.

Virtual Distance (1-16) (Distance virtuelle (1-16)) Nombre virtuel de sauts affectés à l'interface. Cette option permet un réglage minutieux de l'algorithme de routage RIP.

Authentication Mode (Mode d'authentification) Type d'authentification de l'interface, mot de passe ou MD5, utilisé pour authentifier les messages RIP vers. 2.

Authentication Password (Mot de passe d'authentification) Mot de passe d'authentification.

Authentication Key-Chain (Chaîne de clés d'authentification) Chaîne de clés d'authentification.

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime l'interface RIP.

Ajout d'une interface RIP

1. Ouvrez la page **RIP Interface Parameters** (Paramètres d'interface RIP).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **New RIP Interface** (Nouvelle interface RIP).
3. Renseignez les champs de cette page.

   Les champs de cette page sont les mêmes que ceux de la page **RIP Interface Parameters** (Paramètres d'interface RIP).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Modification des paramètres d'interface RIP

1. Ouvrez la page **RIP Interface Parameters** (Paramètres d'interface RIP).
2. Modifiez les champs comme vous le désirez.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

   Les paramètres d'interface RIP sont modifiés et le périphérique est mis à jour.

Suppression d'une interface RIP

1. Ouvrez la page **RIP Interface Parameters** (Paramètres d'interface RIP).
2. Sélectionnez une interface RIP dans le menu déroulant **RIP Interface** (Interface RIP).
3. Cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

   L'interface RIP est supprimée et le périphérique est mis à jour.

Configuration des interfaces RIP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour la configuration des paramètres globaux RIP.

Tableau 8-7. Commandes CLI Configuration RIP

Commande CLI	Description
`rip`	Active le protocole RIP sur une interface.
`rip version {1 | 2}`	Définit la version RIP.
`rip passive-interface`	Désactive l'envoi de mises à jour de routage sur une interface.
	Détecte automatiquement si des informations RIP doivent être envoyées sur l'interface.

`rip auto-send`	
`rip offset offset`	Ajoute un décalage à une métrique apprise via le protocole RIP avant de l'ajouter à la table des interfaces.
`rip default-route offset offset`	Génère une route par défaut dans le protocole RIP en appliquant une valeur de décalage.
`rip authentication {text text | md5 name-of-chain}`	Active l'authentification des paquets RIP Version 2 et définit le type d'authentification.
`show ip rip`	Affiche les informations RIP IP.
`show ip rip md5`	Affiche les informations MD5 RIP IP.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# router rip enable

Console (config)# interface ip 100.1.1.1

Console (config-ip)# rip

Console (config-ip)# rip version 1

Console (config-ip)# rip passive interface

Console (config-ip)# rip auto-send

Console (config-ip)# rip offset 5

Console (config-ip)# rip default-route offset 5

Console (config-ip)# rip authorization text dell

Console (config-ip)# exit

Console (config)# exit

Console# show ip rip

RIP is enabled.

OSPF leaking is enabled.

Static leaking is enabled.
```

```
Interface State Ver Offset Default Route Passive Auto Send Auth


176.16.0.0/16 Enabled 2 1 Disabled No Yes MD5


192.168.0.0/16 Enabled 2 1 Disabled No No Text
```

Configuration des paramètres et des filtres OSPF

Le protocole de passerelle interne OSPF(Open Shortest Path First) permet aux routeurs d'échanger des messages d'état de liaison en réunissant les informations réseau et en déterminant le meilleur chemin de routage en fonction de la distance du noeud.

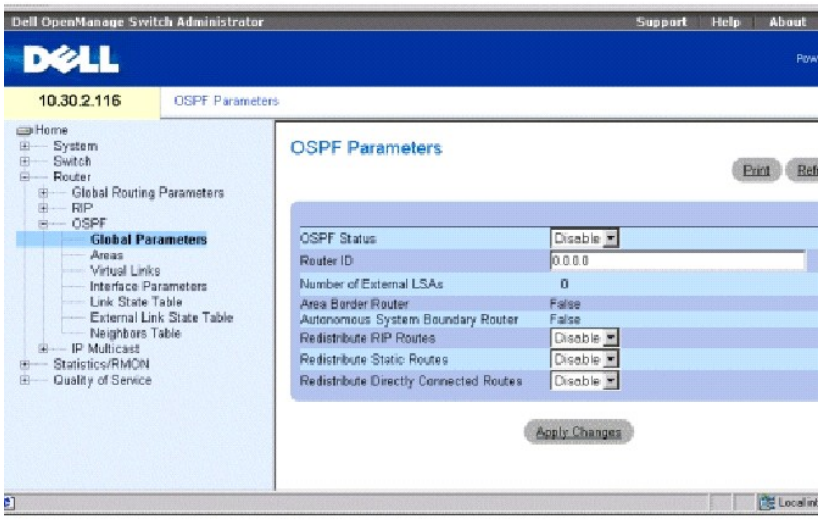
Le protocole OSPF est un protocole à état de liaison plutôt qu'un protocole à vecteur de distance et nécessite, par conséquent, moins de bande passante que le protocole RIP. Le protocole OSPF est activé et défini par :

- Configuration des paramètres OSPF
- Configuration des zones OSPF
- Configuration des liaisons virtuelles OSPF
- Affichage de la table des états de liaison
- Affichage de la table des états de liaison externe
- Affichage de la table des voisins OSPF

Configuration des paramètres OSPF

Le protocole OSPF détecte le meilleur chemin de routage en fonction de la distance du noeud. L'activation du protocole OSPF s'effectue dans la page **OSPF Parameters** (Paramètres OSPF). Pour ouvrir la page **OSPF Parameters** (Paramètres OSPF), cliquez sur **Router** (Routeur)→ **OSPF**→ **Global Parameters** (Paramètres globaux) dans l'*arborescence*.

Figure 8-10. Page Paramètres globaux OSPF



OSPF Status (État OSPF) Active le protocole OSPF sur au moins une interface ou désactive le protocole OSPF pour toutes les interfaces.

Router ID (ID Routeur) Numéro d'identification du routeur. Par défaut, l'ID du routeur est une adresse IP sur le périphérique. **Router ID** (ID de routeur) est un champ facultatif. Sa valeur par défaut est définie sur la plus petite interface IP du périphérique.

Number of External LSAs (Nombre de LSA externes) Nombre d'annonces externes d'état de liaison (LSA) présentes dans la base de données d'états de liaison.

Area Border Router (ABR) (Routeur de frontière de zone (ABR)) Indique si le périphérique est un routeur de frontière de zone. Si le périphérique est configuré comme un ABR, il est connecté à deux zones ou plus. Une zone est la zone de segment principal.

Autonomous System Boundary Router (ASBR) (Routeur de limites de systèmes autonomes [ASBR]) Indique si le périphérique est configuré comme un ASBR. Si le périphérique est configuré comme un ASBR, il importe les données de routage depuis les protocoles de routage non OSPF.

Redistribute RIP Routes (Redistribuer les routes RIP) Active or désactive la redistribution des routes insérées dans la table de routage IP par le protocole RIP pour les annoncer au protocole OSPF comme étant des routes externes.

Redistribute Static Routes (Redistribuer les routes statiques) Active toutes les routes configurées statiquement à annoncer comme étant des routes externes OSPF ou désactive la redistribution des routes statiques.

Redistribute Directly Connected Routes (Redistribuer les routes connectées directement) Active toutes les routes externes pour les annoncer au protocole OSPF comme étant des routes externes ou désactive la redistribution des routes directes externes.

Activation du protocole OSPF

1. Ouvrez la page **OSPF Parameters** (Paramètres OSPF).
2. Renseignez les champs **OSPF Status** (État OSPF), **Router ID** (ID de routeur), **Redistribute RIP Routes** (Redistribuer les routes RIP), **Redistribute Static Routes** (Redistribuer les routes statiques) et **Redistribute Directly Connected Routes** (Redistribuer les routes connectées directement).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le protocole OSPF est activé sur le périphérique.

REMARQUE : Les processus OSPF ne peuvent être effacées qu'à l'aide de la commande CLI **clear ip ospf process**.

Activation du protocole OSPF à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'activation du protocole OSPF.

Tableau 8-8. Commandes CLI OSPF

Commande CLI	Description
`router ospf enable`	Active le processus de routage OSPF.
`router ospf router-id ip-address`	Configure un ID de routeur OSPF.
`router ospf redistribute rip`	Active les routes d'annonce, apprises par le processus RIP, dans le processus de routage OSPF.
`router ospf redistribute static`	Routes d'annonce, configurées statiquement, dans le processus de routage OSPF.
	Routes d'annonce directement connectée.

outer ospf redistribute connected	

Vous trouverez ci-dessous un exemple de commande CLI :

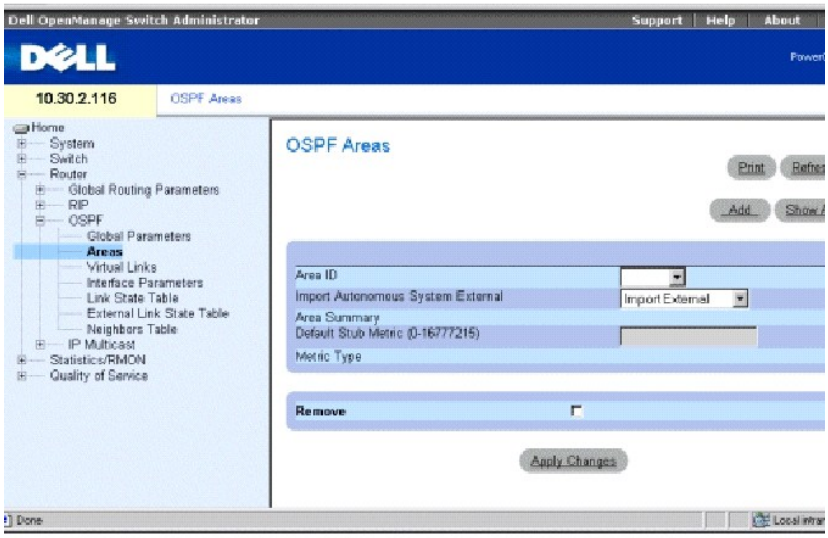
```
Console (config)# router ospf enable

Console (config)# router ospf router-id 196.127.2.1

Console (config)# router ospf redistribute rip

Console (config)# router ospf redistribute static
```

Configuration des zones OSPF

La page **OSPF Areas** (Zones OSPF) contient des informations concernant la définition et la maintenance des zones OSPF au sein desquelles les interfaces et les liaisons virtuelles sont définies. Une fois une zone OSPF créée, le protocole OSPF est automatiquement activé sur toutes les interfaces IP.

Pour afficher la page **OSPF Areas** (Zones OSPF), cliquez sur **Router** (Routeur)→ **OSPF**→ **Areas** (Zones) dans l'*arborescence*.

Figure 8-11. Page Zones OSPF



Area ID (ID de zone) ID de la zone. Le format est une adresse IP.

Import Autonamous System External (Importer des LSA externes au système autonome) Indique s'il s'agit d'une zone de stub. Ce champ peut prendre les valeurs suivantes :

Import External (Importer des LSA externes) Des annonces d'état de liaison (LSA) externes au système autonome peuvent être importées dans la zone

Import No External (Ne pas importer de LSA externes) Aucune LSA externe ne peut être importée dans la zone ; il s'agit donc d'une zone de stub.

Area Summary (Résumé zone) Contrôle l'importation des LSA de résumé dans les zones de stub. Cette variable n'agit pas sur les autres zones. Ce champ peut prendre les valeurs suivantes :

No Area Summary (Pas de résumé zone) Indique qu'il s'agit d'une zone entièrement de stub.

Send Area Summary (Envoyer le résumé zone) Indique qu'il ne s'agit pas d'une entièrement de stub.

Une zone de stub est une zone dans laquelle les LSA externes ne sont pas inondées. Les zones entièrement de stub utilisent une route par défaut pour atteindre non seulement les destinations externes au système autonome mais aussi toutes les destinations externes à la zone. Pour tirer parti de la prise en charge des zones de stub, le routage par défaut doit être utilisé dans la zone de stub.

Default Stub Metric (0-16777216) (Métrique de stub par défaut (1-16777216)) Métrique de la route par défaut créée pour la zone de stub. Les zones de stub n'effectuent pas d'importations externes à l'AS. Par conséquent, une route par défaut est créée par le routeur de frontière de zone pour la zone de stub.

Metric Type (Type de métrique) Type de métrique du protocole.

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime l'adresse IP de la table des zones OSPF.

Définition d'une nouvelle zone OSPF

1. Ouvrez la page **OSPF Areas** (Zones OSPF).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add an OSPF Area** (Ajout d'une zone OSPF).
3. Renseignez les champs de la boîte de dialogue.

REMARQUE : Le champ **Stub Metric** (Métrique de stub) est défini pour les routeurs de frontière de zone.

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

La nouvelle zone est ajoutée à la table des zones OSPF.

Modification des paramètres des zones OSPF

1. Ouvrez la page **OSPF Areas** (Zones OSPF).
2. Sélectionnez un **ID de zone**.

Les paramètres de la zone OSPF s'affichent.

3. Modifiez les champs comme vous le désirez.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de la zone sont modifiés et enregistrés sur le périphérique.

Suppression d'une zone OSPF

1. Ouvrez la page **OSPF Areas** (Zones OSPF).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table des zones OSPF.
3. Sélectionnez une zone OSPF et cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La zone OSPF est supprimée de la table et le périphérique est mis à jour.

Définition de zones OSPF à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour la définition des zones OSPF.

Tableau 8-9. Commandes CLI Zone OSPF

Commande CLI	Description
`router ospf area area- id stub`	Définit une zone comme une zone de stub. Pour désactiver cette fonction, utilisez la forme no de cette commande.
`router ospf area area- id default-cost cost`	Définit un coût pour la route de résumé par défaut envoyée dans une zone de stub.

Vous trouverez ci-dessous un exemple de commande CLI :

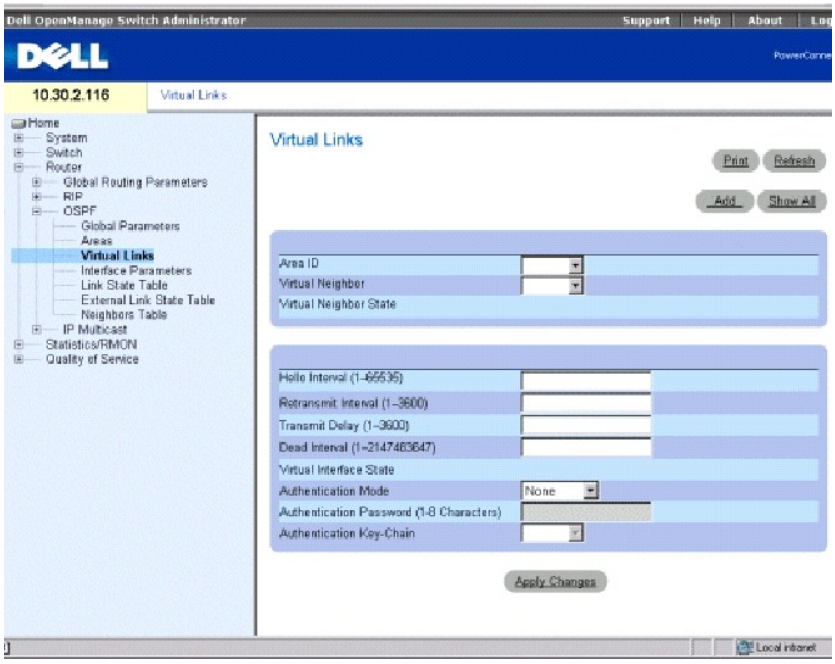
```
Console (config)# router ospf enable

Console (config)# router ospf area 7.7.7.7 stub

Console (config)# router ospf area 192.168.3.1 default-cost 10000
```

Configuration des liaisons virtuelles OSPF

Le protocole OSPF exige que toutes les zones soient reliées par une zone de segment principal. Toutefois, si une zone n'est pas connectée à un segment principal, vous pouvez connecter deux routeurs de frontière de zone par une liaison virtuelle. Les liaisons virtuelles sont définies en configurant un voisin virtuel. Les liaisons virtuelles ne peuvent pas être configurées par une zone de stub.

Définissez les liaisons virtuelles dans la page **Virtual Links** (Liaisons virtuelles). Pour afficher la page **Virtual Links** (Liaisons virtuelles), cliquez sur **Router** (Routeur)→ **OSPF**→ **Virtual Links** (Liaisons virtuelles) dans l'*arborescence*.

Figure 8-12. Page Liaisons virtuelles



Area ID (ID de zone) ID de la zone d'interface OSPF de la zone de transit.

Virtual Neighbor (Voisin virtuel) ID du routeur du voisin virtuel.

Virtual Neighbor State (État du voisin virtuel) État du voisin virtuel.

Hello Interval (1-65535) (Intervalle Hello (1-65535)) Durée (en secondes) entre les paquets Hello. Toutes les périphériques connectés à un réseau commun doivent avoir le même intervalle Hello. La valeur par défaut est 10 secondes.

Retransmit Interval (0-3600) (Intervalle de retransmission (1-3600)) Durée (en secondes) entre les retransmission des annonces d'état de liaison (LSA) pour les adjacences appartenant à l'interface. La valeur doit être supérieure au délai d'aller-retour attendu entre deux routeurs du réseau connecté. La valeur par défaut est 5 secondes.

Transmit Delay(0-3600) (Délai de transmission (1-3600)) Durée estimée (en secondes) nécessaire pour envoyer un paquet de mise à jour d'état de liaison sur l'interface. L'âge des LSA dans le paquet de mise à jour est incrémenté par ce nombre avant la transmission. La valeur par défaut est 1 seconde.

Dead Interval (0-2147483647) (Intervalle d'inactivité (0-2147483647)) Durée (en secondes) pendant laquelle les paquets Hello du routeur n'ont pas été détectés. Le routeur se met alors en état de pause. La valeur doit être un multiple de la valeur **Hello Interval** (Intervalle Hello). La valeur de ce paramètre doit être définie pour tous les routeurs connectés à un réseau commun. La valeur par défaut est 60 secondes.

Virtual Interface State (État de l'interface virtuelle) Indique l'état de l'interface virtuelle.

Authentication Mode (Mode d'authentification) Type d'authentification de l'interface, mot de passe ou MD5, utilisé pour authentifier les messages d'état de liaison OSPF.

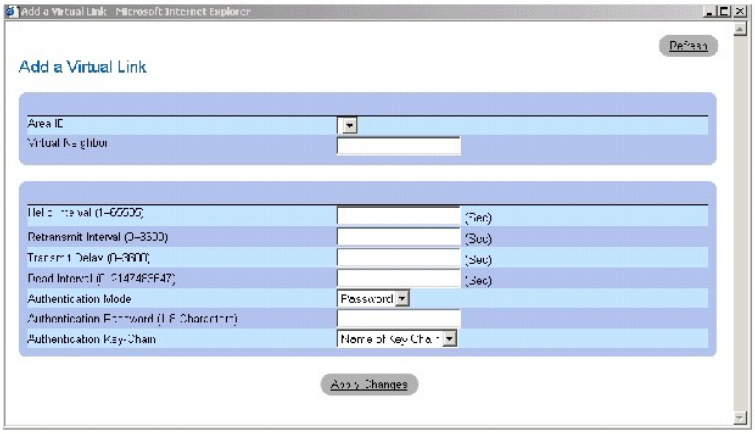
Authentication Password (1-8 Characters) (Mot de passe d'authentification (1-8 caractères)) Mot de passe (huit caractères maximum) utilisé pour authentifier les messages d'état de liaison OSPF.

Authentication Key-Chain (Chaîne de clés d'authentification) Chaîne de clés MD5 utilisée pour authentifier les messages d'état de liaison OSPF.

Ajout d'une liaison virtuelle

1. Ouvrez la page **Virtual Links** (Liaisons virtuelles).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add a Virtual Link** (Ajout d'une liaison virtuelle).

Figure 8-13. Page Ajout d'une liaison virtuelle



3. Renseignez les champs de cette page.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle liaison virtuelle OSPF est ajoutée.

Modification d'une liaison virtuelle

1. Ouvrez la page **Virtual Links** (Liaisons virtuelles).
2. Sélectionnez un ID de zone dans le menu déroulant **Area ID** (ID de zone).

Les paramètres de champ s'affichent.

3. Modifiez les champs comme vous le désirez.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres de la liaison virtuelle OSPF sont modifiés et enregistrés sur le périphérique.

Suppression d'une liaison virtuelle OSPF

1. Ouvrez la page **Virtual Links** (Liaisons virtuelles).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **Virtual Links Table** (Table des liaisons virtuelles).
3. Sélectionnez une liaison virtuelle.

Les paramètres de champ pour l'entrée de table sélectionnée s'affichent.

4. Cochez la case **Remove** (Supprimer).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La liaison virtuelle est supprimée et le périphérique est mis à jour.

Affichage des liaisons virtuelles OSPF à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour la définition des zones OSPF.

Tableau 8-10. Commandes CLI Liaison virtuelle OSPF

Commande CLI	Description
`show ip ospf virtual-links [area area-id] [router router- id]`	Affiche les paramètres et l'état actuel des liaisons virtuelles OSPF.
`router ospf area area-id virtual- link router-id`	Ajoute une liaison virtuelle.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# show ip ospf virtual-links

Virtual Link to router 192.168.101.2 is up

Virtual link has simple password authentication

Transit area 0.0.0.1

Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Retransmit 5

Adjacency State FULL

Console (config)# router ospf area 176.16.1.0 virtual-link 176.16.8.7

Console (config)# router ospf area 176.16.1.0 virtual-link 176.16.8.7
```

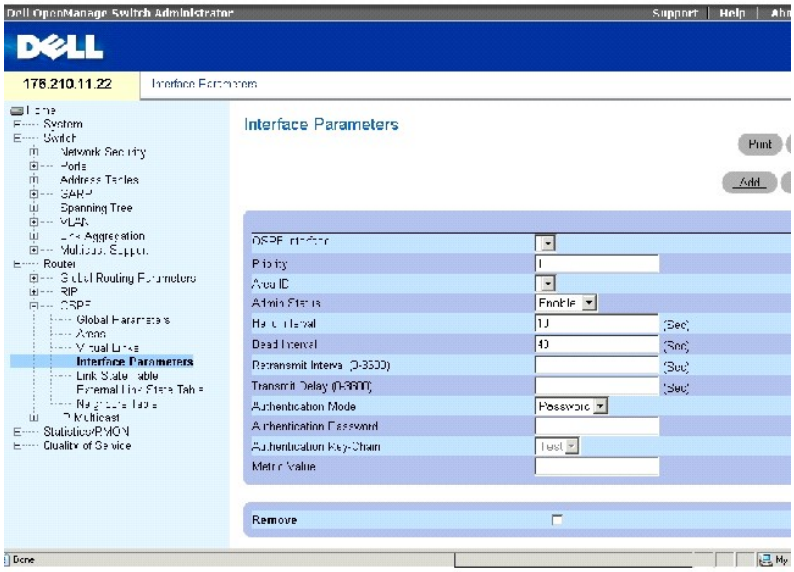
Configuration des paramètres d'interface OSPF

Une fois les paramètres globaux et les zones OSPF définis, vous pouvez configurer le protocole OSPF sur chaque interface.

La création automatique permet de configurer le protocole OSPF automatiquement sur chaque interface lorsqu'une zone a été définie. Les interfaces OSPF peuvent également être définies par l'utilisateur. La table des interfaces OSPF active le routage IP à l'aide des informations spécifiques au protocole OSPF.

Pour afficher la page **Interface Parameters** (Paramètres d'interface), cliquez sur **Router** (Routeur)→ **OSPF**→ **Interface Parameters** (Paramètres d'interface) dans l'*arborescence*.

Figure 8-14. Page Paramètres d'interface



OSPF Interface (Interface OSPF) Adresse IP de l'interface OSPF.

Priority (Priorité) Priorité de l'interface. La valeur 0 indique que le périphérique ne peut pas être défini comme périphérique désigné sur le réseau actuel. Si plusieurs périphériques ont la même priorité, l'ID de routeur ID est utilisé. Les valeurs possibles pour ce champ sont comprises entre 0 et 255. La valeur par défaut est 1.

Area ID (ID de zone) ID de la zone d'interface OSPF.

Admin Status (État admin) Active ou désactive le processus OSPF.

Hello Interval (Intervalle Hello) Intervalle en secondes entre les paquets Hello. Toutes les périphériques connectés à un réseau commun doivent avoir le même intervalle Hello. Les valeurs possibles pour ce champ sont comprises entre 1 et 65535. La valeur par défaut est 10 secondes.

Dead Interval (Intervalle d'inactivité Intervalle en secondes pendant lequel les paquets Hello du routeur n'ont pas été détectés. Le routeur se met alors en état de pause. La valeur doit être un multiple de la valeur **Hello Interval** (Intervalle Hello). La valeur de ce paramètre doit être définie pour tous les routeurs connectés à un réseau commun. Les valeurs possibles pour ce champ sont comprises entre 1 et 2147483647. La valeur par défaut est quatre fois la valeur **Hello Interval** (Intervalle Hello).

Retransmit Interval (0-3600) (Intervalle de retransmission (1-3600)) Intervalle (en secondes) entre les retransmissions des annonces d'état de liaison (LSA) pour les adjacences appartenant à l'interface. La valeur doit être supérieure au délai d'aller-retour attendu entre deux routeurs du réseau connecté. La valeur par défaut est 5 secondes.

Transmit Delay (0-3600) (Délai de transmission (1-3600)) Durée estimée (en secondes) nécessaire pour envoyer un paquet de mise à jour d'état de liaison sur l'interface. L'âge des LSA dans le paquet de mise à jour est incrémenté par ce nombre avant la transmission. La valeur par défaut est 1 seconde.

Authentication Mode (Mode d'authentification) Type d'authentification de l'interface, mot de passe ou MD5, utilisé pour authentifier les messages d'état de liaison OSPF.

Authentication Password (Mot de passe d'authentification) Mot de passe utilisé pour authentifier les messages d'état de liaison OSPF. La longueur maximale du mot de passe est de huit caractères.

Authentication Key-Chain (Chaîne de clés d'authentification) Chaîne de clés MD5 utilisée pour authentifier les messages d'état de liaison OSPF.

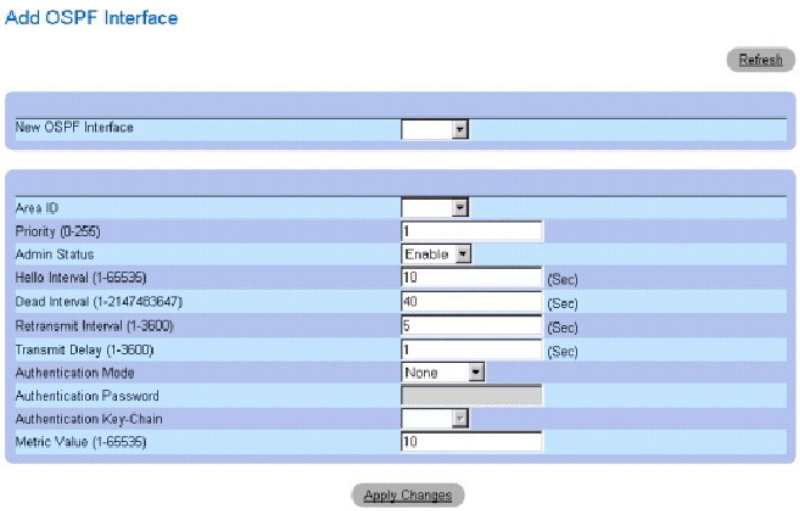
Metric Value (Valeur métrique) Métrique pour ce type de service sur l'interface. Les valeurs possibles pour ce champ sont comprises entre **1 et 65535.**

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime une interface OSPF.

Ajout d'une interface OSPF

1. Ouvrez la page **Interface Parameters** (Paramètres d'interface).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add OSPF Interface** (Ajout d'une interface OSPF).

Figure 8-15. Ajout d'une interface OSPF



3. Renseignez les champs de cette page.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle interface OSPF est ajoutée au périphérique.

Modification des paramètres OSPF

1. Ouvrez la page **Interface Parameters** (Paramètres d'interface).
2. Sélectionnez une interface OSPF pour afficher les paramètres de champ pour l'entrée de table.
3. Modifiez les paramètres comme vous le désirez.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres d'interface OSPF sont modifiés et enregistrés sur le périphérique.

Suppression d'une interface OSPF

1. Ouvrez la page **Interface Parameters** (Paramètres d'interface).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **OSPF Interface Table** (Table des interfaces OSPF).
3. Sélectionnez une interface OSPF.
4. Cochez la case **Remove** (Supprimer).

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

L'interface OSPF est supprimée.

Définition des interfaces OSPF à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour la définition des interfaces OSPF.

Tableau 8-11. Commandes CLI Interface OSPF

Commande CLI	Description
`ospf`	Crée un processus de routage OSPF sur une interface.
`ospf area area-id`	Définit un ID de zone d'interface.
`ospf enable`	Active le protocole OSPF sur une interface.
`ospf priority number- value`	Définit la priorité de routeur, utilisée pour l'élection du routeur désigné du réseau.
`ospf hello-interval seconds`	Définit l'intervalle entre les paquets hello que le logiciel envoie sur une interface.
`ospf dead-interval seconds`	Définit l'intervalle pendant lequel les paquets hello ne doivent pas être envoyés tant que les voisins n'ont pas déclaré le routeur inactif.
`ospf retransmit-interval seconds`	Définit l'intervalle entre les retransmissions des annonces d'état de liaison (LSA) pour les adjacences d'interfaces appartenant à l'interface.
`ospf transmit-delay seconds`	Définit une estimation de la durée nécessaire pour envoyer un paquet de mise à jour d'état de liaison sur une interface.
`ospf authentication {text text | md5 name-of-chain}`	Active l'authentification pour les paquets OSPF et définit le type d'authentification.
`clear ip ospf process [interface]`	Efface la redistribution basée sur le routage OSPF.
`show ip ospf interface [interface]`	Affiche des informations sur les interfaces OSPF.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface ip 1.100.100.100

Console (config-ip)# ospf

Console (config-ip)# ospf area 192.168.2.1

Console (config-ip)# ospf enable

Console (config-ip)# ospf priority 100
```

```
Console (config-ip)# ospf hello-interval 100

Console (config-ip)# ospf dead-interval 100

Console (config-ip)# ospf retransmit-interval 60

Console (config-if)# ospf retransmit-delay 60

Console (config-ip)# ospf authentication text abab

Console (config-ip)# ospf authentication md5 mychain

Console (config-ip)# exit

Console (config)# exit

Console# clear ip ospf process 192.168.3.1

Console# exit

Console# show ip ospf interface 192.168.1.1

IP interface 192.168.1.1/16 is up, OSPF is enabled

Area 0.0.0.0, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10

Interface has simple password authentication

Transmit Delay is 1 sec, State OTHER, Priority 1

Designated Router id 192.168.1.11, Interface address 192.168.1.11

Backup Designated router id 192.168.1.28, Interface addr 192.168.1.28

Timer intervals configured, Hello 10, Dead 60, Retransmit 5

Neighbor Count is 8, Adjacent neighbor count is 2

Adjacent with neighbor 192.168.1.28 (Backup Designated Router)
```

Affichage de la table des états de liaison

La page **OSPF Link State Table** (Table des états de liaison) contient des informations sur les annonces d'état de liaison pour les zones auxquelles le périphérique est connecté. Cliquez sur **Router** (Routeur)→ **OSPF**→ **Link State Table** (Table des états de liaison) dans l'*arborescence*.

Figure 8-16. Table des états de liaison OSPF

Area ID (ID de zone) ID de la zone.

Link Type (Type de liaison) Indique le type de liaison pour la zone.

Link ID (ID de liaison) Élément du domaine de routage décrit par l'annonce. Il s'agit soit d'un ID de routeur, soit d'une adresse IP.

Router ID (ID routeur) Routeur de départ dans le système autonome.

Sequence Number (Numéro de séquence) Numéro de séquence de la liaison. Le numéro de séquence détecte les anciennes annonces d'état de liaison et les annonces doubles. Plus le numéro de séquence est élevé, plus l'annonce est récente.

Age (Âge) Indique en secondes l'âge de l'annonce d'état de liaison.

Checksum (Somme de contrôle) Somme de contrôle du contenu complet de l'annonce, à l'exception de la valeur **Age** (Âge).

Affichage de la table des états de liaison OSPF à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage de la table des états de liaison OSPF.

Tableau 8-12. Commandes CLI État de liaison OSPF

Commande CLI	Description
`show ip OSPF [area-id] database`	Affiche des listes d'informations se rapportant à la base de données OSPF pour un routeur spécifique.

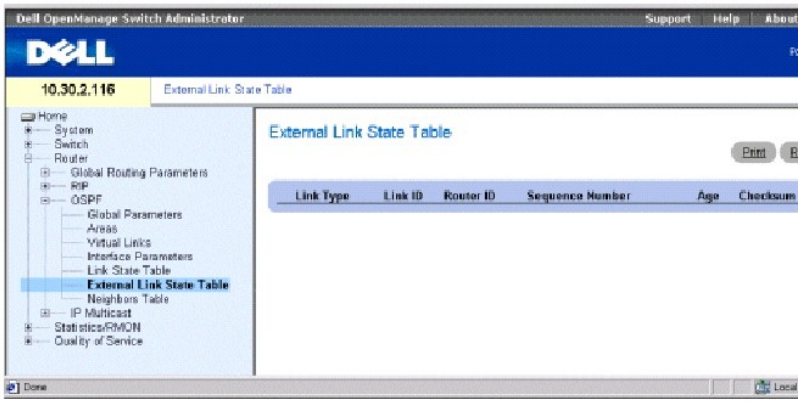
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console> show ip ospf database

OSPF Router with ID 200.1.1.11

Router Link States(Area 0)

Link ID     ADV Router    Age     Seq#         Checksum     Link count

200.1.1.8   200.1.1.8     1381    0x8000010D   0xEF60       2

200.1.1.11  200.1.1.11    1460    0x800002FE   0xEB3D       4

200.1.1.12  200.1.1.12    2027    0x80000090   0x875D       3

200.1.1.27  200.1.1.27    1323    0x800001D6   0x12CC       3



Net Link States(Area 0)

Link ID     ADV Router    Age     Seq#         Checksum

140.1.1.27  200.1.1.27    1323    0x8000005B   0xA8EE

141.1.1.11  200.1.1.11    1461    0x8000005B   0x7AC
```

Affichage de la table des états de liaison externe

La table des états de liaison externe contient des informations sur les annonces d'état de liaison externes. Les informations de la table des états de liaison externe sont apprises à partir de sources autres que les routes OSPF. Pour afficher la page External Link State Table (Table des états de liaison externe), cliquez sur **Router** (Routeur)→ **OSPF**→ **External Link State Table** (Table des états de liaison externe) dans l'*arborescence*.

Figure 8-17. Table des états de liaison externe



Link Type (Type de liaison) Type de liaison externe. Chaque annonce d'état de liaison a un format spécifique. La valeur de ce champ est toujours liaison externe.

Link ID (ID de liaison) Élément du domaine de routage décrit par l'annonce. Il s'agit soit d'un ID de routeur, soit d'une adresse IP.

Router ID (ID routeur) Routeur de départ dans le système autonome.

Sequence Number (Numéro de séquence) Numéro de séquence de la liaison externe. Le numéro de séquence détecte les anciennes annonces d'état de liaison et les annonces doubles. Plus le numéro de séquence est élevé, plus l'annonce est récente.

Age (Âge) Indique en secondes l'âge de l'annonce d'état de la liaison externe.

Checksum (Somme de contrôle) Somme de contrôle du contenu complet de l'annonce, à l'exception de la valeur **Age** (Âge).

Affichage de la table des routes externes OSPF à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage de la table des routes externes OSPF.

Tableau 8-13. Commandes CLI Table des routes externes OSPF

Commande CLI	Description
`show ip OSPF [area-id] database [external] [link- state-id]`	Répertorie la base de données OSPF pour un routeur spécifique.

Vous trouverez ci-dessous un exemple de commande CLI :

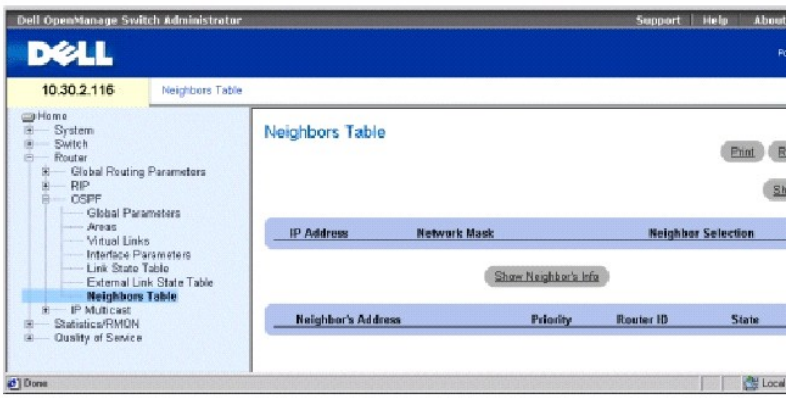
```
Console> show ip ospf database
```

Affichage de la table des voisins OSPF

La table des voisins OSPF décrit tous les voisins dans la localité du routeur objet. Pour ouvrir la page **Neighbor Table** (Table des voisins), cliquez sur **Router**

(Routeur)→ **OSPF**→ **Neighbors Table** (Table des voisins) dans l'*arborescence*.

Figure 8-18. Table des voisins



IP Address (Adresse IP) Adresse IP qu'utilise ce voisin dans son adresse IP source.

Network Mask (Masque de réseau) Masque de réseau de l'interface voisine.

Neighbor Selection (Sélection du voisin) Définit les informations du voisin du périphérique à afficher.

Neighbor's Address (Adresse du voisin) Adresse IP du voisin.

Priority (Priorité) Priorité du voisin.

Router ID (ID de routeur) ID du routeur du voisin.

State (État) État actuel du voisin.

Affichage de la liste des voisins

1. Ouvrez la page **OSPF Neighbors Table** (Table des voisins OSPF).
2. Dans la colonne **Neighbor Selection** (Sélection du voisin), cliquez sur le bouton d'option du voisin pour lequel vous souhaitez afficher des informations.
3. Cliquez sur **Show Neighbor's Info** (Afficher infos du voisin).

Les informations du voisin s'affichent en bas de la page.

Affichage de la table de tous les voisins

1. Ouvrez la page **Neighbors Table** (Table des voisins).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **All Neighbors Table** (Table de tous les voisins).

Affichage des informations des voisins OSPF à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage de la table des informations des voisins OSPF.

Tableau 8-14. Commandes CLI Voisin OSPF

Commande CLI	Description
`show ip ospf neighbor [`*`interface`*`]`	Affiche les informations des voisins OSPF pour chaque interface.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console> show ip ospf neighbor

ID            Pri  State         Address       IP interface

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

192.168.1.11  1    FULL          /DR           192.168.1.11 192.168.1.1

192.168.1.12  2    FULL          /DROTHER      192.168.1.12 192.168.1.1

192.168.2.11  1    FULL          /DR           192.16 8.2.11 192.168.2.1

192.168.2.12  2    FULL          /DROTHER      192.168.2.12 192.168.2.1

Console> show ip ospf neighbor 192.168.1.1

Neighbor 192.168.1.11, Address 192.168.1.11

In the area 0.0.0.0

Neighbor priority is 1, State is FULL

Options 2

Neighbor 192.168.1.12, Address 192.168.1.12

In the area 0.0.0.0

Neighbor priority is 2, State is FULL

Options 2
```

Configuration du routage de multidiffusion IP

Le routage de multidiffusion accroît les ressources réseau. Un hôte envoie des données à un groupe d'hôtes (plutôt qu'à un seul hôte) au sein du réseau IP à l'aide de l'adresse du groupe de multidiffusion IP. Le routage de multidiffusion IP est mis en oeuvre dans le PowerConnect 6024/6024F à l'aide des protocoles suivants :

- **Protocole des membres du groupe Internet (IGMP)** Fournit une méthode d'identification des clients intéressés par la réception de transmissions spécifiques.
- **Protocole de routage de multidiffusion à vecteur de distance (DVMRP)** Permet aux routeurs de définir une arborescence des transmissions et de copier les paquets dans l'arborescence de routage des transmissions.

Définition des paramètres globaux IPM

L'activation du routage de multidiffusion IP s'effectue dans la page **IPM Global Parameters** (Paramètres globaux IPM). Pour afficher la page **IPM Global Parameters** (Paramètres globaux IPM), cliquez sur **Router** (Routeur)→ **IP Multicast** (Multidiffusion IP)→ **Global Parameters** (Paramètres globaux) dans l'*arborescence*.

Figure 8-19. Paramètres globaux IPM

IP Multicast Status (État de la multidiffusion IP) Active ou désactive le routage IPM sur le périphérique.

Activation du routage IPM sur le périphérique

1. Ouvrez la page **IPM Global Parameters** (Paramètres globaux IPM).
2. Sélectionnez **Enable** (Activer) dans le champ **IPM Multicast Status** (État de la multidiffusion IPM).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le routage de multidiffusion IP est activé sur le périphérique.

Activation du routage de multidiffusion à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'activation du routage de multidiffusion.

Tableau 8-15. Commandes CLI Routage de multidiffusion

Commande CLI	Description
	Active le routage de multidiffusion IP.

`ip multicast- routing`	

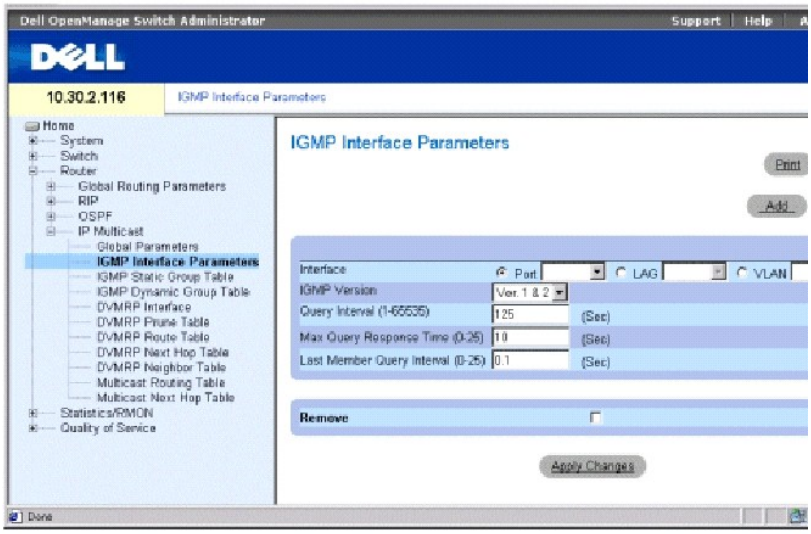
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# ip multicast-routing
```

Définition des paramètres d'interface IGMP

Le protocole d'appartenance à un groupe Internet (IGMP) définit des appartenance à un hôte au sein d'un groupe de multidiffusion. Le protocole IGMP permet aux hôtes d'informer les routeurs qu'ils peuvent recevoir des paquets de multidiffusion adressés à des groupes de multidiffusion spécifiques. Pour ouvrir la page **IGMP Interface Parameters** (Paramètres d'interface IGMP), cliquez sur **Router** (Routeur)→ **IP Multicast** (Multidiffusion IP)→ **IGMP Interface Parameters** (Paramètres d'interface IGMP) dans l'*arborescence*.

Figure 8-20. Paramètres d'interface IGMP



Interface Contient une liste d'adresses IP d'interfaces pour lesquelles le protocole IGMP a été activé.

IGMP Version (Version IGMP) Version logicielle actuelle du protocole IGMP. La valeur par défaut est **Ver. 1&2** (Vers. 1 et 2).

Query Interval (1-65535) (Intervalle de requête [1-65535]) Délai de transmission en secondes des messages de requête. Vous pouvez définir le nombre de messages IGMP envoyés sur les sous-réseaux en ajustant la valeur de l'intervalle de requête. Plus la valeur est élevée, moins le nombre de messages envoyés est important. La valeur par défaut est 125 secondes.

Max Query Response Time (0-25) (Délai de réponse maxi à une requête [0-25]) Délai de réponse maximum pour l'annonce de requêtes IGMP. Le délai de réponse ajuste la quantité de trafic sur chaque sous-réseau. La variation du délai de réponse affecte le taux de rafale du trafic réseau. Plus la valeur est élevée, plus la période entre les réponses de l'hôte est importante. La valeur par défaut est 10 secondes.

Last Member Query Interval (0-25) (Intervalle de requête de dernier membre [0-25]) Modifie la latence de disparition du réseau. Une valeur faible réduit la durée nécessaire pour détecter la perte du dernier membre du groupe. La valeur par défaut est 0.1 (0,1).

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime l'interface IGMP.

Ajout d'une interface IGMP

1. Ouvrez la page **IGMP Interface Parameters** (Paramètres d'interface IGMP).
2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add an IGMP Interface** (Ajout d'une interface IGMP).
3. Sélectionnez une interface dans le menu déroulant **New Interface** (Nouvelle interface).
4. Renseignez les champs de cette page.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

La nouvelle interface IGMP est ajoutée au périphérique.

Modification d'une interface IGMP

1. Ouvrez la page **IGMP Interface Parameters** (Paramètres d'interface IGMP).
2. Sélectionnez l'interface à modifier.
3. Modifiez les champs comme vous le désirez.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres d'interface IGMP sont modifiés et enregistrés sur le périphérique.

Suppression d'une interface IGMP

1. Ouvrez la page **IGMP Interface Parameters** (Paramètres d'interface IGMP).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la page **IGMP Interface Table** (Table des interfaces IGMP).
3. Sélectionnez une interface IGMP et cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'interface IGMP est supprimée.

Configuration des paramètres d'interface IGMP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour la configuration des paramètres d'interface IGMP.

Tableau 8-16. Commandes CLI Paramètres d'interface IGMP

Commande CLI	Description
`ip igmp`	Crée le protocole IGMP sur une interface.
`ip igmp query-interval` *`seconds`*	Définit la fréquence à laquelle le logiciel envoie des messages de requête hôte IGMP.
`ip igmp query-max-response- time` *`seconds`* `[`*`tenths-of- seconds`*`]`	Définit le délai de réponse maximum annoncé dans les requêtes IGMP.
`ip igmp last-member-query- interval` *`seconds`* `[`*`tenths-of- seconds`*`]`	Définit la fréquence à laquelle le routeur envoie des messages de requête hôte IGMP spécifiques à un groupe.
`show ip igmp interface [ethernet` *`interface-number`* `| vlan` *`vlan-id`* `|` *`port-channel number`*`]`	Affiche des informations IGMP sur une interface.

Vous trouverez ci-dessous un exemple de commande CLI :

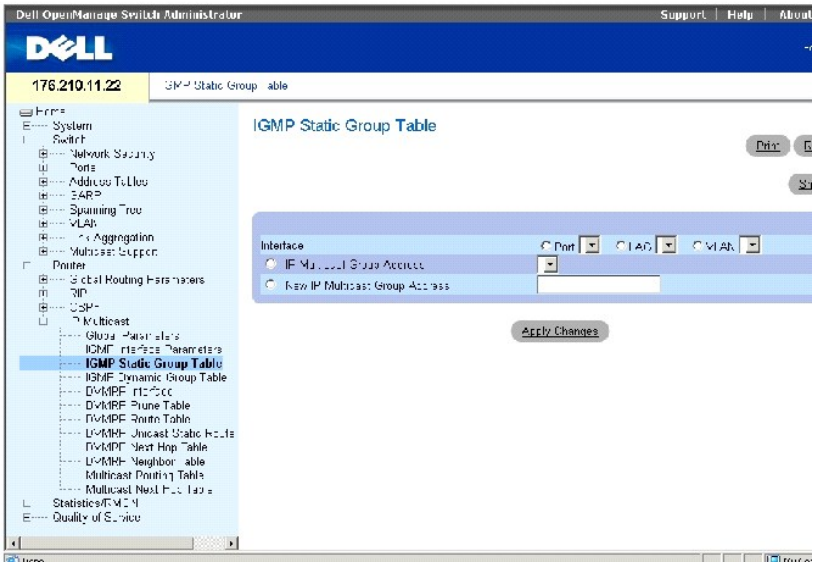
```
Console (config)# interface ethernet g1

Console (config-if)# ip igmp

Console (config-if)# ip igmp query-interval 60

Console (config-if)# ip igmp query-max-response-time 20

Console (config-if)# ip igmp last-member-query-interval 200

Console (config-if)# exit

Console (config)# exit

Console# disable

Console> show ip igmp interface

Interface  Version Query  Last     Max     Querier Interval     Member     response     router

           [sec]          [mSec]   [Sec]

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

eth g1     2              60       1000    10                   198.92.37.33

eth g2     60             1000     10                           198.92.36.131
```

Définition des groupes d'interfaces statiques IGMP

La table **IGMP Static Group Table** (Table des groupes d'interfaces statiques IGMP) permet une définition statique de groupes IGMP sur des interfaces spécifiques.

Pour ouvrir la page **IGMP Static Group Table** (Table des groupes statiques IGMP), cliquez sur **Router** (Routeur)→ **IP Multicast** (Multidiffusion IP)→ **IGMP Static Group Table** (Table des groupes statiques IGMP) dans l'*arborescence*.

Figure 8-21. Table des groupes statiques IGMP



Interface Définit le port, le VLAN ou le LAG auquel est affecté le groupe de multidiffusion spécifique.

IP Multicast Group Address (Adresse du groupe de multidiffusion IP) Adresse du groupe de multidiffusion IP affecté à une interface.

New IP Multicast Group Address (Nouvelle adresse du groupe de multidiffusion IP) Nouvelle adresse du groupe de multidiffusion IP affecté à une interface.

Affectation d'une interface à un groupe de multidiffusion

1. Ouvrez la page **IGMP Static Group Table** (Table des groupes statiques IGMP).
2. Sélectionnez une interface dans le champ **Interface**.
3. Sélectionnez une adresse IP dans le champ **Multicast Group Address** (Adresse du groupe de multidiffusion) ou définissez une nouvelle adresse dans le champ **New Multicast Group Address** (Nouvelle adresse du groupe de multidiffusion).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Affichage de la table des groupements d'interfaces statiques

1. Ouvrez la page **IGMP Static Group Table** (Table des groupes statiques IGMP).
2. Cliquez sur **Show All** (Afficher tout) pour afficher la table **Static Interface Grouping Table** (Table des groupements d'interfaces statiques).

Cette page contient les champs suivants :

- **Interface** Adresse du groupe de multidiffusion IP dont le port est membre.
- **IP Multicast Group** (Groupe de multidiffusion IP) Groupe de multidiffusion IP dont cette interface est membre.
- **Group Up Time** (Durée de fonctionnement du groupe) Indique en marques de graduation le temps passé depuis la création de l'entrée. Le format est heures/minutes/secondes.
- **Last Reporter** (Dernier correspondant) Dernier membre à rejoindre le groupe de multidiffusion IP. Si aucun membre n'a rejoint le groupe de multidiffusion, la valeur est 0.0.0.0.
- **Remove** (Supprimer) Lorsqu'elle est cochée, cette option supprime une interface IGMP.

Configuration des groupements d'interfaces statiques à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour le groupement d'interfaces statiques.

Tableau 8-17. Commandes CLI Groupement d'interfaces statiques

Commande CLI	Description
`ip igmp static- group group- address`	Configure le routeur comme étant un membre connecté statiquement du groupe spécifié sur l'interface.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface ethernet g5
```

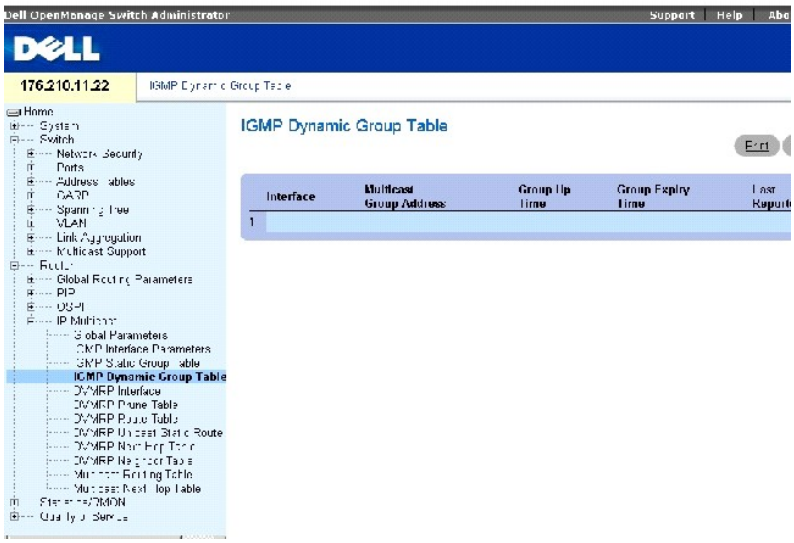
```
Console (config-if)# ip igmp static-group 192.168.4.1
```

Affichage de la table des groupes dynamiques IGMP

La page **IGMP Dynamic Group Table** (Table des groupes dynamiques IGMP) affiche des informations IGMP concernant chaque groupe de multidiffusion IP dont les membres ont été affectés dynamiquement à une interface sur un port physique.

Pour ouvrir la page **IGMP Dynamic Group Table** (Table des groupes dynamiques IGMP), cliquez sur **Router** (Routeur)→ **IP Multicast** (Multidiffusion IP)→ **IGMP Dynamic Group Table** (Table des groupes dynamiques IGMP) dans l'*arborescence*.

Figure 8-22. Table des groupes dynamiques IGMP



Interface Définit une interface appartenant au groupe de multidiffusion IP.

Multicast Group Address (Adresse du groupe de multidiffusion IP) Adresse IP de multidiffusion IGMP.

Group Up Time (Durée de fonctionnement du groupe) Indique en marques de graduation le temps passé depuis la création de l'entrée. Le format est heures/minutes/secondes.

Group Expiry Time (Délai d'expiration du groupe) Délai à partir duquel l'entrée dynamique arrive à expiration. Le format est heures/minutes/secondes.

Last Reporter (Dernier correspondant) Dernier membre à rejoindre le groupe de multidiffusion IP. Si aucun membre n'a rejoint le groupe de multidiffusion, la valeur est 0.0.0.0.

Affichage des groupes IGMP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage des groupes IGMP.

Tableau 8-18. Commandes CLI Groupe IGMP

Commande CLI	Description
`show ip igmp groups [group ip-address] [ethernet interface- number | vlan vlan-id | port-channel number]`	Affiche les groupes de multidiffusion ainsi que les récepteurs directement connectés au routeur et appris par le biais du protocole d'appartenance à un groupe Internet (IGMP).

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console> show ip igmp groups

Group Address   Interface  Uptime    Expires    Last Reporter

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

239.255.255.254  eth g1     1w0d     00:02:19   172.21.200.159

224.0.1.40       eth g3     1w0d     00:02:15   172.21.200.1

224.0.1.40       eth g3     1w0d     00:02:1    static

224.0.1.1        eth g1     1w0d     00:02:11   172.21.200.11

224.9.9.2        eth g1     1w0d     00:02:17   172.21.200.155

232.1.1.1        eth g1     5d21h    00:02:11   172.21.200.206
```

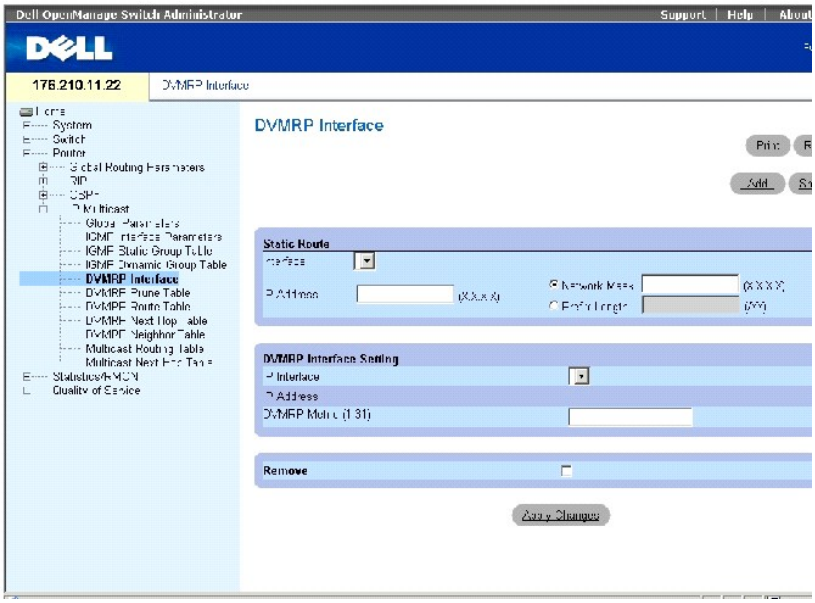
Configuration des interfaces DVMRP

Le protocole de routage de multidiffusion à vecteur de distance (DVMRP) utilise l'algorithme de multidiffusion de transmission selon les chemins inverses (RPF) pour créer des arborescences de multidiffusion basées sur la source. Le protocole DVMRP est un protocole de contrôle de l'algorithme RPF basé sur les informations de routage DVMRP. Les informations de routage sont recueillies pendant le routage des échanges.

La page **DVMRP Interface** (Interface DVMRP) contient des informations sur les configurations d'interface DVMRP.

Pour ouvrir la page **DVMRP Interface** (Interface DVMRP), cliquez sur **Router** (Routeur)→ **IP Multicast** (Multidiffusion IP)→ **DVMRP Interface** (Interface DVMRP) dans l'*arborescence*.

Figure 8-23. Interface DVMRP



La page **DVMRP Interface** (Interface DVMRP) contient les champs suivants classés sous deux rubriques :

STATIC ROUTE (ROUTE STATIQUE)

Interface Indique le numéro de l'interface sur laquelle le protocole DVMRP est activé.

IP Address (X.X.X.X) (Adresse IP [X.X.X.X]) Indique l'adresse IP source du port sur lequel le protocole DVMRP est activé.

Network Mask (X.X.X.X) (Masque de réseau [X.X.X.X]) Indique le masque de sous-réseau de l'adresse IP source.

(Prefix Length /XX) (Longueur du préfixe /XX) Indique le nombre de bits qui comprennent le préfixe IP source ou le masque de réseau de l'adresse IP source.

DVMRP INTERFACE SETTING (PARAMÈTRE D'INTERFACE DVMRP)

IP Interface (Interface IP) Indique le numéro de l'interface sur laquelle le protocole IP est activé.

IP Address (Adresse IP) Indique l'adresse IP source du port sur lequel le protocole DVMRP est activé.

DVMRP Metric (1-31) (Métrique DVMRP (1-31)) Indique la distance utilisée pour calculer le vecteur de distance. La métrique DVMRP est la distance d'interface entre le routeur à l'origine du rapport et le réseau source. La valeur par défaut est 1.

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime une interface DVMRP.

Ajout d'une nouvelle interface DVMRP

1. Ouvrez la page **DVMRP Interface** (Interface DVMRP).

2. Cliquez sur **Add** (Ajouter) pour afficher la page **Add a DVMRP Interface** (Ajout d'une interface DVMRP).
3. Renseignez le numéro d'interface et la métrique DVMRP.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'interface DVMRP est ajoutée à la **liste des interfaces IP** et le périphérique est mis à jour.

Modification d'une interface DVMRP

1. Ouvrez la page **DVMRP Interface** (Interface DVMRP).
2. Sélectionnez une interface dans la liste **IP Interface** (Interfaces IP).
3. Modifiez les champs comme vous le désirez.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'interface DVMRP sélectionnée est ajoutée à la **liste des interfaces DVMRP** et le périphérique est mis à jour.

Suppression d'une interface DVMRP

1. Ouvrez la page **DVMRP Interface** (Interface DVMRP).
2. Sélectionnez une interface dans la liste **IP Interface** (Interface IP).
3. Cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'interface DVMRP modifiée est supprimée de la **liste des interfaces IP** et le périphérique est mis à jour.

Configuration des interfaces DVMRP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour la configuration et l'affichage des interfaces DVMRP.

Tableau 8-19. Commandes CLI DVMRP

Commande CLI	Description
`ip dvmrp`	Active le protocole DVRMP sur une interface.
`no ip dvmrp`	Désactive le protocole DVRMP sur une interface.
`ip dvmrp metric` *`metric`*	Configure la métrique d'interface pour le protocole DVMRP. La métrique peut être comprise entre 1 et 31.
`no ip dvmrp metric`	Désactive la métrique d'interface pour le protocole DVMRP.
`show ip dvmrp interface [ethernet` *`interface-number`* `| vlan` *`vlan-id`* `| port-channel` *`number`*`]`	Affiche la table des interfaces.

Vous trouverez ci-dessous un exemple de commande CLI :

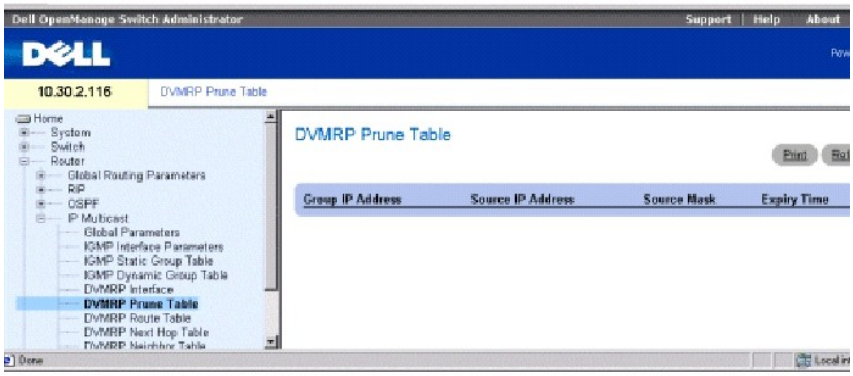
```
Console (config-if)# interface ethernet g5

Console (config-if)# ip dvmrp
```

```
Console (config-if)# ip dvmrp metric 15

Console (config-if)# exit

Console (config)# exit

Console> show ip dvmrp interface

Multicast routing enabled.

Multicast routing protocol is DVMRP.

Interface  IP address    Metric   RCV Bad  RCV Bad  Sent  Packets  Routes  Routes

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

eth g1     172.16.1.1    10       0        12
```

Table des élagages DVMRP

La page **DVMRP Prune Table** (Table des élagages DVMRP) répertorie l'état «prune» (élagage) en amont des routeurs. Pour ouvrir la page **DVMRP Prune Table** (Table des élagages DVMRP), cliquez sur **Router** (Routeur)→ **IP Multicast** (Multidiffusion IP)→ **DVMRP Prune Table** (Table des élagages DVMRP) dans l'*arborescence*.

Figure 8-24. Table des élagages DVMRP



Group IP Address (Adresse IP du groupe) Adresse IP du groupe d'élagage.

Source IP Address (Adresse IP source) Adresse IP source à élaguer.

Source Mask (Masque source) Masque IP source ayant été élagué.

Expiry Time (Délai d'expiration) Durée restante avant élagage du flux amont.

Affichage de la table d'élagage DVMRP à l'aide de commandes CLI

Le tableau suivant récapitule la commande CLI pour l'affichage de la table des élagages.

Tableau 8-20. Commandes CLI Table DVRMP

Commande CLI	Description
show ip dvmrp prune [group *group-address*] [*source- address*]	Affiche la table.

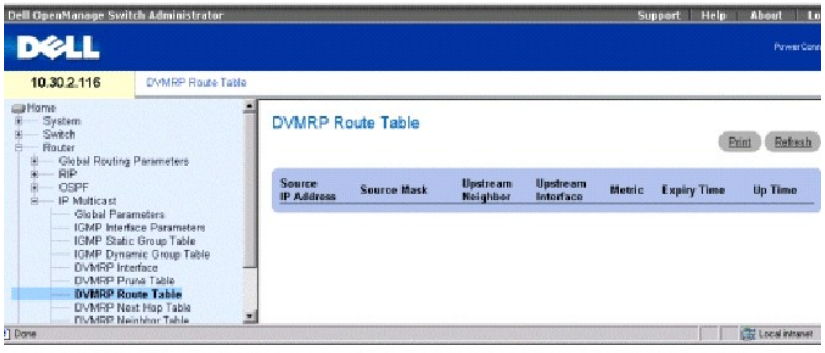
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console> show ip dvmrp prune

Group          Source         Expiry Time

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

224.192.78.88  171.68.0.0/16  00:02:52

224.192.78.89  171.68.0.0/16  00:08:52
```

Table des routes DVMRP

La page **DVMRP Route Table** (Table des routes DVMRP) contient des informations sur les routes apprises par les échanges du routeur DVMRP. Pour ouvrir la page **DVMRP Route Table** (Table des routes DVMRP), Cliquez sur **Router** (Routeur)→ **IP Multicast** (Multidiffusion IP)→ **DVMRP Route Table** (Table des routes DVMRP) dans l'*arborescence*.

Figure 8-25. Table des routes DVMRP



Source IP Address (Adresse IP source) Adresse IP de la source des informations de routage de multidiffusion.

Source Mask (Masque source) Masque de réseau de l'adresse IP source.

Upstream Neighbor (Voisin en amont) Adresse IP du voisin RPF en amont, à partir duquel les datagrammes IP sources sont reçus.

Upstream Interface (Interface en amont) Adresse IP de l'interface en amont.

Metric (Métrique) Distance en sauts jusqu'au sous-réseau source.

Expiry Time (Délai d'expiration) Délai à partir duquel l'entrée arrive à expiration.

Up Time (Durée de fonctionnement) Temps écoulé depuis l'apprentissage du routeur par le routeur.

Affichage de la table des routes DVMRP à l'aide de commandes CLI

Le tableau suivant récapitule la commande CLI pour l'affichage de la table des routes DVMRP.

Tableau 8-21. Commande CLI Table des routes DVRMP

Commande CLI	Description
`show ip dvmrp route [ip- address] [ip-address]`	Affiche la table des routes DVMRP.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console> show ip dvmrp route

Source          Neighbor        Interface       Metric       Expiry       Up Time       Time

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

171.68.0.0/16   192.168.1.2816  eth             g116         11016        100:02:5216   107:55:50
```

Table des prochains sauts DVMRP

La page **DVMRP Next Hop Table** (Table des prochains sauts DVMRP) contient des informations concernant le prochain saut d'interface de sortie pour les paquets de multidiffusion IP. Pour ouvrir la page **DVMRP Next Hop Table** (Table des prochains sauts DVMRP), cliquez sur **Router** (Routeur)→ **IP Multicast** (Multidiffusion IP)→ **DVMRP Next Hop Table** (Table des prochains sauts DVMRP) dans l'*arborescence*.

Figure 8-26. Table des prochains sauts DVMRP

Source IP Address (Adresse IP source) Adresse IP source pour le prochain saut d'une interface de sortie.

Source Mask (Masque source) Masque source pour le prochain saut d'une interface de sortie.

Downstream Interface (Interface en aval) Interface de sortie du prochain saut.

Type Définit le type du prochain saut. Ce champ peut prendre les valeurs suivantes :

Branch (Branche) Indique un autre saut après ce saut.

Leaf (Feuille) Indique qu'il s'agit du dernier saut de la route.

Affichage de la table des prochains sauts DVMRP à l'aide de commandes CLI

Le tableau suivant récapitule la commande CLI pour l'affichage de la table des prochains sauts DVMRP.

Tableau 8-22. Commandes CLI Table des prochains sauts DVMRP

Commande CLI	Description
show ip dvmrp next-hop [ethernet *interface-number* | vlan *vlan-id* | port-channel *number*]	Affiche la table des prochains sauts DVMRP.

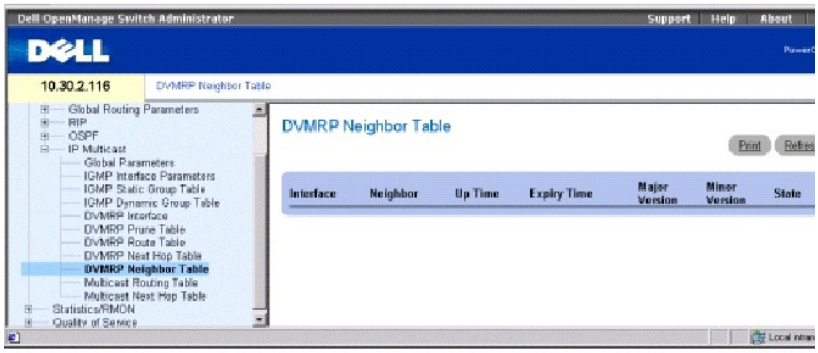
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console> show ip dvmrp next-hop

Source           Interface    Hop Type

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

198.92.37.100/32  eth g2       Leaf
```

Table des voisins DVMRP

La page **DVMRP Neighbor Table** (Table des voisins DVMRP) contient des informations sur les interfaces de port voisines. Les voisins DVMRP sont identifiés par les messages DVMRP. Pour ouvrir la page **DVMRP Neighbor Table** (Table des voisins DVMRP), cliquez sur **Router** (Routeur)→ **IP Multicast** (Multidiffusion IP)→ **DVMRP Neighbor Table** (Table des voisins DVMRP) dans l'*arborescence*.

Figure 8-27. Table des voisins DVMRP



Interface Numéro de l'interface sur laquelle le protocole DVMRP est activé.

Neighbor (Voisin) Adresse IP de l'interface voisine.

Up Time (Durée de fonctionnement) Temps écoulé depuis que l'interface voisine est devenue un voisin.

Expiry Time (Délai d'expiration) Indique la durée maximale avant expiration de l'interface.

Major Version (Version majeure) Numéro de version majeure du routeur voisin.

Minor Version (Version mineure) Numéro de version mineure du routeur voisin.

State (État) État du périphérique voisin.

Affichage de la table des voisins DVMRP à l'aide de commandes CLI

Le tableau suivant récapitule la commande CLI pour l'affichage de la table des voisins DVMRP.

Tableau 8-23. Commandes CLI Table des voisins DVMRP

Commande CLI	Description
`show ip dvmrp neighbor [ethernet` *`interface-number`* `| vlan` *`vlan-id`* `| port-channel` *`number`*`]`	Affiche la table des voisins DVMRP.

Vous trouverez ci-dessous un exemple de commande CLI :

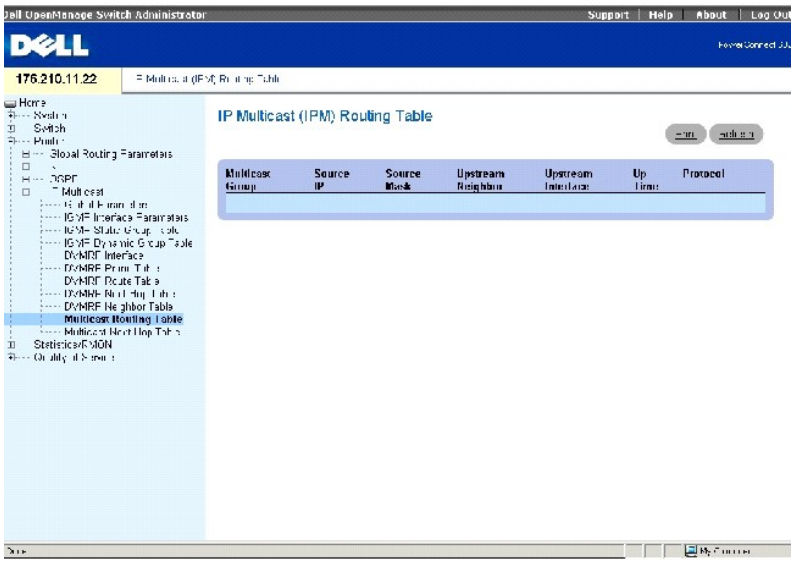
```
Console> show ip dvmrp neighbor ethernet g1

Interface  Neighbor      Up   Expiry            Version  Capabilities  RCV   Bad  State  Time  Time  Routes  Routes

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

eth g1     192.168.1.28  2    0:20:00 0:02:55   3.255    L,P,G,M       11    0    Active

eth g1     192.168.1.10  2    0:20:00 0:02:55   3.255    L,P,G,M       18    0    Active

eth g2     192.168.1.28  2    0:20:00 0:02:55   3.255    L,P,G,M       11    0    Active

eth g2     192.168.1.89  2    0:20:00 0:02:55   3.255    L,P,G,M       18    0    Active
```

Affichage de la table des routages de multidiffusion IP

La table **IP Multicast (IPM) Routing Table** (Table des routages de multidiffusion IP [IPM]) contient les informations de routage de multidiffusion des paquets IP envoyés à partir d'une source spécifique aux groupes de multidiffusion IP connus du routeur de multidiffusion IP.

Pour ouvrir la table **IP Multicast (IPM) Routing Table** (Table des routages de multidiffusion IP [IPM]), cliquez sur **Router** (Routeur)→ **IP Multicast** (Multidiffusion IP)→ **Multicast Routing Table** (Table des routages de multidiffusion) dans l'*arborescence*.

Figure 8-28. Table des routages de multidiffusion IP (IPM)



La table **IP Multicast (IPM) Routing Table** (Table des routages de multidiffusion IP [IPM]) contient les champs suivants :

Multicast Group (Groupe de multidiffusion) Adresse IP du groupe de multidiffusion.

Source IP (IP source) Adresse IP source du périphérique auquel les informations de multidiffusion s'appliquent.

Source Mask (Masque source) Masque tout ou une partie de l'adresse IP source.

Upstream Neighbor (Voisin en amont) Adresse IP du prochain périphérique en amont à partir duquel les paquets envoyés à l'adresse IP sont reçus.

Upstream Interface (Interface en amont) Numéro du port sur lequel les paquets de multidiffusion envoyés sont reçus.

Up Time (Durée de fonctionnement) Indique le temps écoulé depuis l'apprentissage des informations de multidiffusion par le routeur.

Protocol (Protocole) Identifie le type de protocole utilisé pour l'apprentissage des informations de multidiffusion. Pour ce projet, la seule valeur possible est **DVMRP**. Elle indique que le protocole de routage de multidiffusion à vecteur de distance a été utilisé pour l'apprentissage des informations de multidiffusion.

Affichage de la table des routages de multidiffusion IP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage de la table des routages de multidiffusion IP.

Tableau 8-24. Commandes CLI Table des routages de multidiffusion IP

Commande CLI	Description
show ip mroute [group *group-address*] [source *source-address*] [ethernet *interface-number* | *vlan vlan-id* | *port-channel number*]	Affiche le contenu de la table des routages de multidiffusion IP.

Vous trouverez ci-dessous un exemple de commande CLI :

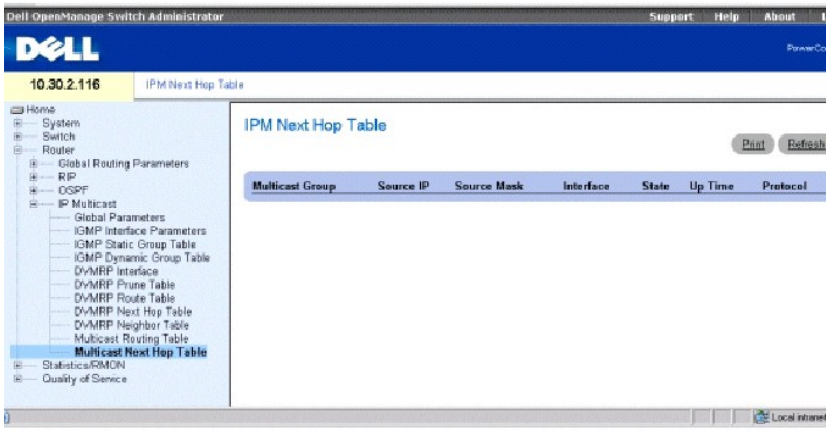
```
Console> show ip mroute

Group        Source           Upstream     Interface  Up Time    Expiry Time  Owner

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

224.0.255.1  198.92.37.100/32  10.20.37.33  eth g1     20:20:00   0:02:55      dvmrp

224.0.255.1  199.92.37.100/32  10.20.37.33  eth g1     1d:4h:20m  0:02:55      dvmrp

224.1.255.1  198.92.37.100/32  10.20.37.33  eth g1     21:20:00   0:02:55      dvmrp

224.1.255.1  199.92.37.100/32  10.20.37.33  eth g1     1d:5h:20m  0:02:55      dvmrp

224.8.255.1  179.82.17.200/32  10.20.37.33  vlan 127   1w:1d:2h   0:02:55      dvmrp

224.8.255.1  179.82.17.200/32  10.20.37.33  vlan 128   3m:2w:2d   0:02:55      dvmrp
```

```
224.8.255.1   179.82.17.200/32  10.20.37.33  vlan 129   1y:2m:2w   0:02:55      dvmrp

224.9.255.1   179.82.17.200/32  10.20.37.33  p-c 7      1d:5h:20m 0:02:55      dvmrp
```

Affichage de la table des prochains sauts de multidiffusion IP

La page **IPM Next Hop Table** (Table des prochains sauts IPM) contient des informations sur les prochains sauts de multidiffusion. Pour ouvrir la page, cliquez sur **Router** (Routeur)→ **IP Multicast** (Multidiffusion IP)→ **Multicast Next Hop Table** (Table des prochains sauts de multidiffusion).

Figure 8-29. Table des prochains sauts IPM



Multicast Group (Groupe de multidiffusion) Adresse IP du groupe de multidiffusion.

Source IP (IP source) Adresse IP source du périphérique auquel les informations de multidiffusion s'appliquent.

Source Mask (Masque source) Masque tout ou une partie de l'adresse IP source.

Interface Numéro du port sur lequel les paquets de multidiffusion envoyés sont reçus.

State (État) Indique si le port et le prochain saut sont actuellement utilisés pour la transmission des paquets de multidiffusion. Ce champ peut prendre les valeurs suivantes :

Pruned (Élagué) Le port et le prochain saut ne sont pas actuellement utilisés pour la transmission des paquets de multidiffusion.

Forwarding (Transmission) Le port et le prochain saut sont actuellement utilisés pour la transmission des paquets de multidiffusion.

Up Time (Durée de fonctionnement) Temps écoulé depuis l'apprentissage des informations de multidiffusion par le routeur.

Protocol (Protocole) Type de protocole utilisé pour l'apprentissage des informations de multidiffusion. Pour ce produit, la seule valeur possible est **DVMRP**. Elle indique que le protocole de routage de multidiffusion à vecteur de distance a été utilisé pour l'apprentissage des informations de multidiffusion.

Affichage de la table des prochains sauts IPM à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage de la table des prochains sauts de multidiffusion IP.

Tableau 8-25. Commandes CLI Prochain saut IPM

Commande CLI	Description
`show ip mroute-next-hop [group group-address] [source source-address]`	Affiche le contenu de la table des prochains sauts de multidiffusion IP.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console> show ip mroute-next-hop


Group        Source           Interface   Up Time   Expiry Time  State    Owner

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

224.0.255.1  198.92.37.100/32  eth g2 2     0:20:00  0:02:55      Forward  igmp

224.0.255.1  199.92.37.100/32  eth g2 1     :4d:20m  0:02:55      Forward  igmp

224.1.255.1  198.92.37.100/32  eth g2 2     1:20:00  0:02:55      Forward  dvmrp

224.1.255.1  199.92.37.100/32  eth g2 1     :4d:20m  0:02:55      Forward  dvmrp
```

Retour à la page du sommaire

Retour à la page du sommaire

Configuration de la qualité de service

Systèmes Dell PowerConnect 6024/6024F

La page **Quality of Service** (Qualité de service) contient des liens vers les principales pages de configuration de la fonction QdS (Qualité de Service). Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service) dans l'*arborescence*.

Présentation de la qualité de service

Dans un réseau, le trafic est généralement imprévisible et la seule garantie que peut offrir l'administrateur réseau est une distribution du trafic «au mieux». Pour relever ce défi, les administrateurs réseau appliquent une Qualité de Service (QdS) sur l'ensemble du réseau. Cette fonction permet de rendre prioritaire le trafic du réseau en fonction de certains critères et d'accorder au trafic spécifique un traitement préférentiel. La QdS optimise les performances du réseau et comporte deux fonctions de base :

- La classification du trafic entrant en classes de gestion, en fonction d'un attribut, qui peut être :
  - L'interface d'entrée
  - Le contenu du paquet
  - Une combinaison de ces deux attributs
- La fourniture de mécanismes permettant d'affecter des ressources réseau à différentes classes de gestion :
  - Affectation de trafic à une file d'attente matérielle particulière
  - Affectation de ressources internes
  - Mise en forme du trafic

Dans ce document, les termes Classe de service (CdS) et Qualité de service (QdS) sont utilisés dans le contexte suivant :

- CdS fournit différents services de trafic de couche 2. CdS se réfère à la classification du trafic en classes de trafic gérées en tant qu'agrégat, sans paramètres par flux. La fonction CdS est habituellement liée au service 802.1p qui permet de classer les flux en fonction de leur priorité de couche 2, comme dans l'en-tête du VLAN.
- QdS se réfère au trafic de couches 2 et supérieures. QdS permet de gérer les paramètres par flux, y compris à l'intérieur d'une classe de trafic unique.

La fonction QdS comprend les éléments suivants :

- **Access Control Lists (ACLs)** (Listes de contrôle d'accès (ACL)) Utilisées pour choisir le trafic qui sera autorisé à entrer dans le système et celui qui sera ignoré. Seul le trafic répondant à ce critère sera soumis au paramétrage de CdS ou QdS. Les ACL sont utilisées pour la fonction QdS et la sécurité du réseau.
- **Traffic Classification** (Classification du trafic) Classe chaque paquet entrant dans une classe de trafic, déterminée en fonction du contenu et/ou du contexte du paquet.
- **Assignment to Hardware Queues** (Affectation à des files d'attente matérielles) Affecte les paquets entrants à des files d'attente de transmission. Les paquets sont envoyés dans une file d'attente déterminée par la classe de trafic à laquelle ils appartiennent, tel que défini par le mécanisme de classification.
- Traffic Class-Handling Attributes (Attributs de gestion en fonction de la classe de trafic) Applique les mécanisme QdS/CdS à différentes classes, incluant :
  - La gestion de la bande passante
  - La mise en forme du trafic
  - Le contrôle du trafic

Les listes de contrôle d'accès

Les ACL inspectent les paquets entrants et les classent en groupes logiques, en fonction de différents critères. Les groupes d'ACL peuvent effectuer certaines actions sur chaque paquet du groupe. Les actions activées par les ACL sont les suivantes :

- Transmettre
- Refuser
- Refuser et désactiver le port

Les fonctions principales des ACL sont les suivantes :

- En tant que mécanisme de sécurité, elles autorisent ou refusent l'accès aux paquets d'un groupe. Ce mécanisme est décrit dans la section sur la sécurité du réseau.
- En tant que mécanisme de classification des paquets dans des classes de trafic pour lesquelles différentes actions de gestion de CdS/QdS sont réalisées.

Les ACL contiennent plusieurs règles et actions de classification. Un élément de contrôle d'accès (ACE) est composé d'une seule règle de classification et de son action correspondante. Une seule ACL peut contenir plusieurs ACE.

L'ordre des ACE à l'intérieur d'une ACL est important, car ils sont appliqués selon la méthode dite de la première convenance (first-fit). Les ACE sont traités de façon séquentielle en commençant par le premier. Lorsqu'un paquet correspond à une classification ACE, l'action ACE est effectuée et le traitement de l'ACL s'arrête. Si plusieurs ACL doivent être traitées, l'action de rejet par défaut s'applique uniquement une fois que le traitement de toutes les ACL est terminé. L'action de rejet par défaut requiert que l'utilisateur autorise de façon explicite l'ensemble du trafic, y compris le trafic de gestion tel que Telnet, HTTP ou SNMP, destiné au routeur.

Il existe deux types d'ACL :

- **IP ACL** (ACL IP) S'applique uniquement aux paquets IP. Tous les champs de classification sont liés aux paquets IP.
- **MAC ACL** (ACL MAC) S'applique à tous les paquets, y compris aux paquets non IP. Les champs de classification se basent uniquement sur L2.

Il existe deux façons d'appliquer les ACL à une interface :

- **Policy** (Réglementation) De cette façon, les ACL sont regroupées en une structure plus complexe appelée réglementation. La réglementation peut à la fois contenir des règles ACL et des règles QdS. L'utilisateur peut appliquer la réglementation à une interface (reportez-vous à la section «Mode avancé de la qualité de service»).
- **Simple** Dans sa forme simple, une ACL (MAC ou IP) est appliquée à une interface. Même lorsqu'une réglementation ne peut pas être appliquée à une interface, il est possible de lui imposer des règles QdS de base pour classer les paquets dans des files d'attente de sortie (reportez-vous à la section «Mode de base de qualité de service»).

Adressage aux files d'attente

Vous pouvez sélectionner un comportement Trust (Confiance) ou bien renseigner les champs du service de sortie :

- **VLAN Priority Tags (VPT)** (Marques de priorité VLAN (VPT)) Les VPT sont adressées à des files d'attente en fonction de leur valeur. L'adressage aux files d'attente peut être configuré par l'utilisateur, alors que l'adressage par défaut de la VPT à la file d'attente de sortie se fait de la façon suivante. Lors de l'adressage par défaut de la VPT, la file d'attente 1 possède la priorité la plus basse, comme illustré dans le tableau suivant :

Tableau 10-1. Table d'adressage par défaut de la VPT

Valeur VPT	Numéro de file d'attente
0	3
1	1
2	2
3	4
4	5
5	6
6	7
7	8

REMARQUE : L'adressage de la VPT aux files d'attente de sortie est réalisé au niveau du système et peut être activé (enabled) ou désactivé (disabled) sur chaque port.

- **802.1p Port-Based** (802.1p en fonction du port) Les paquets qui arrivent non marqués sont affectés à une VPT par défaut qui peut être configurée par l'utilisateur sur chaque port. Une fois la VPT affectée, le paquet est traité comme s'il était arrivé avec cette marque. L'adressage de la VPT à la file d'attente de sortie se fait en fonction des définitions 802.1p configurées par le même utilisateur.
- **Layer 3 Predefined Field** (Champ prédéfini L3) L'utilisateur peut configurer le système de manière à pouvoir utiliser le DSCP IP du paquet entrant

vers les files d'attente de priorité de sortie. L'adressage du DSCP IP à une file d'attente de priorité se fait au niveau du système. Si ce mode est activé, un paquet non IP sera toujours classé dans la file d'attente en mode «au mieux». L'adressage par défaut est illustré dans le tableau ci-après :

Tableau 10-2. Table d'adressage par défaut du DSCP

Valeur DSCP	Numéro de file d'attente
0-7	q1 (priorité la plus faible)
8-15	q2
16-23	q3
24-31	q4
32-39	q5
40-47	q6
48-55	q7
55-63	q8 (priorité la plus élevée)

REMARQUE : Les valeurs DSCP 3, 11, 19, 27, 35, 43, 51 et 59 sont adressées à q1, q2 ... q8. Ces paramètres ne peuvent pas être modifiés.

- **Layer 4 Predefined Fields** (Champs prédéfinis L4) Configure le système pour qu'il utilise le port de destination TCP/UDP du paquet entrant pour adresser le paquet aux files d'attente de priorité de sortie. L'adressage du port de destination TCP/UDP à une file d'attente de priorité se fait au niveau du système, dans deux tables séparées. Il peut être activé (enabled) ou désactivé (disabled) sur chaque port.
- **None** (Aucun) Tout le trafic est classé dans le service «au mieux».

Une fois les paquets affectés à une file d'attente spécifique, des services peuvent y être affectés en fonction de la méthode de classification choisie. Vous pouvez configurer les files d'attente de sortie avec un schéma de planification, en suivant l'une des méthodes suivantes :

- Priorité stricte.
- WRR (pondération WRR)
- Une combinaison de ces deux méthodes.

Les schémas de planification sont définis par système. Les pondérations WRR des files d'attente peuvent être affectées dans n'importe quel ordre. Les paramètres de pondération sont disponibles sur chaque port.

Pour chaque interface ou file d'attente, la mise en forme de sortie suivante peut également être configurée :

- Taille des rafales.
- Débit minimum garanti (CIR).
- Actions sur le trafic hors-limites.

Modes QdS

La fonction QdS est activée pour le PowerConnect 6024/6024F en mode de base ou en mode avancé.

mode QdS de base

En mode QdS de base, vous pouvez activer l'un des modes Trust (Confiance) suivants :

- VPT
- DSCP
- TCP
- UDP
- Aucun

De plus, une ACL MAC ou IP simple peut être directement rattachée à l'interface (reportez-vous à la section Configuration de la sécurité du réseau pour plus d'informations). Seuls les paquets possédant une action **Forward** (Transmettre) sont affectés à la file d'attente de sortie, en fonction de la classification appliquée.

En configurant correctement les files d'attente de sortie, vous pouvez paramétrer les services suivants pour le mode de base :

- **Minimum Delay** (Attente minimale) La file d'attente est affecté à un contrat de priorité stricte et le trafic est affecté à la file d'attente ayant la priorité la plus élevée.
- **Best Effort** (Au mieux) Le trafic est affecté à la file d'attente de priorité la plus faible
- **Bandwidth Assignments** (Affectations de bande passante) En configurant le schéma de planification WRR et en choisissant les pondérances appropriées, vous pouvez affecter des bandes passantes.

mode QdS avancé

Le mode QdS avancé fournit des règles de classification du flux et d'affectation d'actions relatives à la gestion de la bande passante. Ces règles sont définies dans des listes de contrôle de classification (CCL).

Les CCL sont configurées en fonction de la classification définie dans l'ACL et ne peuvent l'être que si une ACL valide a été définie. Une fois les CCL définies, les ACL et les CCL peuvent être regroupées dans une structure plus complexe appelée «réglementation». Les réglementations peuvent être appliquées à une interface. Les ACL/CCL, regroupées dans une réglementation, sont appliquées selon leur ordre d'apparition. Une seule réglementation peut être associée à un port.

En mode QdS avancé, les ACL peuvent être directement appliquées à une interface. Toutefois, vous ne pouvez pas appliquer en même temps une réglementation et une ACL à une interface.

Une fois les paquets affectés à une file d'attente spécifique, vous pouvez y appliquer des services comme la configuration des files d'attente de sortie pour le schéma de planification ou la configuration de la mise en forme de sortie pour la taille des rafales, le CIR ou le CBS par interface ou par file d'attente.

Configuration des Services - Exemples

Vous pouvez utiliser des paramètres du mode QdS avancé pour appliquer au trafic les services ci-après :

- **Best Effort** (Au mieux) Le trafic est affecté à la file d'attente de priorité la plus faible.
- **802.1p** La valeur VPT est configurée en fonction de la classification.
- **IP DSCP** (DSCP IP) La valeur est configurée en fonction de la classification.
- **Minimum Delay** (Attente minimale) La file d'attente est affectée à un contrat de priorité stricte et le trafic est affecté à la file d'attente ayant la priorité la plus élevée.
- **Ingress Metering/Rate Limiting** (Comptage en entrée/Limitation du débit) Une bande passante maximale est définie, au-delà de laquelle le trafic est ignoré. Ce paramètre est défini en configurant un compteur à l'entrée pour la bande passante maximale et en paramétrant une réglementation de refus en cas de dépassement. Pour que ce service reste efficace, la bande passante totale du port de sortie ne doit pas dépasser le débit du port.

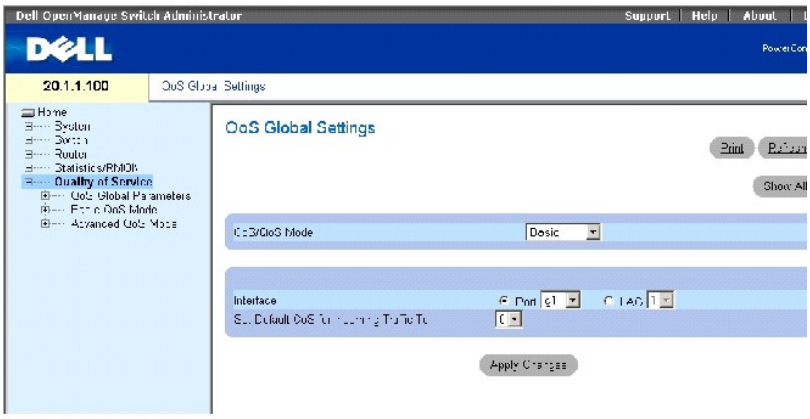
Configuration des paramètres globaux de la qualité de service

La page **QoS Global Parameters** (Paramètres globaux de QdS) contient des liens vers des pages permettant d'activer la fonction QdS, d'adresser les valeurs et les paramètres DSCP, de mettre en file d'attente le trafic du réseau et de définir la classification du trafic. Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service)→ **QoS Global Parameters** (Paramètres globaux de QdS) dans l'*arborescence*.

Définition des paramètres de la qualité de service

La page **QoS Global Settings** (Paramètres globaux de QdS) permet de sélectionner un mode QdS et de configurer la CdS par défaut du trafic entrant sur une interface sélectionnée.Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service)→ **QoS Global Parameters** (Paramètres globaux de QdS)→ **QoS Settings** (Paramètres QdS) dans l'*arborescence*.

Figure 10-1. Page Paramètres globaux QdS



QoS Mode (Mode QdS) Désactive ou active le mode QdS de base ou avancé. Le mode de base est activé par défaut.

REMARQUE : Lorsque vous passez du mode QdS de base au mode QdS avancé et inversement, certains paramètres peuvent être perdus.

Interface Port ou LAG pour lequel la réglementation CdS par défaut est définie.

Set Default CoS for Incoming Traffic To (Définir la valeur CdS par défaut pour le trafic entrant) Détermine la valeur CdS par défaut des paquets entrants sans marque VLAN. Les valeurs possibles pour ce champ sont comprises **entre 0 et 7**. La valeur CdS par défaut est **0**.

Sélection d'un mode de service

1. Ouvrez la page **QoS Settings** (Paramètres QdS).
2. Sélectionnez un mode de service dans le champ **QoS Mode** (Mode QdS).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mode QdS est sélectionné et le périphérique est mis à jour.

Définition de la valeur CdS par défaut pour le trafic entrant sur une interface

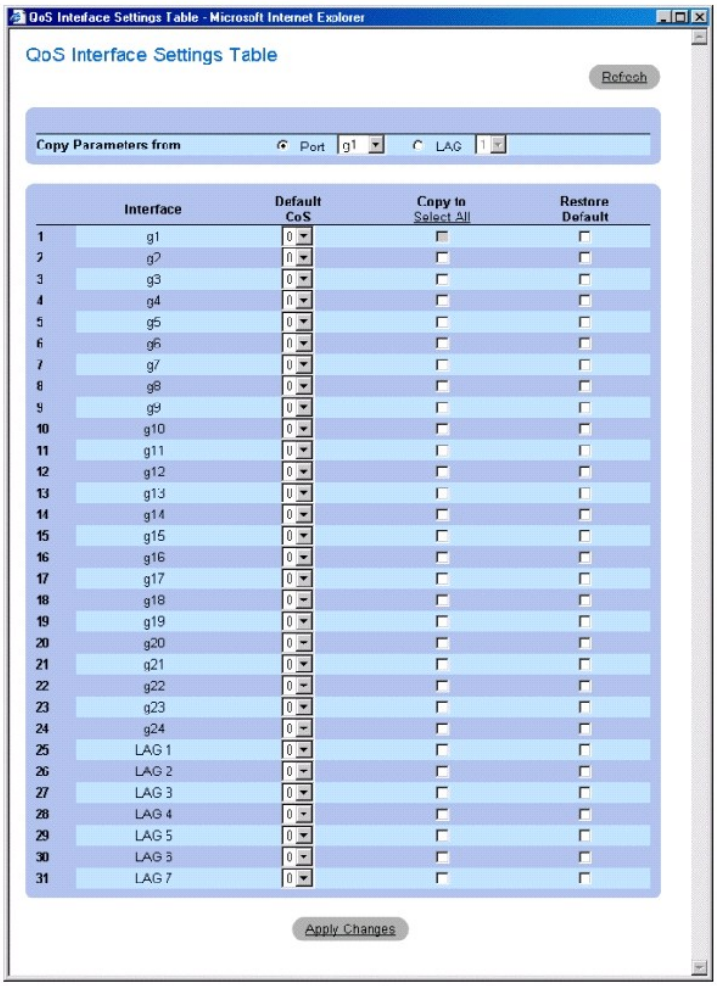
1. Ouvrez la page **QoS Settings** (Paramètres QdS).
2. Sélectionnez une interface et choisissez une valeur CdS par défaut pour le trafic entrant dans le menu déroulant.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La valeur CdS par défaut pour le trafic entrant sur l'interface est sélectionnée et le périphérique est mis à jour.

Copie des paramètres de l'interface CdS

1. Ouvrez la page **QoS Settings** (Paramètres QdS).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **QoS Interface Settings Table** (Table des paramètres d'interface QdS).
3. Sélectionnez l'interface où se trouvent les paramètres QdS à copier vers une autre interface parmi celles listées dans la table des paramètres d'interface QdS.
4. Cochez la case **Copy to** (Copier vers) de chaque interface où seront copiés les paramètres QdS ou bien cliquez sur **Select All** (Tout sélectionner) pour copier les paramètres QdS dans toutes les interfaces listées.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Figure 10-2. Page Table des paramètres d'interface QdS



Définition des paramètres QdS à l'aide de commandes CLI

Tableau 10-3. Commandes CLI Définition des paramètres QdS

Commande CLI	Description
qos [*advanced*]	Active/désactive la fonction QdS en mode de base/avancé sur tout le périphérique.
show qos	Affiche le mode QdS pour tout le périphérique.
qos cos default- cos	Configure la valeur CdS par défaut de l'interface.

Vous trouverez ci-dessous un exemple de commande CLI :

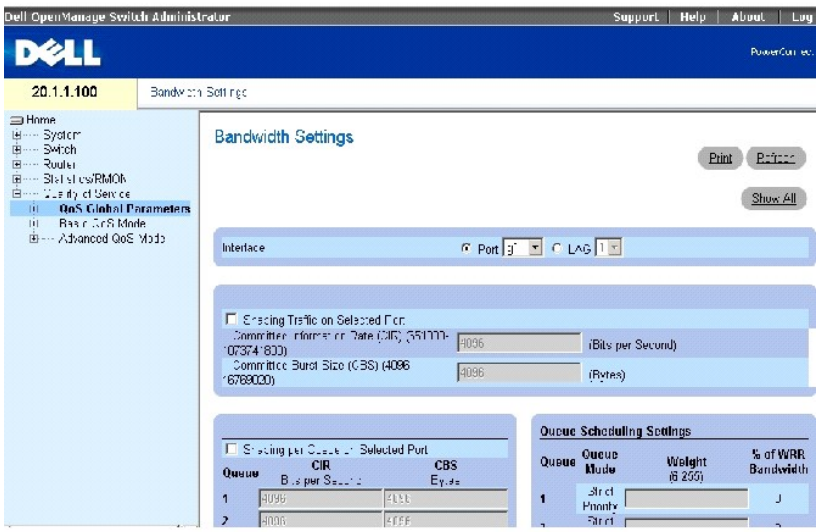
```
Console (config)# qos

Console (config)# interface ethernet g5
```

```
Console (config-if)# qos cos 3


Console (config-if)# exit


Console (config)# exit


Console# show qos


QoS: basic


Basic trust: vpt
```

Définition des paramètres de la bande passante

La page **Bandwidth Settings** (Paramètres de la bande passante) permet de définir les paramètres de la bande passante d'une interface d'entrée spécifique. La modification de la planification des files d'attente affecte les paramètres des files d'attente de façon globale. Pour ouvrir la page **Bandwith Settings** (Paramètres de la bande passante), cliquez sur **Quality of Service** (Qualité de service)→ **QoS Global Parameters** (Paramètres globaux de QdS)→ **Bandwidth Settings** (Paramètres de la bande passante) dans l'*arborescence*.

Figure 10-3. Paramètres de la bande passante



La page **Bandwidth Settings** (Paramètres de la bande passante) contient les champs suivants :

Interface Port ou LAG auquel s'appliquent les paramètres de la bande passante.

Shaping Traffic on Selected Port (Mettre en forme le trafic sur le port sélectionné) Configure le débit minimum garanti (CIR) et la taille des rafales garantie (CBS) sur l'interface. La mise en forme du trafic à la fois par file d'attente et par interface est possible. La mise en forme est déterminée par la valeur la plus faible.

Shaping per Queue on Selected Port (Mettre en forme par file d'attente sur le port sélectionné) Configure le débit minimum garanti (CIR) et la taille des

rafales garantie (CBS) au niveau de chaque file d'attente. La mise en forme du trafic à la fois par file d'attente et par interface est possible. La mise en forme est déterminée par la valeur la plus faible.

Queue Scheduling Settings (Paramètres de planification pour les files d'attente) Configuration la pondération de chaque file d'attente WRR (permutation circulaire pondérée).

WRR Weight (0-255) (Pondération WRR (0-255)) Affecte des pondérations à chaque file d'attente WRR. Les files d'attente WRR sont définies par port. Les valeurs possibles pour ce champ sont comprises entre 6 et 255. Une pondération de 0 peut être affectée à chaque file d'attente. Dans ce cas, la file d'attente n'est pas opérationnelle et est fermée.

Mise en forme du trafic sur une interface sélectionnée

1. Ouvrez la page **Bandwidth Settings** (Paramètres de la bande passante).
2. Sélectionnez une interface.
3. Cochez la case **Shaping Traffic on Selected Port** (Mettre en forme le trafic sur le port sélectionné).
4. Entrez des valeurs pour le CIR et la CBS de l'interface.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le CIR et la CBS de l'interface sélectionnée sont configurés et le périphérique est mis à jour.

Mise en forme du trafic par file d'attente

1. Ouvrez la page **Bandwidth Settings** (Paramètres de la bande passante).
2. Sélectionnez une interface.
3. Cochez la case **Shaping per Queue on Selected Port** (Mettre en forme par file d'attente sur le port sélectionné).
4. Entrez des valeurs pour le CIR et la CBS de chaque file d'attente.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le CIR et la CBS de chaque file d'attente de l'interface sélectionnée sont configurés et le périphérique est mis à jour.

Configuration des paramètres de planification par port pour les files d'attente

1. Ouvrez la page **Bandwidth Settings** (Paramètres de la bande passante).

REMARQUE : La page **Global Queue Settings** (Paramètres globaux de file d'attente) permet de modifier des paramètres de planification pour les files d'attente.

2. Pour chacune des huit files d'attente, configurez le paramètre **Strict Priority** (Priorité stricte) ou entrez une **pondération**.
3. Pour chaque file d'attente configurée au niveau du système comme une file d'attente WRR, entrez une pondération.

Le rapport de pondération détermine la fréquence à laquelle le programmateur de paquets sort les paquets de chaque file d'attente. Le rapport de chaque file d'attente est défini par la pondération de la file d'attente divisée par la somme de toutes les pondérations des files d'attente (pondération normalisée), ce qui permet de configurer l'allocation de bande passante de chaque file d'attente.

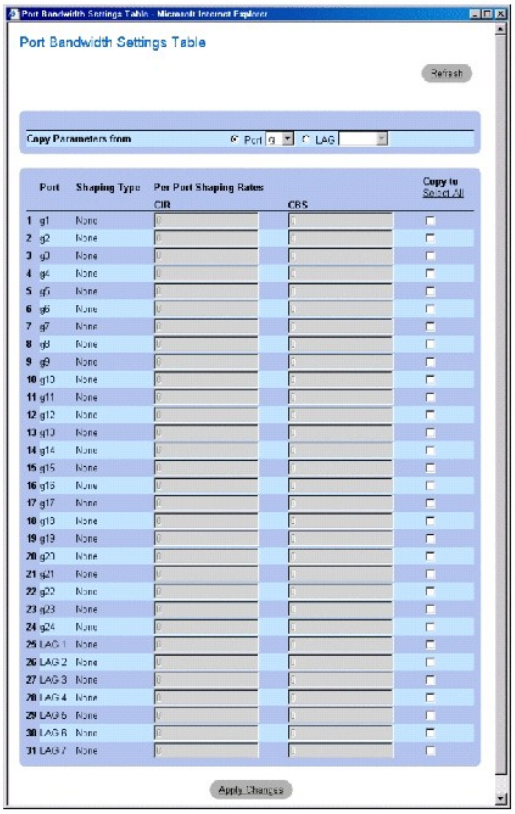
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le périphérique est mis à jour.

Affichage de la table des paramètres de la bande passante du port

1. Ouvrez la page **Bandwidth Settings** (Paramètres de la bande passante).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Port Bandwidth Settings Table** (Table des paramètres de la bande passante du port).

Figure 10-4. Table des paramètres de la bande passante du port



Shaping Type (Type de mise en forme) Peut être par port, par file d'attente, les deux ou aucun des deux.

Per Port Shaping Rates (Débits de mise en forme par port) Le CIR et la CBS sont définis par port. Pour afficher la mise en forme par file d'attente, ouvrez la page de modification.

Copie des paramètres de la bande passante du port

1. Ouvrez la page **Bandwidth Settings** (Paramètres de la bande passante).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Port Bandwidth Settings Table** (Table des paramètres de la bande passante du port).
3. Sélectionnez l'interface où se trouvent les paramètres de la bande passante du port à copier vers une autre interface parmi celles listées dans la table des paramètres de la bande passante du port.
4. Cochez la case **Copy to** (Copier vers) de chaque interface où seront copiés les paramètres de la bande passante du port ou bien cliquez sur **Select All** (Tout sélectionner) pour copier les paramètres de la bande passante du port dans toutes les interfaces listées.
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Définition des paramètres de la bande passante à l'aide de commandes CLI

Tableau 10-4. Commandes CLI Paramètres de la bande passante

Commande CLI	Description
`traffic-shape {committed- rate committed-burst} [queue-id]`	Configure l'outil de mise en forme du trafic sur le port ou la file de sortie.
`wrr-queue bandwidth weight1 weight2 ... weight_n`	Affecte des pondérations WRR (permutation circulaire pondérée) aux files d'attente de sortie.
	Configure le nombre de files d'attente de priorité stricte.

priority-queue out num- of-queues *number-of- queues*	
show qos interface [ethernet *interface- number* | vlan *vlan-id* | port-channel *number*] [buffers | queuing | policers | shapers]	Affiche des informations sur l'interface QdS.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface ethernet g5

Console (config-if)# traffic-shape 124000 96000

Console (config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8

Console (config-if)# exit

Console (config)# priority-queue out num-of-queues 2

Console (config)# exit

Console> show qos interface ethernet g1 buffers

Ethernet g1

Notify Q depth:

qid-size

1 - 125

2 - 125

3 - 125

4 - 125

5 - 125

6 - 125

7 - 125

8 - 125
```

qid	WRED	thresh0	thresh1	thresh2
1	dis	100	100	100
2	dis	100	100	100
3	dis	100	100	100
4	dis	100	100	100
5	Ena	N/A	N/A	N/A
6	Ena	N/A	N/A	N/A
7	Ena	N/A	N/A	N/A
8	Ena	N/A	N/A	N/A

qid	MinDP0	MaxDP0	ProbDP0	MinDP1	MaxDP1	ProbDP1	MinDP2	MaxDP2	ProbDP2	weight
1	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
5	50	60	13	65	80	6	85	95	4	2
6	50	60	13	65	80	6	85	95	4	2
7	50	60	13	65	80	6	85	95	4	2
8	50	60	13	65	80	6	85	95	4	2

```
Console> show qos interface ethernet g1 queueing

Ethernet g1

wrr bandwith weights and EF priority:
```

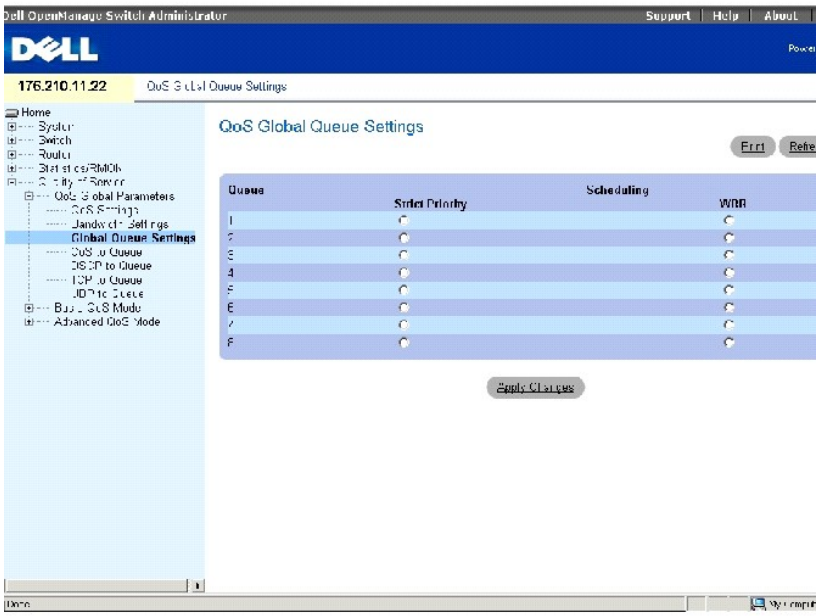
```
qid-weights Ef - Priority

1 - 125 dis- N/A

2 - 125 dis- N/A

3 - 125 dis- N/A

4 - 125 dis- N/A

5 - N/A ena- 5

6 - 125 dis- N/A

7 - 125 dis- N/A

8 - N/A ena- 8

Cos-queue map:

cos-qid

0 - 3

1 - 1

2 - 2

3 - 4

4 - 5

5 - 6

6 - 7
```

Définition des paramètres globaux de file d'attente

La page **Global Queue Settings** (Paramètres globaux de file d'attente) permet de modifier les paramètres globaux de planification de mise en file d'attente.

Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service)→ **QoS Global Parameters** (Paramètres globaux de QdS)→ **Queue Settings** (Paramètres de file d'attente) dans l'*arborescence*.

Figure 10-5. Paramètres globaux de file d'attente



La page **Global Queue Settings** (Paramètres globaux de file d'attente) contient les champs suivants :

Queue (File d'attente) Indique le numéro de file d'attente.

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

WRR Indique si la planification du trafic est basée sur la permutation circulaire pondérée (**Weigted Round Robin** (**WRR**)) des files d'attente de sortie assignées. Les pondérations WRR sont définies dans la page **Bandwidth Settings** (Paramètres de la bande passante).

Configuration des paramètres globaux de planification des mises en file d'attente

1. Ouvrez la page **Global Queue Settings** (Paramètres globaux de file d'attente).
2. Pour chaque file d'attente, cliquez sur **Strict Priority** (Priorité stricte) ou **WRR** (Weighted Round Robin - permutation circulaire pondérée).

   Les paramètres WRR réels sont configurés par port, sur la page **Bandwidth Settings** (Paramètres de la bande passante).

   Le fait de cocher un bouton d'option d'une file d'attente sélectionne automatiquement le type de planification pour toutes les files d'attente suivantes. Chaque file d'attente précédant la file d'attente sélectionnée utilise la planification de priorité opposée. Par exemple, si vous choisissez **Strict Priority** (Priorité stricte) pour la file d'attente 6, les files d'attente 7 et 8 seront du même type ; les files d'attente 1 à 5 seront du type **WRR**.

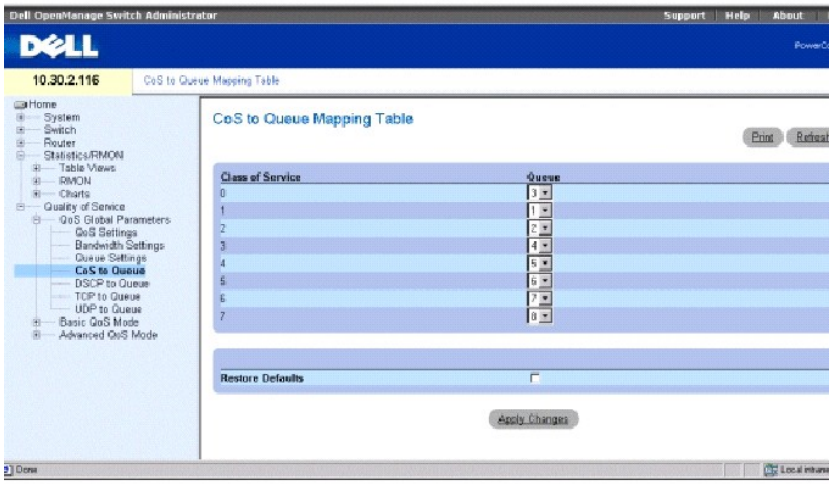
REMARQUE : Deux files d'attentes doivent au moins être configurées comme des files d'attente WRR.

3. Cliquez sur **Apply Changes** (Appliquer les modifications) pour mettre à jour le périphérique.

Définition de l'adressage de valeurs CdS aux files d'attente

La page **CoS to Queue Mapping Table** (Table d'adressage de valeurs CdS aux files d'attente) permet d'adresser des valeurs CdS à des files d'attente spécifiques. Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service)→ **QoS Global Parameters** (Paramètres globaux de QdS)→ **CoS to Queue** (CdS à file d'attente) dans l'*arborescence*.

Figure 10-6. Page Table d'adressage de valeurs CdS aux files d'attente



Class of Service (Classe de service) Marque de priorité VLAN 802.1Q dans le paquet entrant.

Queue (File d'attente) File d'attente à laquelle la valeur CdS est adressée. Les valeurs possibles pour ce champ sont comprises **entre 1 et 8**.

Les paquets entrants qui possèdent la valeur de CdS indiquée sont adressés à la file d'attente correspondante, si le mode **Trust** (Confiance) a été activé pour cette CdS.

Restore Defaults (Restaurer les valeurs par défaut) Redonne à chaque file d'attente sa classe de service par défaut.

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

1. Ouvrez la page **CoS to Queue Mapping Table** (Table d'adressage de valeurs CdS aux files d'attente).
2. Sélectionnez une file d'attente pour chaque entrée **Class of Service** (Classe de services).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La valeur CdS est adressée aux files d'attente et le périphérique est mis à jour.

Réinitialisation de l'adressage de valeurs CdS aux files d'attente par défaut :

1. Ouvrez la page **CoS to Queue Mapping Table** (Table d'adressage de valeurs CdS aux files d'attente).
2. Cochez la case **Restore Defaults** (Restaurer les valeurs par défaut).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Les paramètres par défaut de l'adressage de valeurs CdS aux files d'attente sont restaurés et le périphérique est mis à jour.

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

Le tableau suivant récapitule les commandes CLI pour l'adressage de valeurs CdS aux files d'attente.

Tableau 10-5. Commandes CLI Adressage de valeurs CdS aux files d'attente

Commande CLI	Description
`wrr-queue cos-map` *`queue-id cos1 ... cos8`*	Adresse les valeurs CdS affectées pour sélectionner l'une des files d'attente de sortie.
`show qos map [dscp- queue | tcp-port- queue | udp-port- queue | dscp-policed | dscp-mutation]`	Affiche tous les adressages de QdS

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# wrr-queue cos-map 7 246

Console (config)# show qos map dscp-queue

Dscp-queue map:

d1 : d2   0   1   2   3   4   5   6   7   8   9

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

0  : 01   01  01  01  01  01  01  01  02  02

1  : 02   02  02  02  02  02  03  03  03  03

2  : 03   03  03  03  04  04  04  04  04  04

3  : 04   04  05  05  05  05  05  05  05  05

4  : 06   06  06  06  06  06  06  06  07  07

5  : 07   07  07  07  07  07  08  08  08  08

6  : 08   08  08  08

Console (config)# show qos map tcp-port-queue

Tcp port-queue map:

Port queue

----- ------
```

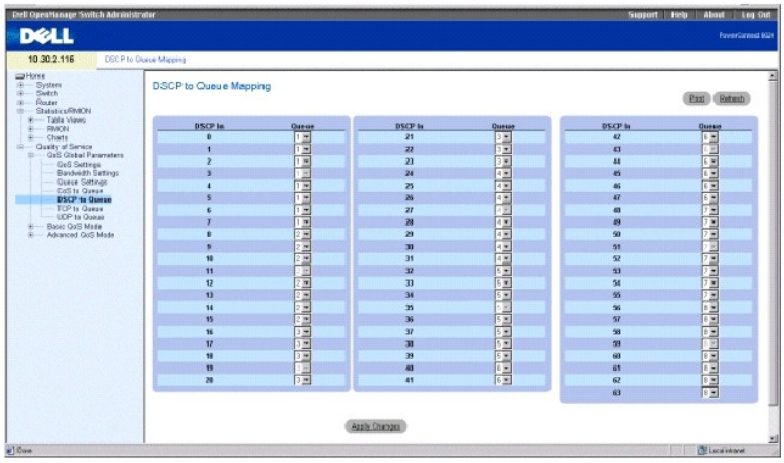
```
6000    1

6001    2

6002    3

Console (config)# show qos map udp-port-queue

Udp port-queue map:

Port queue

----- -----

8000    1

8001    2

Console (config)# show qos map dscp-policed

Policed-dscp map:

d1 :  d2  0   1   2   3   4   5   6   7   8   9

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

0  :  00  01  02  03  04  05  06  07  08  09

1  :  10  11  12  13  14  15  16  17  18  19

2  :  20  21  22  23  24  25  26  27  28  29

3  :  30  31  32  33  34  35  36  37  38  39

4  :  40  41  42  43  44  45  46  47  48  49

5  :  50  51  52  53  54  55  56  57  58  59

6  :  60  61  62  63

Console (config)# show qos map dscp-mutation
```

```
Dscp-dscp mutation map:

d1 :  d2  0   1   2   3   4   5   6   7   8   9

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

0  :  00  01  02  03  04  05  06  07  08  09

1  :  10  11  12  13  14  15  16  17  18  19

2  :  20  21  22  23  24  25  26  27  28  29

3  :  30  31  32  33  34  35  36  37  38  39

4  :  40  41  42  43  44  45  46  47  48  49

5  :  50  51  52  53  54  55  56  57  58  59

6  :  60  61  62  63
```

Définition de l'adressage de valeurs DSCP aux files d'attente

La page **DSCP to Queue Mapping** (Adressage de valeurs DSCP aux files d'attente) permet d'adresser des valeurs DSCP à des files d'attente spécifiques. Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service)→ **QoS Global Parameters** (Paramètres globaux de QdS)→ **DSCP to Queue** (DSCP à file d'attente) dans l'*arborescence*.

Figure 10-7. Page Adressage de valeurs DSCP aux files d'attente



DSCP In (Entrée DSCP) Indique la valeur du code d'accès aux services différenciés dans le paquet entrant

Queue (File d'attente) File d'attente à laquelle la valeur DSCP est adressée.

Les paquets entrants qui possèdent la valeur de DSCP indiquée sont adressés à la file d'attente correspondante, si le mode **Trust** (Confiance) est activé pour le DSCP. Les valeurs de DSCP 3, 11, 19, 27, 35, 43, 51 et 59 sont adressées à q1, q2 ... q8. Ces paramètres ne peuvent pas être modifiés.

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

1. Ouvrez la page **DSCP to Queue Mapping** (Adressage de valeurs DSCP aux files d'attente).
2. Sélectionnez une file d'attente pour chaque niveau de DSCP.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La valeur DSCP est adressée aux files d'attente et le périphérique est mis à jour.

Adressage de valeurs DSCP aux files d'attente à l'aide de commandes CLI

Tableau 10-6. Commandes CLI Adressage de valeurs DSCP aux files d'attente

Commande CLI	Description
qos map dscp-queue *dscp- list* to *queue-id*	Modifie l'adressage de valeurs DSCP à CdS.
show qos map [dscp-queue | tcp-port-queue | udp-port-queue | dscp-policed | dscp-mutation]	Affiche tous les adressages de QdS.

Vous trouverez ci-dessous un exemple de commande CLI :

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

Console (config)# exit

Console # show qos map dscp-queue

Dscp-queue Map

d1:  d2 0  1  2  3  4  5  6  7  8  9

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

0:   01 01 01 01 01 01 02 02

1:   02 02 02 02 02 03 03 03

2:   03 03 03 04 04 04 04 04

3:   04 04 05 05 05 05 05 05

4:   06 06 06 06 06 06 07 07
```

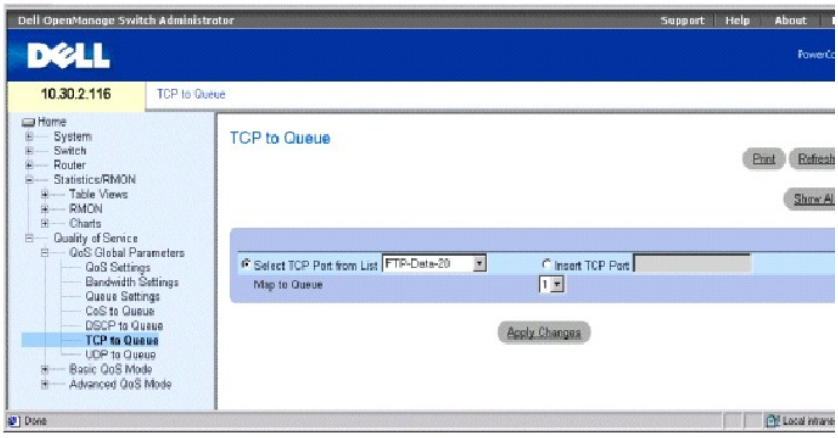
5: 07 07 07 07 08 08 08 08

6: 08 08 08 08

Définition de l'adressage de ports TCP QdS aux files d'attente

La page **QoS TCP to Queue** (TCP QdS à file d'attente) permet d'adresser un port TCP à une file d'attente. Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service)→ **QoS Global Parameters** (Paramètres globaux de QdS)→ **TCP to Queue** (TCP à file d'attente) dans l'*arborescence*.

Figure 10-8. Page Adressage de ports TCP QdS aux files d'attente



Select TCP Port from List (Sélectionner un port TCP dans la liste) Sélectionne un port TCP connu pour l'adresser à une file d'attente.

Insert TCP Port (Insérer un port TCP) Active l'insertion manuelle d'un port TCP à adresser à une file d'attente.

Map to Queue (Adressage à file d'attente) Indique la file d'attente à laquelle le port TCP est adressé.

Adressage d'un port TCP connu à une file d'attente

1. Ouvrez la page **TCP to Queue** (TCP à file d'attente).
2. Choisissez l'option **Select TCP Port from List** (Sélectionner un port TCP dans la liste).
3. Sélectionnez un port TCP.
4. Sélectionnez une file d'attente dans la liste **Map to Queue** (Adressage à file d'attente).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port TCP est adressé à la file d'attente sélectionnée et le périphérique est mis à jour.

Adressage d'un port TCP non inclus dans la liste à une file d'attente

1. Ouvrez la page **QoS TCP to Queue** (TCP QdS à file d'attente).
2. Choisissez l'option **Insert TCP Port** (Insérer un port TCP).
3. Entrez le numéro et la description du port TCP dans le champ **Insert TCP Port** (Insérer un port TCP).
4. Sélectionnez une file d'attente dans la liste **Map to Queue** (Adressage à file d'attente).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port TCP est adressé à la file d'attente sélectionnée et le périphérique est mis à jour.

Suppression de l'adressage d'un port TCP à une file d'attente

1. Ouvrez la page **QoS TCP to Queue** (TCP QdS à file d'attente).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **TCP to Queue Mapping Table** (Table d'adressage de ports TCP aux files d'attente).
3. Cochez la case **Remove** (Supprimer) de chaque port TCP dont l'adressage à une file d'attente doit être supprimé.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Définition de l'adressage de ports TCP aux files d'attente à l'aide de commandes CLI

Tableau 10-7. Commandes CLI Adressage de ports TCP aux files d'attente

Commande CLI	Description
`qos map tcp-port- queue port1 ... port 8 to queue-id`	Modifie l'adressage port TCP à file d'attente.
`show qos map [dscp- queue | tcp-port- queue | udp-port- queue | dscp-policed | dscp-mutation]`	Affiche tous les adressages de QdS.

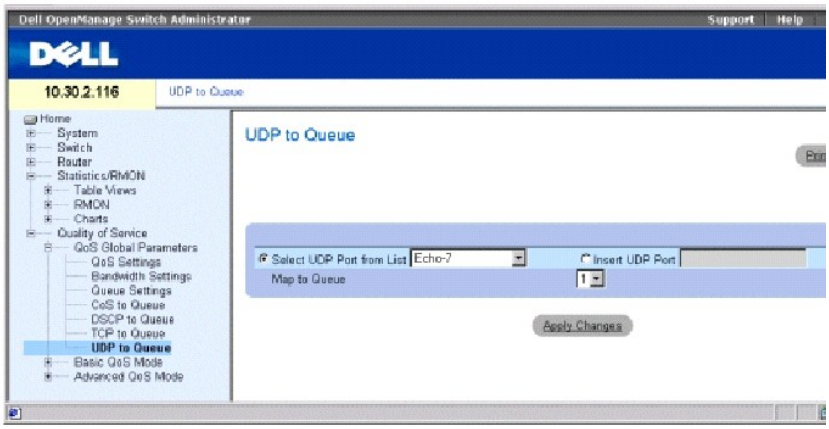
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# qos map tcp-port-queue 2000 80 to 2

Console (config)# exit

Console# show qos map tcp-port-queue

Tcp port - queue map

Port        queue

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

6000        1

6001        2

6002        3
```

Définition de l'adressage de port UDP QdS aux files d'attente

La page **QoS UDP to Queue** (UDP QdS à file d'attente) permet d'adresser un port UDP à une file d'attente. Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service)→ **QoS Global Parameters** (Paramètres globaux de QdS)→ **UDP to Queue** (UDP à file d'attente) dans l'*arborescence*.

Figure 10-9. Page Adressage de ports UDP aux files d'attente



Select UDP Port from List (Sélectionner un port UDP dans la liste) Sélectionne un port UDP connu pour l'adresser à une file d'attente.

Insert UDP Port (Insérer un port UDP) Active l'insertion manuelle d'un port UDP à adresser à une file d'attente.

Map to Queue (Adressage à file d'attente) Indique la file d'attente à laquelle le port UDP est adressé.

Adressage d'un port UDP connu à une file d'attente

1. Ouvrez la page **UDP to Queue** (UDP à file d'attente).
2. Choisissez l'option **Select UDP Port from List** (Sélectionner un port UDP dans la liste).
3. Sélectionnez un port UDP.
4. Sélectionnez une file d'attente dans la liste **Map to Queue** (Adressage à file d'attente).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port UDP est adressé à la file d'attente sélectionnée et le périphérique est mis à jour.

Adressage d'un port UDP non inclus dans la liste à une file d'attente

1. Ouvrez la page **UDP to Queue** (UDP à file d'attente).
2. Choisissez l'option **Insert UDP Port** (Insérer un port UDP).
3. Entrez le numéro du port UDP dans le champ **Insert UDP Port** (Insérer un port UDP).
4. Sélectionnez une file d'attente dans la liste **Map to Queue** (Adressage à file d'attente).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le port UDP est adressé à la file d'attente sélectionnée et le périphérique est mis à jour.

Suppression de l'adressage d'un port UDP à une file d'attente

1. Ouvrez la page **UDP to Queue** (UDP à file d'attente).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **UDP to Queue Mapping Table** (Table d'adressage de ports UDP aux files d'attente).
3. Cliquez sur **Remove** (Supprimer) pour chaque port UDP dont l'adressage à une file d'attente doit être supprimé.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Définition de l'adressage de ports UDP aux files d'attente à l'aide de commandes CLI

Tableau 10-8. Commandes CLI Adressage de ports UDP aux files d'attente

Commande CLI	Description
qos map udp-port-queue *port1 ... port 8 to queue- id*	Modifie l'adressage port UDP à file d'attente.
show qos map [dscp-queue | tcp-port-queue | udp-port- queue | dscp-policed | dscp-mutation]	Affiche tous les adressages de QdS.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# qos map udp-port-queue 68 to 1

Console (config)# exit

Console# show qos map udp-port-queue

Udp port-queue map:

Port      queue

-----     -----

8000      1

8001      2
```

Configuration du mode de base de la qualité de service

La page **Basic QoS Mode** (Mode QdS de base) contient des liens vers les pages de configuration du mode Trust (Confiance) et de la réécriture DSCP. Pour ouvrir la page **Basic QoS Mode** (Mode QdS de base), cliquez sur **Quality of Service** (Qualité de service)→ **Basic QoS Mode** (Mode QdS de base) dans l'*arborescence*.

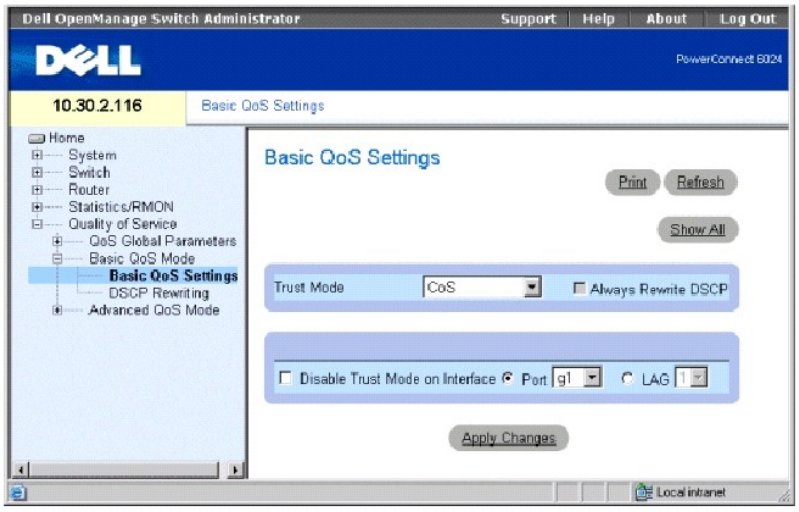
Définition des paramètres QdS de base

La page **Basic QoS Settings** (Paramètres QdS de base) permet de configurer le mode Trust (Confiance) global, défini sur des interfaces spécifiques. Les paquets entrant dans un domaine QdS sont classés à la frontière du domaine QdS. Lorsque les paquets sont classés à la frontière, le mode Confiance peut être configuré sur des ports.

Les valeurs DSCP peuvent être réécrites sur les frontières du domaine administratif de QdS. Lorsque deux domaines QdS possèdent des définitions de DSCP différentes, les valeurs DSCP peuvent être réécrites. L'adressage de valeurs DSCP s'applique uniquement sur des ports d'entrée, DSCP et en mode Trust.

Pour ouvrir la page **Basic QoS Settings** (Paramètres QdS de base), cliquez sur **Quality of Service** (Qualité de service)→ **Basic QoS Mode** (Mode QdS de base) → **Basic QoS Settings** (Paramètres QdS de base) dans l'*arborescence*.

Figure 10-10. Page Paramètres QdS de base



Trust Mode (Mode Confiance) Sélectionnez le mode Confiance. Lorsqu'une marque CdS, une marque DSCP et un adressage TCP/UDP d'un paquet sont adressés à des files d'attente différentes, le **Trust Mode** (Mode Confiance) indique la file d'attente à laquelle le paquet est affecté. Ce champ peut prendre les valeurs suivantes :

CoS (CdS) Configure le mode Confiance pour CdS sur le périphérique. L'adressage de CdS indique la file d'attente du paquet.

DSCP Configure le mode Confiance pour DSCP sur le périphérique. L'adressage de DSCP indique la file d'attente du paquet.

TCP/UDP Port (Port TCP/UDP) Configure le mode Confiance pour le port TCP/UDP sur le périphérique. L'adressage du port TCP/UDP indique la file d'attente du paquet.

Always Rewrite DSCP (Toujours réécrire DSCP) Réécrit la marque DSCP du paquet en fonction de la configuration de la réécriture DSCP QdS. Cette option ne peut être sélectionnée que si le mode **Confiance** est **DSCP**.

Disable Trust Mode on Interface (Désactiver le mode Confiance sur l'interface) Désactive le mode Confiance pour le port ou le LAG sélectionné.

Interface Port ou LAG sur lequel le mode Confiance est désactivé.

Configuration du mode Trust (Confiance)

1. Ouvrez la page **Basic QoS Settings** (Paramètres QdS de base).
2. Sélectionnez une valeur pour **Trust Mode** (Mode Confiance).
3. Si le **mode Confiance** est **DSCP**, cochez la case **Always Rewrite DSCP** (Toujours réécrire DSCP) pour que les marques DSCP soient indiquées comme adressées.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le mode Confiance est sélectionné et le périphérique est mis à jour.

Désactivation du mode Confiance sur les interfaces

1. Ouvrez la page **Basic QoS Settings** (Paramètres QdS de base).

2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Basic QoS Settings Table** (Table des paramètres QdS de base).
3. Cochez **Disable Trust Mode** (Désactiver le mode Confiance) pour toutes les interfaces sur lesquelles le mode Confiance doit être désactivé.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Définition des paramètres de QdS de base à l'aide de commandes CLI

Tableau 10-9. Commandes CLI Paramètres QdS de base

Commande CLI	Description
`qos trust cos | dscp | tcp-udp-port`	Dans un contexte global, cette commande configure le système en mode de base et l'état Confiance.
`qos trust`	Dans un contexte de configuration de l'interface, cette commande active l'état Confiance de chaque port.
`qos dscp-mutation`	Applique l'adressage de mutation DSCP à un port en mode Confiance DSCP (réécrit toujours le DSCP sur ce port).

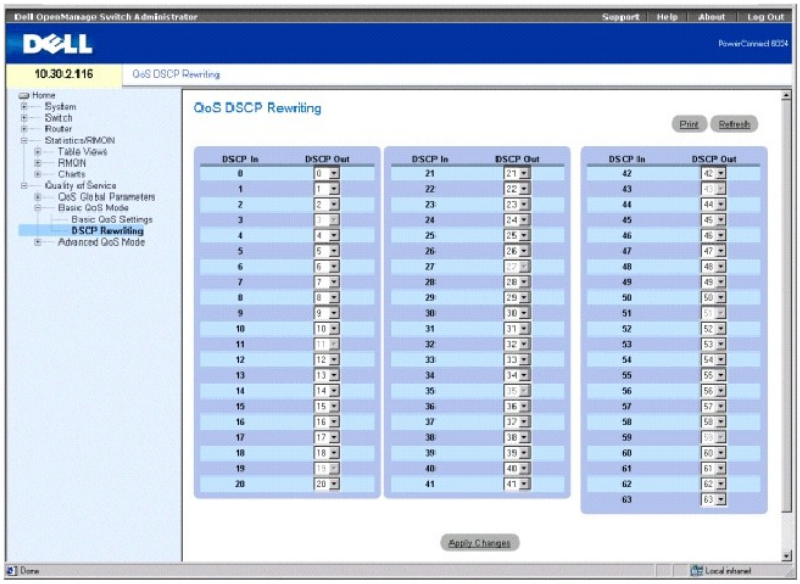
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# qos trust dscp

Console (config)# qos dscp-mutation

Console (config)# interface ethernet g5

Console (config-if) qos trust
```

Définition des paramètres de réécriture DSCP QdS

La page **QoS DSCP Rewriting** (Réécriture DSCP QdS) permet de configurer la méthode de réécriture des marques DSCP.Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service)→ **Basic QoS Settings** (Paramètres QdS de base)→ **DSCP Rewriting** (Réécriture DSCP) dans l'*arborescence*.

Figure 10-11. Page Réécriture DSCP QdS



DSCP In (Entrée DSCP) Valeur de la marque DSCP sur un paquet entrant.

DSCP Out (Sortie DSCP) Valeur de la marque DSCP sur les paquets sortants.

Configuration de la réécriture DSCP

1. Ouvrez la page **QoS DSCP Rewriting** (Réécriture DSCP QdS).
2. Pour chaque marque **DSCP In** (Entrée DSCP), sélectionnez une valeur **DSCP Out** (Sortie DSCP) dans le menu déroulant.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

La réécriture DSCP est configurée et le périphérique est mis à jour.

Configuration de la réécriture DSCP à l'aide de commandes CLI

Tableau 10-10. Commandes CLI Réécriture DSCP

Commande CLI	Description
`qos map dscp- mutation` *`in-dscp`* `to` *`out-dscp`*	Modifie l'adressage de mutation DSCP vers DSCP.

Vous trouverez ci-dessous un exemple de commande CLI permettant de définir un adressage de mutation DSCP :

```
Console (config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

Configuration du mode QdS avancé

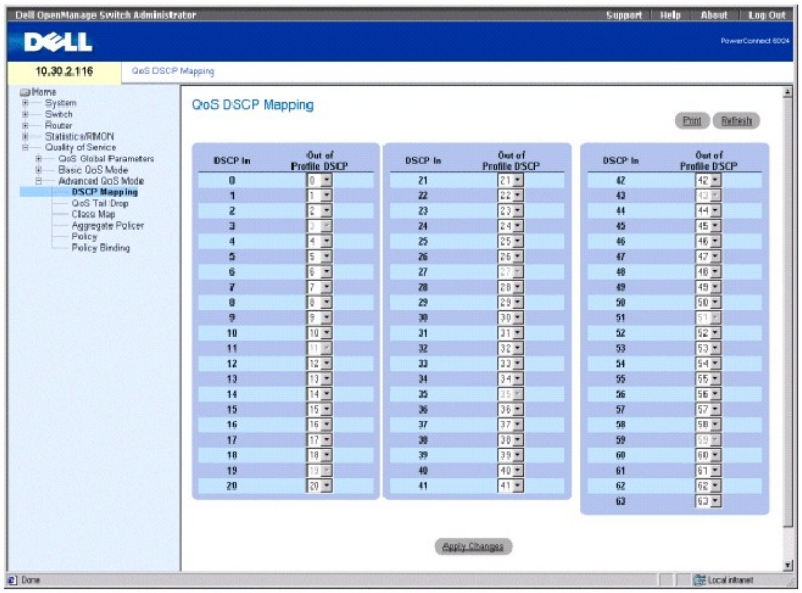
La page **Advanced QoS Mode** (Mode QdS avancé) contient des liens vers les pages de configuration des paramètres avancés. Pour ouvrir cette page, cliquez

sur **Quality of Service** (Qualité de service)→ **Advanced QoS Mode** (Mode QdS avancé) dans l'*arborescence*.

Définition des paramètres d'adressage DSCP QoS

Lorsque le trafic dépasse les limites définies par l'utilisateur, la page **QoS DSCP Mapping** (Adressage DSCP QdS) permet de configurer la marque DSCP à utiliser à la place des marques DSCP entrantes. Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service)→ **Advanced QoS Mode** (Mode QdS avancé)→ **DSCP Mapping** (Adressage DSCP) dans l'*arborescence*.

Figure 10-12. Page Adressage DSCP QdS



DSCP In (Entrée DSCP) Valeur de la marque DSCP sur un paquet entrant.

Out of Profile DSCP (DSCP hors profil) Attribue une nouvelle marque DSCP à la marque entrante.

Configuration de l'adressage DSCP

1. Ouvrez la page **QoS DSCP Mapping** (Adressage DSCP QdS).
2. Sélectionnez une valeur dans le menu déroulant **Out of Profile DSCP** (DSCP hors profil).

   Cette valeur remplace la valeur de la marque **DSCP In** (Entrée DSCP).
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

   L'adressage DSCP est configuré et le périphérique est mis à jour.

Configuration de l'adressage DSCP à l'aide de commandes CLI

Tableau 10-11. Commandes CLI Adressage DSCP

Commande CLI	Description
	Modifie l'adressage DSCP surveillé pour le nouveau marquage.

qos map policed- *dscp dscp-list to dscp-mark-down*	

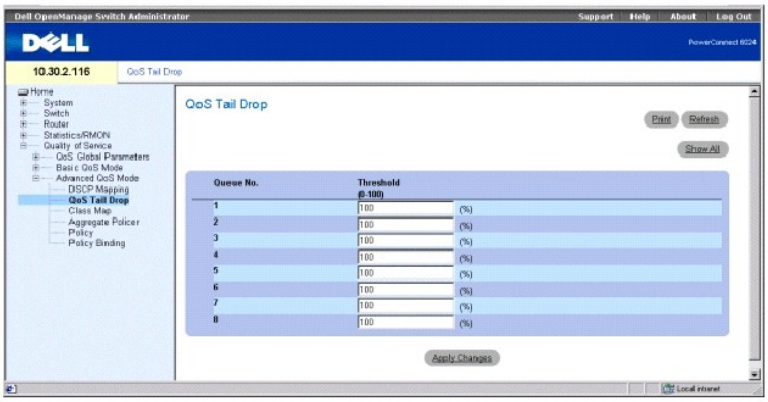
Vous trouverez ci-dessous un exemple de commande CLI permettant d'adresser les valeurs DSCP 12 et 18 à la valeur 56, lorsque le DSCP est hors profil :

```
Console (config)# qos map policed-dscp 12 18 to 56
```

Définition des paramètres de rejet en queue QdS

Le phénomène de Tail drop (rejet en queue) se produit lorsqu'une rafale de paquets sature une mémoire tampon. Les derniers paquets de la rafale sont rejetés à cause du manque d'espace disponible dans la mémoire tampon. La page **QoS Tail Drop** (Rejet en queue QdS) permet de définir des paramètres de rejet en queue pour chaque file d'attente. Pour ouvrir la page **QoS Tail Drop** (Rejet en queue QdS), cliquez sur **Quality of Service** (Qualité de service)→ **Advanced QoS Mode** (Mode QdS avancé)→ **QoS Tail Drop** (Rejet en queue QdS) dans l'*arborescence*.

Figure 10-13. Page Rejet en queue QdS



Queue No. (N° de file d'attente) Indique la file d'attente pour laquelle les paramètres de rejet en queue s'appliquent.

Threshold (1-100) (Seuil (1-100)) Seuil (en pourcentage) du rejet en queue pour la file d'attente. Lorsque ce seuil est dépassé, les paquets sont rejetés jusqu'à ce que le seuil ne soit plus dépassé.

Configuration d'un seuil pour le rejet en queue

1. Ouvrez la page **QoS Tail Drop** (Rejet en queue QdS).
2. Sélectionnez un seuil pour chaque file d'attente.
3. Cliquez sur **Apply Changes** (Appliquer les modifications).

Le seuil du rejet en queue est configuré et le périphérique est mis à jour.

Configuration des paramètres de rejet en queue pour une interface :

1. Ouvrez la page **QoS Tail Drop** (Rejet en queue QdS).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Tail Drop Table** (Table des rejets en queue).
3. Sélectionnez un état pour chaque interface.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).
5. L'état du rejet en queue est défini pour les interfaces.

Définition des paramètres de rejet en queue QdS à l'aide de commandes CLI

Tableau 10-12. Commandes CLI Paramètres de rejet en queue

Commande CLI	Description
`qos wrr-queue threshold queue-id threshold- percentage`	Affecte des seuils de rejet en queue.

Vous trouverez ci-dessous un exemple de commande CLI permettant de définir des paramètres de rejet en queue :

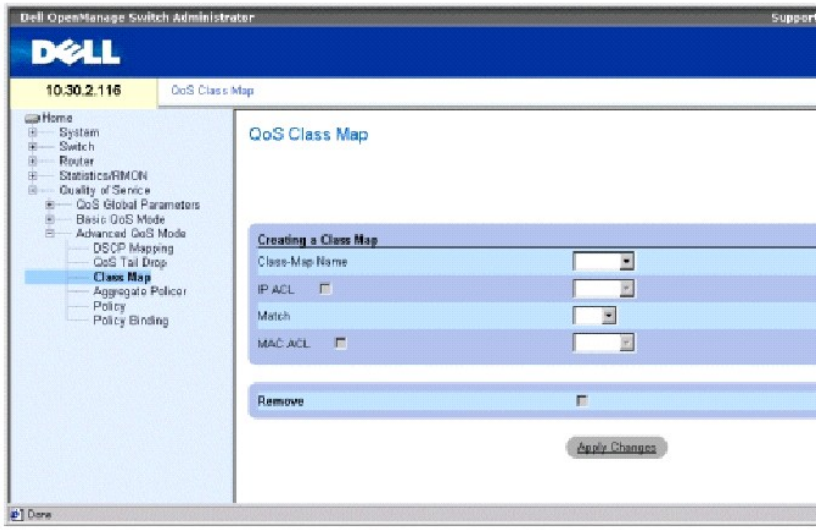
```
Console (config)# qos wrr-queue threshold 8 80
```

Définition des adressages de classes QoS

Les ACL IP et les ACL MAC contiennent un adressage de classes. Les adressages de classes sont configurés de manière à correspondre à des critères de paquet et sont mis en correspondance avec les paquets selon la méthode dite de la première convenance (first-fit). Par exemple, l'adressage de classes A est affecté à des paquets en fonction d'une ACL basée sur IP ou d'une ACL basée sur MAC. L'adressage de classes B est affecté à des paquets à la fois en fonction d'ACL basées sur IP et d'ACL basées sur MAC.

La page **QoS Class Map** (Adressage de classes QdS) permet d'affecter et de modifier des adressages de classes. Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service)→ **Advanced QoS Mode** (Mode QdS avancé)→ **Class Map** (Adressage de classes) dans l'*arborescence*.

Figure 10-14. Page Adressage de classes QdS



Class-Map Name (Nom de l'adressage de classes) Nom de l'adressage de classes défini par l'utilisateur.

IP ACL (ACL IP) ACL IP de la liste de contrôle d'accès IP (ACL). Pour plus d'informations sur la définition des ACL basées sur IP, reportez-vous à la section «Définition des ACL basées sur IP».

Match (Correspondance) Critère utilisé pour mettre en correspondance des adresses IP et/ou des adresses MAC avec une adresse ACL. Ce champ peut prendre les valeurs suivantes :

And (Et) L'ACL basée sur MAC et l'ACL basée sur IP doivent toutes les deux correspondre à un paquet.

Or (Ou) L'ACL basée sur MAC ou l'ACL basée sur IP doit correspondre à un paquet.

MAC ACL (ACL MAC) ACL MAC de la liste de contrôle d'accès MAC. Pour obtenir des informations sur la définition des ACL basées sur MAC, reportez-vous à la section «Définition des ACL basées sur MAC».

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime l'adressage de classes de la table des adressages de classes.

Ajout d'un adressage de classes

1. Ouvrez la page **QoS Class Map** (Adressage de classes QdS).
2. Cliquez sur **Add** (Ajouter) pour ouvrir la page **Add a Class-Map** (Ajout d'un adressage de classes).
3. Entrez un nom (16 caractères max.) pour l'adressage de classes dans le champ **Class-Map Name** (Nom de l'adressage de classes).
4. Effectuez l'une des opérations suivantes :
   - Pour rattacher une ACL IP à l'adressage de classes, cochez la case **IP ACL** (ACL IP) et sélectionnez une ACL IP dans le menu déroulant.
   - Pour rattacher une ACL MAC à l'adressage de classes, cochez la case **MAC ACL** (ACL MAC) et sélectionnez une ACL MAC dans le menu déroulant.
5. Sélectionnez **And** (Et) ou **Or** (Ou) dans le menu déroulant **Match** (Correspondance) si les cases **IP ACL** (ACL IP) et **MAC ACL** (ACL MAC) sont toutes les deux cochées.
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adressage de classes est créé et le périphérique est mis à jour.

Modification d'un adressage de classes

1. Ouvrez la page **QoS Class Map** (Adressage de classes QdS).
2. Sélectionnez un adressage de classes dans le menu déroulant **Class-Map Name** (Nom de l'adressage de classes).
3. Modifiez les autres champs de la page.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).
5. L'adressage de classes est modifié et le périphérique est mis à jour.

Suppression d'un adressage de classes

1. Ouvrez la page **QoS Class Map** (Adressage de classes QdS).
2. Sélectionnez un adressage de classes dans le menu déroulant **Class-Map Name** (Nom de l'adressage de classes).
3. Cochez la case **Remove** (Supprimer).
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

L'adressage de classes est supprimé et le périphérique est mis à jour.

Affichage de la table des adressages de classes

1. Ouvrez la page **QoS Class Map** (Adressage de classes QdS).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Class Map Table** (Table des adressages de classes).

Définition des adressages de classes QdS à l'aide de commandes CLI

Tableau 10-13. Commandes CLI Adressages de classes QdS

Commande CLI	Description

`class-map class-map- name [match-all | match-any]`	Crée un adressage de classe et passe en mode de configuration des adressages de classes.
`match access-group acl- name`	Définit le critère de correspondance permettant de classer le trafic ; activé uniquement en mode configuration des adressages de classes.
`show class-map [class- map-name]`	Affiche tous les adressages de classes.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# class-map class1 match-all

Console (config-cmap)# match access-group dell

Console (config-cmap)# exit

Console (config)# exit

Console> show class-map class1

Class Map match-all class1 (id4)
```

Définitions des contrôleurs d'agrégat QdS

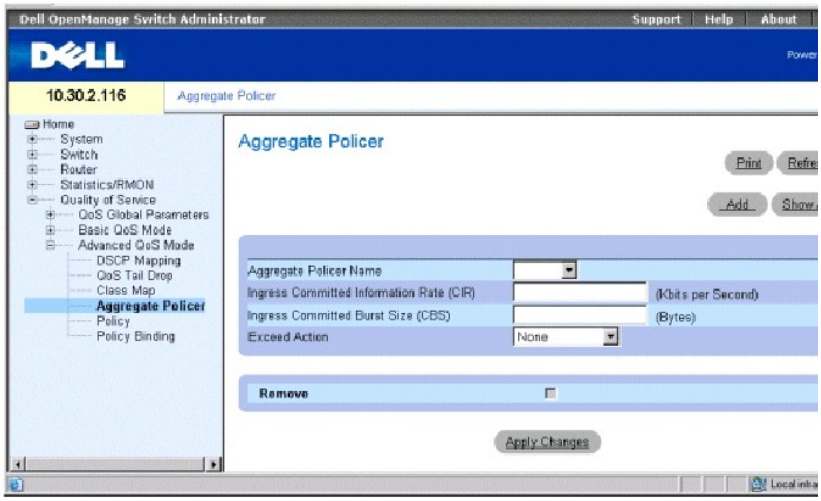
Une fois le paquet classé, le processus de contrôle du trafic commence. Un contrôleur indique la limite de bande passante pour le trafic entrant sur le flux classé et des actions sont définies pour les paquets qui dépassent cette limite. Ces actions peuvent être la transmission des paquets, leur rejet ou leur marquage par une nouvelle valeur DSCP.

Votre commutateur prend en charge les contrôleurs par flux et les contrôleurs d'agrégat.

Les contrôleurs d'agrégat fixent les limites sur un groupe de flux. Un contrôleur d'agrégat ne peut pas être supprimé lorsqu'il est utilisé dans un adressage de réglementation. Supprimez d'abord le contrôleur d'agrégat de tous les adressages de réglementation en utilisant la commande **no police aggregate** avant d'utiliser la commande **no qos aggregate-policer**.

Utilisez la page **QoS Aggregate Policer** (Contrôleur d'agrégat QdS) pour définir les limites de bande passante et les actions à effectuer sur les paquets qui dépassent ces limites. Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service)→ **Advanced QoS Mode** (Mode QdS avancé)→ **Aggregate Policer** (Contrôleur d'agrégat) dans l'*arborescence*.

Figure 10-15. Page Contrôleur d'agrégat QdS



Aggregate Policer Name (Nom du contrôleur d'agrégat) Indique le nom du contrôleur d'agrégat.

Ingress Committed Information Rate (CIR) (Débit minimum garanti en entrée (CIR)) CIR en bits par seconde.

Ingress Committed Burst Size (CBS) (Taille des rafales garantie (CBS) en entrée) CBS en octets par seconde.

Exceed Action (Action si dépassement) Action effectuée si des informations entrantes dépassent les limites du trafic. Ce champ peut prendre les valeurs suivantes :

Drop (Rejet) Les paquets qui dépassent les limites sont rejetés.

Remark DSCP (Nouveau marquage DCSP) Les paquets qui dépassent les limites sont transmis avec une valeur DSCP marquée/indiquée.

None (Aucune action) Les paquets qui dépassent les limites sont transmis.

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime le contrôleur d'agrégat de la table des contrôleurs d'agrégat.

Ajout d'un contrôleur d'agrégat

1. Ouvrez la page **QoS Aggregate Policer** (Contrôleur d'agrégat QdS).
2. Cliquez sur **Add** (Ajouter) pour ouvrir la page **Add Aggregate Policer** (Ajout d'un contrôleur d'agrégat).
3. Renseignez les champs de la fenêtre et cliquez sur **Apply Changes** (Appliquer les modifications).

Le contrôleur d'agrégat est créé et le périphérique est mis à jour.

Suppression d'un contrôleur d'agrégat

1. Ouvrez la page **QoS Aggregate Policer** (Contrôleur d'agrégat QdS).
2. Sélectionnez un contrôleur d'agrégat dans le menu déroulant.
3. Cochez la case **Remove** (Supprimer), puis cliquez sur **Apply Changes** (Appliquer les modifications).

Le contrôleur d'agrégat est supprimé et le périphérique est mis à jour.

Modification d'un contrôleur d'agrégat

1. Ouvrez la page **QoS Aggregate Policer** (Contrôleur d'agrégat QdS).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Aggregate Policer Table** (Table des contrôleurs d'agrégat).
3. Modifiez les informations correspondant aux contrôleurs concernés.
4. Cliquez sur **Apply Changes** (Appliquer les modifications).

Définition des contrôleurs d'agrégat à l'aide de commandes CLI

Tableau 10-14. Commandes CLI Contrôleur d'agrégat

Commande CLI	Description
qos aggregate- policer *aggregate- policer-name committed-rate-bps excess-burst-byte exceed-action* {drop | policed-dscp- transmit}	Définit les paramètres de contrôle qui peuvent être appliqués à plusieurs classes de trafic à l'intérieur du même adressage de réglementation.
show qos aggregate police [*aggregate- policer-name*]	Affiche les paramètres du contrôleur d'agrégat.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# qos aggregate policer policer1 124000 96000 exceed-action drop
```

```
Console> show qos aggregate police policer1
```

```
aggregate-policer policer1 96000 4800 exceed-action drop
```

```
not used by any policy map
```

Définition de réglementation

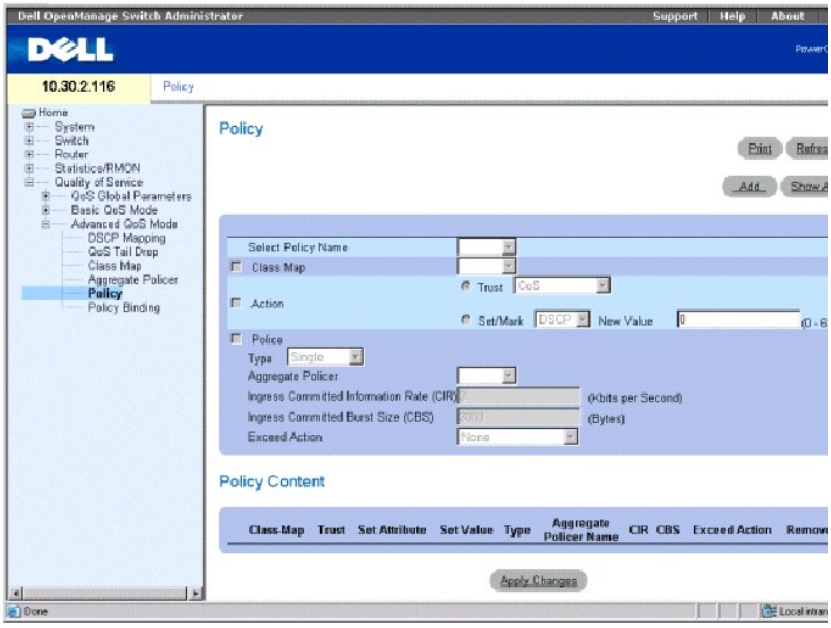
Une réglementation est un ensemble de classes, elles-mêmes étant composées d'un adressage de classes et d'une action QdS à effectuer sur le trafic correspondant. Les classes sont appliquées selon la méthode dite de la première convenance (first-fit) à l'intérieur d'une réglementation.

Avant de configurer des réglementations pour des classes dont les critères de correspondance sont définis dans un adressage de classes, vous devez définir un adressage de classes ou indiquer le nom de l'adressage de classes à créer, à ajouter ou à modifier. Les réglementations de classes peuvent être configurées dans un adressage de réglementation uniquement si les classes ont défini des critères de correspondance.

Un contrôleur d'agrégat peut être affecté à plusieurs classes à l'intérieur d'un adressage de réglementations, mais il ne peut pas être utilisé pour différents adressages de réglementations. Vous pouvez définir un contrôleur d'agrégat lorsque celui-ci est partagé par plusieurs classes. Les contrôleurs d'un port ne peuvent pas être partagés avec d'autres contrôleurs d'un autre périphérique. Le trafic provenant de deux ports différents peut être agrégé à des fins de contrôle.

Pour ouvrir la page **QoS Policy** (Réglementation QdS), cliquez sur **Quality of Service** (Qualité de service)→ **Advanced QoS Mode** (Mode QdS avancé)→ **Policy** (Réglementation) dans l'*arborescence*.

Figure 10-16. Page Réglementation QdS



Select Policy Name (Sélectionnez un nom de réglementation) Sélectionne un nom de réglementation.

Class Map (Adressage de classes) Sélectionnez un adressage de classes pour la classe.

Action Action facultative à effectuer sur la classe. Ce champ peut prendre les valeurs suivantes :

Trust (Confiance) Active le mode Confiance pour la classe. Cette commande sert à distinguer le comportement confiance QdS du trafic concerné. Lorsqu'un type donné est en mode confiance, le mécanisme QdS fait correspondre un paquet à une file d'attente en utilisant la valeur reçue ou la valeur par défaut et l'adressage correspondant, tel que défini dans la page **QoS Global Parameters** (Paramètres globaux de QdS). Vous ne pouvez faire passer en mode Confiance que le trafic entrant possédant certaines valeurs DSCP.

Set / Mark (Configurer/Marquer) Configure manuellement le mode Confiance.

New Value (Nouvelle valeur) Valeur de la méthode **Set / Mark** (Configurer/Marquer) choisie.

Police Type (Type de contrôleur) Type de contrôleur appliqué à la classe. Ce champ peut prendre les valeurs suivantes :

Aggregate (Agrégat) Configure la classe pour utiliser un contrôleur d'agrégat configuré choisi dans le menu déroulant. Vous pouvez définir un contrôleur d'agrégat lorsque celui-ci est partagé par plusieurs classes. Le trafic provenant de deux ports différents peut être configuré à des fins de contrôle. Un contrôleur d'agrégat peut être affecté à plusieurs classes à l'intérieur d'un adressage de réglementations, mais il ne peut pas être utilisé pour différents adressages de réglementations.

Single (Simple) Configure la classe pour utiliser des actions sur dépassement et des débits configurés manuellement.

Aggregate Policer (Contrôleur d'agrégat) Contrôleurs d'agrégat définis par l'utilisateur.

Ingress Committed Information Rate (CIR) (Débit minimum garanti en entrée (CIR)) CIR en bits par seconde. Ce champ ne compte que lorsque la valeur **Police** (Contrôleur) est configurée sur **Single** (Simple).

Ingress Committed Burst Size (CBS) (Taille des rafales garantie (CBS) en entrée) CBS en octets par seconde. Ce champ ne compte que lorsque la valeur **Police** (Contrôleur) est configurée sur **Single** (Simple).

Exceed Action (Action si dépassement) Action effectuée si des paquets entrants dépassent le CIR. Ce champ ne compte que lorsque la valeur **Police** (Contrôleur) est configurée sur **Single** (Simple). Ce champ peut prendre les valeurs suivantes :

Drop (Rejet) Rejette les paquets qui dépassent la valeur CIR définie.

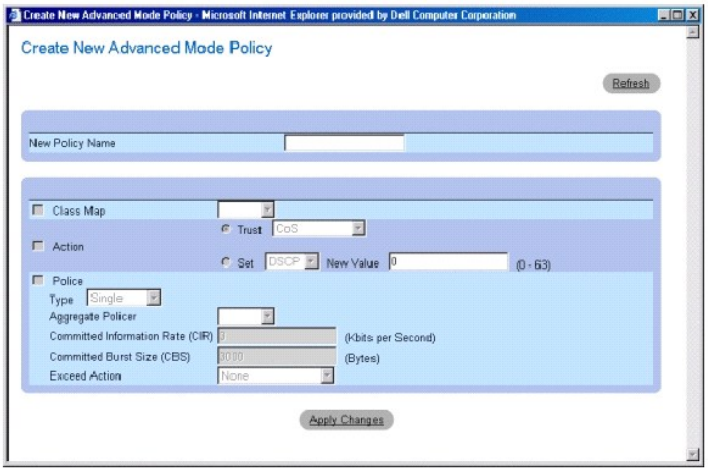
Remark DSCP (Nouveau marquage DCSP) Marque à nouveau les valeurs DSCP des paquets qui dépassent la valeur CIR définie.

None (Aucune action) Transmet les paquets qui dépassent la valeur CIR définie.

Ajout d'une réglementation et de sa première classe

1. Ouvrez la page **QoS Policy** (Réglementation QdS).
2. Cliquez sur **Add** (Ajouter) pour ouvrir la page **Create New Advanced Mode Policy** (Création d'une nouvelle réglementation pour le mode avancé).

Figure 10-17. Page Création d'une nouvelle réglementation pour le mode Avancé



3. Entrez un nom pour la réglementation dans le champ **New Policy Name** (Nom de la nouvelle réglementation).
4. Effectuez l'une des opérations suivantes :
   - Pour configurer un adressage de classes pour la classe, cliquez sur **Class Map** (Adressage de classes) et sélectionnez un adressage de classes dans le menu déroulant.
   - Pour configurer une action de passage en mode Confiance de la classe, cliquez sur **Action**, **Trust** (Confiance) et sélectionnez une méthode dans le menu déroulant.
   - Pour configurer des actions Set/Mark (Configurer/Marquer), cliquez sur **Set** (Configurer), sélectionnez une méthode dans le menu déroulant et entrez une valeur dans le champ **New Value** (Nouvelle valeur).
5. Pour contrôler le trafic d'une classe, cliquez sur **Police** (Contrôleur) et sélectionnez un type de contrôleur dans le menu déroulant.
   - Pour configurer un contrôleur d'agrégat, choisissez-en un dans le menu déroulant **Aggregate Policer** (Contrôleur d'agrégat).
   - Pour configurer un contrôleur simple, renseignez les champs **Committed Information Rate (CIR)** (Débit minimum garanti (CIR)), **Committed Burst Size (CBS)** (Taille des rafales garantie (CBS)) et **Exceed Action** (Action si dépassement).
6. Cliquez sur **Apply Changes** (Appliquer les modifications).

La réglementation et sa première classe sont créées et le périphérique est mis à jour.

Ajout d'une classe

1. Ouvrez la page **QoS Policy** (Réglementation QdS).

2. Sélectionnez une réglementation dans le menu déroulant.
3. Modifiez les champs de la page et cliquez sur **Apply Changes** (Appliquer les modifications).

La classe est ajoutée à la réglementation et le périphérique est mis à jour.

Suppression de réglementations

1. Ouvrez la page **QoS Policy** (Réglementation QdS).
2. Cliquez sur **Show All** (Afficher tout) pour ouvrir la page **Policy Table** (Table des réglementations).
3. Cliquez sur **Remove** (Supprimer) en regard de chaque réglementation à supprimer, puis sur **Apply Changes** (Appliquer les modifications).

Les réglementations sont supprimées du système et le périphérique est mis à jour.

Définition de réglementations à l'aide de commandes CLI

Tableau 10-15. Commandes CLI Reglementation

Commande CLI	Description
policy-map *policy-map- name*	Crée un adressage de réglementations et passe en mode de configuration des adressages de réglementations.
class *class-map-name* [access-group *acl-name*]	Définit la classification du trafic et passe en mode de configuration des adressages de réglementations.
trust [cos | dscp | tcp-udp-port]	Configure l'état Confiance qui sélectionne la valeur que QdS utilise comme source de la valeur DSCP interne.
set {dscp *new-dscp* | queue *queue-id* | cos *new-cos*}	Configure de nouvelles valeurs dans le paquet IP. Remarque : Cette commande et la commande de passage en mode Confiance s'excluent mutuellement.
police *committed-rate- bps committed-burst- byte* [exceed-action {drop | policed-dscp- transmit}]	Définit un contrôleur simple pour le trafic classé.
qos aggregate-policer *aggregate-policer-name committed-rate-bps excess-burst-byte* exceed-action {drop | policed-dscp-transmit}	Définit les paramètres de contrôle qui peuvent être appliqués à plusieurs classes de trafic à l'intérieur du même adressage de réglementation.

Vous trouverez ci-dessous un exemple de commande CLI :

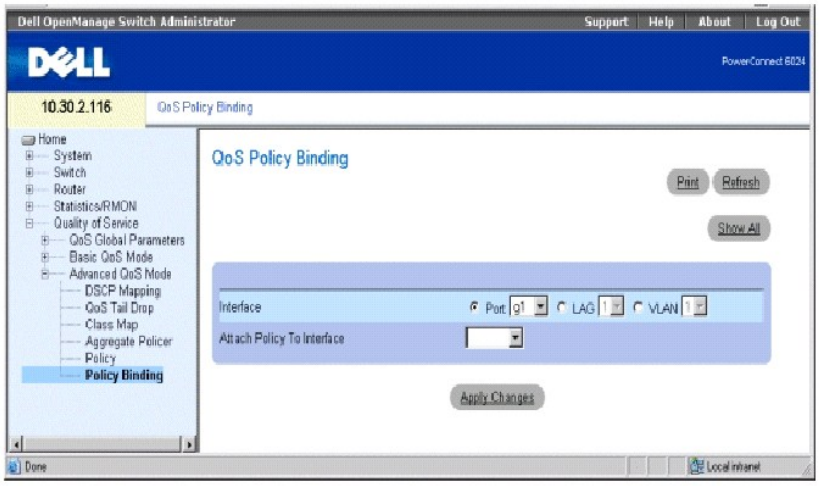
```
Console (config)# policy map policy1

Console (config-pmap)# class class1 access-group dell

Console (config-pmap)# trust cos

Console (config-pmap)# set dscp 56

Console (config-pmap)# police 124000 96000 exceed-action drop

Console (config-pmap)# exit
```

```
Console (config)# qos aggregate-policer policer1 124000 96000 exceed-action drop
```

Application de réglementations à des interfaces

La page **QoS Policy Binding** (Association de réglementations QdS) permet de mettre en place des réglementations sur des interfaces. Pour ouvrir cette page, cliquez sur **Quality of Service** (Qualité de service)→ **Advanced QoS Mode** (Mode QdS avancé)→ **Policy Binding** (Association de réglementations) dans l'*arborescence*.

Figure 10-18. Page Association de réglementations QdS



Interface Sélectionne une interface.

Attach Policy to Interface (Rattacher réglementation à interface) Réglementation mise en place sur l'interface.

REMARQUE : Un adressage de réglementations qui contient une commande de configuration des adressages de réglementations Configurer ou Confiance ou qui possède une classification ACL ne peut pas être rattaché à une interface de sortie.

Association d'une réglementation à une interface

1. Ouvrez la page **QoS Policy Binding** (Association de réglementations QdS).
2. Sélectionnez un type d'interface.

   Seul un adressage de réglementations par interface et par direction est supporté. Toutefois, le même adressage de réglementations peut être appliqué à plusieurs interfaces et plusieurs directions.
3. Sélectionnez un numéro de port, de LAG ou de VLAN dans le menu déroulant correspondant.
4. Sélectionnez une réglementation dans le menu déroulant **Attach Policy to Interface** (Rattacher réglementation à interface).
5. Cliquez sur **Apply Changes** (Appliquer les modifications).

   La réglementation sélectionnée est mise en place sur l'interface et le périphérique est mis à jour.

Suppression de réglementations d'interfaces

1. Ouvrez la page **QoS Policy Binding** (Association de réglementations QdS).

2. Cliquez sur **Show All** (Afficher tout) pour afficher la page **PTI Reference Table** (Table de référence des associations de réglementations aux interfaces).

3. Cliquez sur **Remove** (Supprimer) pour chaque interface dont vous souhaitez supprimer les réglementations et cliquez sur **Apply Changes** (Appliquer les modifications).

La réglementation est supprimée du port mais reste dans le système.

Application de réglementations à des interfaces à l'aide de commandes CLI

Tableau 10-16. Commandes CLI Association de réglementations à des interfaces

Commande CLI	Description
`service-policy input` *`policy-map-name`*	Applique un adressage de réglementations à l'entrée ou à la sortie d'une interface donnée.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config-if)# service-policy input policy1
```

Retour à la page du sommaire

Retour à la page du sommaire

Configuration du commutateur

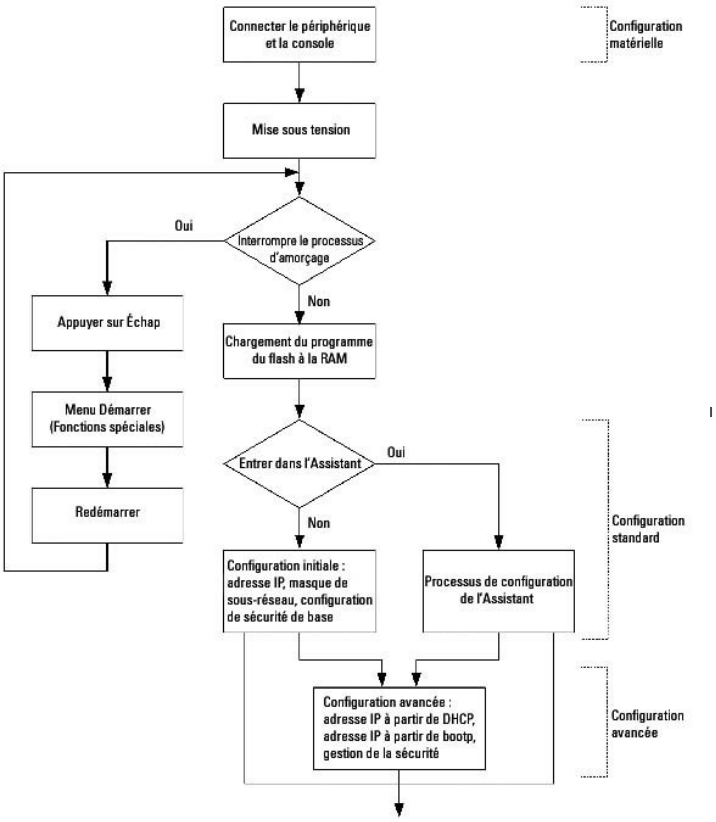
Systèmes Dell PowerConnect 6024/6024F

Cette section décrit la configuration initiale du périphérique.

Une fois toutes les connexions externes du périphérique en place, vous devez connecter celui-ci à un terminal de façon à pouvoir contrôler diverses procédures (démarrage, etc.). La Figure 5-1 indique l'ordre des procédures d'installation et de configuration. Pour la configuration initiale, la procédure standard est effectuée. D'autres fonctions peuvent être utilisées, mais leur exécution interrompt l'installation et réinitialise le système. Cette option est décrite ultérieurement dans cette section.

AVIS : Avant toute chose, lisez les notes de mise à jour relatives à ce produit. Vous pouvez les télécharger à partir de l'adresse **www.support.dell.com**.

Figure 5-1. Ordre des procédures d'installation et de configuration



Informations de configuration générale

Votre commutateur est fourni avec des fonctionnalités et une configuration prédéfinies.

Négociation automatique

La négociation automatique permet à un périphérique de négocier un mode de fonctionnement et de partager des informations avec un autre périphérique via une liaison point à point. Cette fonctionnalité configure automatiquement les deux périphériques de manière à profiter du maximum de leurs capacités.

La négociation automatique est entièrement exécutée dans les couches physiques lors de l'initialisation des liaisons, sans aucune charge supplémentaire imposée aux couches de protocole MAC ou supérieures. La négociation automatique permet aux ports d'exécuter les fonctions suivantes :

- Annonce des capacités
- Accusé de réception et compréhension des modes de fonctionnement communs aux deux périphériques
- Refus d'utiliser des modes de fonctionnement qui ne sont pas partagés par les deux périphériques
- Configuration des deux ports sur le mode de fonctionnement commun le plus élevé pris en charge

Si vous connectez un port du commutateur à la carte d'interface réseau (NIC) d'une station de travail ou d'un serveur qui ne prend pas en charge la négociation automatique ou sur lequel celle-ci n'est pas activée, le port de commutation et la carte NIC doivent être définis manuellement sur la même vitesse et en mode duplex à l'aide de l'interface de navigation Web ou des commandes CLI.

AVIS : Si la station qui partage la liaison tente de négocier automatiquement avec un port qui a été configuré manuellement en duplex intégral, la négociation automatique aboutit à une tentative de fonctionnement de la station en mode semi-duplex. L'incompatibilité qui en résulte peut conduire à une perte de trame significative. Ce phénomène est inhérent aux normes utilisées par la négociation automatique.

Paramètres par défaut des ports de commutation

Le tableau suivant décrit les paramètres par défaut du port de commutation.

Tableau 5-1. Paramètres par défaut des ports

Fonction	Paramètre par défaut
Vitesse et mode du port	1000M Auto-negotiation (Négociation automatique 1000M)
État de transmission du port	Enabled (Activé)
Prévention des blocages en tête de ligne	On (Activé)
Contrôle de flux	Off (Désactivé)
Contre-pression	Off (Désactivée)

Vous trouverez ci-dessous un exemple de modification de la vitesse du port sur le port g1 à l'aide des commandes CLI :

```
Console (config)# interface ethernet g1

Console (config-if)# speed 100
```

Vous trouverez ci-dessous un exemple d'activation du contrôle de flux sur le port g1 à l'aide des commandes CLI :

```
Console (config)# interface ethernet g1

Console (config-if)# flowcontrol on
```

Vous trouverez ci-dessous un exemple d'activation de la contre-pression sur le port g1 à l'aide des commandes CLI. La contre-pression ne peut être activée qu'en mode de fonctionnement à 10 Mo/s.

```
Console (config)# interface ethernet g1

Console (config-if)# speed 10

Console (config-if)# back-pressure
```

Configuration de la connexion du terminal

Votre commutateur requiert les paramètres suivants pour la configuration de la connexion du terminal :

- no parity
- one stop bit
- 8 data bits

Débit

Les débits en baud peuvent être modifiés manuellement de manière à correspondre aux valeurs suivantes :

- 2400
- 4800
- 9600
- 19 200
- 115 200

REMARQUE : Le débit par défaut est 115 200 bauds.

REMARQUE : L'arrêt du périphérique ne rétablit pas le débit par défaut. Celui-ci doit être configuré de manière spécifique.

REMARQUE : La configuration du débit en bauds de la Console n'est pas sauvegardée dans le fichier de configuration générale du commutateur. Elle est directement stockée dans la mémoire permanente du commutateur.

Vous trouverez ci-dessous un exemple de configuration pour la modification du débit par défaut à l'aide des commandes CLI :

```
Console# configure

Console (config)# line Console

Console (config-line)# speed 115200
```

Autres exigences en matière de configuration

Les éléments suivants sont requis pour le téléchargement du logiciel intégré et pour la configuration du périphérique :

- Terminal ASCII (ou émulation) connecté au port série (câble croisé) situé à l'avant du périphérique

- Adresse IP affectée au commutateur pour permettre son contrôle à distance via Telnet, SSH, etc.

REMARQUE : Le processus de configuration ne définit qu'un seul port.

Amorçage du commutateur

Si le système est mis sous tension alors que le terminal local est déjà connecté, le commutateur effectue un POST (auto-test de mise sous tension). 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'amorçage.

Si un problème critique est détecté, le flux du programme s'arrête. Si le POST réussit, une image exécutable valide est chargée dans la mémoire vive (RAM).

Les messages de POST qui s'affichent sur le terminal indiquent la réussite ou l'échec du test.

Pour démarrer le commutateur, effectuez les étapes suivantes :

1. Assurez-vous que le câble ASCII est connecté au terminal.
2. Connectez le bloc d'alimentation au commutateur.
3. Allumez le commutateur.

Le POST 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 :

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

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

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

Testing CPU PCI Bus Device Configuration.........PASS



BOOT Version 1.0.0.13 Date 13-Aug-2003 Time 15:28:31



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

Le processus d'amorçage dure environ 30 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.

À ce stade, vous pouvez accéder au menu **Startup** (Démarrer) pour exécuter des procédures particulières. Dans ce cas, appuyez sur la touche <Échap> ou <Entrée> moins de deux secondes après l'affichage du message d'amorçage automatique. Pour plus d'informations sur le menu **Démarrer**, reportez-vous à la section «Fonction du menu Startup (Démarrer)».

Si vous n'intervenez pas en appuyant sur la touche <Échap> ou <Entrée>, l'amorçage se poursuit et le système décompresse le code dans la mémoire 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.

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

```
Preparing to decompress...



Decompressing SW from image-1

d04000

OK

Running from RAM...



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

** Running SW Ver. 1.0.1.06 Date 15-Sep-2003 Time 17:48:07 **

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



HW version is 00.01.64

Base Mac address is: 00:00:b0:16:00:00

Dram size is : 256M bytes

Dram first block size is : 235520K bytes

Dram first PTR is : 0x1800000

Dram second block size is : 1984K bytes

Dram second PTR is : 0xFE00000

Flash size is: 16M

Tuning File info. Ver: 0.2.80 Creation date: Aug 20 2003 11:20:13

PowerConnect 6024

Tapi Version: v1.1a1-P18
```

```
Core Version: v1.1a1-P18

18-May-2003 16:24:41 %INIT-I-InitCompleted: Initialization task is completed

Start the sync process between devices 0 - 1

Sync OK

18-May-2003 16:24:41 %Box-W-PS-STAT-CHNG: PS# 1 status changed - not operational

.

18-May-2003 16:24:41 %Box-I-PS-STAT-CHNG: PS# 2 status changed - operational.

18-May-2003 16:24:41 %Box-W-FAN-STAT-CHNG: FAN# 1 status changed - operational.

18-May-2003 16:24:41 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

Console> 18-May-2003 16:24:41 %DELL-I-STATUS: The product global status has chan

ged from ok to non-critical at time 900.

18-May-2003 16:24:42 %LINK-W-Down: g1

18-May-2003 16:24:42 %LINK-W-Down: g2
```

Une fois le commutateur amorcé, l'invite du système apparaît (`Console>`) et le processus de configuration du commutateur peut être lancé à partir du terminal local. Toutefois, avant de configurer le commutateur, assurez-vous que la version du logiciel installé sur le périphérique est à jour. Si nécessaire, téléchargez et installez la dernière version. Reportez-vous à la section «Téléchargement des logiciels et réamorçage».

Présentation de la configuration

Votre commutateur prend en charge un port de gestion hors bande Ethernet 10/100 Mb/s directement raccordé au périphérique. Ce port prend en charge les applications de gestion administrateur et système. Le port hors bande est considéré comme une interface IP vers le système et toutes les interfaces de gestion sont disponibles sur ce port. Le port hors bande ne gère pas le trafic utilisateur. Les paquets de données ne sont pas basculés ni acheminés d'un port intrabande (Ethernet ou non hors bande) vers le port hors bande.

Avant de procéder à la configuration initiale du périphérique, procurez-vous les informations suivantes auprès de l'administrateur de réseau :

- Adresse IP du port hors bande
- Masque de sous-réseau IP du réseau
- Adresse IP de la passerelle (routeur de saut suivant) par défaut permettant de configurer la route par défaut

Il existe deux types de configuration : la configuration initiale définit les fonctions de base en matière de configuration et de sécurité, tandis que la configuration avancée inclut la configuration de l'adresse IP dynamique et permet de mettre en place des fonctions de sécurité plus évoluées.

AVIS : 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

Le configuration initiale peut être définie à l'aide de l'Assistant Configuration ou de l'interface de ligne de commande. L'Assistant Configuration se lance automatiquement lorsque le fichier de configuration du périphérique est vide. Pour appeler l'interface de ligne de commande, tapez [ctrl+z].

Ce guide explique l'utilisation de l'Assistant Configuration pour la configuration initiale du périphérique. L'Assistant Configuration configure les champs suivants.

- Chaîne de communauté SNMP et adresse IP du système de gestion SNMP (facultatif)
- Nom d'utilisateur et mot de passe
- Adresse IP du périphérique
- Adresse de la passerelle hors bande par défaut

Une fois que le périphérique a terminé le POST et est initialisé, le message suivant s'affiche :

```
Welcome to Dell Easy Setup Wizard (Bienvenue sur l'Assistant Configuration aisée de Dell)

The Setup Wizard guides you through the initial switch configuration, and gets you up and running easily and quickly. (L'Assistant
Configuration vous guide tout au long de la configuration initiale du commutateur, et vous permet d'être rapidement et facilement
opérationnel.) You can also skip the setup wizard, and enter CLI mode to manually configure the switch if you prefer. (Vous pouvez
également vous passer de l'Assistant Configuration et entrer en mode CLI pour configurer le commutateur manuellement si vous le
souhaitez.)

You can exit the Setup Wizard at any time by entering [ctrl+Z]. (Vous pouvez quitter l'Assistant Configuration à tout moment en tapant
[ctrl+Z].)

The system will prompt you with a default answer; by pressing enter, you accept the default. (Le système vous propose une réponse par
défaut ; vous pouvez l'accepter en appuyant sur Entrée.)

After you configure basic settings using the Setup Wizard, you can manage the device from the Out-of-band management port. (Après avoir
configuré les paramètres de base à l'aide de l'Assistant Configuration, vous pouvez gérer le périphérique à partir du port de gestion
hors bande.)

Would you like to enter the setup wizard? (Souhaitez-vous entrer dans l'Assistant Configuration ?) [Y/N] Y (O/N [O])
```

1. Si vous entrez [N], vous l'Assistant Configuration se ferme. Si vous n'entrez pas de réponse dans les 60 secondes, l'Assisant Configuration se ferme automatiquement et l'invite de Console CLI s'affiche. Si entrez [Y] (O), l'Assistant Configuration fournit des directives interactives tout au long de la configuration initiale du périphérique.

REMARQUE : Si vous n'entrez pas de réponse dans les 60 secondes, et que le réseau dispose d'un serveur BootP, une adresse est extraite du serveur BootP.

REMARQUE : L'utilisateur peut quitter l'Assistant Configuration à tout moment en tapant [ctrl+z].

Assistant Étape 1

Si vous tapez [Y] (O), le message suivant s'affiche :

The system is not setup for SNMP management by default (Le système n'est pas configuré pour la gestion SNMP par défaut). To manage the switch using SNMP (required for Dell Network Manager) you can : (Pour gérer le commutateur à l'aide de SNMP [requis pour le gestionnaire de réseau Dell], vous pouvez :)

- Setup the initial SNMP version 2 account now. (Configurer le compte SNMP initial version 2 maintenant.)
- Return later and setup the SNMP version 2 account. (Revenir plus tard pour configurer le compte SNMP version 2.) (For more information on setting up a SNMP version 2 account, see the user documentation) (Pour en savoir plus sur la configuration du compte SNMP version 2, reportez-vous à la documentation de l'utilisateur).

Would you like to setup the SNMP management interface now? (Souhaitez-vous configurer l'interface de gestion SNMP maintenant ?) [Y/N] Y ([O/N] O)

2. Tapez [N] pour passer à l'étape 2 ou [Y] pour poursuivre avec l'Assistant Configuration. Si vous tapez [Y] (O), le message suivant s'affiche :

To setup the SNMP management account you must specify the management system IP address and the «community string» or password that the particular management system uses to access the switch. (Pour configurer le compte de gestion SNMP, vous devez spécifier l'adresse IP du système de gestion et la «chaîne communautaire» ou mot de passe utilisé par ce système de gestion particulier pour accéder au commutateur.) The wizard automatically assigns the highest access level [Privilege Level 15] to this account (L'Assistant assigne automatiquement le plus haut niveau d'accès [Niveau de privilège 15] à ce compte). You can use Dell Network Manager or other management interfaces to change this setting later, and to add additional management system later. (Vous pouvez utiliser le gestionnaire de réseau Dell ou une autre interface de gestion pour modifier ce paramètre et ajouter un autre système de gestion dans le futur.) For more information on adding management systems, see the user documentation. (Pour en savoir plus sur l'ajout de systèmes de gestion, reportez-vous à la documentation de l'utilisateur.)

To add a management station: (Pour ajouter une Management station :)

Please enter the SNMP community string to be used: (Entrez le nom de la chaîne de communauté SNMP à utiliser :)

Please enter the Management System IP address(A.B.C.D) or wildcard (0.0.0.0) to manage from any Management Station: (Entrez l'adresse IP du système de gestion (A.B.C.D) ou le caractère générique (0.0.0.0) à gérer à partir de n'importe quelle station de gestion :)

3. Tapez ce qui suit :
   - Chaîne de communauté SNMP utilisateur, par exemple «MYSETUPWIZARD»
   - Adresse IP du système de gestion, par exemple «0.0.0.0».
4. Appuyez sur Entrée.

Assistant Étape 2

Le message suivant s'affiche :

Now we need to setup your initial privilege (Level 15) user account. (Maintenant il faut configurer votre compte utilisateur privilège initial (Niveau 15).) This account is used to login to the CLI and Web interface. (On utilise ce compte pour se connecter aux interfaces CLI et Web.) You may setup other accounts and change privilege levels later. (Vous pouvez configurer d'autres comptes et modifier les niveaux de privilège plus tard.) For more information on setting up user accounts and changing privilege levels, see the user documentation. (Pour en savoir plus sur la configuration des comptes utilisateur et la modification des niveaux de privilège, reportez-vous à la documentation de l'utilisateur.)

To setup a user account: (Pour configurer un compte utilisateur :)

Please enter the user name: (Veuillez entrer le nom de l'utilisateur :)

Please enter the user password: (Veuillez entrer le mot de passe de l'utilisateur :)

Please reenter the user password: (Veuillez entrer de nouveau le mot de passe de l'utilisateur :)

5. Tapez ce qui suit :
    - Nom d'utilisateur, par exemple «admin»
    - Mot de passe et confirmation du mot de passe.

REMARQUE : Si le premier et le deuxième mot de passe ne sont pas saisis à l'identique, l'Assistant vous invite à entrer des mots de passe identiques.

6. Appuyez sur **Entrée**.

Assistant Étape 3

7. Le message suivant s'affiche :

```
Next, an IP address is setup. (Ensuite, une adresse IP est configurée.) The IP address is defined on the OOB port. (L'adresse IP est définie sur le port OOB.) This is the IP address you use to access the CLI, Web interface, or SNMP interface for the switch. (Cette adresse IP est celle que vous devez utiliser pour accéder à la CLI, à l'interface Web ou SNMP du commutateur.)

To setup an IP address: (Pour configurer une adresse IP :)

Please enter the device IP address(A.B.C.D): (Entrez l'adresse IP du périphérique (A.B.C.D) :)

Please enter the IP subnet mask (A.B.C.D or /nn): (Veuillez entrer le masque de sous-réseau IP (A.B.C.D ou /nn) :)
```

8. Entrez l'adresse IP et le masque de sous-réseau IP, par exemple 192.168.1.100 comme adresse IP et 255.255.255.0 comme masque de sous-réseau IP.

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

9. Appuyez sur **Entrée**.

Assistant Étape 4

Le message suivant s'affiche :

```
Finally, setup the default gateway/ (Enfin, configurez la passerelle par défaut.) Please enter the gateway IP address from which this network is reachable (e.g. 192.168.1.1): (Entrez l'adresse IP de la passerelle par défaut qui permet l'accès à ce réseau (192.168.1.1 par exemple) :)
```

10. Entrez la passerelle par défaut.
11. Appuyez sur Entrée. Les informations suivantes s'affichent (selon les paramètres utilisés comme exemple) :

```
This is the configuration information that has been collected: (Voici les informations de configuration qui ont été réunies :)

SNMP Interface = MYSETUPWIZARD@0.0.0.0 (Interface SNMP = MYSETUPWIZARD@0.0.0.0)

User Account setup = admin (Configuration compte utilisateur = admin)

Password = ********** (Mot de passe = **********)

Management IP address = 192.168.1.100 255.255.255.0 (Adresse IP de gestion = 192.168.1.100 255.255.255.0)
```

```
Default Gateway = 192.168.1.1 (Passerelle par défaut = 192.168.1.1)
```

Assistant Étape 5

Le message suivant s'affiche :

```
If the information is correct, please select (Y) to save the configuration, and copy to the start-up configuration file. (Si les informations sont correctes, veuillez sélectionner (Y) pour enregistrer la configuration et copier dans le fichier de configuration de démarrage.) If the information is incorrect, select (N) to discard configuration and restart the wizard: (Si les informations sont incorrectes, sélectionnez (N) pour annuler la configuration et redémarrer l'Assistant :) [Y/N] (O/N)
```

12. Tapez [N] pour redémarrer directement l'Assistant Configuration ou [Y] pour terminer la configuration. Si vous tapez [Y] (O), le message suivant s'affiche :

```
Configuring SNMP management interface. (Configuration interface de gestion SNMP.)

Configuring user account..... (Configuration compte utilisateur.....)

Configuring IP and subnet..... (Configuration IP et sous-réseau.....)

.............................

Thank you for using Dell Easy Setup Wizard. (Merci d'avoir utilisé l'Assistant Configuration aisée de Dell.) You will now enter CLI mode. (Vous entrez maintenant en mode CLI.)
```

Assistant Étape 6

L'invite CLI s'affiche.

Il est maintenant possible de gérer le périphérique depuis le port Console déjà connecté ou à distance au moyen de l'interface hors bande définie au cours de la configuration initiale.

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).

Lors de la configuration/réception d'adresses IP via DHCP et BootP, la configuration reçue de la part de ces serveurs inclut l'adresse IP et éventuellement le masque de sous-réseau et la passerelle par défaut.

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

Lorsque le protocole DHCP est utilisé pour obtenir une adresse IP, le périphérique agit en tant que client DHCP.

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.

- Allocation d'adresses IP dynamiques (sur un port intrabande) :

```
Console# configure

Console (config)# interface ethernet g1

Console (config-if)# ip address dhcp hostname <string>

Console (config-if)# exit
```

- Affectation d'adresses IP dynamiques (sur un port hors bande)

```
Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address dhcp hostname dell

Console (config-oob)# exit

Console (config)# exit
```

L'interface reçoit automatiquement l'adresse IP.

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

IP Address    I/F       Type      Directed Broadcast

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

100.1.1.1/24  vlan 1    static    disable


OOB ip interfaces


Gateway IP Address       Activity status

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

10.6.12.1                active
```

```
IP Address      I/F                   Type

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

10.6.12.20/24   Oob-eth 1             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 commutateur récupère le nouveau fichier de configuration et démarre à partir de celui-ci. Il active alors le DHCP en suivant les instructions du 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 commutateur 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 n'importe quel port et connectez-le à un serveur BootP ou à un sous-réseau contenant ce type de serveur de manière à obtenir l'adresse IP.
2. À l'invite du système, tapez la commande **delete startup configuration** de manière à supprimer la configuration de démarrage de la mémoire flash.

   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

Startup file was deleted

Console# reload

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

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

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

/* the device reboots */
```

Pour vérifier l'adresse IP, 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, Accounting) qui gère les droits d'accès des utilisateurs, les privilèges et les méthodes de gestion. AAA utilise des bases de données utilisateur à la fois locales et distantes. Le cryptage des données est traité via le mécanisme SSH.

Le système est livré sans mot de passe par défaut ; les mots de passe sont tous définis par l'utilisateur. Si un mot de passe défini par l'utilisateur est perdu, une procédure de récupération peut être lancée à partir du menu **Démarrage**. 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 :

- Console
- Telnet
- SSH
- HTTP
- HTTPS

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

REMARQUE : Lors de la création d'un nom d'utilisateur, la priorité par défaut est «1», ce qui signifie que l'utilisateur peut accéder au système mais pas aux fonctions de configuration. L'accès à la configuration n'est possible que si le niveau de priorité «15» a été défini. 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 Console initial

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

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

Console (config)# aaa authentication enable default line

Console (config)# line Console

Console (config-line)# login authentication default

Console (config-line)# enable authentication default

Console (config-line)# password george
```

- Lorsque vous vous connectez à un périphérique pour la première fois via une session de Console, tapez **george** à l'invite du mot de passe.
- Lorsque vous passez 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
```

- Lorsque vous vous connectez à un périphérique pour la première fois via une session Telnet, tapez `bob` à l'invite du mot de passe.
- Lorsque vous passez 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.
```

- Lorsque vous vous connectez à un périphérique pour la première fois via une session SSH, tapez `jones` à l'invite du mot de passe.
- Lorsque vous passez 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
```

REMARQUE : Vous devez générer un nouveau certificat de cryptographie lors de chaque mise à jour (installation d'une nouvelle version) du logiciel de contrôle sur le périphérique.

Tapez une fois les commandes suivantes lorsque vous configurez une session Console, Telnet ou SSH pour utiliser une session HTTPS.

Activez SSL version 2.0 ou supérieure dans le navigateur Web 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.

Téléchargement des logiciels et réamorçage

Téléchargement d'un logiciel via XModem

Cette section contient des instructions pour le téléchargement des logiciels du périphérique (images système et d'amorçage) à l'aide du protocole XModem de transfert de données pour la mise à jour des fichiers de configuration de sauvegarde.

Pour télécharger un fichier d'amorçage via XModem :

1. Tapez la commande **Console# xmodem: boot**.

   Le commutateur est prêt à recevoir le fichier via le protocole XModem et affiche le texte ci-après :

   ```
   Console# copy xmodem: boot
   ```

   ```
   Please download program using XMODEM.
   ```

   ```
   Console#
   ```

2. Indiquez le chemin d'accès au fichier source dans les 20 secondes qui suivent.

Si le chemin n'est pas indiqué dans les 20 secondes qui suivent, la commande expire.

Pour télécharger un fichier image de logiciel via XModem :

1. Tapez la commande **Console# xmodem: image**.

   Le commutateur est prêt à recevoir le fichier via le protocole XModem.

2. Indiquez le chemin d'accès au fichier source pour commencer le transfert.

   Vous trouverez ci-dessous un exemple des informations qui s'affichent :

```
Console# copy xmodem: image

Please download program using XMODEM.

Console#
```

Téléchargement de logiciels via un serveur TFTP

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

Le commutateur 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 stockée. La nouvelle image téléchargée est enregistrée dans une zone réservée à la copie de l'image système.

Au cours de l'amorçage suivant, le commutateur décompresse et exécute l'image système activée à moins qu'une sélection différente ait été faite.

Pour télécharger une image via un 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. Vérifiez que le fichier à télécharger est enregistré sur le serveur TFTP (fichier DOS).
3. Tapez la commande **Console# show version** pour vérifier quelle version du logiciel est actuellement exécutée sur le périphérique.

   Vous trouverez ci-dessous un exemple des informations qui s'affichent :

```
Console# show version
SW version 3.31.42 ( date 22-Jul-2003 time 13:42:41 )
Boot version 1.31.03 (date 01-Jun-2003 time 15:12:20 )
HW version
```

4. Tapez la commande **Console# show bootvar** pour vérifier quelle version d'image système est active. Vous trouverez ci-dessous un exemple des informations qui s'affichent :

```
Console# show bootvar
Images currently available on the Flash
Image-1 active (selected for next boot)
Image-2 not active
Console#
```

5. Tapez la commande **Console# copy tftp://{adresse tftp}/{nom de fichier} image** pour copier une nouvelle image système vers 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 image
Accessing file file1 on 176.215.31.3...


Loading file1 from
176.215.31.3: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy took 00:01:11 [hh:mm:ss]
```

Les points d'exclamation (!) indiquent que le processus de copie est en cours. 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**. Après cette commande, tapez **Console# show bootvar** pour vérifier que la copie choisie dans la commande du système d'amorçage est sélectionnée pour le prochain amorçage.

   Vous trouverez ci-dessous un exemple des informations qui s'affichent :

```
Console# boot system image-2
Console# sh bootvar
Images currently available on the Flash
Image-1 active
Image-2 not active (selected for next boot)
```

   Si l'image du prochain amorçage n'est pas sélectionnée, le système s'amorce à partir de l'image active (image-1 dans l'exemple).

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

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

8. Tapez **Y**(O) pour réamorcer le commutateur.

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 se charge lorsque le commutateur est allumé.

Pour télécharger un fichier 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. Vérifiez que le fichier à télécharger (fichier **.rfb**) est enregistré sur le serveur TFTP.
3. Tapez la commande **Console# show version** pour vérifier quelle version d'amorçage est actuellement exécutée sur le périphérique.

   Vous trouverez ci-dessous un exemple des informations qui s'affichent :

```
Console# show version
SW version 3.31.42 ( date 22-Jul-2003 time 13:42:41 )
Boot version 1.31.03 (date 01-Jun-2003 time 15:12:20 )
HW version 00.00.01 (date 01-May-2003 time 12:12:20 )
```

4. Tapez la commande **Console# copy tftp://{tftp address}/{file name} boot** pour copier l'image d'amorçage vers le commutateur.

   Vous trouverez ci-dessous un exemple des informations qui s'affichent :

```
Console# copy tftp://176.215.31.3/6024_boot-10013.rfb
Erasing
```

```
file ...done. !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Copy: 393232 bytes copied in 00:00:05 [hh:mm:ss]
```

5. Tapez la commande **reload**.

Le message suivant s'affiche :

```
Console# reload
This command will reset the whole system and disconnect your current session. (Cette commande va réinitialiser tout le système et vous
déconnectera de la session en cours.) Do you want to continue (y/n) [n] ? (Êtes-vous certain de vouloir continuer (o/n) [n] ?)
```

6. Tapez **Y** (O) pour réamorcer le commutateur.

Exemple de processus de configuration

Le but de cette section est de présenter les étapes de base requises pour établir une connexion de gestion de réseau à distance avec le commutateur. Les différentes configurations disponibles sur le périphérique et les commandes correspondantes ne sont pas abordées.

Cette section décrit également comment accéder pour la première fois à un commutateur avec les configurations et les définitions paramétrées en usine. Si une configuration créée précédemment pose problème, effacez le fichier de configuration au démarrage configuration du périphérique à la mise sous tension et redémarrez le périphérique (reportez-vous à la section «Paramètres par défaut du périphérique».

Exigences relatives à la configuration du périphérique

Les composants suivants sont requis pour cet exemple :

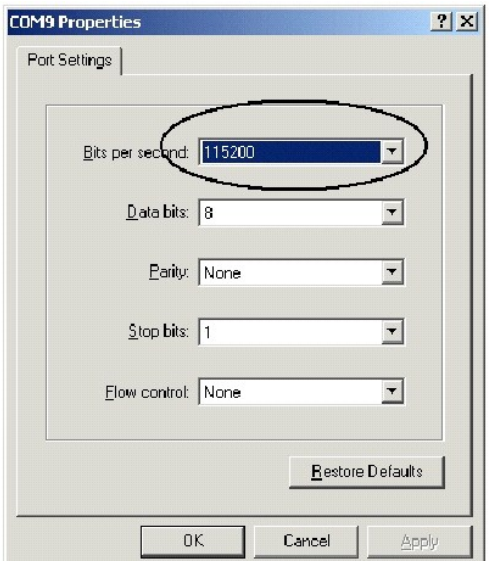
- Commutateur PowerConnect 6024/6024F.
- Station de travail avec les éléments suivants installés :
  - Carte adaptateur réseau
  - Application pour terminal ASCII (Microsoft® Windows® HyperTerminal ou Procomm Plus Terminal par exemple)
  - Une application de navigation
- Câble F2F de simulateur de modem.
- Câble(s) UTP (cat 5) croisé(s) ou droit(s).

Connexion initiale

1. Connectez le commutateur à la station de travail à l'aide du port RS-232.
2. Paramétrez comme suit le terminal ASCII et sélectionnez le port COM approprié.

Cet exemple utilise l'application Windows Hyper Terminal.

Figure 5-2. Fenêtre de propriétés de HyperTerminal



REMARQUE : Le débit en bauds par défaut est de 115 200 pour le nouveau périphérique. Le périphérique peut avoir un autre débit. Si l'utilisation d'un débit de 115 200 ne permet pas d'afficher le terminal du périphérique, essayez avec un autre débit en bauds.

3. Utilisez un câble F2F de simulateur de modem pour connecter la station de travail au commutateur.
4. Insérez le cordon d'alimentation du périphérique dans une prise électrique pour mettre le périphérique sous tension.

L'écran suivant s'affiche :

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

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

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


Booting...


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

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

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

Testing CPU PCI Bus Configuration.................PASS


BOOT Version 1.0.0.13 Date 13-Aug-2003 Time 15:28:31
```

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

À ce stade, vous pouvez accéder au menu **Startup** (Démarrer) pour exécuter des procédures particulières. Sinon, le système continue en décompressant le code dans la mémoire 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'affiche.

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

```
Preparing to decompress...



Decompressing SW from image-1

d04000

OK

Running from RAM...



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

*** Running SW Ver. 1.0.1.06 Date 15-Sep-2003 Time 17:48:07 ***

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



HW version is 00.01.64

Base Mac address is: 00:00:b0:16:00:00

Dram size is : 256M bytes

Dram first block size is : 235520K bytes

Dram first PTR is : 0x1800000

Dram second block size is : 1984K bytes

Dram second PTR is : 0xFE00000

Flash size is: 16M
```

```
Tuning File info. Ver : 0.2.80 Creation date: Aug 20 2003 11:20:13

PowerConnect 6024

Tapi Version: v1.1a1-P18

Core Version: v1.1a1-P18

18-May-2003 16:24:41 %INIT-I-InitCompleted: Initialization task is completed




Start the sync process between devices 0 - 1


Sync OK


18-May-2003 16:24:41 %Box-W-PS-STAT-CHNG: PS# 1 status changed - not operational

.

18-May-2003 16:24:41 %Box-I-PS-STAT-CHNG: PS# 2 status changed - operational.

18-May-2003 16:24:41 %Box-W-FAN-STAT-CHNG: FAN# 1 status changed - operational.

18-May-2003 16:24:41 %Box-I-FAN-STAT-CHNG: FAN# 2 status changed - operational.

Console> 18-May-2003 16:24:41 %DELL-I-STATUS: The product global status has chan

ged from ok to non-critical at time 900.

18-May-2003 16:24:42 %LINK-W-Down: g1

18-May-2003 16:24:42 %LINK-W-Down: g2
```

Le périphérique est prêt à être configuré.

Paramètres par défaut du périphérique

Pour revenir aux paramètres par défaut, utilisez la commande `delete startup-config` à l'invite du mode privileged (#) et réamorcez le périphérique. Le périphérique redémarre avec les paramètres par défaut.

```
Console>

Console> enable

<Console# delete startup-config

Startup file was deleted

Console# reload

This command will reset the whole system and disconnect your current

session. Do you want to continue (y/n) [n] ?

y



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

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

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

.

.

.

.
```

Activation de la gestion à distance

1. Tapez comme suit la commande **enable** sur la Console pour accéder au mode d'affichage Privileged EXEC (EXEC privilégié) :

```
Console> enable

Console#
```

2. Connectez la station de gestion (PC) au périphérique via l'un des ports Ethernet ou via un réseau connecté au périphérique, à l'aide d'un câble CAT5.

   Le port g1 est utilisé dans cet exemple.

3. Vérifiez (au niveau du terminal ASCII) que l'état de l'interface est passé sur «up» (disponible) et que l'état du STP est passé sur Forwarding (transmission) (au bout de 30 secondes) :

```
Console#


01-Jan-2000 01:43:03 %LINK-I-Up: Vlan 1


01-Jan-2000 01:43:03 %LINK-I-Up: g1


01-Jan-2000 01:43:34 %STP-I-PORTSTATUS: Port g1: STP status Forwarding
```

4. Tapez comme suit la commande **config** sur la Console pour accéder au mode d'affichage Configuration :

```
Console# config
```

5. Tapez comme suit la commande **interface vlan** sur la Console pour accéder au mode d'affichage Configuration VLAN, via VLAN 1 (marque = 1) par défaut :

```
Console (config)# interface vlan 1


Console (config-if)#
```

6. Définissez une adresse IP pour le périphérique en affectant une adresse IP (50.1.1.1 dans cet exemple) au VLAN contenant l'interface connectée à la station de gestion. Si la station de gestion est directement connectée à l'interface, l'adresse IP du VLAN doit avoir le même sous-réseau que la station de gestion.

```
Console (config)#


Console (config-if)# ip address 50.1.1.1 225.0.0.0


Console (config-if)#
```

7. Si la station de gestion fait partie d'un réseau distant et n'est pas directement connectée à l'interface, définissez un chemin statique.

   L'adresse IP configurée doit appartenir au même sous-réseau que celle des interfaces IP du périphérique. Dans cet exemple, l'adresse statique est 50.1.1.100.

```
Console (config-if)# exit


Console (config)# ip route 0.0.0.0.0.0.0.0 50.1.1.100


Console (config)#
```

8. À l'aide de la commande ping, interrogez la station de gestion à partir du commutateur pour vous assurer que la connexion est opérationnelle.

   Attendez 30 secondes pour que le port passe en mode «STP forwarding» avant d'effectuer cette opération. L'IP de la station de gestion est 50.1.1.2 (dans cet exemple) :

```
Console (config)#

Console (config)# exit

Console# ping 50.1.1.2

64 bytes from 50.1.1.2: icmp_seq=1. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=2. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=3. time=0 ms

64 bytes from 50.1.1.2: icmp_seq=4. time=0 ms



----50.1.1.2 PING Statistics----

4 packets transmitted, 4 packets received, 0% packet loss

round-trip (ms) min/avg/max = 0/0/0

Console#
```

9. Définissez un nom d'utilisateur et un mot de passe pour permettre à un utilisateur distant d'accéder au périphérique avec le niveau de privilège le plus élevé (15) via HTTP et HTTPS.

   Dans cet exemple, le nom d'utilisateur et le mot de passe sont «Dell» et le niveau de privilège est 15. Les niveaux de privilège vont de 1 à 15, 15 étant le niveau le plus élevé. Le niveau d'accès 15 est le seul niveau permettant d'accéder à l'interface Web.

```
Console# config

Console (config)# username Dell password Dell privilege 15

Console (config)# ip http authentication local

Console (config)# ip https authentication local

Console (config)# crypto certificate generate key_generate

Generating RSA private key, 1024 bit long modulus

Console (config)# ip https server
```

10. Définissez un nom d'utilisateur et un mot de passe pour permettre à un utilisateur local (Console, Telnet, serveur Web) d'accéder au périphérique.

    Dans cet exemple, le nom d'utilisateur et le mot de passe sont «Dell» et le niveau de privilège est 15.

```
Console (config)# username Dell password Dell privilege 15

Console (config)#

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)# passwordtom

Console (config-line)# exit

Console (config)# line telnet

Console (config-line)# login authentication default

Console (config-line)# enable authentication default

Console (config-line)# password bob

Console (config-line)# exit

Console (config)# line ssh

Console (config-line)# login authentication default

Console (config-line)# enable authentication default

Console (config-line)# passwordjones

Console (config-line)# exit
```

11. Enregistrez le fichier **running-config** dans le fichier **startup-config**.

Cela permet de s'assurer que la configuration qui vient de se terminer sera celle utilisée lors du prochain redémarrage du périphérique.

```
Console (config-line)# exit


Console (config)# exit


Console# copy running-config startup-config
```

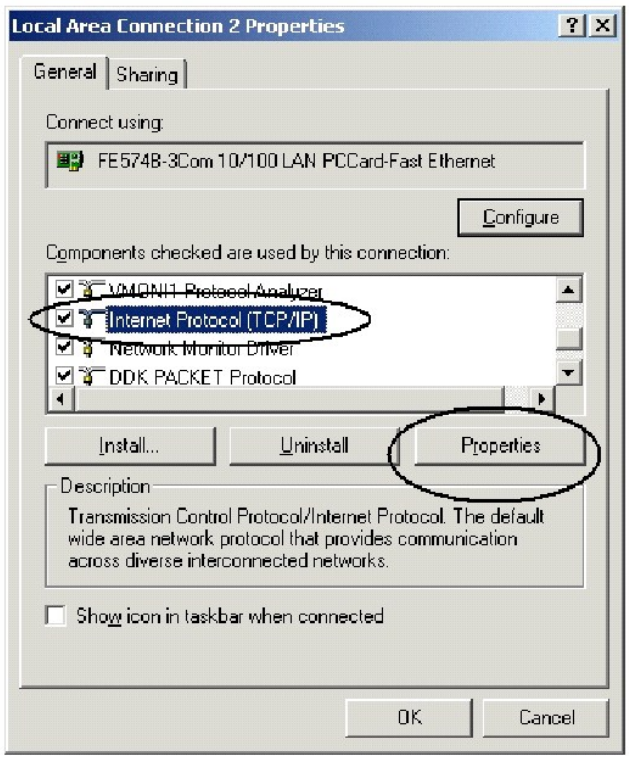
Le périphérique est maintenant configuré et peut être géré via différents options comme Telnet ou l'interface du navigateur Web.

Configuration de l'adresse IP de la station de gestion

1. Sur la station de gestion, cliquez sur **Start** (Démarrer)→ **Settings** (Paramètres)→ **Network and Dial-up Connections** (Connexions réseau et accès à distance).
2. Cliquez avec le bouton droit sur la connexion réseau utilisée pour la gestion, puis cliquez sur **Properties** (Propriétés).

La fenêtre des propriétés de la connexion apparaît.

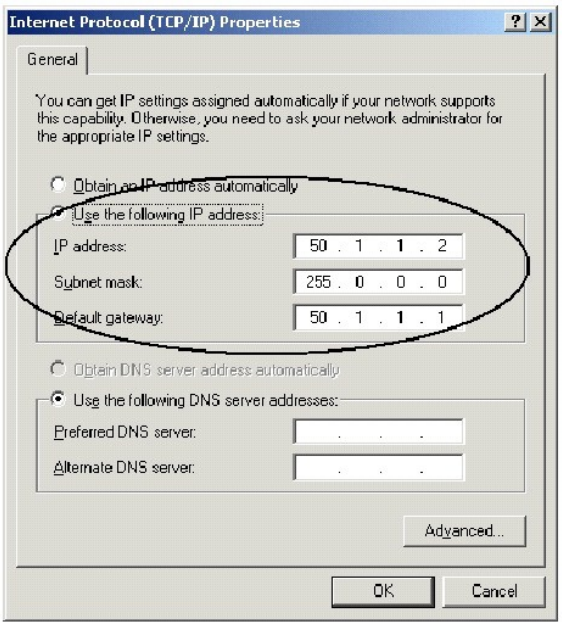
Figure 5-3. Fenêtre de propriétés de la connexion locale



3. Cliquez sur **Internet Protocol (TCP/IP)** (Protocole internet (TCP/IP)), puis sur **Properties** (Propriétés).

La fenêtre **Internet Protocol (TCP/IP) Properties** (Propriétés du protocole Internet (TCP/IP)) s'ouvre.

Figure 5-4. Fenêtre de propriétés du protocole Internet (TCP/IP)



4. Cliquez sur **Use the following IP address** (Utiliser l'adresse IP suivante).
5. Définissez des adresses pour la station de gestion dans les champs **IP address** (Adresse IP), **Subnet mask** (Masque de sous-réseau) et **Default gateway** (Passerelle par défaut).

REMARQUE : Si la station de gestion est connecté à un routeur et non pas directement au commutateur 6024/6024F, la passerelle par défaut doit être configurée en tant qu'adresse IP de l'interface du routeur connecté à la station de gestion (qui mène au commutateur 6024/6024F).

Activation de l'accès Telnet

Utilisez une ligne de commande Windows/DOS ou une application Telnet pour accéder au périphérique via Telnet. Tapez le mot de passe approprié. La connexion est établie avec l'adresse IP définie au niveau du périphérique.

Une fois l'accès autorisé, l'utilisation des commandes est la même que dans la gestion directe du périphérique :

1. Sur la station de gestion, cliquez sur **Start** (Démarrer)→ **Run** (Exécuter).
2. Dans la fenêtre **Run** (Exécuter), tapez cmd et cliquez sur **OK**

L'interface standard de saisie de ligne de commande de Windows apparaît.

3. Tapez la commande **Telnet** et l'adresse IP du périphérique comme ci-dessous :

```
Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-2000 Microsoft Corp.

C:\>telnet 50.1.1.1

11-Aug-20 03 11:14:06 %MSCM-I-NEWTERM: New TELNET connection from 50.1.1.2

Password:***
```

```
Console> enable

Password:***

Console# show ip interface

Proxy ARP is disabled

IP Address     I/F        Type      Directed Broadcast

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

100.1.1.1/24   vlan 1     static    disable


OOB ip interfaces

Gateway IP Address       Activity status

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

10.6.12.1                active


IP Address               I/F                    Type

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

10.6.12.20/24            Oob-eth 1              dhcp
```

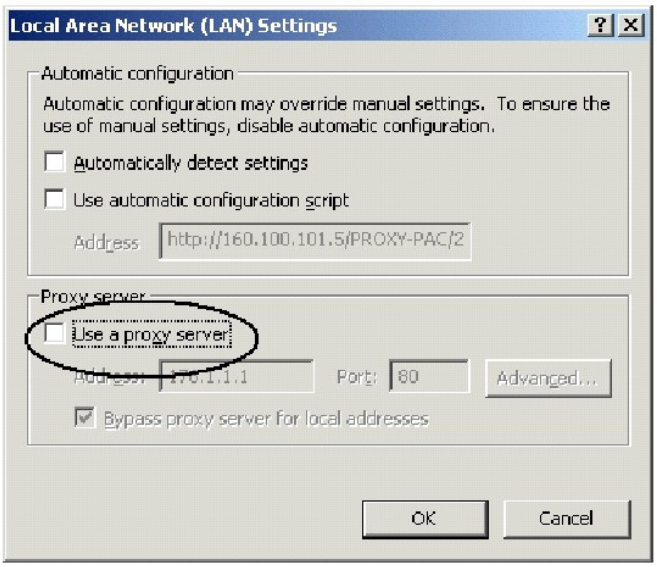
Le commutateur indique l'état de la session Telnet :

```
Console> 01-Jan-2000 02:39:04 %MSCM-I-NEWTERM: New TELNET connection from 50.1.1.2

01Jan-2000 02:39:11 %MSCM-I-TERMTERMINATED: TELNET connection from 50.1.1.2 terminated
```

Activation de l'accès Web (serveur HTTP)

1. Pour éviter certains problèmes liés à l'utilisation d'un serveur proxy HTTP, désélectionnez la case à cocher activant cette option.
   a. Dans Microsoft Internet Explorer, cliquez sur **Tools** (Outils)→ **Internet Options** (Options Internet).
   b. Cliquez sur l'onglet **Connections** (Connexions), puis sur **LAN Settings** (Paramètres réseau local) pour ouvrir la fenêtre **Local Area Network (LAN) Settings** (Paramètres du réseau local (LAN)).
   c. Vérifiez que la case à cocher **Use a proxy server** (Utiliser un serveur proxy) est désactivée, puis cliquez sur **OK**.

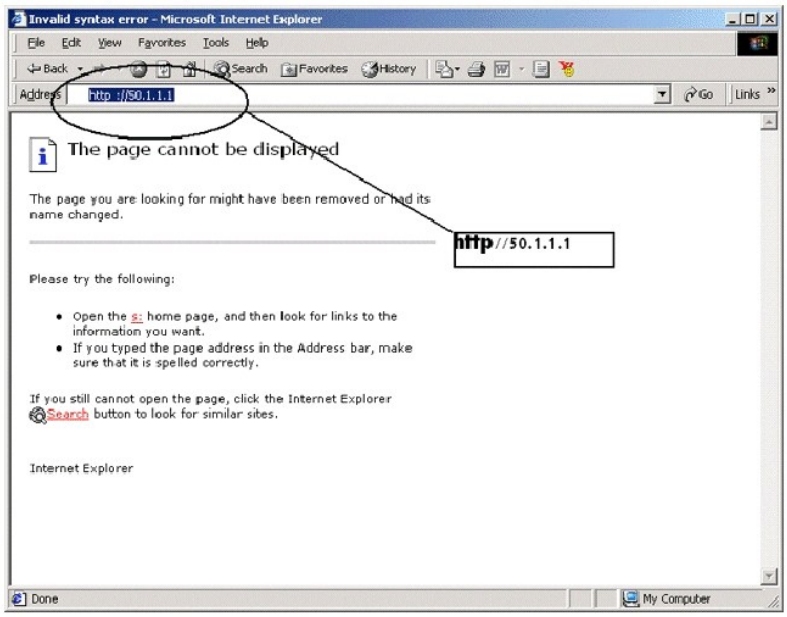
Figure 5-5. Fenêtre des paramètres du réseau local (LAN)



d. Cliquez sur **OK** pour fermer la fenêtre **Internet Options** (Options Internet).

2. Dans la fenêtre du navigateur, tapez l'IP préalablement configuré sur le périphérique (avec ou sans le préfixe http://).

Figure 5-6. Connexion à l'interface Web



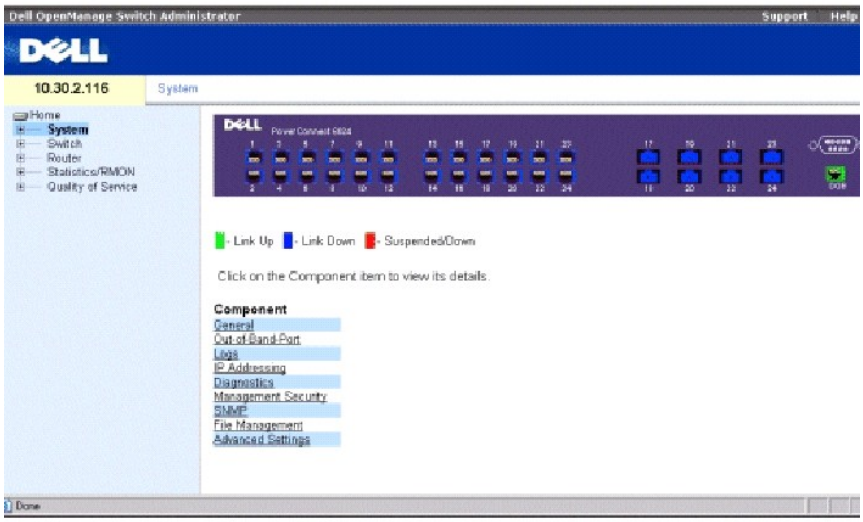
La fenêtre d'authentification du mot de passe s'affiche.

3. Tapez votre nom d'utilisateur et votre mot de passe.

Le Dell OpenManage Switch Administrator s'affiche.

REMARQUE : Si aucun mot de passe n'est défini, n'importe quel mot de passe est accepté.

Figure 5-7. Page Dell OpenManage Switch Administrator



Configuration de l'accès de gestion sécurisé (HTTPS)

Vous pouvez gérer le périphérique de façon sécurisée via le navigateur Web standard, en utilisant le protocole de sécurité SSL (Secure Socket Layer).

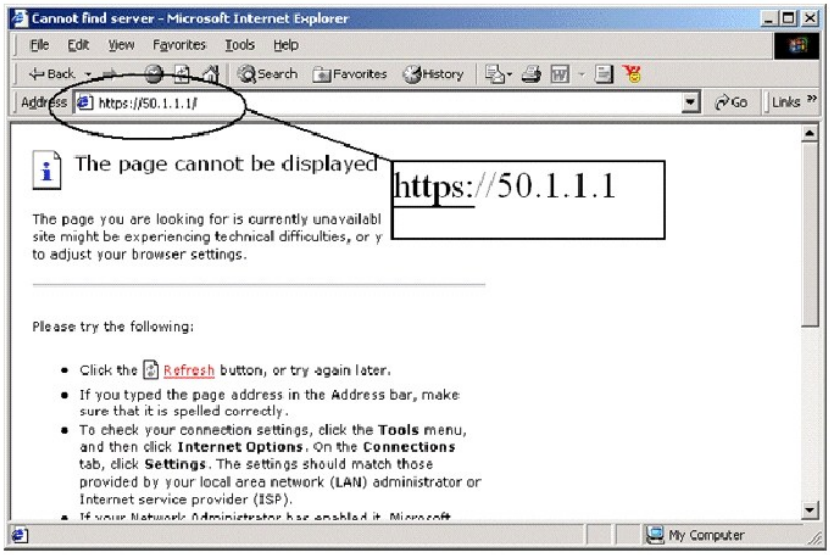
Pour cela, effectuez les opérations suivantes :

1. Configurez le commutateur pour autoriser le serveur HTTPS et créer une clé de sécurité, en utilisant les commandes **ip https server** et **crypto certificate generate key-generate** :

```
Console# configure

Console (config)# ip https server

Console (config)# crypto certificate generate key-generate

Generating RSA private key, 1024 bit long modulus

Console (config)#
```

2. Configurez la station de gestion comme pour une connexion HTTP classique (reportez-vous à la section «Activation de l'accès Web [serveur HTTP]»).
3. Connectez-vous au périphérique via HTTPS en tapant l'adresse `https://<adresse IP du périphérique>` dans la fenêtre du navigateur (saisissez obligatoirement https) :

Figure 5-8. Connexion à l'interface Web via une connexion sécurisée



La fenêtre **Security Alert** (Alerte sécurité) s'ouvre.

4. Cliquez sur **Yes** (Oui) pour accepter le certificat de sécurité (s'il n'est pas authentifié par un tiers).
5. La fenêtre **Enter Network Password** (Saisie du mot de passe réseau) s'ouvre.
6. Tapez votre nom d'utilisateur et votre mot de passe.

La fenêtre Dell OpenManage Switch Administrator du périphérique s'affiche.

Fonctions du menu Startup (Démarrer)

D'autres fonctions de configuration du périphérique sont exécutées à partir du menu **Startup** (Démarrer).

Pour afficher le menu **Startup** (Démarrer) :

1. Pendant l'amorçage, après la fin de la première partie du POST, appuyez sur <Échap> ou <Entrée> dans les deux secondes qui suivent l'affichage du message ci-dessous :

```
Autoboot in 2 seconds -press RETURN or Esc.to abort and enter prom. (Amorçage automatique dans 2 secondes - appuyez sur RETOUR ou Échap pour annuler et accéder à la mémoire PROM.)
```

Le menu **Startup** (Démarrer) contient les fonctions de configuration suivantes :

```
[1] Download Software (Téléchargement des logiciels)

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

[3] Erase Flash Sectors (Effacement des secteurs FLASH)

[4] Password Recovery Procedure (Récupération des mots de passe)
```

```
[5] Enter Diagnostic Mode (Accès au mode Diagnostic)

[6] Back Enter your choice or press 'ESC' to exit (Faites votre choix ou appuyez sur «ÉCHAP» pour sortir) :
```

Les sections qui suivent décrivent les options du menu **Startup** (Démarrer). Par défaut, vous disposez de 25 secondes pour effectuer une sélection une fois le menu affiché.

Seul le personnel du support technique peut utiliser le mode Diagnostic. L'option **Enter Diagnostic Mode** (Accès au mode Diagnostic) du menu **Startup** (Démarrer) n'est donc pas décrite dans ce guide.

Téléchargement des logiciels

Utilisez l'option de téléchargement de logiciels pour remplacer des fichiers corrompus ou mettre à jour ou à niveau le logiciel système.

Pour télécharger un logiciel via le menu **Startup** (Démarrer) :

1. Dans le menu **Startup** (Démarrer), tapez <1>.

   L'invite suivante s'affiche :

   ```
   Downloading code using XMODEM
   ```

2. Si vous utilisez HyperTerminal, cliquez sur **Transfer** (Transfert) dans la barre de menus **HyperTerminal**.
3. Dans le menu **Transfer** (Transfert), cliquez sur **Send File** (Envoi de fichier).

   La fenêtre **Send File** (Envoi de fichier) s'ouvre.

4. Saisissez le chemin d'accès du fichier à télécharger.
5. Assurez-vous que le protocole Xmodem est sélectionné.
6. Cliquez sur **Send** (Envoyer).

   Le logiciel est téléchargé. Le téléchargement peut prendre quelques minutes. L'application d'émulation de terminal, comme HyperTerminal, peut afficher la progression du chargement.

   Après le téléchargement, le périphérique est réamorcé automatiquement.

Effacement du fichier FLASH

Dans certains cas, la configuration du périphérique doit être effacée. Dans ce cas, tous les paramètres qui ont été configurés via l'interface CLI, l'interface du navigateur Web ou SNMP doivent être reconfigurés.

Pour effacer la configuration du périphérique :

1. Dans le menu **Startup** (Démarrer), tapez <2> dans les 6 secondes pour effacer le fichier de mémoire Flash.

   Le message suivant s'affiche :

   ```
   Warning! (Avertissement !) About to erase a Flash file. (Vous êtes sur le point d'effacer un fichier FLASH.)
   ```

```
Are you sure (Y/N)? (Êtes-vous certain de vouloir continuer (O/N) ?) y (o)
```

2. Tapez <Y> (O).

REMARQUE : N'appuyez pas sur <Entrée>.

Le message suivant s'affiche.

```
Write Flash file name (Up to 8 characters, Enter for none.):config File config (if present) will be erased after system initialization
(Tapez le nom du fichier FLASH (8 caractères max., Entrée pour aucun nom) : la config du fichier de config (le cas échéant) sera effacée
après initialisation du système)

======== Press Enter To Continue (Appuyez sur Entrée pour continuer) ========
```

3. Saisissez **config** comme nom de fichier Flash.

La configuration est effacée et le périphérique redémarre.

4. Effectuez la configuration initiale du commutateur.

Effacement des secteurs FLASH

À des fins de dépannage, vous pouvez avoir besoin d'effacer des secteurs FLASH. Si la mémoire FLASH est effacée, tous les fichiers des logiciels doivent être téléchargés et installés à nouveau.

Pour effacer la mémoire FLASH :

1. Dans le menu **Startup** (Démarrer), tapez <3> dans les 6 secondes.

Le message suivant s'affiche :

```
Warning! (Avertissement !) About to erase Flash Memory! (Vous êtes sur le point d'effacer la mémoire FLASH !) FLASH size = 16252928.
blocks = 64 Are you sure (Y/N) (Taille de la mémoire FLASH = 16 252 928 blocs = 64 Êtes-vous certain de vouloir continuer (O/N) ?)
```

2. Tapez <Y> (O) pour confirmer.

Le message suivant s'affiche :

```
Enter First flash block (1 - 63): (Accédez au premier bloc FLASH (1 - 63) :)
```

3. Saisissez le premier bloc Flash à effacer et appuyez sur <Entrée>.

La plage de valeurs est comprise entre 1 et 64. Le message suivant s'affiche :

```
Enter Last flash block (1 - 63): (Accès au dernier bloc Flash (1 - 63) :)
```

4. Saisissez le dernier bloc Flash à effacer et appuyez sur <Entrée>.
5. Le message suivant s'affiche :

```
Are you sure (Y/N) (Êtes-vous certain de vouloir continuer (O/N) ?)
```

6. Tapez <Y> (O) pour confirmer.

Le message suivant s'affiche :

```
Erasing flash blocks 1 - 63: Done. (Effacement des blocs FLASH 1 à 63 : Terminé.)
```

Récupération de mots de passe

Pour récupérer un mot de passe perdu, utilisez l'option **Password Recovery** (Récupération mot de passe) du menu **Startup** (Démarrer). La procédure permet à l'utilisateur d'accéder au périphérique une seule fois sans mot de passe.

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

1. Dans le menu **Startup** (Démarrer), sélectionnez **[4]** et appuyez sur <Entrée>.

   Le mot de passe est supprimé.

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

Port de gestion hors bande (OOB)

Le port de gestion hors bande est un port Ethernet 10/100 Mb/s que vous pouvez utiliser pour vous connecter directement au commutateur et lancer des fonctions de gestion de l'administrateur système. Ce port est considéré comme une interface IP normale vers le système et toutes les interfaces de gestion sont disponibles sur ce port.

Vous ne pouvez accéder à aucune interface intrabande via le port hors bande. De même, vous ne pouvez pas accéder au port hors bande via les ports intrabande. Il est recommandé d'utiliser le port hors bande pour toutes les fonctions de gestion du réseau, notamment la gestion Web, le téléchargement/chargement de l'image, de l'amorçage et de la configuration, Telnet ou la gestion SNMP.

À la différence des ports intrabande, le port hors bande ne sert pas à des fins de routage ni de commutation. Le fait d'utiliser le port hors bande plutôt que le port intrabande pour la gestion du réseau permet qu'un port intrabande supplémentaire d'1 Go reste actif pour le routage.

Les sections qui suivent contiennent des exemples de commandes hors bande.

Affectation des adresses IP dynamiques (sur un port hors bande)

```
Console#configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address dhcp hostname dell

Console (config-oob)# exit

Console (config)# exit

Console#
```

Affectation des adresses IP statiques (sur un port hors bande)

```
Console> enable

Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address 10.1.1.1 255.0.0.0

Console (config-oob)# exit

Console (config)# ip default-gateway 10.1.1.10

Console (config)# exit

Console#
```

Allocation d'une passerelle IP par défaut

```
Console>

Console> enable

Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip address 10.0.0.1 /8

Console (config-oob)# ip default-gateway 10.1.1.1

Console (config-oob)#
```

Commande Ping via un port hors bande

```
Console#ping oob/10.6.12.25
```

Copie image/amorçage

```
copy tftp://oob/10.6.12.25/ves_115.dos image
```

```
copy tftp://oob/10.6.12.25/boot_013.rfb boot
```

Passerelle IP par défaut vers un port hors bande

```
Console# configure

Console (config)# interface out-of-band-eth

Console (config-oob)# ip default-gateway 10.1.1.10
```

Informations supplémentaires

Pour plus d'informations sur la configuration des ports hors bande, reportez-vous à la section «Configuration des ports de gestion hors bande (OOB)».

Retour à la page du sommaire

Retour à la page du sommaire

Obtention d'aide

Guide d'utilisation

Assistance technique

Si vous avez besoin d'assistance pour un problème technique, consultez l'ensemble des services proposés par Dell sur le site **support.dell.com**. Vous y trouverez de l'aide pour l'installation et des procédures de dépannage. Pour en savoir plus, reportez-vous à la section «Services en ligne».

Si vous ne parvenez pas à résoudre le problème à l'aide des services en ligne, appelez Dell pour obtenir une assistance technique. Reportez-vous à la section «Contacter Dell».

REMARQUE : Pour faciliter les procédures, appelez le support technique depuis un téléphone qui se trouve à portée de votre ordinateur.

REMARQUE : Il se peut que le système de code de service express de Dell ne soit pas disponible dans tous les pays.

Lorsque le système téléphonique automatisé de Dell vous le demande, entrez votre code de service express pour que votre appel soit directement acheminé vers l'équipe de support technique appropriée. Si vous n'avez pas de code de service express, ouvrez le dossier des **Accessoires Dell**, double-cliquez sur l'icône **Code de service express** et suivez les instructions qui s'affichent.

Pour des instructions sur le service de support technique, consultez les sections «Service de support technique» et «Avant d'appeler».

REMARQUE : Certains des services suivants ne sont pas toujours disponibles en dehors des États-Unis. Veuillez contacter votre représentant Dell local pour obtenir des informations sur leur disponibilité.

Services en ligne

Vous pouvez accéder au site de support technique de Dell à l'adresse **support.dell.com**. Sélectionnez votre région sur la page **WELCOME TO DELL SUPPORT** (Bienvenue au site de support technique de Dell) et fournissez les informations demandées afin d'accéder aux outils et aux informations sur l'aide.

Vous pouvez contacter Dell par voie électronique aux adresses suivantes :

- Site Web

  www.dell.com/

  www.dell.com/ap/ (pays d'Asie et du Pacifique uniquement)

  www.dell.com/jp (Japon uniquement)

  www.euro.dell.com (Europe uniquement)

  www.dell.com/la (pays d'Amérique Latine)

www.dell.ca (Canada uniquement)

- FTP (File Transfert Protocol - protocole de transfert de fichiers) anonyme

ftp.dell.com/

Connectez-vous en tant que user : anonymous (utilisateur anonyme) et utilisez votre adresse électronique comme mot de passe.

- Service de support électronique

support@us.dell.com

apsupport@dell.com (pays d'Asie et du Pacifique uniquement)

support.jp.dell.com (Japon uniquement)

support.euro.dell.com (Europe uniquement)

- Service de devis électronique

sales@dell.com

apmarketing@dell.com (pays d'Asie et du Pacifique uniquement)

sales_canada@dell.com (Canada uniquement)

- Service d'informations électronique

info@dell.com

Service AutoTech

Le service de support technique automatique de Dell, AutoTech, fournit des réponses enregistrées aux questions les plus fréquentes des clients de Dell à propos des systèmes de leurs ordinateurs portables et de bureau.

Lorsque vous appelez AutoTech, utilisez votre téléphone à clavier pour sélectionner les sujets correspondant à vos questions.

Le service AutoTech est accessible 24 heures sur 24, 7 jours sur 7. Vous pouvez aussi accéder à ce service par l'intermédiaire du service de support technique. Reportez-vous à la liste des numéros d'appel de votre région.

Service d'état des commandes automatisé

Pour vérifier l'état de vos commandes de produits Dell™, vous pouvez visiter le site Web **support.dell.com** ou appeler le service d'état des commandes automatisé. Un enregistrement vous demande les informations nécessaires pour repérer votre commande et en faire un rapport. Reportez-vous à la liste des numéros d'appel de votre région.

Service de support technique

Le service de support technique de Dell est disponible à toute heure et tous les jours de la semaine pour répondre à vos questions au sujet du matériel Dell. Nos employés du support technique utilisent des diagnostics sur ordinateur pour fournir rapidement des réponses exactes.

Pour contacter le service de support technique de Dell, reportez-vous à la section «Avant d'appeler» et consultez la liste des numéros d'appel de votre région.

Formation et certification Dell Enterprise

La formation et la certification Dell Enterprise sont maintenant disponibles. Pour plus d'informations, visitez le site Web **www.dell.com/training**. Ce service n'est pas disponible partout.

Problèmes liés à votre commande

Si vous avez un problème lié à votre commande, comme des pièces manquantes ou non adaptées, ou une facturation erronée, contactez le Service clientèle de Dell. Gardez votre facture ou votre fiche d'expédition à portée de main lorsque vous appelez. Reportez-vous à la liste des numéros d'appel de votre région.

Informations concernant le produit

Si vous avez besoin d'informations sur les autres produits disponibles auprès de Dell ou si vous voulez passer une commande, visitez le site Web de Dell à l'adresse **http://www.dell.com**. Pour connaître le numéro à composer afin de consulter un spécialiste des ventes, reportez-vous à la liste des numéros d'appel de votre région.

Renvoi d'articles pour une réparation sous garantie ou une mise en crédit

Préparez tous les articles à retourner, pour réparation ou mise en crédit, comme indiqué ci-après :

1. Contactez Dell pour obtenir un numéro d'autorisation de retour de matériel et écrivez-le clairement et bien visiblement sur l'extérieur de la boîte.

   Pour obtenir le numéro de téléphone à composer, reportez-vous à la liste des numéros d'appel de votre région.

2. Joignez une copie de la facture et une lettre expliquant le motif du retour.
3. Joignez une copie de toutes les informations de diagnostic.
4. Joignez tous les accessoires qui font partie du matériel renvoyé (comme les câbles d'alimentation, les supports, tels que les CD et les disquettes, et les guides) s'il s'agit d'un retour pour mise en crédit.
5. Empaquetez l'équipement à renvoyer dans son emballage d'origine (ou équivalent).

   Les frais d'envoi sont à votre charge. L'assurance des articles retournés vous incombe également et vous acceptez le risque de leur perte au cours de leur acheminement vers Dell. Les envois port dû ne sont pas acceptés.

Les retours ne comportant pas les éléments décrits ci-dessus seront refusés à notre quai de réception et vous seront retournés.

Avant d'appeler

REMARQUE : Ayez à portée de main votre code de service express lorsque vous appelez. Le code permet au système d'assistance téléphonique automatisé de Dell de diriger votre appel plus efficacement.

Si possible, allumez votre système avant d'appeler Dell pour obtenir une assistance technique et utilisez un téléphone qui se trouve à proximité de votre ordinateur. On vous demandera peut-être de taper certaines commandes sur le clavier, de transmettre des informations détaillées pendant les opérations, ou d'effectuer certaines manœuvres de dépannage sur le système informatique lui-même. Assurez-vous que la documentation du système est disponible.

⚠ **PRÉCAUTION : Avant de réparer les composants à l'intérieur de votre ordinateur, reportez-vous au *Guide des Informations Système* pour prendre connaissance des consignes de sécurité.**

Contacter Dell

Vous pouvez contacter Dell par voie électronique, par l'intermédiaire des sites Web suivants :

- **www.dell.com**
- **support.dell.com** (support technique)
- **premiersupport.dell.com** (support technique pour les clients de l'éducation, du gouvernement, de la santé et des grands comptes, comprenant les clients Premier, Platinum et Gold)

Pour les adresses Internet de votre pays, recherchez la section appropriée du pays dans le tableau ci-dessous.

REMARQUE : Les numéros gratuits sont valables dans le pays pour lequel ils sont renseignés.

Si vous devez contacter Dell, utilisez les adresses électroniques, les numéros de téléphone et les indicatifs fournis dans le tableau ci-dessous. Si vous avez besoin d'assistance pour connaître les indicatifs à utiliser, contactez avec un opérateur local ou international.

Pays (Ville) Indicatifs international, national et de la ville	**Nom du département ou zone de service, site Web et adresse électronique**	**Indicatifs régionaux, numéros locaux et numéros gratuits**
Afrique du Sud (Johannesburg)	Site Web : **support.euro.dell.com**	
	E-mail : dell_za_support@dell.com	
Indicatif international :	Support technique	011 709 7710
09/091	Service clientèle	011 709 7707
	Ventes	011 709 7700
Indicatif national : **27**	Télécopieur	011 706 0495
Indicatif de la ville : **11**	Standard	011 709 7700
Allemagne (Langen)	Site Web : **support.euro.dell.com**	
Indicatif international : **00**	E-mail : tech_support_central_europe@dell.com	
	Support technique	06103 766-7200
Indicatif national : **49**	Service clientèle auprès du grand public et des PME	0180-5-224400
Indicatif de la ville : **6103**	Service clientèle pour le segment global	06103 766-9570
	Service clientèle pour les comptes privilégiés	06103 766-9420
	Service clientèle pour les grandes entreprises	06103 766-9560
	Service clientèle pour les comptes publics	06103 766-9555
	Standard	06103 766-7000
Amérique Latine	Support technique clientèle (Austin, Texas, États-Unis)	512 728-4093
	Service clientèle (Austin, Texas, États-Unis)	512 728-3619
	Fax (Support technique et Service clients) (Austin, Texas, États-Unis)	512728-3883
	Ventes (Austin, Texas, États-Unis)	512 728-4397
	Ventes par fax (Austin, Texas, États-Unis)	512 728-4600 ou 512 728-3772
Anguilla	Support technique général	numéro gratuit : 800-335-0031
Antigua et Barbade	Support technique général	1-800-805-5924
Antilles néerlandaises	Support technique général	001-800-882-1519
Argentine (Buenos Aires)	Site Web : **www.dell.com.ar**	
Indicatif international : **00**	Support technique et Service clientèle	numéro gratuit : 0-800-444-0733
	Ventes	0-810-444-3355
Indicatif national : **54**	Télécopieur pour Support technique	11 4515 7139
Indicatif de la ville : **11**	Télécopieur pour service clientèle	11 4515 7138

Aruba	Support technique général	numéro gratuit : 800 -1578
Asie du Sud-Est et pays du Pacifique	Support technique clientèle, service clientèle et ventes (Penang, Malaisie)	604 633 4810
Australie (Sydney) Indicatif international : **0011** Indicatif national : **61** Indicatif de la ville : **2**	E-mail (Australie) : au_tech_support@dell.com	
	E-mail (Nouvelle-Zélande) : nz_tech_support@dell.com	
	Grand public et PME	1-300-65-55-33
	Gouvernement et entreprises	numéro gratuit : 1-800-633-559
	Division des comptes privilégiés (PAD)	numéro gratuit : 1-800-060-889
	Service clientèle	numéro gratuit : 1-800-819-339
	Ventes aux grandes entreprises	numéro gratuit : 1-800-808-385
	Ventes transactionnelles	numéro gratuit : 1-800-808-312
	Télécopieur	numéro gratuit : 1-800-818-341
Autriche (Vienne) Indicatif international : **900** Indicatif national : **43** Indicatif de la ville : **1**	Site Web : **support.euro.dell.com**	
	E-mail : tech_support_central_europe@dell.com	
	Ventes au grand public et aux PME	082024053000
	Télécopieur pour le grand public et les PME	0820 240 530 49
	Service clientèle auprès du grand public et des PME	082024053014
	Service clientèle auprès des comptes privilégiés/des grandes entreprises	0820 240 530 16
	Support technique auprès du grand public et des PME	0820 240 530 14
	Support technique auprès des comptes privilégiés/des grandes entreprises	0660 8779
	Standard	0820 240 530 00
Bahamas	Support technique général	numéro gratuit : 1-866-278-6818
Barbade	Support technique général	1-800-534-3066
Belgique (Bruxelles) Indicatif international : **00** Indicatif national : **32** Indicatif de la ville : **2**	Site Web : **support.euro.dell.com**	
	E-mail : tech_be@dell.com	
	E-mail pour les clients francophones : **support.euro.dell.com/be/fr/emaildell/**	
	Support technique	02 481 92 88
	Service clientèle	02 481 91 19
	Ventes aux grandes entreprises	02 481 91 00
	Télécopieur	02 481 92 99
	Standard	02 481 91 00
Bermudes	Support technique général	1-800-342-0671
Bolivie	Support technique général	numéro gratuit : 800-10-0238
Brésil Indicatif international : **00** Indicatif national : **55** Indicatif de la ville : **51**	Site Web : **www.dell.com/br**	
	Support clients, support technique	0800 90 3355
	Télécopieur pour Support technique	51 481 5470
	Télécopieur pour service clientèle	51 481 5480
	Ventes	0800 90 3390
Brunei Indicatif national : **673**	Support technique clientèle (Penang, Malaisie)	604 633 4966
	Service clientèle (Penang, Malaisie)	604 633 4949
	Ventes transactionnelles (Penang, Malaisie)	604 633 4955
Canada (North York, Ontario) Indicatif international : **011**	État de commandes en ligne : **www.dell.ca/ostatus**	
	AutoTech (support technique automatisé)	numéro gratuit : 1-800-247-9362
	TechFax	numéro gratuit : 1-800-950-1329
	Service clientèle (grand public et PME)	numéro gratuit : 1-800-847-4096
	Service clientèle (grands comptes et gouvernement)	numéro gratuit : 1-800-326-9463
	Support technique (grand public et PME)	numéro gratuit : 1-800-847-4096
	Support technique (grands comptes et gouvernement)	numéro gratuit :1-800-387-5757
	Ventes au grand public/PME	numéro gratuit : 1-800-387-5752
	Ventes (grands comptes et administration)	numéro gratuit : 1-800-387-5755
	Ventes de pièces au détail et Services étendus	1 866 440 3355
Chili (Santiago) Indicatif national : **56** Indicatif de la ville : **2**	Ventes, service clientèle et support technique	numéro gratuit : 1230 -020 -4823
Chine (Xiamen) Indicatif national : **86** Indicatif de la ville : **592**	Site Web pour support technique : **support.ap.dell.com/china**	
	E-mail du support technique : cn_support@dell.com	
	Télécopieur pour Support technique	818 1350
	Support technique pour le grand public et les PME	numéro gratuit : 800 858 2437
	Support technique pour les entreprises	numéro gratuit : 800 858 2333

	Commentaires clients	numéro gratuit : 800 858 2060
	Grand public et PME	numéro gratuit : 800 858 2222
	Division des comptes privilégiés	numéro gratuit : 800.858 2557
	Comptes grandes entreprises GCP	numéro gratuit : 800 858 2055
	Comptes clés des grandes entreprises	numéro gratuit : 800 858 2628
	Comptes grandes entreprises - Nord	numéro gratuit : 800 858 2999
	Comptes grandes entreprises Administration et éducation Nord	numéro gratuit : 800 858 2955
	Comptes grandes entreprises - Est	numéro gratuit : 800 858 2020
	Comptes grandes entreprises Administration et éducation Est	numéro gratuit : 800 858 2669
	Comptes grandes entreprises Queue Team	numéro gratuit : 800 858 2222
	Comptes grandes entreprises Sud	numéro gratuit : 800 858 2355
	Comptes grandes entreprises Ouest	numéro gratuit : 800 858 2811
	Comptes grandes entreprises Pièces détachées	numéro gratuit : 800 858 2621
Colombie	Support technique général	980-9-15-3978
Corée (Séoul) Indicatif international : **001** Indicatif national : **82** Indicatif de la ville : **2**	Support technique	numéro gratuit : 080-200-3800
	Ventes	numéro gratuit : 080-200-3600
	Service clientèle (Séoul, Corée)	numéro gratuit : 080-200-3800
	Service clientèle (Penang, Malaisie)	604 633 4949
	Télécopieur	2194-6202
	Standard	2194-6000
Costa Rica	Support technique général	0800-012-0435
Danemark (Copenhague) Indicatif international : **00** Indicatif national : **45**	Site Web : **support.euro.dell.com**	
	Support E-mail (ordinateurs portables) : den_nbk_support@dell.com	
	Support E-mail (ordinateurs de bureau) : den_support@dell.com	
	Support E-mail (serveurs) : Nordic_server_support@dell.com	
	Support technique	7023 0182
	Service clientèle (relations)	7023 0184
	Service clientèle auprès du grand public et des PME	3287 5505
	Standard (relations)	3287 1200
	Standard télécopieur (relations)	3287 1201
	Standard (grand public et PME)	3287 5000
	Télécopieur (grand public et PME)	3287 5001
Dominique	Support technique général	numéro gratuit : 1-866-278-6821
Équateur	Support technique général	numéro gratuit : 999-119
Espagne (Madrid) Indicatif international : **00** Indicatif national : **34** Indicatif de la ville : **91**	Site Web : **support.euro.dell.com**	
	E-mail : **support.euro.dell.com/es/es/emaildell/**	
	Grand public et PME	
	Support technique	902 100 130
	Service clientèle	902 118 540
	Ventes	902 118 541
	Standard	902 118 541
	Télécopieur	902 118 539
	Grandes entreprises	
	Support technique	902 100 130
	Service clientèle	902 118 546
	Standard	91 722 92 00
	Télécopieur	91 722 95 83
États-Unis (Austin, Texas) Indicatif international : **011** Indicatif national : **1**	Service d'état des commandes automatisé	numéro gratuit : 1-800-433-9014
	AutoTech (ordinateurs portables et de bureau)	numéro gratuit : 1-800-247-9362
	Client (activités à domicile et activités professionnelles à domicile)	
	Support technique	numéro gratuit : 1-800-624-9896
	Service clientèle	numéro gratuit : 1-800-624-9897
	Support technique Dellnet™	numéro gratuit : 1-877-Dellnet (1-877-335-5638)
	Clients du programme d'achats pour employés (EPP)	numéro gratuit : 1-800-695-8133
	Site Web des services financiers : **www.dellfinancialservices.com**	
	Services financiers (leasing/prêts)	numéro gratuit : 1-877-577-3355
	Services financiers (Comptes privilégiés Dell [DPA])	numéro gratuit : 1-800-283-2210

	Secteur privé	
	Service clientèle et Support technique	numéro gratuit : 1-800-822-8965
	Clients du programme d'achats pour employés (EPP)	numéro gratuit : 1-800-695-8133
	Support technique pour les projecteurs	numéro gratuit : 1-877-459-7298
	Public (gouvernements, éducation et santé)	
	Service clientèle et Support technique	numéro gratuit : 1-800-456-3355
	Clients du programme d'achats pour employés (EPP)	numéro gratuit : 1-800-234-1490
	Ventes Dell	numéro gratuit :1-800-289-3355 ou 1-800-879-3355
	Points de vente Dell (ordinateurs Dell recyclés)	numéro gratuit : 1-888-798-7561
	Ventes de logiciels et de périphériques	numéro gratuit : 1-800-671-3355
	Ventes de pièces détachées	numéro gratuit : 1-800-357-3355
	Service étendu et ventes sous garantie	numéro gratuit : 1-800-247-4618
	Télécopieur	numéro gratuit : 1-800-727-8320
	Services Dell pour les sourds, malentendants ou dysphasiques	numéro gratuit : 1-877-DELLTTY (1-877-335-5889)
Finlande (Helsinki) Indicatif international : **990** Indicatif national : **358** Indicatif de la ville : **9**	Site Web : **support.euro.dell.com**	
	E-mail : fin_support@dell.com	
	Support E-mail (serveurs) : Nordic_support@dell.com	
	Support technique	09 253 313 60
	Support technique par fax	09 253 313 81
	Suivi clientèle	09 253 313 38
	Service clientèle auprès du grand public et des PME	09 693 791 94
	Télécopieur	09 253 313 99
	Standard	09 253 313 00
France (Paris) (Montpellier) Indicatif international : **00** Indicatif national : **33** Indicatifs des villes : **(1) (4)**	Site Web : **support.euro.dell.com**	
	E-mail : **support.euro.dell.com/fr/fr/emaildell/**	
	Grand public et PME	
	Support technique	0825 387 270
	Service clientèle	0825 823 833
	Standard	0825 004 700
	Standard (appels extérieurs à la France)	04 99 75 40 00
	Ventes	0825 004 700
	Télécopieur	0825 004 701
	Télécopieur (appels extérieurs à la France)	04 99 75 40 01
	Grandes entreprises	
	Support technique	0825 004 719
	Service clientèle	0825 338 339
	Standard	01 55 94 71 00
	Ventes	01 55 94 71 00
	Télécopieur	01 55 94 71 01
Grèce Indicatif international : 00 Indicatif national : 30	Site Web : **support.euro.dell.com**	
	E-mail : support.euro.dell.com/gr/en/emaildell/	
	Support technique	080044149518
	Support technique Gold	08844140083
	Standard	2108129800
	Ventes	2108129800
	Télécopieur	2108129812
Grenade	Support technique général	numéro gratuit : 1-866-540-3355
Guatemala	Support technique général	1-800-999-0136
Guyane	Support technique général	numéro gratuit : 1-877-270-4609
Hong Kong Indicatif international : **001** Indicatif national : **852**	Site Web : **support.ap.dell.com**	
	E-mail : ap_support@dell.com	
	Support Technique (Dimension™ et Inspiron™)	2969 3189
	Support technique (OptiPlex™, Latitude™ et Dell Precision™)	2969 3191
	Support technique (PowerApp™ et PowerVault™)	2969 3196
	Service d'assistance téléphonique CEE Gold Queue	2969 3187
	Service pour les clients	3416 0910

	Gros comptes grandes entreprises	3416 0907
	Programmes pour clients internationaux	3416 0908
	Division Petites et moyennes entreprises	3416 0912
	Division Grand public et PME	2969 3105
Îles Caïman	Support technique général	1-800-805-7541
Îles Turks et Caicos	Support technique général	numéro gratuit : 1-866-540-3355
Îles Vierges britanniques	Support technique général	numéro gratuit : 1-866-278-6820
Îles Vierges des États-Unis	Support technique général	1-877-673-3355
Inde	Support technique	1600 33 8045
	Ventes	1600 33 8044
Irlande (Cherrywood) Indicatif international : **16** Indicatif national : **353** Indicatif de la ville : **1**	Site Web : **support.euro.dell.com**	
	E-mail : dell_direct_support@dell.com	
	Support technique	1850 543 543
	Support technique pour le Royaume-Uni (interne au Royaume-Uni uniquement)	0870 908 0800
	Service clientèle pour les particuliers	01 204 4014
	Service clientèle pour les petites entreprises	01 204 4014
	Service clientèle pour le Royaume-Uni (interne au Royaume-Uni uniquement)	0870 906 0010
	Service clientèle auprès des grandes entreprises	1850 200 982
	Service clientèle pour les grandes entreprises (interne au Royaume-Uni uniquement)	0870 907 4499
	Ventes pour l'Irlande	01 204 4444
	Ventes pour le Royaume-Uni (interne au Royaume-Uni uniquement)	0870 907 4000
	Télécopieur/Télécopieur pour les ventes	01 204 0103
	Standard	01 204 4444
Italie (Milan) Indicatif international : **00** Indicatif national : **39** Indicatif de la ville : **02**	Site Web : **support.euro.dell.com**	
	E-mail : **support.euro.dell.com/it/it/emaildell/**	
	Grand public et PME	
	Support technique	02 577 826 90
	Service clientèle	02 696 821 14
	Télécopieur	02 696 821 13
	Standard	02 696 821 12
	Grandes entreprises	
	Support technique	02 577 826 90
	Service clientèle	02 577 825 55
	Télécopieur	02 575 035 30
	Standard	02 577 821
Jamaïque	Support technique général (appel à partir de la Jamaïque uniquement)	1-800-682-3639
Japon (Kawasaki) Indicatif international : **001** Indicatif national : **81** Indicatif de la ville : **44**	Site Web : **support.jp.dell.com**	
	Support technique (serveurs)	numéro gratuit : 0120-198-498
	Support technique à l'extérieur du Japon (serveurs)	81-44-556-4162
	Support Technique (Dimension™ et Inspiron™)	numéro gratuit : 0120-198-226
	Support technique à l'extérieur du Japon (Dimension et Inspiron)	81-44-520-1435
	Support technique (Dell Precision™, OptiPlex™ et Latitude™)	numéro gratuit : 0120-198-433
	Support technique à l'extérieur du Japon (Dell Precision, OptiPlex et Latitude)	81-44-556-3894
	Support technique (Axim™)	numéro gratuit : 0120-981-690
	Support technique à l'extérieur du Japon (Axim)	81-44-556-3468
	Service Faxbox	044-556-3490
	Service de commandes automatisé 24 heures sur 24	044-556-3801
	Service clientèle	044-556-4240
	Division Ventes aux entreprises (jusqu'à 400 salariés)	044-556-1465
	Division Ventes aux Comptes privilégiés (plus de 400 salariés)	044-556-3433
	Ventes aux Comptes grandes entreprises (plus de 3 500 salariés)	044-556-3430
	Ventes secteur public (agences gouvernementales, établissements d'enseignement et institutions médicales)	044-556-1469
	Segment International - Japon	044-556-3469
	Utilisateur individuel	044-556-1760
	Standard	044-556-4300
Luxembourg Indicatif international : **00**	Site Web : **support.euro.dell.com**	
	E-mail : tech_be@dell.com	

Indicatif national : **352**	Support technique (Bruxelles, Belgique)	3420808075
	Ventes au grand public et aux PME (Bruxelles, Belgique)	numéro gratuit : 080016884
	Ventes aux grandes entreprises (Bruxelles, Belgique)	024819100
	Service clientèle (Bruxelles, Belgique)	02 481 91 19
	Fax (Bruxelles, Belgique)	02 481 92 99
	Standard (Bruxelles, Belgique)	02 481 91 00
Macao	Support technique	numéro gratuit : 0800 582
Indicatif national : **853**	Service clientèle (Penang, Malaisie)	604 633 4949
	Ventes transactionnelles	numéro gratuit : 0800 581
Malaisie (Penang)	Support technique	numéro gratuit : 1 800 888 298
Indicatif international : **00**	Service clientèle	04 633 4949
Indicatif national : **60**	Ventes transactionnelles	numéro gratuit : 1 800 888 202
Indicatif de la ville : **4**	Ventes aux grandes entreprises	numéro gratuit : 1 800 888 213
Mexique	Support technique clientèle	001-877-384-8979 ou 001-877-269-3383
Indicatif international : **00**	Ventes	50-81-8800 ou 01-800-888-3355
Indicatif national : **52**	Service clientèle	001-877-384-8979 ou 001-877-269-3383
	Principal	50-81-8800 ou 01-800-888-3355
Montserrat	Support technique général	numéro gratuit : 1-866-278-6822
Nicaragua	Support technique général	001-800-220-1006
Norvège (Lysaker)	Site Web : **support.euro.dell.com**	
Indicatif international : **00**	Support E-mail (ordinateurs portables) : nor_nbk_support@dell.com	
Indicatif national : **47**	Support E-mail (ordinateurs de bureau) : nor_support@dell.com	
	Support E-mail (serveurs) : nordic_server_support@dell.com	
	Support technique	671 16882
	Suivi clientèle	671 17514
	Service clientèle auprès du grand public et des PME	23162298
	Standard	671 16800
	Standard par fax	671 16865
Nouvelle-Zélande	E-mail (Nouvelle-Zélande) : nz_tech_support@dell.com	
Indicatif international : **00**	E-mail (Australie) : au_tech_support@dell.com	
Indicatif national : **64**	Grand public et PME	0800 446 255
	Gouvernement et entreprises	0800 444 617
	Ventes	0800 441 567
	Télécopieur	0800 441 566
Panama	Support technique général	001-800-507-0962
Pays-Bas (Amsterdam)	Site Web : **support.euro.dell.com** E-mail (Support technique) : (Entreprise) : nl_server_support@dell.com (Latitude) : nl_latitude_support@dell.com (Inspiron) : nl_inspiron_support@dell.com Dimension) : nl_dimension_support@dell.com (OptiPlex) : nl_optiplex_support@dell.com Dell Precision) : nl_workstation_support@dell.com	
Indicatif international : **00**		
Indicatif national : **31**		
Indicatif de la ville : **20**		
	Support technique	020 674 45 00
	Support technique par fax	020 674 47 66
	Service clientèle auprès du grand public et des PME	020 674 42 00

	Suivi clientèle	020 674 4325
	Ventes au grand public et aux PME	020 674 55 00
	Relations ventes	020 674 50 00
	Ventes par fax au grand public et aux PME	020 674 47 75
	Télécopieur pour les relations ventes	020 674 47 50
	Standard	020 674 50 00
	Télécopieur du standard	020 674 47 50
Pérou	Support technique général	0800-50-669
Pologne (Varsovie) Indicatif international : **011** Indicatif national : **48** Indicatif de la ville : **22**	Site Web : **support.euro.dell.com**	
	E-mail : pl_support@dell.com	
	Service clientèle (téléphone)	57 95 700
	Service clientèle	57 95 999
	Ventes	57 95 999
	Service clientèle (télécopieur)	57 95 806
	Réception (télécopieur)	57 95 998
	Standard	57 95 999
Porto Rico	Support technique général	1-800-805-7545
Portugal Indicatif international : **00** Indicatif national : **351**	Site Web : **support.euro.dell.com**	
	E-mail : **support.euro.dell.com/pt/en/emaildell/**	
	Support technique	707200149
	Service clientèle	800 300 413
	Ventes	800 300 410 ou 800 300 411 ou 800 300 412 ou 21 422 07 10
	Télécopieur	21 424 01 12
République Dominicaine	Support technique général	1-800-148-0530
République tchèque (Prague) Indicatif international : **00** Indicatif national : **420** Indicatif de la ville : **2**	Site Web : **support.euro.dell.com**	
	E-mail : czech_dell@dell.com	
	Support technique	02 2186 27 27
	Service clientèle	02 2186 27 11
	Télécopieur	02 2186 27 14
	TechFax	02 2186 27 28
	Standard	02 2186 27 11
Royaume-Uni (Bracknell) Indicatif international : **00** Indicatif national : **44** Indicatif de la ville : **1344**	Site Web : **support.euro.dell.com**	
	Site Web du service clientèle : **support.euro.dell.com/uk/en/ECare/Form/Home.asp**	
	E-mail : dell_direct_support@dell.com	
	Support technique (grandes entreprises/comptes privilégiés/PAD [plus de 1000 employés])	0870 908 0500
	Support technique (direct/Division Comptes privilégiés et général)	0870 908 0800
	Service clientèle des comptes globaux	01344 373 186
	Service clientèle pour le grand public et les PME	0870 906 0010
	Service clientèle auprès des grandes entreprises	01344 373 185
	Service clientèle Comptes privilégiés (500-5000 salariés)	0870 906 0010
	Service clientèle des comptes gouvernementaux centralisés	01344 373 193
	Service clientèle Gouvernement local et Éducation	01344 373 199
	Service clientèle (Santé)	01344 373 194
	Ventes au grand public et aux PME	0870 907 4000
	Ventes aux grandes entreprises/au secteur public	01344 860 456
	Télécopieur pour le grand public et les PME	0870 907 4006
Salvador	Support technique général	01-899-753-0777
Singapour (Singapour) Indicatif international : **005** Indicatif national : **65**	Support technique	numéro gratuit : 800 6011 051
	Service clientèle (Penang, Malaisie)	604 633 4949
	Ventes transactionnelles	numéro gratuit : 800 6011 054
	Ventes aux grandes entreprises	numéro gratuit : 800 6011 053
St- Kitts-et-Nevis	Support technique général	numéro gratuit : 1-877-441-4731
Ste- Lucie	Support technique général	1-800-882-1521
St- Vincent-et-les Grenadines	Support technique général	numéro gratuit : 1-877-270-4609
Suède (Upplands Vasby)	Site Web : **support.euro.dell.com**	

Indicatif international : **00** Indicatif national : **46** Indicatif de la ville : **8**	E-mail : swe_support@dell.com	
	Support E-mail pour Latitude et Inspiron : Swe-nbk_kats@dell.com	
	Support E-mail pour OptiPlex : Swe_kats@dell.com	
	Support E-mail pour les serveurs : Nordic_server_support@dell.com	
	Support technique	08 590 05 199
	Suivi clientèle	08 590 05 642
	Service clientèle auprès du grand public et des PME	08 587 70 527
	Support du programme d'achats pour employés (EPP, Employee Purchase Program)	20 140 14 44
	Support technique par télécopieur	08 590 05 594
	Ventes	08 590 05 185
Suisse (Genève) Indicatif international : **00** Indicatif national : **41** Indicatif de la ville : **22**	Site Web : **support.euro.dell.com**	
	E-mail : swisstech@dell.com	
	E-mail pour les clients francophones (grand public et PME et grandes entreprises) : **support.euro.dell.com/ch/fr/emaildell/**	
	Support technique (grand public et PME)	0844 811 411
	Support technique (grandes entreprises)	0844 822 844
	Service clientèle (grand public et PME)	0848 802 202
	Service clientèle (grandes entreprises)	0848 821 721
	Télécopieur	022 799 01 90
	Standard	022 799 01 01
Taïwan Indicatif international : **002** Indicatif national : **886**	Support technique (ordinateurs portables et de bureau)	numéro gratuit : 00801 86 1011
	Support technique (serveurs)	numéro gratuit : 0080 60 1256
	Ventes transactionnelles	numéro gratuit : 0080 651 228
	Ventes aux grandes entreprises	numéro gratuit : 0080 651 227
Thaïlande Indicatif international : **001** Indicatif national : **66**	Support technique	numéro gratuit : 0880 060 07
	Service clientèle (Penang, Malaisie)	604 633 4949
	Ventes	numéro gratuit : 0880 060 09
Trinité et Tobago	Support technique général	1-800-805-8035
Uruguay	Support technique général	numéro gratuit : 000-413-598-2521
Venezuela	Support technique général	8001-3605

Retour à la page du sommaire

Retour à la page du sommaire

Utilisation de Dell OpenManage Switch Administrator

Guide d'utilisation

Démarrage de l'application

1. Ouvrez un navigateur Web.
2. Saisissez l'adresse IP du commutateur (telle que définie dans la CLI) dans la barre d'adresses et appuyez sur <Entrée>.

   Pour des informations sur l'affectation d'une adresse IP à un commutateur, reportez-vous à la section «Configuration initiale».
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 commutateur 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 oublié, 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.

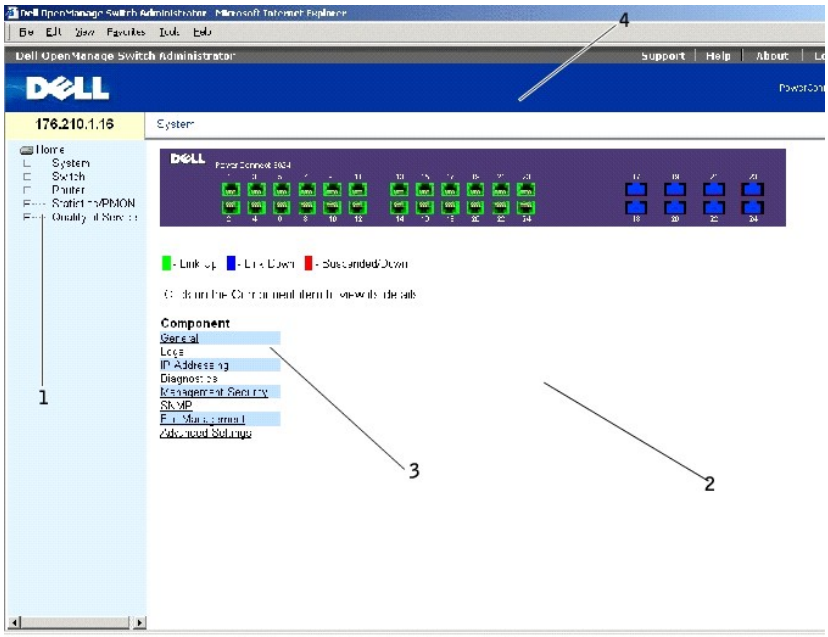
4. Cliquez sur **OK**.
5. La page d'accueil de **Dell OpenManage Switch Administrator** s'ouvre.

Comprendre l'interface

La page d'accueil (reportez-vous à la Figure 4-1) se compose des vues suivantes :

- 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.
- 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 4-1. Composants de Switch Administrator



Le Tableau 4-1 répertorie les composants de l'interface et les numéros qui leur sont associés.

Tableau 4-1. 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. La couleur associée à un port permet de déterminer s'il est actif. Vert indique que le port est activé, rouge indique qu'une erreur est survenue sur le port et bleu indique que la liaison est désactivée. **REMARQUE :** Les DEL n'apparaissent pas sur la vue du périphérique. 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». En fonction des options sélectionnées, la zone au bas de la vue du périphérique affiche d'autres informations et/ou des boîtes de dialogue pour la configuration des paramètres.
3	La liste des composants inclut une liste des composants des fonctionnalités. 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 aux commutateurs et aux services Dell. Pour plus d'informations, reportez-vous à la section «Boutons d'information».

Utilisation des boutons de Switch Administrator

Boutons d'information

Tableau 4-2. Boutons d'information

Bouton	Description
Support (Assistance technique)	Ouvre la page Web du support technique de Dell, accessible à l'adresse **www.support.dell.com**
Help (Aide)	Aide en ligne qui fournit des informations qui vous aideront à configurer et à gérer le commutateur. Les pages d'aide en ligne sont

	directement liées aux pages. Par exemple, si la page **IP Addressing** (Adressage IP) est ouverte, la rubrique d'aide de cette page s'affiche 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

Tableau 4-3. 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 Neighbor's Info (Afficher infos du voisin)	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.
Clear Log (Effacer le journal)	Efface les messages du tampon de journalisation.
Reset (Réinitialiser)	Réinitialise le commutateur.
Test Now (Tester maintenant)	Exécute le test de diagnostic pour les câbles en cuivre.

Définition des champs

Les champs définis par l'utilisateur contient entre 1 et 159 caractères sauf indication contraire sur la page Web de Dell OpenManage Switch Administrator.

Tous les caractères sont acceptés à l'exception des caractères suivants :

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

Accès au commutateur via l'interface de ligne de commande (CLI)

Le commutateur peut être géré par le biais d'une connexion directe avec le port de la Console ou par l'intermédiaire d'une connexion Telnet. Pour des informations sur les ports de gestion hors bande, reportez-vous à la section «Port de gestion hors bande».

L'utilisation de l'interface de ligne de commande (CLI) 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 des informations sur la configuration d'un adresse IP initiale, reportez-vous à la section «Configuration initiale».

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 commutateur 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, fermez 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.

Votre commutateur peut prendre en charge 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.
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

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 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), tapez `configure` à l'invite du mode **Privileged EXEC** (EXEC priviligié) et appuyez sur <Entrée>. L'invite du mode **Global Configuration** (Configuration globale) se compose du nom d'hôte du périphérique suivi du symbole # et de (config).

```
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. Il existe plusieurs modes de configuration de l'interface :

- **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.
- **Port Channel** (Canal de port) — Contient les commandes qui permettent de configurer des LAG.
- **IP** — Contient les commandes qui permettent de gérer les interfaces IP.
- **Out-of-Band-Ethernet** (Ethernet hors bande) — Contient les commandes qui permettent de gérer et de configurer les connexions de gestion.

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 de l'interface de ligne de commande de votre commutateur.

Retour à la page du sommaire

Retour à la page du sommaire

Description matérielle

Guide d'utilisation

Cette section contient des informations sur les caractéristiques du périphérique et les configurations matérielles du module.

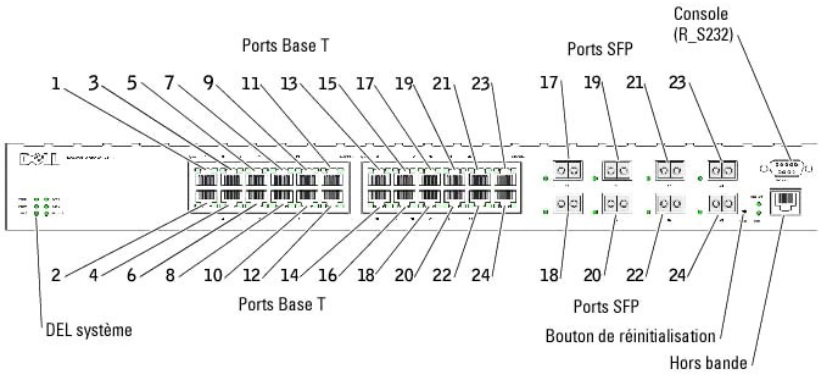
Description des ports

PowerConnect 6024

Les ports 1 à 16 sont des ports 10/100/1000 et les ports 17 à 24 sont des ports Combo. Les numéros des ports sont illustrés dans la figure ci-dessous.

Un port Combo est un port logique unique avec deux connexions physiques : une connexion RJ-45 et une connexion SFP. Lorsqu'un connecteur est inséré dans le port SFP, ce dernier s'active, à moins qu'un connecteur en cuivre du port Base-T portant le même numéro soit inséré et possède une liaison.

Figure 2-1. PowerConnect 6024 doté de 24 ports 10/100/1000 Base-T



Le commutateur détecte automatiquement la différence entre les câbles croisés et les câbles droits reliés aux ports RJ-45. Les ports SFP prennent en charge les modules SX et LX.

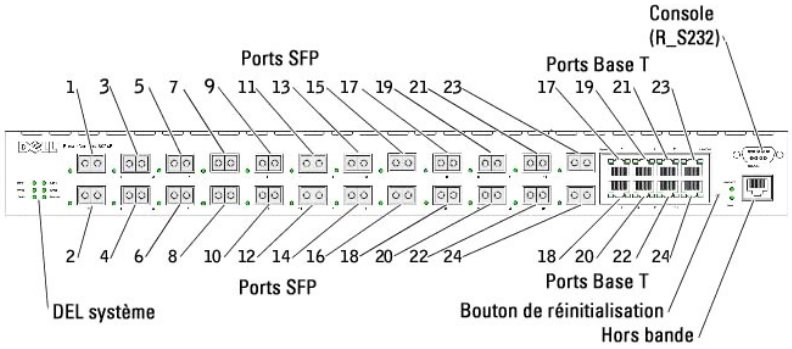
Les ports RJ-45 prennent en charge le mode semi-duplex et duplex intégral à 10/100/1000 Mb/s.

PowerConnect 6024F

Les ports du PowerConnect 6024F diffèrent des ports du PowerConnect 6024 uniquement dans leur désignation : Les ports 1 à 16 sont des ports SFP et les ports 17 à 24 sont des ports Combo. Les numéros des ports sont illustrés dans la figure ci-dessous.

Pour plus d'informations sur le mode de fonctionnement de ces ports, reportez-vous à la description des ports du PowerConnect 6024.

Figure 2-2. PowerConnect 6024F doté de 24 ports SFP



Port de gestion hors bande (OOB)

Le port de gestion hors bande (OOB) est un port Ethernet 10/100 Mb/s que vous pouvez utiliser pour vous connecter directement au commutateur et lancer les applications de gestion de l'administrateur système. Le port hors bande est considéré comme une interface IP normale vers le système et toutes les interfaces de gestion sont disponibles sur ce port.

Pour plus d'informations sur la configuration des ports hors bande, reportez-vous à la section «Port de gestion hors bande».

Port de Console (RS-232)

Le port de la Console (RS-232) sert uniquement à des fins de gestion via une interface série. Ce port constitue une connexion directe vers le commutateur et permet d'accéder à l'interface de ligne de commande (CLI) depuis un terminal de Console relié à un port EIA/TIA-232.

Le port de la Console prend en charge les données synchrones à huit bits de données, un bit d'arrêt et aucune parité. Le débit en bauds par défaut est 115 200 bps.

Composants matériels

Dimensions

Les dimensions du commutateur sont les suivantes :

- 440 x 460 x 44 mm (l x P x H).
- 17,32 x 18,11 x 1,73 po. (l x P x H).

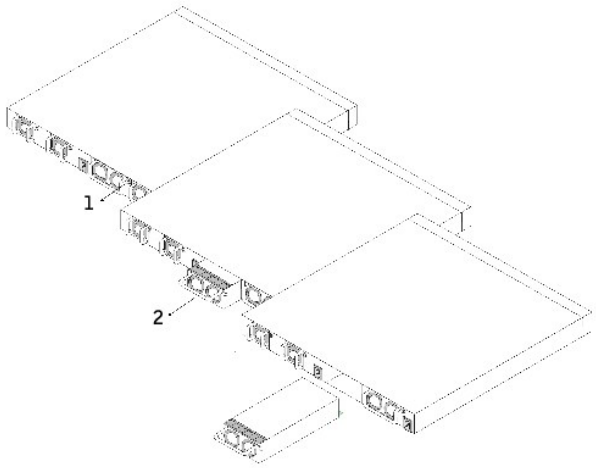
Blocs d'alimentation

Votre commutateur est livré avec deux blocs d'alimentation internes. Vous pouvez contrôler leur fonctionnement en observant leurs diodes électro-luminescentes (DEL). Pour en savoir plus, reportez-vous à la section «DEL système».

Pour remplacer un bloc d'alimentation :

1. Retirez le bloc d'alimentation défectueux en dévissant la vis du panneau arrière et en le tirant vers vous.
2. Insérez un nouveau bloc d'alimentation dans l'emplacement en vous assurant de l'avoir bien enfoncé dans le commutateur.

Figure 2-3. Insertion du bloc d'alimentation



3. Insérez la vis dans le bloc d'alimentation et serrez-la.
4. Connectez chaque bloc d'alimentation à une source d'alimentation électrique externe distincte.

Lorsque vous vous connectez à une source d'alimentation électrique distincte, la probabilité que le commutateur tombera en panne en cas de coupure de courant diminue.

Bouton de réinitialisation

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

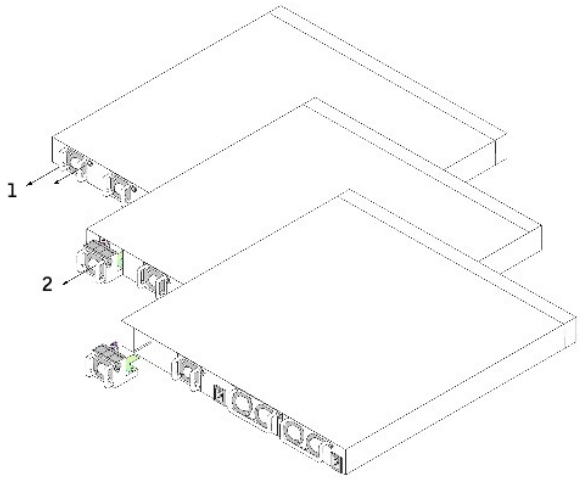
Système de ventilation

Le système comporte deux ventilateurs. Vous pouvez contrôler leur fonctionnement en observant leurs diodes électro-luminescentes (DEL). Pour en savoir plus, reportez-vous à la section «DEL système».

Pour remplacer un ventilateur :

1. Retirez les deux vis et tirez délicatement le ventilateur défectueux.
2. Insérez avec précaution le nouveau ventilateur dans l'emplacement.

Figure 2-4. Installation/Remise en place du ventilateur



3. Insérez la vis dans le ventilateur et serrez-la.

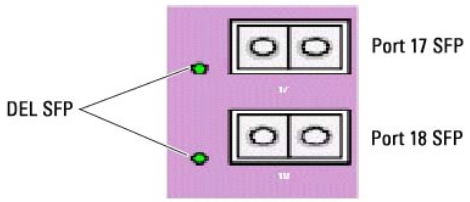
Signification des DEL

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 SFP

La Figure 2-5 représente les DEL des ports SFP, situées à côté de chaque port SFP.

Figure 2-5. DEL des ports SFP



Le Tableau 2-1 donne la signification des DEL des ports SFP :

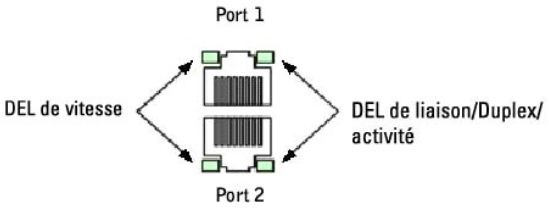
Tableau 2-1. Signification des DEL des ports SFP

DEL	Couleur	Signification
SFP	Vert	Le port est connecté.
	Vert clignotant	Le port envoie et/ou reçoit le trafic du réseau.
	Éteint	Le port n'est pas connecté.

DEL des ports 10/100/1000 Base-T

Chaque port 10/100/1000 Base-T possède deux DEL. La DEL de vitesse se situe sur le côté gauche du port, tandis que la DEL de liaison/duplex/activité se situe sur le côté droit. La figure ci-dessous représente les DEL des ports 10/100/100 Base-T :

Figure 2-6. DEL des ports 10/100/1000 Base-T



Le Tableau 2-2 donne la signification des DEL des ports 10/100/1000 Base-T.

Tableau 2-2. Signification des DEL des ports 10/100/1000 Base-T Port

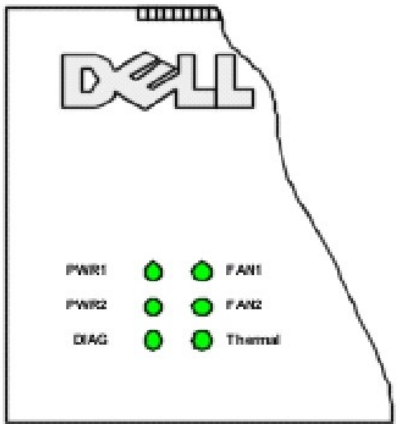
DEL	Couleur	Signification
Vitesse		
	Vert	Le port fonctionne à 1 000 Mb/s.
	Orange	Le port fonctionne à 100 Mb/s.
	Éteint	Le port fonctionne à 10 Mb/s.
État		
	Vert	Le port fonctionne en mode duplex intégral.
	Vert clignotant	Le port envoie ou reçoit des paquets de données en mode duplex intégral.
	Orange	Le port fonctionne en mode semi-duplex.
	Orange clignotant	Le port envoie ou reçoit des paquets de données en mode semi-duplex.
	Éteint	Le port n'est pas connecté.

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 2-7 représente les DEL système.

Figure 2-7. DEL système



Le Tableau 2-3 donne la signification des DEL système.

Tableau 2-3. Signification des DEL système

DEL	Couleur	Signification
Fan 1 (Ventilateur 1)		
	Vert	Le ventilateur 1 est présent et opérationnel.
	Rouge	Le ventilateur 1 est présent mais ne fonctionne pas.
	Éteint	Le ventilateur 1 est absent.
Fan 2 (Ventilateur 2)		
	Vert	Le ventilateur 2 est présent et opérationnel.
	Rouge	Le ventilateur 2 est présent mais ne fonctionne pas.
	Éteint	Le ventilateur 2 est absent.
PWR1		
	Vert	Le bloc d'alimentation 1 est présent et opérationnel.
	Rouge	Le bloc d'alimentation 1 est présent mais ne fonctionne pas.
	Éteint	Le bloc d'alimentation 1 est absent.
PWR2		
	Vert	Le bloc d'alimentation 2 est présent et opérationnel.
	Rouge	Le bloc d'alimentation 2 est présent mais ne fonctionne pas.
	Éteint	Le bloc d'alimentation 2 est absent.
Dia (Diagnostic)		
	Vert clignotant	Un diagnostic est en cours.
	Vert	Le diagnostic s'est terminé avec succès.
	Rouge	Le diagnostic a échoué.
Thermal (Gradient thermique)		
	Rouge	Le système a dépassé la température maximale.
	Éteint	La température du système est normale.

Retour à la page du sommaire

Retour à la page du sommaire

Introduction

Guide d'utilisation

AVIS : Avant toute chose, lisez les notes de mise à jour relatives à ce produit. Vous pouvez les télécharger à partir de l'adresse **support.dell.com**.

Le Dell™ PowerConnect™ 6024/6024F est un commutateur autonome de couche 3 qui étend la gamme des produits de commutation LAN PowerConnect de Dell. Ses caractéristiques sont les suivantes :

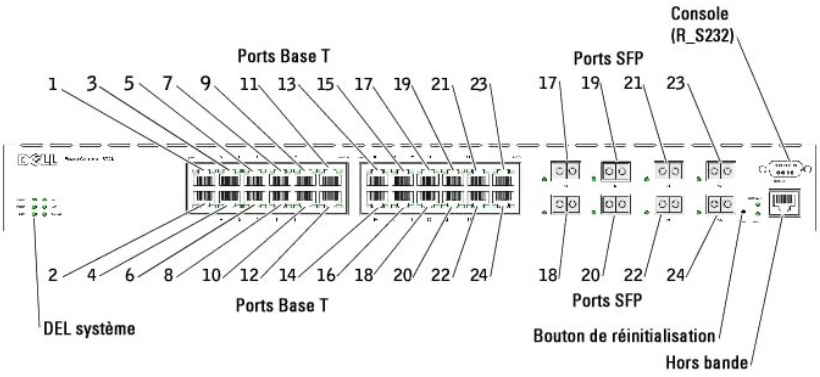
- Facteur de forme 1U, châssis montable en rack
- Port de gestion hors bande pour les connexions RJ-45 et RS-232.
- Prise en charge de toutes les exigences de la communication des données pour un commutateur multicouche, comprenant une suite complète de fonctions de couche 2, de couche 3+, de sécurité et de gestion.
- Haute disponibilité avec blocs d'alimentation et ventilateurs de refroidissement changeables à chaud

---

PowerConnect 6024

Le commutateur PowerConnect 6024 fournit 24 ports 10/100/1000 Base-T RJ-45 et huit ports Combo SFP dotés d'un mode de détection automatique de la vitesse, du contrôle de flux et du mode duplex. Les émetteurs-récepteurs SFP sont vendus séparément.

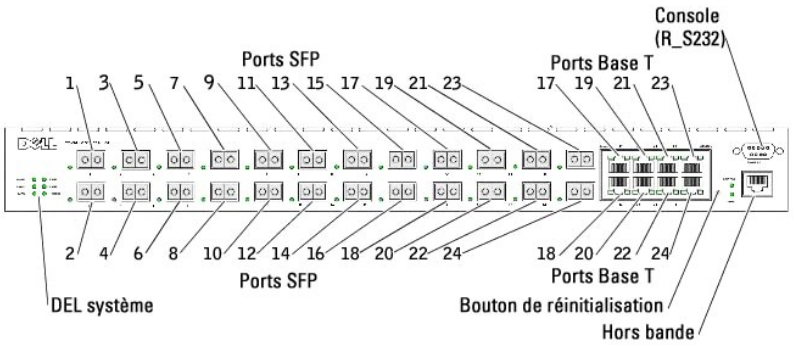
Figure 1-1. PowerConnect 6024



PowerConnect 6024F

Le commutateur PowerConnect 6024F fournit 24 ports SFP et 8 ports combo 10/100/1000 Base-T RJ-45 dotés d'un mode de détection automatique de la vitesse, du contrôle de flux et du mode duplex. Les émetteurs-récepteurs SFP sont vendus séparément.

Figure 1-2. PowerConnect 6024F



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

Le *Guide de référence CLI* fournit des informations sur les commandes CLI utilisées pour configurer le commutateur. Il décrit les commandes CLI ainsi que leur syntaxe et leurs valeurs par défaut.

Fonctions

Cette section décrit les fonctions du commutateur configurables par l'utilisateur. Pour obtenir la liste de toutes les fonctions, reportez-vous aux notes de mises à jour de la version logicielle.

Fonctions basées sur les ports

Contrôle de câble virtuel (VCT)

VCT détecte et signale tout problème potentiel de câblage des liaisons en cuivre (câble ouvert ou en court-circuit par exemple).

Prise en charge des trames Jumbo

Les trames jumbo permettent de transférer des données identiques dans des trames étendues ce qui se traduit par une réduction des surcharges, de la durée de traitement et des interruptions.

Prise en charge MDI/MDIX

Votre commutateur prend en charge la détection automatique entre les câbles croisés et les câbles droits.

Le câblage standard des stations terminales est du type **MDI** (interface dépendante du support) alors que celui des concentrateurs et des commutateurs est du type MDIX (interface croisée dépendante du support).

Pour des informations sur la configuration MDI/MDI pour les ports ou les LAG, reportez-vous à la section «Définition de la configuration des ports» ou «Définition de la configuration des LAG».

Prise en charge de l'horloge de surveillance du matériel

Le commutateur utilise l'horloge de surveillance du matériel pour détecter tout problème et effectuer l'action corrective appropriée lorsque le logiciel ne répond plus.

Négociation automatique

La négociation automatique permet au périphérique d'informer sur ses modes de fonctionnement. La fonction de négociation automatique fournit des moyens d'échanger des informations entre deux périphériques qui partagent un segment de connexion point à point et de configurer automatiquement les deux périphériques pour exploiter au mieux leurs capacités de transmission.

Le PowerConnect 6024/6024F améliore la négociation automatique grâce à la fonction d'annonce de port. L'annonce de port permet à l'administrateur réseau de configurer les vitesses de port annoncées.

Pour des informations sur la négociation automatique, reportez-vous à la section «Définition de la configuration des ports» ou «Définition de la configuration 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 des informations sur la configuration du contrôle du flux pour les ports ou les LAG, reportez-vous à la section «Définition de la configuration des ports» ou «Définition de la configuration des LAG».

Prévention des blocages en tête de ligne

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

Prise en charge de la contre-pression

Sur des liaisons semi-duplex, un récepteur peut empêcher une surcharge de la mémoire tampon en occupant la liaison de façon à ce qu'elle ne soit pas disponible pour le trafic supplémentaire.

Pour des informations sur la configuration de la contre-pression pour les ports ou les LAG, reportez-vous à la section «Définition de la configuration des ports» ou «Définition de la configuration des LAG».

Fonctions de l'adresse MAC prises en charge

Prise en charge des adresses MAC

Le commutateur prend en charge jusqu'à 16 000 adresses MAC et réserve des adresses MAC spécifiques qui seront utilisées par le système.

Apprentissage automatique des adresses MAC

Le commutateur active les adresses MAC devant être automatiquement apprises des paquets en réception.

Expiration automatique des adresses MAC

Les adresses MAC n'ayant véhiculé aucun trafic pendant une période donnée expirent, ce qui évite toute surcharge de la table de pontage.

Pour obtenir des informations sur la configuration de la période d'expiration des adresses MAC, reportez-vous à la section «Affichage des adresses dynamiques».

Entrées MAC statiques

Les entrées MAC définies par l'utilisateur sont mémorisées dans la table de pontage avec les adresses auto-apprises.

Pour obtenir des informations sur la configuration des adresses MAC statiques, reportez-vous à la section «Définition des adresses statiques».

Commutation basée sur MAC sensible au VLAN

Les paquets en provenance d'une adresse source inconnue sont envoyés au périphérique central et ajoutés à la table des matériels. Les futurs paquets adressés vers ou depuis cette adresse sont alors transmis plus efficacement.

Prise en charge de la multidiffusion MAC

Le service de multidiffusion est un service de diffusion restreinte qui permet des connexions 1 à n et n à n. Avec les services de multidiffusion de couche 2, une seule trame adressée à une adresse de multidiffusion spécifique est reçue et des copies de la trame devant être transmise sur chaque port correspondant sont créées.

Pour obtenir des informations sur la configuration de la prise en charge de la multidiffusion MAC, reportez-vous à la section «Prise en charge de la transmission multidiffusion».

Fonctions de couche 2

Surveillance IGMP

La surveillance IGMP examine le contenu des trames IGMP transmises par le commutateur, depuis des stations jusqu'à un routeur de multidiffusion en amont. Elle permet au commutateur d'identifier les stations intéressées par des sessions de multidiffusion et les routeurs envoyant des trames de multidiffusion.

Pour obtenir des informations sur la configuration de la surveillance IGMP, 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 jusqu'à un port de contrôle.

Pour obtenir des informations sur la configuration de la mise en miroir des ports, reportez-vous à la section «Définition de sessions Port Mirroring (Mise en miroir)».

Contrôle des tempêtes de diffusion

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. L'inondation occupe la bande passante et charge tous les noeuds connectés sur tous les ports. La fonction Tempête de diffusion limite le

nombre de trames de diffusion et de multidiffusion acceptées et transmises par le commutateur.

Pour obtenir des informations sur la configuration de la fonction de contrôle des tempêtes informatiques, 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 classés comme appartenant à un VLAN selon qu'ils sont basés sur l'étiquette VLAN ou sur une combinaison port entrant-contenu des paquets. Les paquets partageant des attributs communs peuvent être regroupés dans le même VLAN.

Pour obtenir des informations sur la configuration des VLAN, reportez-vous à la section «Configuration des VLAN».

VLAN basés sur les ports

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

Pour obtenir des informations sur la configuration des VLAN, reportez-vous à la section «Configuration des VLAN».

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 le protocole permettent d'isoler le trafic de couche 2 pour le différencier des protocoles de couche 3.

Pour obtenir des informations sur la définition des VLAN basés sur le protocole, reportez-vous à la section «Définitions des groupes de protocoles VLAN».

Conformité totale au balisage VLAN 802.1Q

La norme IEEE 802.1Q définit une architecture pour les réseaux locaux virtuels pontés, les services fournis dans les VLAN et les protocoles et algorithmes impliqués dans la fourniture de ces services.

Cette norme requiert le marquage des trames par une valeur d'étiquette de classe de service (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 protocole GVRP est activé, le commutateur enregistre et propage l'appartenance à des VLAN sur tous les ports qui font partie de la topologie sous-jacente active du protocole Spanning Tree.

Pour obtenir des informations sur la configuration du protocole GVRP, reportez-vous à la section «Configuration du protocole GVRP».

Fonction Private VLAN Edge

Les ports Private VLAN Edge (PVE) offrent une fonction de sécurité de couche 2 basée sur les ports entre les ports adjacents d'un VLAN. Il s'agit d'une

extension du VLAN courant. Le trafic provenant de ports protégés est envoyé uniquement aux ports ascendants et ne peut pas être envoyé à d'autres ports du VLAN.

Pour obtenir des informations sur la configuration des ports PVE, reportez-vous à la section «Configuration des ports».

Fonctions du protocole Spanning Tree

Protocole Spanning Tree (STP) par périphérique

Le protocole STP 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, via des trames spécifiquement formatées, puis activent et désactivent de manière sélective la transmission sur les ports.

Pour obtenir des informations sur la configuration du protocole STP, reportez-vous à la section «Configuration du protocole Spanning Tree».

Fast Link

Le protocole STP peut avoir besoin de 30 à 60 secondes pour converger s'il détecte des boucles potentielles. Les changements d'état ont alors le temps de se propager et les périphériques concernés de répondre. Ce délai est toutefois trop long pour bon nombre d'applications. Fast Link permet de remédier à ce problème sans exiger pour autant plusieurs chemins d'accès aux données pour garantir la résilience du réseau.

Pour obtenir des informations sur l'activation de Fast Link pour les ports et les LAG, reportez-vous à la section «Définition de la configuration des ports» ou «Définition de la configuration des LAG».

Rapid Spanning Tree respectant le standard IEEE 802.1w

Le protocole RSTP (Rapid Spanning Tree Protocol) détecte et utilise les topologies réseau pour activer la convergence rapide, sans créer pour autant des boucles de transmission.

Pour obtenir des informations sur l'activation du protocole RSTP, reportez-vous à la section «Définition de Rapid Spanning Tree».

Multiple Spanning Tree

Multiple Spanning Tree (MSTP) mappe des VLAN en instances ST. MSTP fournit un scénario d'équilibrage de la charge différent. Les paquets affectés à différents VLAN sont transmis via différents chemins au sein des régions MSTP (régions MST). Les régions sont un ou plusieurs ponts MSTP interconnectés ayant les mêmes paramètres MSTP. Cette norme permet aux administrateurs d'affecter le trafic VLAN à des chemins uniques.

Pour plus d'informations sur MSTP, reportez-vous à la section «Définition de Multiple Spanning Tree».

Agrégation des liaisons

Agrégation des liaisons

Un seul groupe de liaisons agrégées (LAG) peut comprendre jusqu'à sept ports. Il présente les caractéristiques suivantes : fonction de tolérance de pannes qui protège contre les ruptures de liaisons physiques, des connexions de bande passante supérieures et une plus grande granularité de bande passante.

Un LAG est composé de ports de même vitesse, configurés en mode Duplex intégral.

Pour obtenir des informations sur la configuration des LAG, reportez-vous à la section «Définition de la configuration des LAG».

Agrégation de liaisons et LACP

Le protocole LACP utilise les échanges entre homologues via 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. LACP détermine, configure, relie et surveille automatiquement la liaison des ports aux agrégateurs au sein du système.

Pour obtenir des informations sur le protocole LACP, reportez-vous à la section «Définition des paramètres».

Fonctions de routage

Routage IP

Le routage IP transmet vers un périphérique qui suit (next-hop) tous les paquets adressés aux adresses MAC système mais pas ceux adressés à une adresse IP système.

Pour obtenir des informations sur la configuration du routage IP, reportez-vous à la section «Configuration des paramètres globaux de routage IP».

RIP Versions 1 et 2

Le protocole d'information de routage (RIP) est un protocole de routage à vecteur de distance. Il sélectionne les routes selon le nombre de sauts nécessaires pour arriver à la destination. RIP 2 améliore l'efficacité, l'utilisation et les méthodes d'authentification du protocole RIP.

Pour obtenir des informations sur la configuration du protocole RIP, reportez-vous à la section «Configuration du protocole RIP».

OSPF Version 2

Le protocole d'ouverture du chemin d'accès le plus court en priorité (OSPF) est un protocole de routage de passerelle. Pour les réseaux ayant un grand nombre de routeurs interconnectés, le protocole OSPF est plus efficace que le protocole RIP car il utilise moins de bande passante de liaison et converge plus rapidement.

Pour obtenir des informations sur la configuration du protocole OSPF, reportez-vous à la section «Configuration des paramètres et des filtres OSPF».

Protocole ARP (protocole de résolution d'adresses)

Avec le routage IP, les routeurs et les commutateurs de couche 3 utilisent différents protocoles de routage pour détecter la topologie du réseau et définir les tables de routage. ARP détermine automatiquement les adresses MAC de prochain saut de périphériques de systèmes, y compris celles des systèmes finaux directement connectés. Les utilisateurs peuvent également définir des données de tables ARP supplémentaires.

Pour obtenir des informations sur la configuration du protocole ARP, reportez-vous à la section «Définition des paramètres ARP».

Messages ICMP

Les messages du protocole **Internet Control Message Protocol** (ICMP) sont des messages hors bande relatifs au bon ou au mauvais fonctionnement du réseau.

IGMPv2

Le protocole IGMP permet au routeur d'envoyer des requêtes IGMP sous la forme de diffusions L2 sur chaque interface. Lorsqu'un paquet de multidiffusion est envoyé et que sa destination est une adresse MAC de multidiffusion, tous les hôtes sur cette interface routeur reçoivent une copie de ce paquet. Les hôtes écoutent les rapports IGMP. Si des groupes de multidiffusion intéressés ont déjà été interrogés par une station sur la même interface, les autres stations n'envoient pas de requêtes doubles.

Pour obtenir des informations sur la configuration du protocole IGMP, reportez-vous à la section «Définition des paramètres d'interface IGMP».

Prise en charge de la recherche de plus long préfixe

Les recherches de plus long préfixe permettent principalement de déterminer le meilleur chemin de prochain saut pour un paquet et ce uniquement sur la base de l'adresse de destination contenue dans l'en-tête du paquet. Étant donné que les adresses IP sont généralement affectées d'une manière qui reflète la topologie du réseau, le résultat obtenu avec l'opération de recherche de plus long préfixe est normalement le chemin le plus court pour joindre la destination.

DVMRP

Le protocole de routage de multidiffusion à vecteur de distance annonce les chemins les plus courts pour joindre les réseaux sources de multidiffusion avec des hôtes pouvant transmettre un trafic IP de multidiffusion.

Pour obtenir des informations sur la configuration du protocole DVMRP, reportez-vous à la section «Configuration des interfaces DVMRP».

VRRP

Le protocole de redondance des routeurs virtuels (VRRP) élimine les points de pannes uniques dans l'environnement de routage. VRRP utilise un protocole d'élection qui affecte dynamiquement la responsabilité du routeur virtuel à l'un des routeurs VRRP du réseau local.

Le processus d'élection offre un basculement dynamique de la responsabilité de la transmission en cas d'indisponibilité du routeur maître. Toutes les adresses IP du routeur virtuel peuvent être utilisées comme routeur de prochain saut par défaut par les hôtes finaux.

Pour obtenir des informations sur la configuration du protocole VRRP, reportez-vous à la section «Configuration du protocole VRRP».

Fonctions de couche 3

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.

Relais UDP

Le relais UDP permet au périphérique de transmettre des diffusions UDP spécifiques d'une interface à l'autre. Les paquets de diffusion IP en provenance d'une interface ne sont généralement pas transmis à une autre interface. Toutefois, certaines applications utilisent la diffusion UDP pour détecter la disponibilité d'un service. D'autres services nécessitent le routage de paquets de diffusion UDP pour fournir des services aux clients sur un autre sous-réseau.

Clients BootP et DHCP

Le DHCP permet de recevoir des paramètres de configuration supplémentaires à partir d'un serveur réseau au démarrage du système. Le service DHCP est un processus évolutif. Le DHCP est une extension du BootP.

Pour obtenir des informations sur le protocole DHCP, reportez-vous à la section «Définition des paramètres d'interface IP DHCP».

Relais BootP

BootP permet à un périphérique de solliciter et de recevoir des données de configuration en provenance des serveurs. Si le serveur BootP visé n'est pas directement connecté au domaine de diffusion d'un client, un service de relais BootP permet au client d'atteindre le serveur.

Des paramètres

DHCP permet à un périphérique de solliciter et de recevoir des données de configuration en provenance des serveurs. Si le serveur DHCP visé n'est pas directement connecté au domaine de diffusion d'un client, un service de relais DHCHP permet au client d'atteindre le serveur.

Pour obtenir des informations sur la configuration des paramètres de relais DHCP, reportez-vous à la section «Définition des paramètres de relais DHCP».

Fonctions de la qualité de service

Prise en charge de la qualité de service (QdS)

Pour éviter toute surcharge imprévisible du trafic réseau et optimiser les performances, vous pouvez appliquer une qualité de service (QdS) à l'ensemble du réseau et définir ainsi des critères de priorité spécifiques pour le routage du trafic réseau. Votre commutateur prend en charge deux modes de QdS : un mode de base et un mode avancé.

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 à l'étiquetage 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'a été établie ou appliquée. La norme 802.1p définit huit niveaux de priorité, similaires au champ binaire IP Precedence IP Header (En-tête IP de priorité IP).

Mode de base de la qualité de service

En mode de base, il est possible d'activer un mode **Trust** (Confiance) (VPT, DSCP, TCP/UDP ou aucun). Par ailleurs, une liste de contrôle d'accès unique peut être associée à une interface.

Pour obtenir des informations sur l'activation du mode de base QdS, reportez-vous à la section «Configuration du mode de base de la qualité de service».

Mode avancé de la qualité de service

Le mode avancé spécifie une classification des flux et affecte des règles relatives à la gestion de la bande passante. Ces règles peuvent être regroupées dans une réglementation pouvant être appliquée à une interface.

Pour obtenir des informations sur l'activation du mode avancé QdS, reportez-vous à la section «Configuration du mode avancé 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 comme des interruptions SNMP à une liste de destinataires des interruptions.

Pour obtenir des informations sur les alarmes et les interruptions SNMP, reportez-vous à la section «Définition des paramètres SNMP».

Gestion basée sur le Web

Vous pouvez gérer le système à partir de n'importe quel navigateur Web. Le commutateur contient un serveur Web intégré qui donne accès à des pages HTML permettant de surveiller et de configurer le système.

Téléchargement du fichier de configuration

Le fichier de configuration du commutateur comprend les données de configuration des périphériques spécifiques aux ports et à l'échelle du système. Vous pouvez afficher les fichiers de configuration à l'aide de commandes CLI.

Pour obtenir des informations sur le téléchargement des fichiers de configuration, reportez-vous à la section «Téléchargement de fichiers».

Téléchargement des logiciels

Le téléchargement des logiciels permet le stockage d'images de sauvegarde du micrologiciel. Pour obtenir des informations sur le téléchargement des logiciels, reportez-vous à la section «Téléchargement des logiciels et réamorçage».

Protocole de transfert de fichiers trivial (TFTP)

PowerConnect 6024/6024F prend en charge l'exportation/importation d'images, de micrologiciels et de configurations via TFTP.

Surveillance à distance

La télésurveillance (RMON) est une extension de SNMP qui offre des fonctions de surveillance du *trafic* réseau complètes (par opposition au SNMP qui permet une gestion et une 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 obtenir des informations sur RMON, reportez-vous à la section «Affichage des statistiques RMON».

Protocole de gestion de réseau simple (SNMP) versions 1, 2 et 3

Pour contrôler l'accès au système, une liste d'entrées de communauté est définie, chaque entrée étant composée d'une chaîne communautaire et de ses privilèges d'accès. On distingue trois niveaux de sécurité SNMP — lecture seule, lecture-écriture et super. Seul un super utilisateur peut accéder à la table de communautés.

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'aide contextuelle fournit le format et les plages de valeurs autorisés pour les commandes actuelles et l'interpréteur CLI l'exécution des commandes et des mots clés.

Syslog

Syslog est un protocole qui permet d'envoyer les notifications d'événements à un ensemble de serveurs distants donnés où elles peuvent être stockées, examinées et exécutées.

Pour obtenir des 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 commutateur réseau avec une précision d'une milliseconde. La synchronisation de l'heure se fait via un serveur réseau SNTP.

Pour plus d'informations sur le SNTP, reportez-vous à la section «Configuration des paramètres SNTP».

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** (EXEC privilégié).

Prise en charge des ports de gestion hors bande

Un port de gestion hors bande est un port Ethernet externe qui ne transmet du trafic qu'entre l'administrateur système et les applications de gestion. Le port de gestion hors bande fournit une liaison sécurisée physiquement et offre également une tolérance aux pannes.

Caractéristiques de sécurité

Listes de contrôle d'accès (ACL)

L'ACL fournit les règles de transmission et de blocage du trafic réseau. Vous pouvez définir des ACL pour apporter des améliorations de sécurité en définissant des règles de classification et en affectant une action par règle. Vous pouvez affecter une ACL à une interface d'entrée (port ou VLAN).

Pour des informations sur la définition des ACL, reportez-vous à la section «Définition des ACL basées sur IP» et «Définition des ACL basées sur MAC».

Authentification basée sur le port (802.1x)

L'authentification basée sur le port permet d'authentifier les 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 les ports».

Prise en charge des ports verrouillés

Un port verrouillé restreint l'accès à un port uniquement aux utilisateurs possédant des adresses MAC spécifiques. Ces adresses sont définies manuellement ou 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 obtenir des informations sur l'activation de la sécurité par port verrouillé, reportez-vous à la section «Configuration de la sécurité de port».

Sécurité de gestion des mots de passe

La gestion des mot de passe offre une sécurité réseau accrue et un contrôle amélioré du mot de passe. Les mots de passe d'accès SSH, Telnet, HTTP, HTTPS et SNMP sont des fonctions de sécurité affectées.

Pour plus d'informations sur la gestion des mots de passe, reportez-vous à la section «Gestion des mots de passe».

TACACS+

TACACS+ offre une sécurité centralisée pour la vérification des utilisateurs qui accèdent au commutateur. TACACS+ permet d'avoir un système de gestion centralisée des utilisateurs, tout en conservant le RADIUS et les autres processus d'authentification.

Pour obtenir des informations sur la définition des paramètres TACACS+, reportez-vous aux sections «Configuration des serveurs TACACS+ hors bande» et «Configuration des paramètres TACACS+».

Client RADIUS

RADIUS est un protocole client/serveur avec lequel le serveur gère une base de données utilisateur contenant les informations d'authentification pour chaque utilisateur, telles que le nom d'utilisateur, le mot de passe et les informations de comptabilité.

Pour obtenir des informations sur la définition des paramètres RADIUS, reportez-vous à la section «Configuration des paramètres RADIUS».

SSH

Secure Shell (SSH) est un protocole qui fournit une connexion distante sécurisée à un périphérique. La fonction de cette connexion est similaire à celle d'une connexion Telnet entrante.

Retour à la page du sommaire

Retour à la page du sommaire

Guide d'utilisation

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.

Janvier 2005

Retour à la page du sommaire

Retour à la page du sommaire

Affichage des statistiques

Guide d'utilisation

Cette section contient des statistiques relatives aux interfaces, aux réseaux virtuels dynamiques (GVRP), à Etherlike, à la télésurveillance (RMON) et à l'utilisation du périphérique.

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.

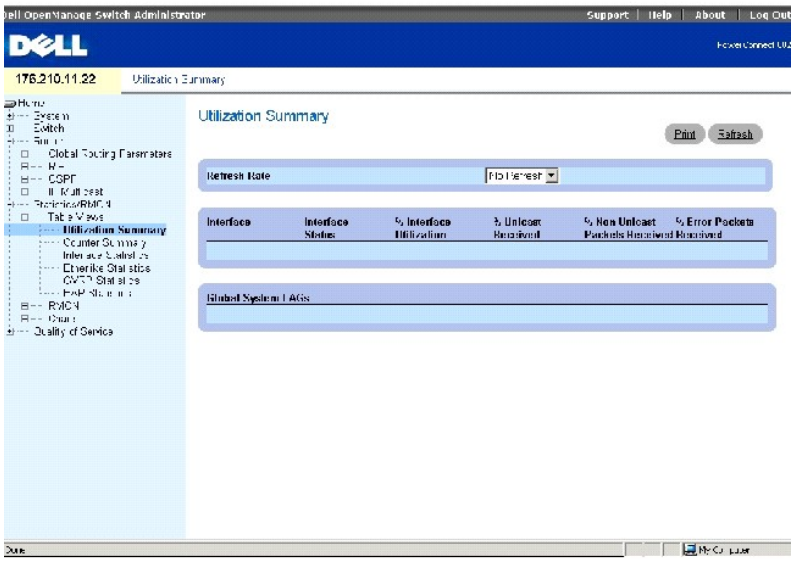
Pour ouvrir cette page, cliquez sur **Statistics / RMON** (Statistiques/RMON)→ **Table Views** (Vues Tables) dans l'*arborescence*.

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 / RMON** (Statistiques/RMON)→ **Table Views** (Vues Tables)→ **Utilization Summary** (Récapitulatif de l'utilisation) dans l'*arborescence*.

Figure 9-1. Récapitulatif de l'utilisation



La page **Utilization Summary** (Récapitulatif de l'utilisation) contient les champs suivants :

Refresh Rate (Taux d'actualisation) Délai qui s'écoule entre deux actualisations des statistiques. Les valeurs possibles pour ce champ sont No Refresh (Pas d'actualisation), 15, 30 et 60 secondes.

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.

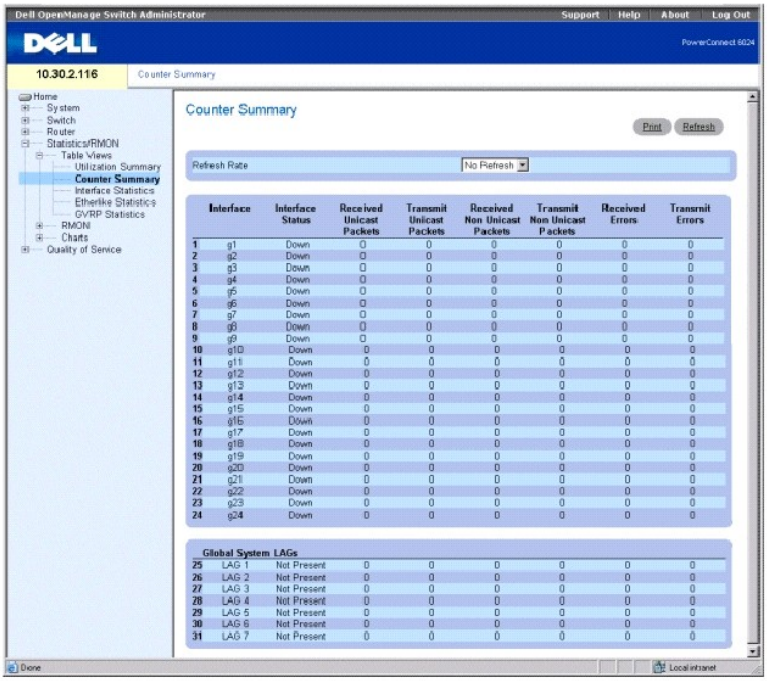
% Error Packets Received (% paquets avec erreurs reçus) Pourcentage de paquets contenant des erreurs, qui ont été reçus sur l'interface.

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 cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON)→ **Table Views** (Vues Tables)→ **Counter Summary** (Récapitulatif des compteurs) dans l'*arborescence*.

Figure 9-2. Page Récapitulatif des compteurs



Refresh Rate (Taux d'actualisation) Délai qui s'écoule entre deux actualisations des statistiques. Les valeurs possibles pour ce champ sont No Refresh (Pas d'actualisation), 15, 30 et 60 secondes.

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.

Transmit Unicast Packets (Paquets monodiffusion transmis) Nombre de paquets monodiffusion transmis depuis l'interface.

Received non-Unicast Packets (Paquets non monodiffusion reçus) Nombre de paquets non monodiffusion reçus sur l'interface.

Transmit non-Unicast Packets (Paquets non monodiffusion transmis) Nombre de paquets non monodiffusion transmis depuis l'interface.

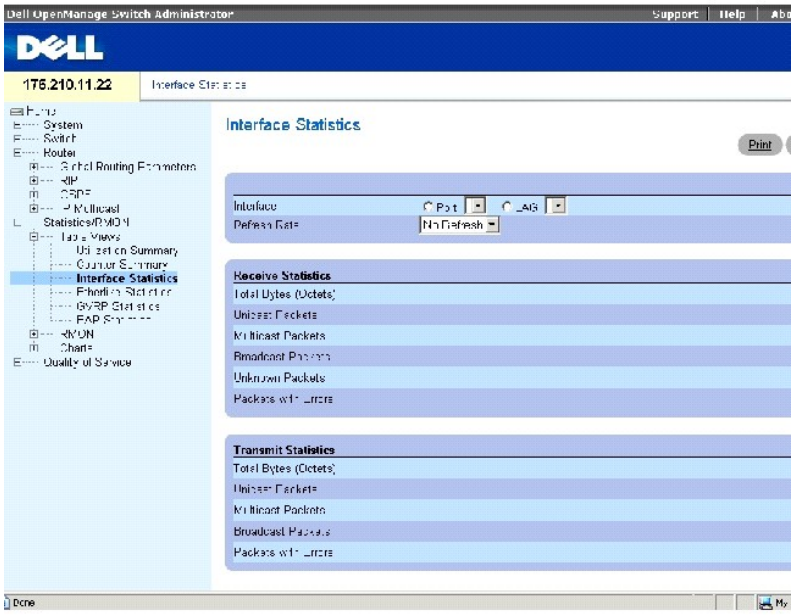
Received Errors (Erreurs reçues) Nombre d'erreurs reçues sur l'interface.

Transmit Errors (Erreurs transmises) Nombre d'erreurs transmises à partir de l'interface.

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 cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON)→ **Table Views** (Vues Tables)→ **Interface Statistics** (Statistiques sur les interfaces) dans l'*arborescence*.

Figure 9-3. Page 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. Les valeurs possibles pour ce champ sont No Refresh (Pas d'actualisation), 15, 30 et 60 secondes.

Statistiques des paquets reçus

Total Bytes (Octets) (Nombre total d'octets) 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 de diffusion) Nombre de paquets de diffusion reçus sur l'interface sélectionnée.

Unknown Packets (Paquets inconnus) Nombre de paquets inconnus reçus sur l'interface sélectionnée.

Packets with Errors (Paquets avec erreurs) Nombre d'erreurs transmises depuis l'interface sélectionnée.

Statistiques des paquets transmis

Total Bytes (Octets) (Nombre total d'octets) 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 de diffusion transmis sur l'interface sélectionnée.

Packets with Errors (Paquets avec erreurs) Nombre d'erreurs transmises depuis 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**.

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).

Affichage des statistiques relatives aux interfaces à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage des statistiques relatives aux interfaces.

Tableau 9-1. Commandes CLI Statistiques relatives aux interfaces

Commande CLI	Description
`show interfaces counters [ethernet` *`interface`* `| port- channel` *`port-channel-number`*`]`	Affiche le trafic enregistré par l'interface physique.

Vous trouverez ci-dessous un exemple de commande CLI.

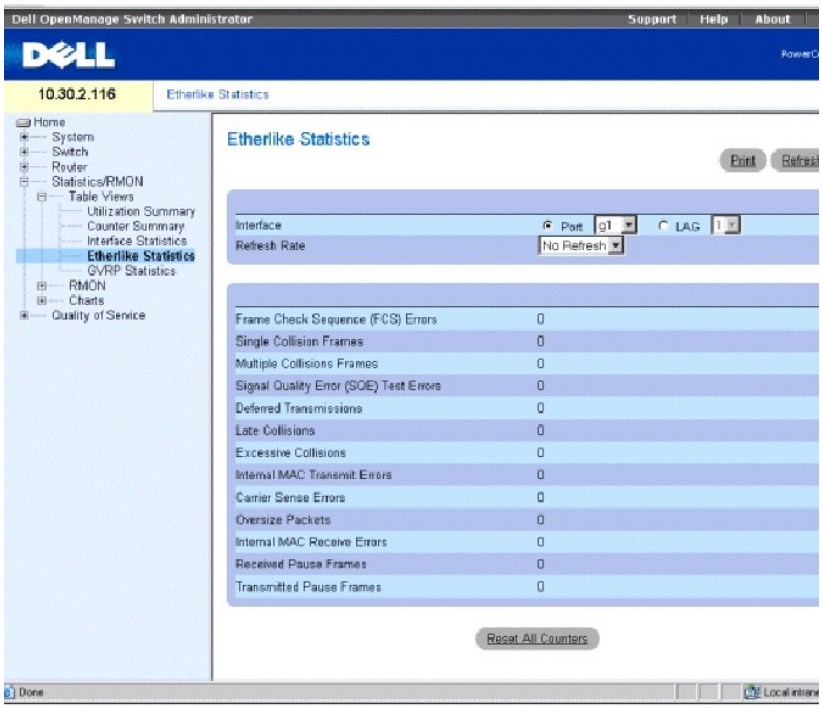
```
          Console> show interfaces counters

Port    InOctets InUcastPkts InMcastPkts InBcastPkts

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

g1          0         0          0           0

g2          0         0          0           0

g3          0         0          0           0

g4          0         0          0           0

g5          0         0          0           0

g6          0         0          0           0
```

g7	0	0	0	0
g8	0	0	0	0
g9	0	0	0	0
g10	0	0	0	0
g11	0	0	0	0
g12	10	685	290	32
g13	0	0	0	0
g14	0	0	0	0
g15	0	0	0	0
g16	0	0	0	0
g17	0	0	0	0
g18	0	0	0	0
g19	0	0	0	0
g20	0	0	0	0
g21	0	0	0	0
g22	0	0	0	0
g23	0	0	0	0
g24	0	0	0	0

Affichage des statistiques relatives à Etherlike

La page **Etherlike Statistics** (Statistiques Etherlike) fournit des statistiques relatives aux interfaces. Pour ouvrir la page, cliquez sur **Statistics/RMON** (Statistiques/RMON)→ **Table Views** (Vues Tables)→ **Etherlike Statistics** (Statistiques Etherlike) dans l'arborescence.

Figure 9-4. Page 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. Les valeurs possibles pour ce champ sont No Refresh (Pas d'actualisation), 15, 30 et 60 secondes.

Frame Check Sequence (FCS) Errors (Erreurs de séquence de contrôle de trame) Nombre d'erreurs de séquence de contrôle de trame reçues sur l'interface sélectionnée.

Signal Collision Frames (Trames monocollision) Nombre d'erreurs de trames monocollision reçues sur l'interface sélectionnée.

Multiple Collision Frames (Trames multicollisions) Nombre d'erreurs de trames multicollisions 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 collisions tardives 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 dépassant la taille limite) Nombre d'erreurs dues à des paquets trop longs 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.

Receive Pause Frames (Trames de pause reçues) Nombre d'erreurs de pause reçues sur l'interface sélectionnée.

Transmitted Paused Frames (Trames de pause transmises) Nombre d'erreurs de pause transmises sur 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**.
3. Cliquez sur **Query** (Interroger) pour afficher les statistiques Etherlike de l'interface.

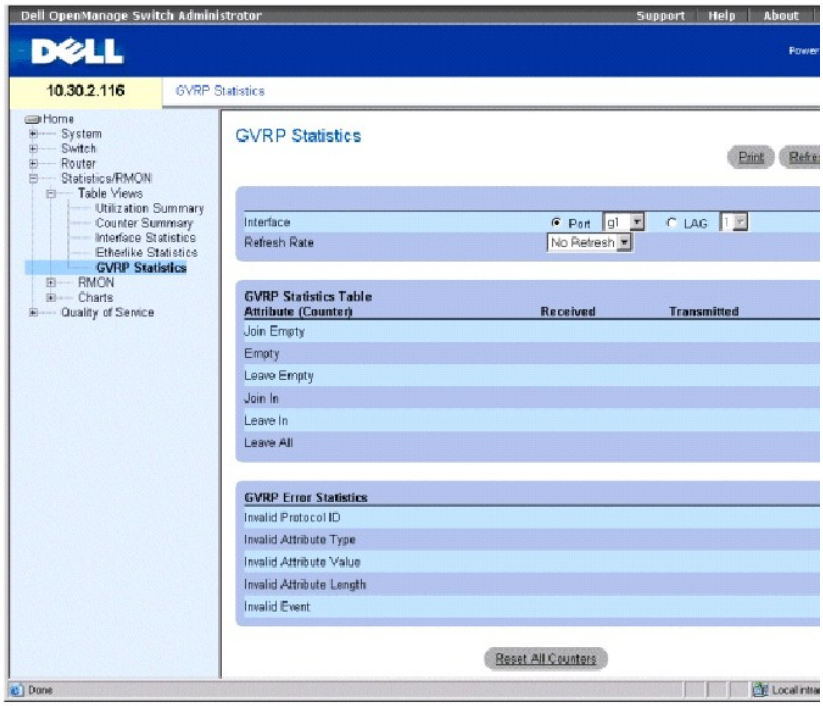
Réinitialisation des statistiques Etherlike

1. Ouvrez la page **Etherlike Statistics** (Statistiques Etherlike).
2. Cliquez sur **Reset All Counters** (Réinitialiser tous les compteurs).

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 9-5. Pages 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. Les valeurs possibles pour ce champ sont No Refresh (Pas d'actualisation), 15, 30 et 60 secondes.

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 Event (Événement incorrect) 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**.

Réinitialisation des statistiques GVRP

1. Ouvrez la page **GVRP Statistics** (Statistiques GVRP).
2. Cliquez sur **Reset All Counters** (Réinitialiser tous les compteurs).

Affichage des statistiques GVRP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage des statistiques GVRP.

Tableau 9-2. Commandes CLI des statistiques GVRP

Commande CLI	Description
	Affiche les statistiques du protocole GVRP.

show gvrp statistics [ethernet *interface* | port-channel *port- channel-number*]	
show gvrp error- statistics [ethernet *interface* | port-channel *port-channel-number*]	Affiche les statistiques des erreurs du protocole GVRP.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# show gvrp statistics

GVRP statistics :

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

Legend :

rJE : Join Empty Received rJIn : Join In Received

rEmp : Empty Received rLIn : Leave In Received

rLE : Leave Empty Received rLA : Leave All Received

sJE : Join Empty Sent sJIn : Join In Sent

sEmp : Empty Sent sLIn : Leave In Sent

sLE : Leave Empty Sent sLA : Leave All Sent

Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE sLA

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

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
```

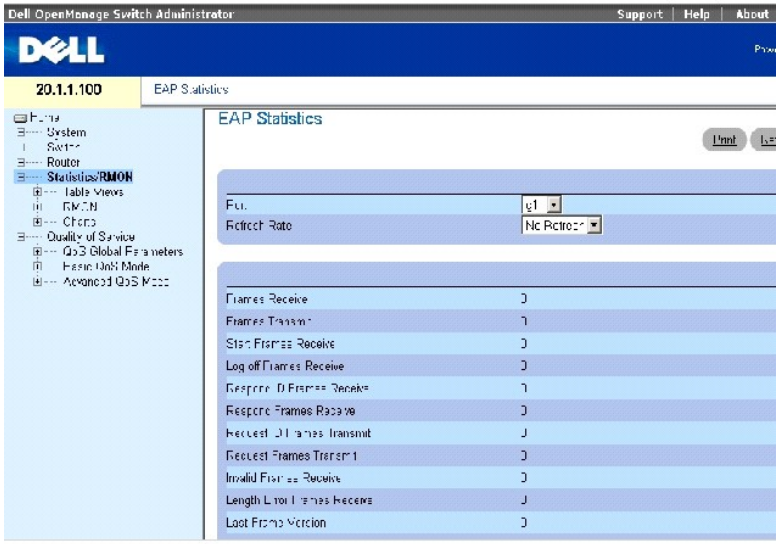
```
g7    0    0    0    0   0   0   0   0   0    0   0   0

g8    0    0    0    0   0   0   0   0   0    0   0   0

Console# show gvrp error-statistics

GVRP error statistics:

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

Legend:

INVPROT : Invalid Protocol Id INVPLEN : Invalid PDU Length

INVATYP : Invalid Attribute Type INVALEN : Invalid Attribute Length

INVAVAL : Invalid Attribute Value INVEVENT : Invalid Event



Port INVPROT INVATYP INVAVAL INVPLEN INVALEN INVEVENT

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

g1      0       0       0       0       0       0

g2      0       0       0       0       0       0

g3      0       0       0       0       0       0

g4      0       0       0       0       0       0

g5      0       0       0       0       0       0

g6      0       0       0       0       0       0

g7      0       0       0       0       0       0

g8      0       0       0       0       0       0
```

Affichage des statistiques EAP

La page **EAP Statistics** (Statistiques EAP) contient des informations sur les paquets EAP reçus sur un port spécifique. Pour plus d'informations sur l'EAP, reportez-vous à la section «Authentification basée sur les ports (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 9-6. Statistiques EAP



La page **EAP Statistics** (Statistiques EAP) contient les champs suivants :

Port Port dont on recherche les statistiques.

Refresh Rate (Taux de rafraîchissement) 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.

Affichage des statistiques EAP à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage des statistiques EAP.

Tableau 9-3. Commandes CLI Statistiques EAP

Commande CLI	Description
show dot1x statistics ethernet *interface*	Affiche les statistiques 802.1X pour l'interface spécifiée.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# show dot1x statistics ethernet g11

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

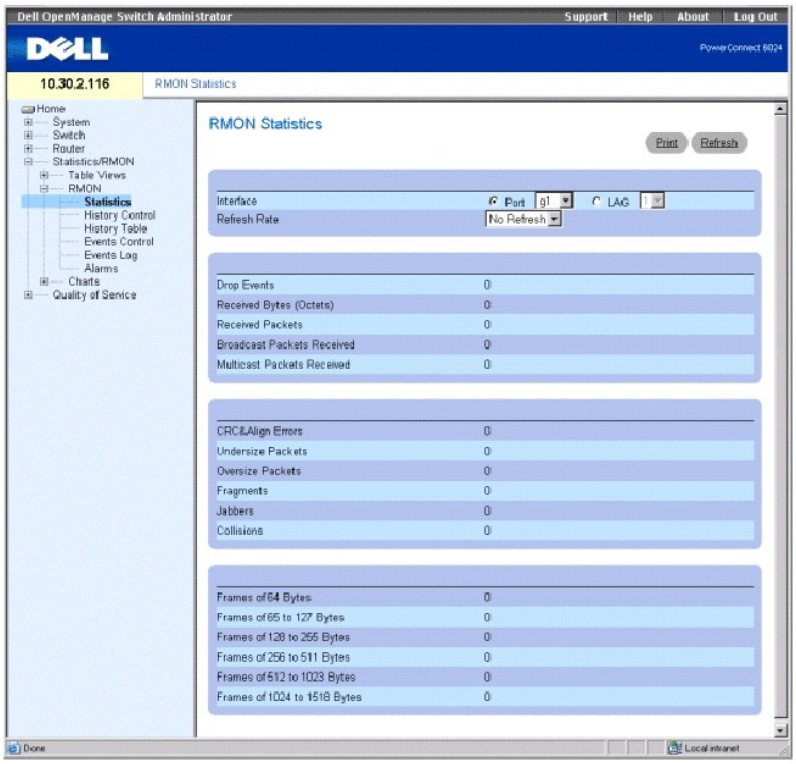
La télésurveillance (RMON) permet aux administrateurs réseau d'afficher des informations relatives au réseau à partir d'un site distant. Pour ouvrir la page **RMON**, cliquez sur **Statistics / RMON** (Statistiques/RMON)→ **RMON** dans l'*arborescence*.

Affichage de groupes de statistiques RMON

La page **RMON Statistics Group** (Groupe de statistiques RMON) permet d'afficher des informations sur l'utilisation du périphérique et les erreurs survenues sur le périphérique.

Pour ouvrir cette page, cliquez sur **Statistics / RMON** (Statistiques/RMON)→ **RMON**→ **Statistics** (Statistiques) dans l'*arborescence*.

Figure 9-7. Page Groupe de statistiques RMON



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. Les valeurs possibles pour ce champ sont No Refresh (Pas d'actualisation), 15, 30 et 60 secondes.

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 paquets de taille supérieure à 1 518 octets et possédant une FCS reçus pendant la session d'échantillonnage.

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 Group** (Groupe de statistiques RMON).
2. Sélectionnez un type et un numéro d'interface dans le champ **Interface**.

Affichage des statistiques RMON à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage des statistiques RMON.

Tableau 9-4. Commandes CLI Statistiques RMON

Commande CLI	Description
show rmon statistics {ethernet *interface* | port-channel *port-channel- number*}	Affiche les statistiques Ethernet RMON.

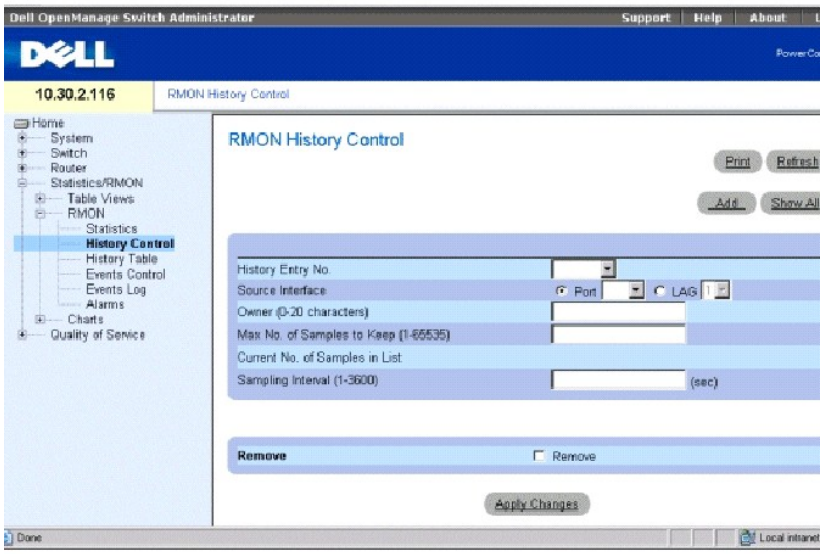
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console# show rmon statistics ethernet g1

Port g1

Dropped: 8

Octets: 878128 Packets: 978

Broadcast: 7 Multicast: 1

CRC Align Errors: 0 Collisions: 0

Undersize Pkts: 0 Oversize Pkts: 0

Fragments: 0 Jabbers: 0

64 Octets: 98 65 to 127 Octets: 0

128 to 255 Octets: 0 256 to 511 Octets: 0

512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

Affichage des statistiques de contrôle de l'historique RMON

La page **RMON History Control** (Contrôle de l'historique RMON) contient des informations sur 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 cette page, cliquez sur **Statistics / RMON** (Statistiques/RMON)→ **RMON**→ **RMON History Control** (Contrôle de l'historique RMON) dans l'*arborescence*.

Figure 9-8. Page Contrôle de l'historique RMON



History Entry No. (Numéro d'entrée d'historique) Numéro d'entrée de la table **RMON History Control Table** (Table de contrôle de l'historique RMON).

Source Interface (Interface source) Port ou LAG à partir duquel les échantillons d'historique ont été prélevés.

Owner (Propriétaire) Utilisateur ou station RMON qui a demandé les informations RMON.

Max No. of Samples to Keep (Nombre max. d'échantillons à conserver) (1-65 535) 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) Indique le nombre d'échantillons existants.

Sampling Interval (1-3600) (Intervalle d'échantillonnage) 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) Lorsqu'elle est cochée, cette option supprime l'entrée de la table **RMON History Control Table** (Table de contrôle de l'historique RMON).

Ajout d'une entrée de contrôle d'historique

1. Ouvrez la page **RMON History Control** (Contrôle de l'historique RMON).
2. Cliquez sur **Add** (Ajouter) pour ouvrir la page **Add History Entry** (Ajout d'une entrée à l'historique).
3. Renseignez les champs de la boîte de dialogue et cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée est ajoutée à la table **RMON History Control Table** (Table de contrôle de l'historique RMON).

Modification d'une entrée de la table de contrôle de l'historique RMON

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 et 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. Sélectionnez **Remove** (Supprimer) puis cliquez sur **Apply Changes** (Appliquer les modifications).

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

Affichage de l'historique RMON à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage des statistiques GVRP.

Tableau 9-5. Commandes CLI Historique RMON

Commande CLI	Description
rmon collection *history index* [owner *ownername* | buckets *bucket-number*] [interval *seconds*]	Active et définit la surveillance RMON sur une interface.
show rmon collection history [ethernet *interface* | port-channel *port-channel-number*]	Affiche les statistiques de l'historique RMON.

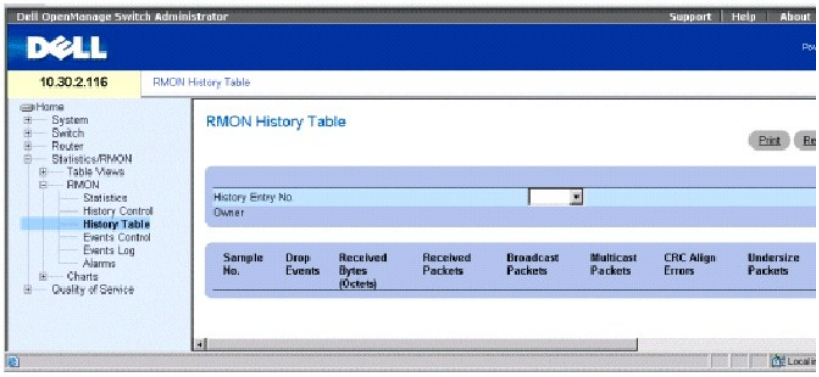
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# interface ethernet g8

Console (config-if)# rmon collection history 1 interval 2400

Console (config-if)# exit

Console (config)# exit

Console# disable

Console> show rmon collection history

Index Interface Interval Requested Samples  Granted Samples   Owner

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

1         1        10        0        50           50         CLI
```

Affichage de la table d'historique RMON

La page RMON History Table (Table d'historique RMON) contient des échantillons de statistiques spécifiques aux interfaces. Chaque entrée de la table représente toutes les valeurs des compteurs compilées lors d'un échantillonnage. Pour ouvrir la page **RMON History Table** (Table d'historique RMON), cliquez sur **Statistics/RMON** (Statistiques/RMON)→ **RMON**→ **History Table** (Table d'historique) dans l'*arborescence*.

Figure 9-9. Table d'historique RMON



REMARQUE : Tous les champs n'apparaissent pas nécessairement dans la table d'historique RMON.

History Entry No. (N° d'entrée d'historique) Contient une liste des numéros d'entrée de la table **RMON History Control Table** (Table de contrôle de l'historique RMON).

Owner (Propriétaire) Si disponible, nom du propriétaire du groupe de statistiques RMON.

Sample No. (N° d'échantillon) Identifie l'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 1 518 octets reçus pendant la session d'échantillonnage. Ces paquets possèdent 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 1 518 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 1 518 octets et possédant une 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 Entry No.** (Numéro d'entrée d'historique).

Les statistiques relatives à l'entrée s'affichent dans la table d'historique RMON.

Affichage de l'historique RMON à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage de l'historique RMON.

Tableau 9-6. Commandes CLI Contrôle de l'historique RMON

Commande CLI	Description
show rmon history index {throughput | errors | other} [period seconds]	Affiche l'historique des statistiques Ethernet RMON.

Vous trouverez ci-dessous un exemple des commandes CLI pour l'affichage des statistiques Ethernet RMON pour un débit sur l'index 1 :

```
Console# show rmon history 1 throughput

Sample Set: 5 Owner: cli

Interface: 24 interval: 10

Requested samples: 50 Granted samples: 50

Maximum table size: 270

Time                Octets Packets Broadcast Multicast  %

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

09-Mar-2003 18:29:32    0      0        0         0      0

09-Mar-2003 18:29:42    0      0        0         0      0

09-Mar-2003 18:29:52    0      0        0         0      0
```

09-Mar-2003 18:30:02 0 0 0 0 0

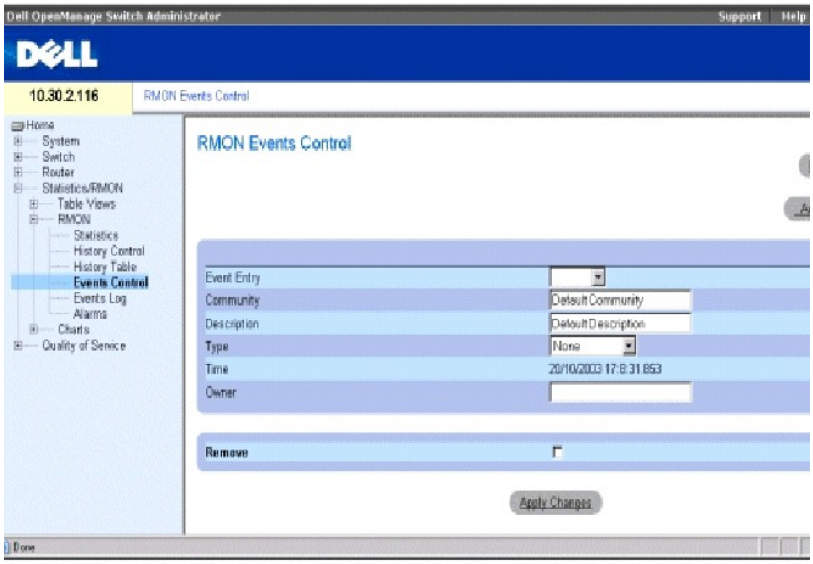
09-Mar-2003 18:30:12 0 0 0 0 0

09-Mar-2003 18:30:22 0 0 0 0 0

Définition d'événements RMON sur le périphérique

La page **R MON Events Control** (Contrôle des événements RMON) permet de définir des événements RMON. Pour ouvrir cette page, cliquez sur **Statistics/RMON** (Statistiques/RMON)→ **RMON**→ **Events Control** (Contrôle des événements) dans l'*arborescence*.

Figure 9-10. Page Contrôle des événements RMON



Event Entry (Entrée d'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) Heure à laquelle l'événement est survenu.

Owner (Propriétaire) Périphérique ou utilisateur qui a défini l'événement.

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime l'événement de la table des événements.

Ajout d'un événement RMON

1. Ouvrez la page **RMON Events Control** (Contrôle des événements RMON).
2. Cliquez sur **Add** (Ajouter) pour ouvrir la page **Add an Event Entry** (Ajout d'une entrée d'événement).
3. Renseignez les informations de la fenêtre de dialogue et cliquez sur **Apply Changes** (Appliquer les modifications).

L'**événement est ajoutée à la RMON Event Table** (Table des événements RMON) 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 le **champ Event Entry** (Entrée d'événement).
3. Modifiez les champs de la page et cliquez sur **Apply Changes** (Appliquer sur les modifications).

L'entrée de la table **RMON Events Table** (Tables des événements RMON) 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) pour afficher la table **RMON Events Table** (Table des événements RMON).
3. Sélectionnez **Remove** (Supprimer) pour le(s) événement(s) à supprimer puis cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée de la table 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 pour la définition des événements du périphérique.

Tableau 9-7. Commandes CLI Définition des événements du périphérique

Commande CLI	Description
`rmon event index type [community text] [description text] [owner name]`	Configure des événements RMON.
`show rmon events`	Affiche la table des événements RMON.

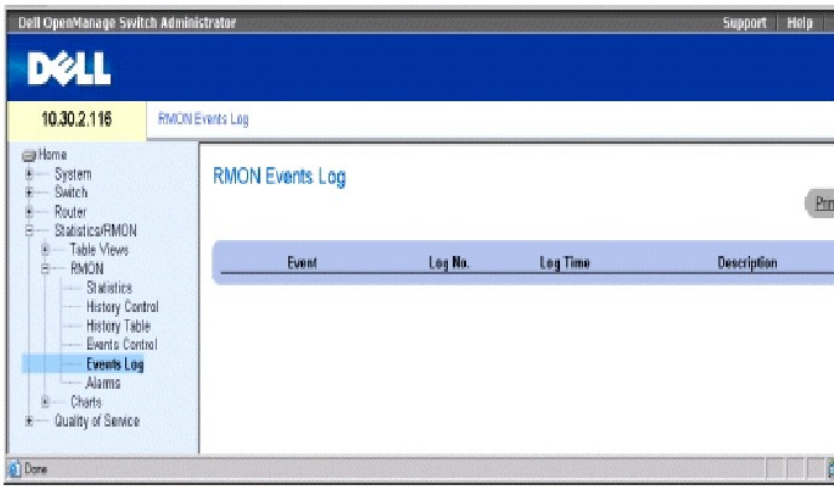
Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# rmon event 10 log

Console (config)# exit

Console# disable

Console> show rmon events

Index     Description     Type     Community     Owner     Last time sent

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

1         Errors          Log      CLI                     Jan 18 2002 23:58:17

2         High Broadcast  Log-Trap router        Manager   Jan 18 2002 23:59:48
```

Affichage du journal des événements RMON

La page **RMON Events Log** (Journal des événements RMON) dresse la liste des événements RMON. Pour ouvrir cette page, cliquez sur **Statistics / RMON** (Statistiques/RMON)→ **RMON**→ **Events Log** (Journal des événements) dans l'*arborescence*.

Figure 9-11. Page 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 pour la définition des événements du périphérique.

Tableau 9-8. Commandes CLI Définition des événements du périphérique

Commande CLI	Description
`show rmon log [event]`	Affiche la table de journalisation RMON.

Vous trouverez ci-dessous un exemple de commande CLI :

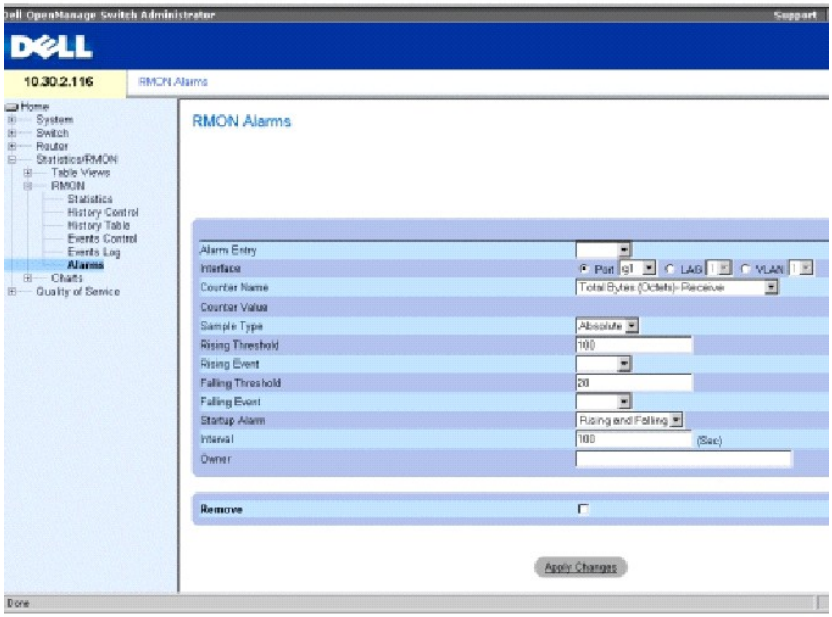
```
Console> show rmon log

Maximum table size: 500

Event   Description                 Time

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

1       Errors                      Jan 18 2002 23:48:19

1       Errors                      Jan 18 2002 23:58:17

2       High Broadcast              Jan 18 2002 23:59:48
```

Définition d'alarmes RMON sur le périphérique

La page **RMON Alarms** (Alarmes RMON) permet de définir des alarmes réseau. Ces alarmes sont émises en cas de détection d'un problème ou d'un événement sur le réseau. La hausse et la baisse des seuils génèrent des événements. Pour plus d'informations sur les événements, reportez-vous à la section «Affichage du journal des événements RMON».

Pour ouvrir cette page, cliquez **Statistics/RMON** (Statistiques/RMON)→ **RMON**→ **Alarms** (Alarmes) dans l'*arborescence*.

Figure 9-12. Page 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, l'événement 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 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 supérieure 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 (Intervalle) (s) Intervalle qui sépare deux alarmes.

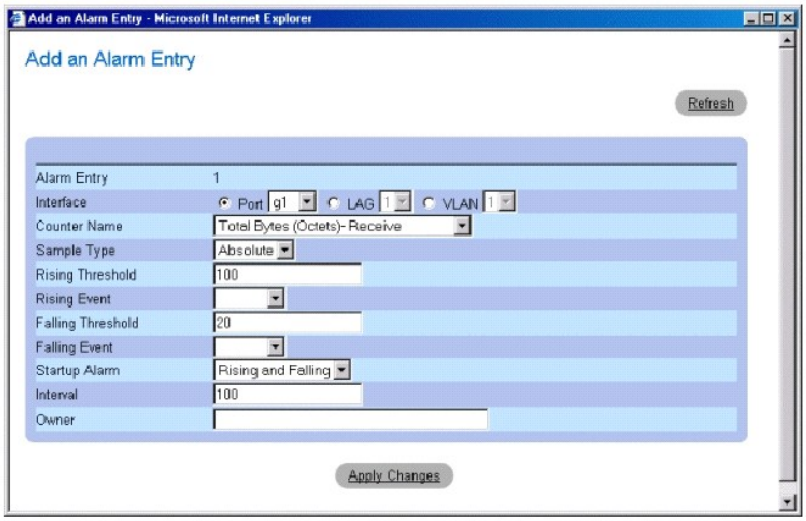
Owner (Propriétaire) Périphérique ou utilisateur qui a défini l'alarme.

Remove (Supprimer) Lorsqu'elle est cochée, cette option supprime une alarme RMON.

Ajout d'une entrée dans la table des alarmes

1. Ouvrez la page **RMON Alarms** (Alarmes RMON).
2. Cliquez sur **Add** (Ajouter) pour ouvrir la page **Add an Alarm Entry** (Ajout d'une entrée d'alarme).

Figure 9-13. Page Ajout d'une entrée d'alarme



3. Sélectionnez une interface.
4. Renseignez les champs de la boîte de dialogue et 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 de la boîte de dialogue et 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) pour afficher la table **RMON Alarms Table** (Table des alarmes RMON).

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) et cliquez sur **Apply Changes** (Appliquer les modifications).

L'entrée 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 pour la définition des alarmes du périphérique.

Tableau 9-9. Commandes CLI Alarmes du périphérique

Commande CLI	Description
rmon alarm *index MIB_Object_ID interval rthreshold fthreshold revent fevent* [type *type*] [startup *direction*] [owner *name*]	Configure des conditions d'alarme RMON.
show rmon alarm-table	Affiche un résumé de la table des alarmes.
show rmon alarm	Affiche la configuration des alarmes RMON.

Vous trouverez ci-dessous un exemple de commande CLI :

```
Console (config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000 1000000 1000000 10 20

Console# show rmon alarm-table

Index  OID                      Owner

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

1      1.3.6.1.2.1.2.2.1.10.1   CLI

2      1.3.6.1.2.1.2.2.1.10.1   Manager

3      1.3.6.1.2.1.2.2.1.10.9   CLI
```

Affichage des graphiques

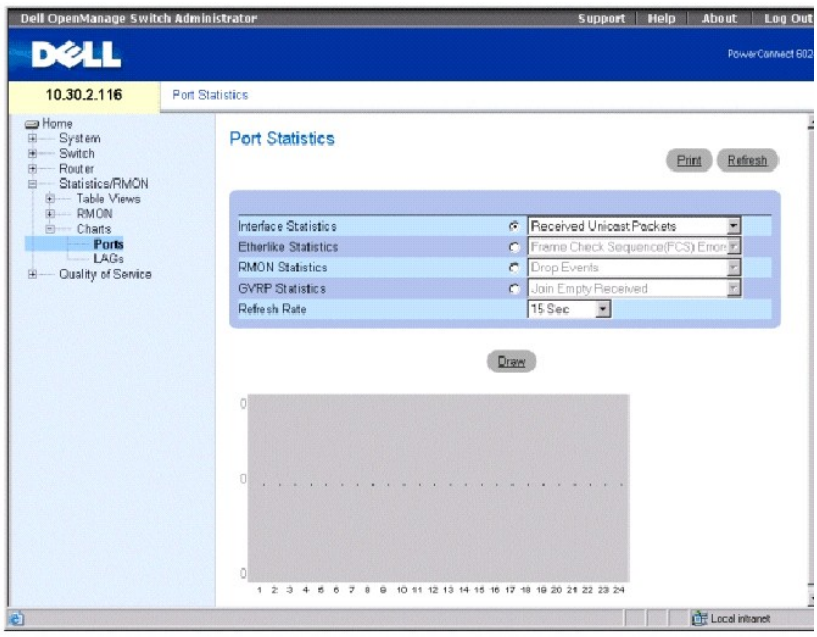
La page **Charts** (Graphiques) contient des liens qui permettent d'afficher les statistiques sous forme graphique. Pour ouvrir la page Charts, cliquez sur **Statistics / RMON** (Statistiques/RMON)→ **Charts** (Graphiques) dans l'*arborescence*.

Affichage des statistiques relatives aux ports

La page **Port Statistics** (Statistiques sur les ports) permet d'affiche des statistiques relatives au port sélectionné, sous forme graphique.

Pour ouvrir cette page, cliquez sur **Statistics / RMON** (Statistiques/RMON)→ **Charts** (Graphiques)→ **Ports** dans l'*arborescence*.

Figure 9-14. Page Statistiques sur les ports



Interface Statistics (Statistiques d'interface) Sélectionne le type de statistiques d'interface à afficher.

Etherlike Statistics (Statistiques Etherlike) Sélectionne le type de statistiques Etherlike à afficher.

RMON Statistics (Statistiques RMON) Sélectionne le type de statistiques RMON à afficher.

GVRP Statistics (Statistiques GVRP) Sélectionne le type de statistiques GVRP à afficher.

Refresh Rate (Taux d'actualisation) Délai qui s'écoule entre deux actualisations des statistiques. Les valeurs possibles pour ce champ sont No Refresh (Pas d'actualisation), 15, 30 et 60 secondes.

Affichage des statistiques relatives aux ports

1. Ouvrez la page **Port Statistics** (Statistiques sur les ports).
2. Sélectionnez la catégorie de statistiques à afficher.
3. Sélectionnez un taux d'actualisation dans le menu **Refresh Rate** (Taux de rafraîchissement).
4. Cliquez sur **Draw** (Dessiner).

Le graphique des statistiques sélectionnées s'affiche.

Affichage des statistiques relatives aux ports à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage des statistiques relatives aux ports.

Tableau 9-10. Commandes CLI Statistiques relatives aux ports

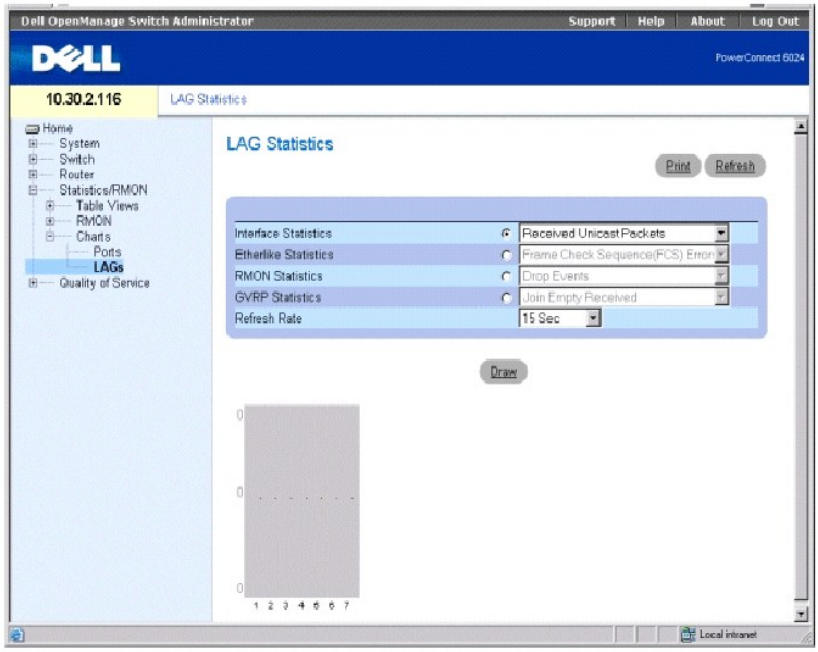
Commande CLI	Description
`show interfaces counters [ethernet interface | port- channel port-channel-number]`	Affiche le trafic enregistré par l'interface physique.
`show rmon statistics {ethernet interface | port-channel port- channel-number}`	Affiche les statistiques Ethernet RMON.
`show gvrp statistics {ethernet interface | port-channel port- channel-number}`	Affiche les statistiques du protocole GVRP.
`show gvrp-error statistics {ethernet interface | port- channel port-channel-number}`	Affiche les statistiques des erreurs du protocole GVRP.

Affichage des statistiques relatives aux LAG

La page **LAG Statistics** (Statistiques sur les LAG) permet d'afficher les statistiques relatives aux LAG sous forme graphique.

Pour ouvrir cette page, cliquez sur **Statistics / RMON** (Statistiques/RMON)→ **Charts** (Graphiques)→ **LAGs** (LAG) dans l'*arborescence*.

Figure 9-15. Page Statistiques sur les LAG



Interface Statistics (Statistiques d'interface) Sélectionne le type de statistiques d'interface à afficher.

Etherlike Statistics (Statistiques Etherlike) Sélectionne le type de statistiques Etherlike à afficher.

RMON Statistics (Statistiques RMON) Sélectionne le type de statistiques RMON à afficher.

GVRP Statistics (Statistiques GVRP) Sélectionne le type de statistiques GVRP à afficher.

Refresh Rate (Taux d'actualisation) Délai qui s'écoule entre deux actualisations des statistiques. Les valeurs possibles pour ce champ sont No Refresh (Pas d'actualisation), 15, 30 et 60 secondes.

Affichage des statistiques relatives aux LAG

1. Ouvrez la page **LAG Statistics** (Statistiques sur les LAG).
2. Sélectionnez la catégorie de statistiques à afficher.
3. Sélectionnez un taux de rafraîchissement dans le menu **Refresh Rate** (Taux de rafraîchissement).
4. Cliquez sur **Draw** (Dessiner).

Le graphique des statistiques sélectionnées s'affiche.

Affichage des statistiques relatives aux LAG à l'aide de commandes CLI

Le tableau suivant récapitule les commandes CLI pour l'affichage des statistiques relatives aux LAG.

Tableau 9-11. Commandes CLI Statistiques relatives aux LAG

Commande CLI	Description
`show interfaces counters [ethernet` *`interface`* `| port- channel` *`port-channel-number`*`]`	Affiche le trafic enregistré par l'interface physique.
`show rmon statistics {ethernet` *`interface`* `| port-channel` *`port- channel-`*`}`	Affiche les statistiques Ethernet RMON.
`show gvrp statistics {ethernet` *`interface`* `| port-channel` *`port- channel-number`*`}`	Affiche les statistiques du protocole GVRP.
`show gvrp-error statistics {ethernet` *`interface`* `| port- channel` *`port-channel-number`*`}`	Affiche les statistiques des erreurs du protocole GVRP.

Retour à la page du sommaire